DATA COMMUNICATION NETWORKS

Complex Engineering Problem (CEP)

Project Report

Fall 2024

Analysis and Optimization of Data Communication Networks (DCN)

Group Information

Student Name	***Roll #***	***Status(Group Leader/Group Member)***
Ahmed Waqar	22I-2217	Group Leader
Ali Majid	22I-9874	Group Member
Sameer Shahid	22I-2206	Group Member
Syed Ali Ahmed Shah	22I-2174	Group Member
Zohaib Saadat	21I-0946	Group Member

Company Information

Company Name	UFONE
Company Address	Street 2,I-9/2,Islamabad
Reference in the Company	Waqar Ibrahim
Name and Designation of the reference	Waqar Ibrahim Group Director PMO Core,IP and Transport Project.

Visit details

The company that we chose for the visit was **Ufone**, a Pakistan-based GSM cellular service provider. Well-known across the country, Ufone boasts one of the largest networks nationwide.

A **single** trip was made to the chosen location.

File Photo: The five team members during the visit to the Ufone Data Center.
(From left to right)
Top row: **Sameer Shahid**, **Ali Ahmed**, and **Ali Majid**.
Bottom row: **Zohaib Saada**t, Mr. Safdar Ali (Senior Manager), and **Ahmed Waqar** (Group Lead)**.**

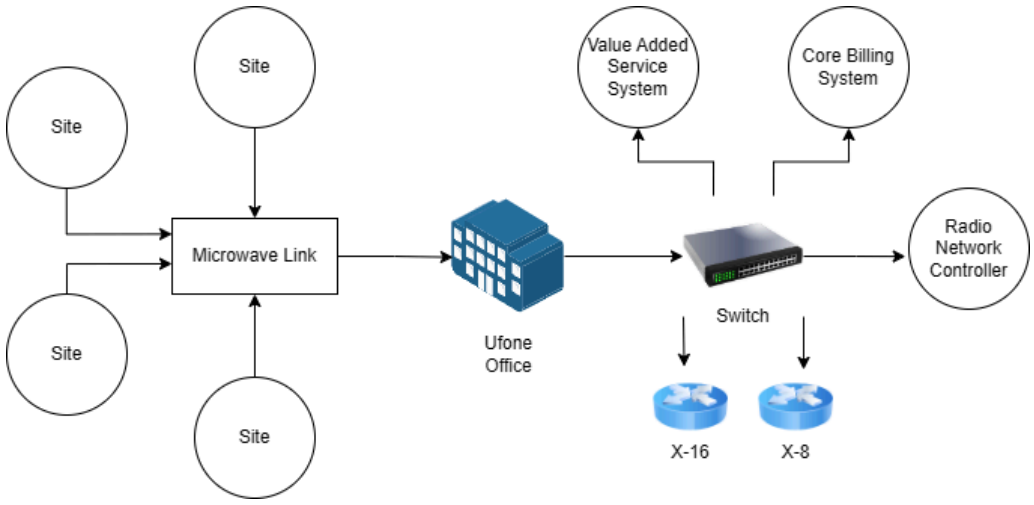
Objectives of our Visit

Today, technology is a big part of everything we do. It's hard to get things done efficiently without using some kind of technology. Almost every part of life has been improved with new inventions. These tools save time and often do tasks better than people can, making our lives easier. Especially with advances in telecommunications, all sorts of communications have become much easier, faster and safer.

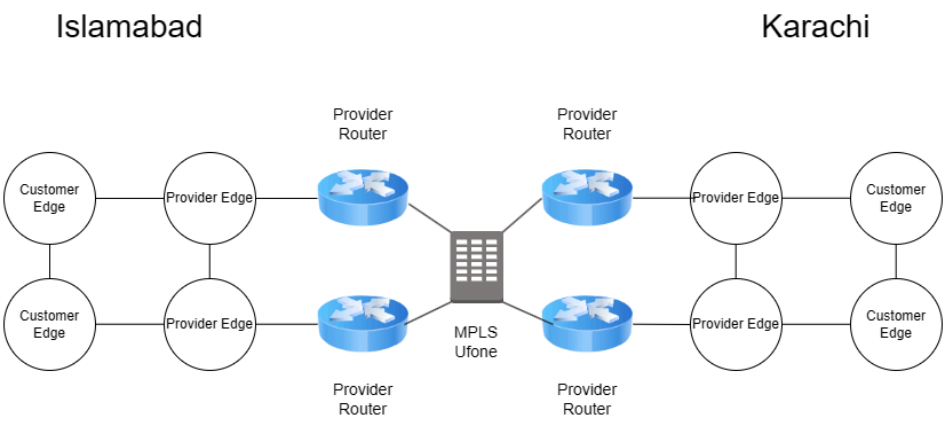
The advancement of technology, along with the introduction of 3G, 4G, and ongoing efforts to implement 5G in Pakistan, has led to rapid growth in the telecommunication infrastructure and industry. To learn more about telecommunication infrastructure and the practical implementation of our course DCN, we visited Ufone's "mobile-switching-centre" (MSC).

The **aim** and the **purpose** of this visit was to learn about the infrastructure of the equipment used in the industry. The team lead guided us, answered our questions, and provided an overview of the equipment, maintenance strategies, and the functioning of various systems.

End-to-End Connectivity Diagram of DCN



End-to-End Connectivity Diagram



Customer and Provider Edge Diagram

Remote Sites and Microwave Links
In many parts of Pakistan, especially in areas where it's not easy to lay down fiber (like hilly or remote regions), operators rely on microwave links. These are basically high-frequency wireless connections—imagine those big dish antennas you see on mobile towers. They're used to bridge long distances and connect back to the core network.

Microwave links often use Layer 2 protocols like Ethernet or PPP (Point-to-Point Protocol). PPP (detailed in RFC 1661) is a classic way to encapsulate data for transmission. It's handy for creating direct, reliable links over wireless or other physical mediums.

Ufone Office – The Core Hub
All these microwave links eventually lead to the Ufone Office, which you can think of as the main hub. Here, you have two big systems:

Value Added Service (VAS) System – This is in charge of user-focused features like SMS, voice mail, caller tunes, and other subscription-based stuff.
The core billing system handles invoicing, charging, and billing. The billing system keeps a real-time record of each time a user calls, sends an SMS, or uses mobile data.
A Layer 2/Layer 3 switch, which is essentially a switch/router combo, manages all internal routing and switching and connects these systems to one another and to other areas of the network.

The **Radio Network Controller (RNC)** is another essential component. It can be compared to the "traffic manager" of a cellular network, overseeing all radio resources. It ensures that the radio spectrum is used effectively and synchronises the communication between mobile devices and the network.

In accordance with the **3GPP TS 25.413** standard, it communicates and exchanges data with the core network elements via RANAP (Radio Access Network Application Part). The RNC maintains communication with the core network in this way.

Devices in between **(X-16 and X-8)**
Network diagrams may use designations such as X-16 or X-8. These are typically routers or special network devices used for tasks like load balancing, redundancy, or specialized routing. They keep the network running smoothly, even if one path goes down (which is essential for reliability).

For **routing protocols**, we might see:

OSPF (Open Shortest Path First) per **RFC 2328**, which is commonly used inside an organization's network.
BGP (Border Gateway Protocol) per **RFC 4271**, mostly seen for routing between large networks or ISPs.
Transport and Security Protocols
On a fundamental level, the entire system relies on **TCP** (Transmission Control Protocol) and **UDP** (User Datagram Protocol).

TCP (as per **RFC 793**) is great for reliable communications—like file downloads or important data that must arrive intact.
UDP (as per **RFC 768**) is often used for real-time traffic—like voice or streaming—where speed is more important than error checking.
And since the microwave links can be considered "untrusted" (anyone might try to intercept over the air), operators usually deploy **IPSec** (**RFC 4301**) or similar encryption protocols to keep data secure.

Remote site → Microwave link → Ufone Office → VAS/Billing and RNC → Back out to the radio network or other systems.

Each component is vital:

- · When it comes to remote communication, microwave links handle the heavy lifting.
- · The internal network's core switches and routers are responsible for forwarding data.
- · The RNC controls connections to the network made by user devices, such as your phone.
- · User services and billing are handled by VAS and Billing.

Customers may utilize data, send SMS, and make calls from any location, and the operator can manage the network and invoicing in real time when all these components are in sync due to standard protocols and a strong design.

Company's DCN Equipment

Ufone's DCN equipment is placed in their control unit, which is a large hall which requires very strict cleanliness protocol i.e. shoes are not allowed, this is done to prevent dust affecting the equipment. The room had routers, switches and other equipment for cellular connectivity placed in large racks made by Huawei that were made to keep the equipment cool and accessible. The control unit was very well ventilated with industrial fans and air conditioners to cater the high heat from machinery

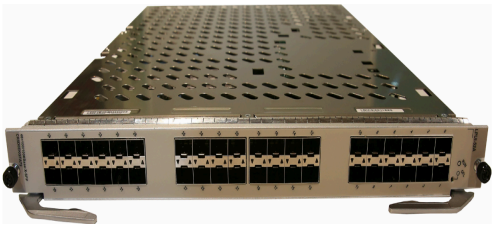
1. Core router:

The core router was manufactured by the company Huawei, specifically the model NetEngine40E series was used. The router has multiple slots available. It has two units, line processing unit and main processing unit. Core routers are the backbone of the DCN, serving wide area networks. These routers function at 50 percent of their max capability to achieve maximum redundancy. Additionally, there are backup free input output ports available incase if there is something wrong with any other port.

Huawei NetEngine40E as core router.

2.Line Processing Unit (LPU):

It is an interface board that has multiple interfaces (slots) with various transmission rates. It is used to send and receive data packets by using ethernet ports and optical fiber input/output ports attached with cables. The data that it receives is forwarded to MPU.

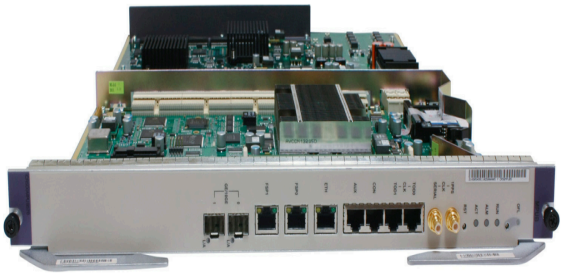


Interface board of router providing physical connectivity.

3. Main Processing Unit (MPU):

Responsible for the control plane and management plane of the system, including route calculations, device management and maintenance, and device monitoring. The MPU interprets the device configuration then transmits it to the LPU.

Main control board providing all the processing.



4. Edge access routers:

Ufone uses edge access routers to deal with local area networks, and these routers are connected to core routers, which deal with WAN. Ufone uses Huawei's X16 and X8 of the NetEngine8000 series. These routers connect users in LAN to the ISP's backbone which is the core access router. Edge routers have lesser traffic than core routers since these deal with a smaller area's user traffic.

Huawei NetEngine8000 series routers.

5. Switches:

The switches used were Huawei's s9300 series, for example s9303, s93012, that have 3 and 12 cards respectively. These switches function in data-link layer and provide very fast switching capabilities to cater the heavy traffic. It uses MAC addresses to locate destinations. In addition to 2-layer switches, 3-layer switches were also used for high speed data forwarding in a local area network. Just like routers, these machines also run at less than 50 percent of their capacity, with multiple switches available to provide a reliable backup. These switches serve smaller areas (LAN) consisting of several sectors e.g F-6 to F-11.

Huawei s9300 series switches

Applications and Services

Applications:

Ufone has one application for the customer. Since its merger with PTCL its name has been changed to UPTCL. This application contains various packages for customers and a billing system running in the background. The customer is informed about how many minutes or gigabytes of mobile data is left and the expiry date of the package if bought. The application is also integrated with some other applications such as spotify and the billing of that app can be added in the UPTCL application. This is the main application where all of the features are present.

Another notable application by Ufone is the Self-Care Portal, which enables customers to recharge their packages, check transaction history, and manage their services. Furthermore, Ufone offers a Value-Added Service (VAS) application, where customers can personalize their experience by setting custom caller ring back tones (CRBT).

Services:
Ufone offers different services, among which one is customer care service where representatives are present to answer and assist the customers in any difficulty they might be facing. Other than that there is also a 24/7 chat available for customers for whom calling the customer care is not an option.

Ufone also has messaging services where messages are sent to the respective customers to alert them of their package limit exceeding, acknowledgement of any purchase made and OTP required by the customers when logging in as a 2 step verification for security purposes.

The main service of Ufone remains to be the cellular service which is spread almost all around Pakistan with the exception of south Waziristan, Extreme northern areas. This service helps seamless communication between two or more than two people at the same time.

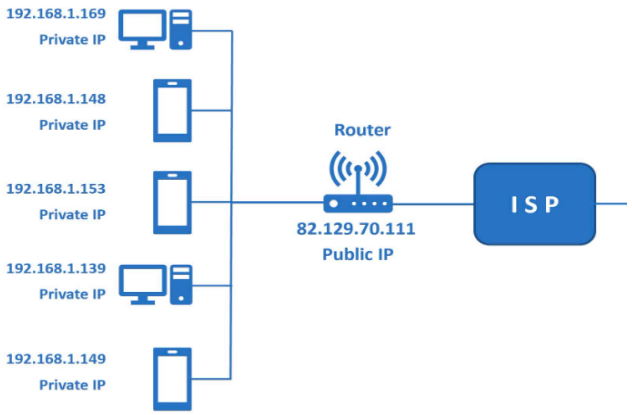
All of the services are well maintained and constantly monitored.

IP Scheme and Routing Protocols

IP schemes:

Ufone uses class A, class B, and class C for classification of IP version 4 addresses. These IP addresses have network ID and host ID of specific lengths according to their practical application. These lengths are decided by the subnet mask, which varies class to class, where class A is for very large networks, i.e this class is given to the public users by Ufone. These IP addresses are dynamically assigned to devices.

On the other hand, within the data center (MSC), Ufone uses private IP addresses for security purposes and a smaller and controlled network. The company uses schemes like “192.168.0.0” and “172.168.0.0”. These IPs are specifically for MSCs, which are assigned with static addressing (manually), this is done to avoid any security breaches and other issues as the devices inside the MSC have to regularly deal with Ufone’s routers, switches and other devices.



Here a private and secure network is attached to a router.

Routing Protocols:

1. ***OSPF:***

   Open Shortest Path First (OSPF), is a routing protocol used within Ufone's core network. It uses Dijkstra's algorithm to find the shortest path between source and destination. Since it does not have any hop count and limit, it is ideal for large networks, just like Ufone's, and its core and edge access routers use this protocol to direct packets to the desired destination. The core router uses this protocol and then forwards the packets to the edge router of the area in which the client is located.

   It is more efficient because it only updates the routing tables when there is a change of routers, i.e. some router is added or subtracted from the network, making OSPF suitable for MSCs of telecommunication companies.

2. ***BGP:***

   The **Border Gateway Protocol** enables the internet to exchange routing information between different networks on the internet.It is designed to check the path taken by various packets and how these packets travel between large networks,under a common administrative control.

   The BGP implemented in the Ufone data center ensured that the data packets found the best path to the destination among the complex network.Upon asking the field engineer, we were told that the Border Gateway Protocol works in tandem with the **mesh topology**,implemented in that specific Ufone data center. BGP uses the mesh topology's multiple connections to find the most optimal path for data transfer. It evaluates paths based on metrics like AS hops and policy preferences.

   In short, by combining BGP with a mesh topology, the Ufone data center achieved enhanced reliability and flexibility,ensuring smooth communication within the data center and with external networks.

3. ***IS-IS:***

   Intermediate System to Intermediate System protocol is also used by Ufone, just like OSPF, it determines the best path for data transmission within a large commercial network. It exchanges information with other routers and periodically sends updates to its neighbors, which then provide routers' links and routing information. It also uses dijkstra's algorithm to find quickest paths. IS-IS is a robust and efficient routing protocol necessary for large networks like Ufone's, to maintain high speed communication with minimal

   IS-IS is known for its scalability and efficiency, as it uses a hierarchical design for management of routing tables, where level 1 of the hierarchy is local area routing and level 2 manages inter-area traffic. This protocol is also easy to implement and integrate because it works for both IPv4 and IPv6 and works with multiprotocol label switching (MPLS).

4. ***IGP :***

An interior gateway protocol (IGP) is a type of protocol used for exchanging routing information between routers within Local.In the Ufone data center,**IGP** is used to facilitate seamless communication between routers and ensure efficient routing within their internal network infrastructure. The Ufone Noc team was employing protocols like OSPF and IS-IS to ensure efficient routing.

Furthermore, IGP ensures redundancy by providing alternate paths for the data packets,avoiding single point of failure. The Noc team in the ufone data center made sure that IGP dynamically updated the routing tables as soon as there was a change in the network. IGP was being used along with BGP to manage both the internal and external traffic simultaneously.This enabled the Ufone data center to maintain a robust and efficient data network.

5. ***EIGRP:***

Enhanced Interior Gateway Routing Protocol is an advanced distance vector routing protocol, which is commonly used in large scale networks like Ufone due to its efficiency and scalability. It is described as a hybrid protocol as it incorporates features of both distance vector and link state protocol.

DNS, DHCP, and AAA Mechanisms

1. **Domain Name System** (DNS):

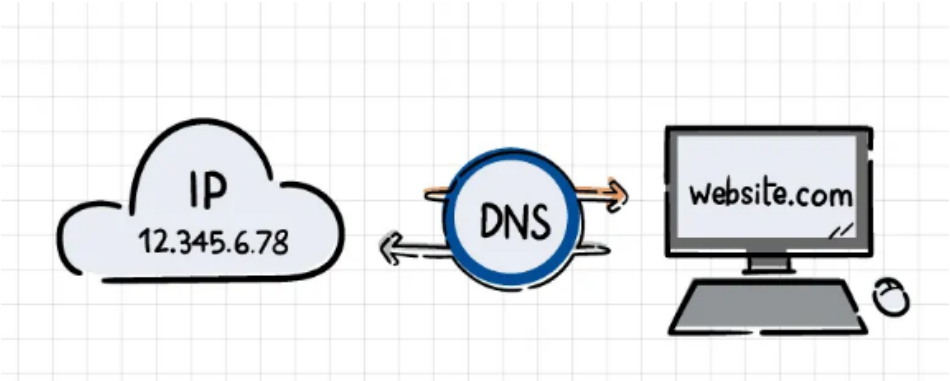
   The Domain Name System or the "phonebook" of the internet as it is stands today,is a fundamental infrastructure, translates the human accessible domain names like www.espncricinfo.com or www.marvel.com into IP addresses like 192.168.1.1,then used by the computers to communicate with each other.

   The implementation of DNS in any Data Center plays a vital role in ensuring reliable and efficient management of services. Now the question arises how does a DNS work? Let us discuss how the DNS Server works in loading a web page.

   - The user will enter www.marvel.com in their browser.
   - This browser will contact a local DNS,usually provided by the ISP(**PTCL**) in this case.This is **DNS Resolution.**
   - The **DNS recursor** will now solve this problem in a 3 step process:
     A. **Route DNS Server:**: Directs to the .com TLD server.
     B. **TLD Server:** It will point to the authoritative DNS server for marvel.com.
     C. **Authoritative DNS Server**: Provides the IP address of the web server hosting www.marvel.com.

The resolved IP will now direct the request of the client to the Data Center, send the request to a specific web server, process the request and share the content back to the client.

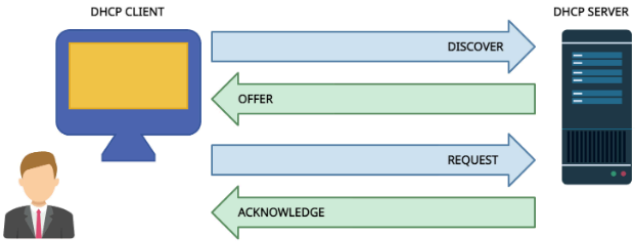
After our visit,we got to know that the DNS for Pakistan is mostly handled by PTCL.



Visualizing the DNS process: translating a human-readable domain name.

2. **Dynamic Host Configuration Protocol** (DHCP):

A network management Protocol that automatically assigns IP addresses to devices on a network.The working of DHCP is simple. The client will send a broadcast request to a DHCP Server which responds with a “DHCP-OFFER”. This simply includes an IP address. The client gives a request reply and will accept the offer and the server responds with an “ACK” message.



DHCP: Client gets an IP address from the server.

How is **DHCP implemented** in a data center?

In the UFONE Data Center we visited:

- A dedicated server managed the pool of IP addresses.
- The subnet mask and lease time for IPs were predefined.
- The DNS was dynamically updated whenever new IPs were assigned.
- For security, internal IP addresses were used to ensure smooth communication within the network.

3. **Authentication,Authorization and Accounting** (AAA)

A security framework for controlling and tracking user access within a computer network, AAA intelligently controls access to computer resources.It enforces policies, audit usage and provides the information necessary to bill for services.These combined processes are vital for effective access management, network management and security.

Network administrators, such as those at PTCL, use AAA to maintain network security while granting users access to required resources. This framework also helps prevent unauthorized access by providing security teams with control and visibility over user activities.

Implementation of AAA in Ufone Data Center:

- **Authentication:**

The NOC Office in the Ufone Data Center used secured login mechanisms like multi-factor Authentication to control access to network resources. Special “Dial-in User Service” servers were present in the NOC Office to authenticate the users.

- **Authorization:**

Following authentication, the user must be authorized to perform certain tasks. After logging in to a system, for instance, they might try to issue commands. The authorization process determines whether the user has the authority to issue such commands. Authorization and user authentication work together in a AAA model; the user is authenticated first, and only then can they be authorized for different types of access or activity.

- **Accounting:**

Accounting records the resources a user consumes during a session to support network management and business operations**.** This includes session statistics like start and end time,duration of the session and the activities done by the user.The NOC team checks the data usage and how the system resources are being used.

AAA protocols:

- **RADIUS**, a client-server protocol that lets remote access servers communicate with a central server for authentication. In the AAA process, RADIUS performs authentication and authorization simultaneously.

- **Terminal Access Controller Access Control System,** a remote authentication AAA protocol that lets a remote access server communicate with an authentication server for user validation.

- **Diameter:**The Diameter AAA protocol evolved from the RADIUS protocol,adds new commands and attributes to the RADIUS protocol, such as capability negotiation, application-layer acknowledgments and failover methods.

Network Protection and Security Measures

The UFONE NOC team had implemented a firewall in their network infrastructure to enhance their security operations.

In simple terms, a data center firewall is a software or hardware device that monitors traffic entering and exiting an organization's network.Now the question arises as to **why a firewall was** installed in the UFONE data center?

Despite the shift to cloud resources, data centers remain vital, hosting critical applications and assets. As vulnerabilities persist, firewalls are essential to safeguard the data centers from cyber threats and unauthorized access, ensuring operational continuity.

Implementation:

The NOC team initially evaluates the existing network and identifies critical assets and the flow of the data.This allows them to evaluate the vulnerabilities in the existing network.Afterwards, they make certain policies for the firewall implementation keeping in mind the requirements and the policies of the company.

UFONE was implementing its own firewall in that specific data center,not only offering deep packet inspection but also checking the application layer to address specific security needs.The firewall also made sure that there was no delay in the real time data traffic.

Incase of any malicious attacks, there was also a redundant firewall. This maintained continuous protection and also prevented a single point of failure.

For blocking SCAM websites,URL filtering, reputation analysis, DNS filtering, and content inspection was used.

As far as **Denial of Service(DOS)** attacks,the “Ufone” firewall employed various tactics to make sure such attacks are prevented .It monitored network traffic patterns to detect unusual spikes that indicate potential attacks. Rate limiting was being used to restrict the number of requests from a single IP or network segment, preventing servers from being overwhelmed. Malicious IP addresses identified as attack sources were blacklisted.

The firewall collaborated with load balancers to ensure legitimate traffic is distributed effectively while filtering out malicious requests. These combined methods created a robust defense against DoS attacks and enhanced the security of the Ufone data center.

Analysis Tools and Observations

During our educational visit to the Ufone Data Center, we had the opportunity to see firsthand how a major telecom operator in Pakistan manages its network infrastructure to maintain reliable voice and data services across the country. The Ufone team demonstrated the different tools they use for network analysis and security, namely **Wireshark**, **Fortinet FortiGate**, and **Cisco Prime Infrastructure**.

Tools Used at Ufone:

Wireshark

At the data center, Wireshark is a tool of choice used by Ufone's network engineers to monitor and debug traffic and diagnose problem services. They described the use of Wireshark for finding bottom-layer information, monitoring communication protocols (such as TCP, UDP, and VoIP signaling), and the real-time diagnosis of latency or jitter issues.

- **Primary Usage at Ufone:**
    - Monitoring voice traffic (VoIP) quality.
    - Identifying unusual DNS or HTTP queries.
    - Troubleshooting customer-reported data or call drops.

According to the Ufone engineers who operated it, Wireshark is a tool currently used in telecom environments because of its simple interface and rich packet capture features.

Fortinet FortiGate

Ufone employs **Fortinet FortiGate** as a core component of its security architecture. During the tour, the security team demonstrated how FortiGate appliances provide features like intrusion prevention systems (IPS), antivirus scanning, and web filtering to shield critical network segments from external threats.

- **Primary Usage at Ufone**:
    - Blocking malicious traffic targeting Ufone's VoIP and data servers
    - Managing unified threat alerts on a centralized dashboard
    - Automating policy updates and security signatures

FortiGate was shown to effectively reduce phishing and malware threats when properly configured and regularly updated, a practice that Ufone's security administrators strongly emphasized.

Cisco Prime Infrastructure

For large-scale network management, Ufone relies on **Cisco Prime Infrastructure** to monitor its extensive array of Cisco routers, switches, and wireless controllers. The platform offers real-time dashboards for device status, bandwidth utilization, and event logs.

- **Primary Usage at Ufone**:
    - Centralized configuration of numerous Cisco devices
    - Automated alerts for hardware performance and abnormal traffic spikes
    - Visual maps of the entire network topology (including nationwide branches)

Weaknesses Observed

Even though Ufone has implemented robust practices, the following potential issues were observed during the visit:

1. **Unencrypted Internal Traffic**
   While external connections are heavily secured, some internal management traffic appears to be using plaintext protocols. This opens the risk of data interception if an internal system is compromised.
2. **Outdated Firmware and Security Signatures**
   In a few FortiGate dashboards, we noticed alerts indicating that certain security signatures were outdated. If not updated regularly, these devices could miss newly emerging threats.
3. **Minimal Network Segmentation**
   Although Ufone has multiple VLANs, certain essential servers seem to share segments with user traffic. This can increase the risk of a successful attacker moving laterally within the data center.
4. **Limited Monitoring for East-West Traffic**
   Intrusion detection is primarily focused on the perimeter (external threats), potentially leaving lateral or “East-West” traffic less monitored once inside the network.

Recommendations for Improvement

1. **Enforce End-to-End Encryption**
   Adopting secure protocols such as SSH, HTTPS, and SFTP, even for internal communication, will significantly reduce the risk of data breaches.
2. **Regular Firmware and Signature Updates**
   Scheduling frequent updates and proactive patch management will keep FortiGate appliances prepared against zero-day exploits.
3. **Enhanced Network Segmentation**
   By separating critical application servers from user traffic through stricter VLAN policies, the impact of any single compromised segment is minimized.
4. **Expand Internal IDS/IPS Coverage**
   Bolster the monitoring of East-West traffic within the data center, either via FortiGate or a dedicated Intrusion Detection/Prevention System.
5. **Leverage Cisco Prime for Proactive Alerts**
   More advanced alerting rules should be set in Cisco Prime Infrastructure to detect unusual internal activities. This includes setting thresholds on bandwidth usage, connection attempts, and resource utilization.

Benefits of this Project

.

The visit offered valuable insights into industrial processes in Pakistan. It allowed us to experience real-time, large-scale communication, providing an excellent practical conclusion to our four months of theoretical study on communication systems. Additionally, we had the opportunity to engage with field experts who provided guidance for making informed professional decisions in the future.

An important benefit was gaining knowledge about commercial-level networks, including how sites communicate with the Ufone center and how the center manages client connectivity effectively

A basic understanding of the NOC team's operations was provided, including its division into specialized parts, each with specific duties. The roles of these divisions in ensuring successful call connections, such as managing background music and messages during call setup, were also explained.

Another advantage was learning how diverse the company actually is in terms of employees. At the time of our visit the NOC team was almost full of Huawei employees as the contract was binded with Huawei.

When visiting the data centre we learned about the latest trends of the industry and how they have made advancements in the telecommunication helping them to stay up to date with the current industry standards and their competitors.

A big exposure to the industry was provided which helped connect the dots studied in theory to the real world application. Some of the soft skills such as communication, teamwork and professionalism were polished which is essential for any career path chosen. Knowledge about regulatory work was also shared in day to day life. Many precautions were also shared which are taken in order to counter any errors be it software or hardware to ensure smooth transmission of cellular services. The most important benefit was the networking opportunities for all the students who visited with the industry professionals which can surely lead to valuable future career opportunities.

Conclusion

The key takeaway points included the network architecture of the company, as each organization has its own unique architecture depending on various factors such as vendors and company budget. We had the opportunity to observe the core router operating within the data center and gain an understanding of how the layers are accessed and how users are connected. Additionally, details about the backhaul and core network were provided

The billing mechanism of the company was also introduced, how the call ends instantly when the balance of the user ends

We were enlightened to the companies protocols such as TCP/IP and UDP; Furthermore some of the firewall implementations when the users are connected to the internet through cellular data. Got to know Ufone's cellular technology including 2G,3G,4G including a picture of the roadmap of their services.
A key takeaway was how Ufone was actually maintaining and monitoring their hardware and the services and the security protocols which were implemented and how the bundles that offered only whatsapp or facebook mobile data only allowed that specific app to run on cellular data.

The overall experience was very learning and developing for each of the individuals as we are now in a position where we can analyze the DCN of a company and most of the operational protocols it uses. The educational bridge has been successfully built to the industry and real world. The power of teamwork and a healthy environment is understood.

The visit not only enhanced our knowledge but also motivated us to dive further into networks of companies and their future proofing. One of the standout aspects of the visit was getting to know the importance of seamless transmission of cellular services and how companies face huge losses when either services go down even after having redundancy or when ordered by the government, the losses are even filed to PTA in Pakistan when services are blocked by the government.

A very important takeaway was that Ufone takes traffic management very seriously and with their upcoming plans for 5G rollouts they could consider the possibility of implementing network slicing, which allows the network to be divided into multiple virtual networks, each tailored for specific services, as the range if 5G is short due to high frequency it needs to be utilized very efficiently; Moreover Ufine has implemented numerous algorithms for congestion detection and correction and in peak hours how they have divided the users in different bandwidths tailored to their use.