File Transfer Protocol

Introduction:

File Transfer Protocol (FTP) is a standard network protocol used for the transfer of files between a client and a server on a computer network. It operates on the application layer of the TCP/IP protocol suite. FTP provides a simple and reliable method for transferring files over the internet.

Aim and Objective:

The primary aim of FTP is to facilitate the efficient, secure, and reliable transfer of files between a client and a server. Its objectives include:

- Enabling users to upload files from their local system to a remote server.
- Allowing users to download files from a remote server to their local system.
- Providing authentication mechanisms to ensure secure access to files.
- Supporting various transfer modes such as ASCII and binary to accommodate different types of files.
- Offering features like directory listing, file renaming, and permission management.

Theory of Operation:

FTP operates using a client-server model, where the client initiates a connection to the server to perform file transfer operations. The key components of FTP operation include:

- Control Connection

  Establishes communication between the client and the server for sending commands and receiving responses.
- Data Connection

  Used to transfer actual file data between the client and the server.
- Commands

  Client sends commands such as login, list directory, upload, download, etc., to the server over the control connection.
- Responses

  Server responds to client commands with status codes indicating success, failure, or other relevant information.

Steps Involved:

The typical steps involved in an FTP session are as follows:

Establish Connection: The client initiates a TCP connection to the FTP server on port 21 (the default control connection port).

Authentication: The client authenticates itself by providing a username and password.

Navigate Directories: The client can navigate directories on the server using commands like CD (change directory) and PWD (print working directory).

Transfer Files: The client can upload files to the server using the PUT command or download files from the server using the GET command.

Close Connection: Once the file transfer is complete, the client can close the connection using the QUIT command.

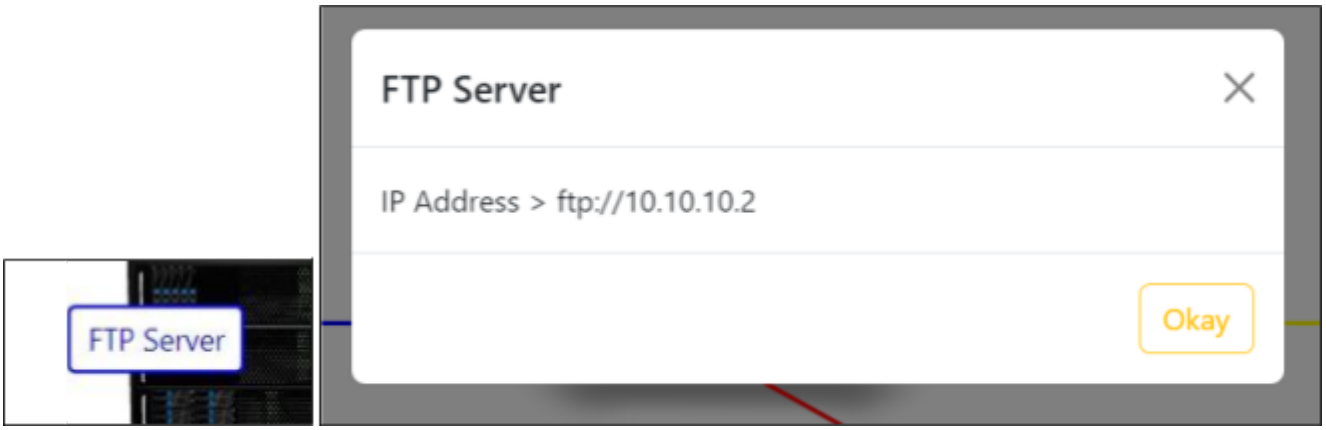
Conclusion:

File Transfer Protocol (FTP) is a fundamental protocol for transferring files over a network. It provides a robust mechanism for users to exchange data between local and remote systems securely. Understanding the theory of operation and following the steps involved enables efficient utilization of FTP for file transfer purposes.

Let's Start Transferring File using FTP (File Transfer Protocol) in AR World!!

1. To obtain the IP addresses of network devices, please click on their respective names. Know IP Address

1.1

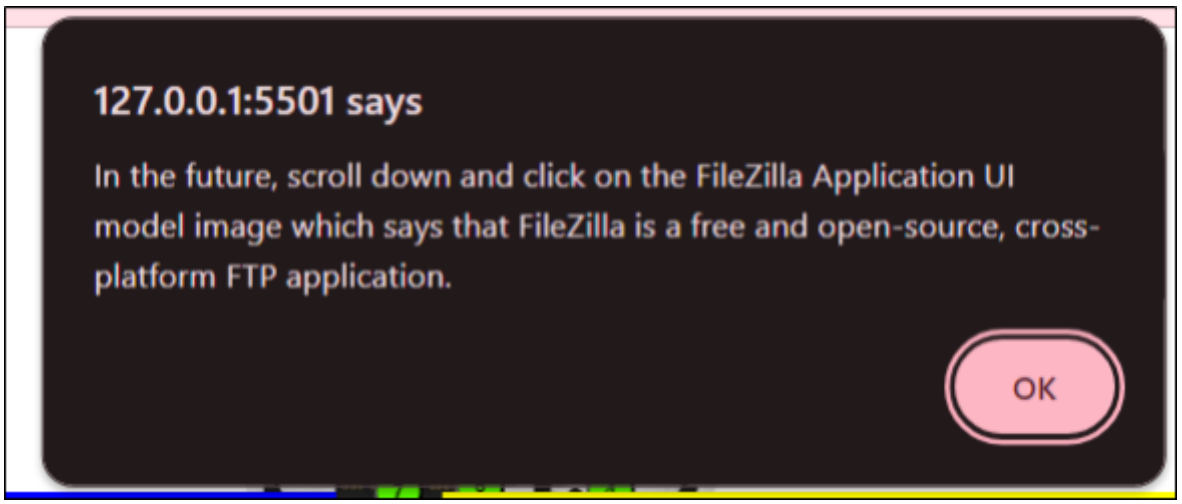


1.2

1.3

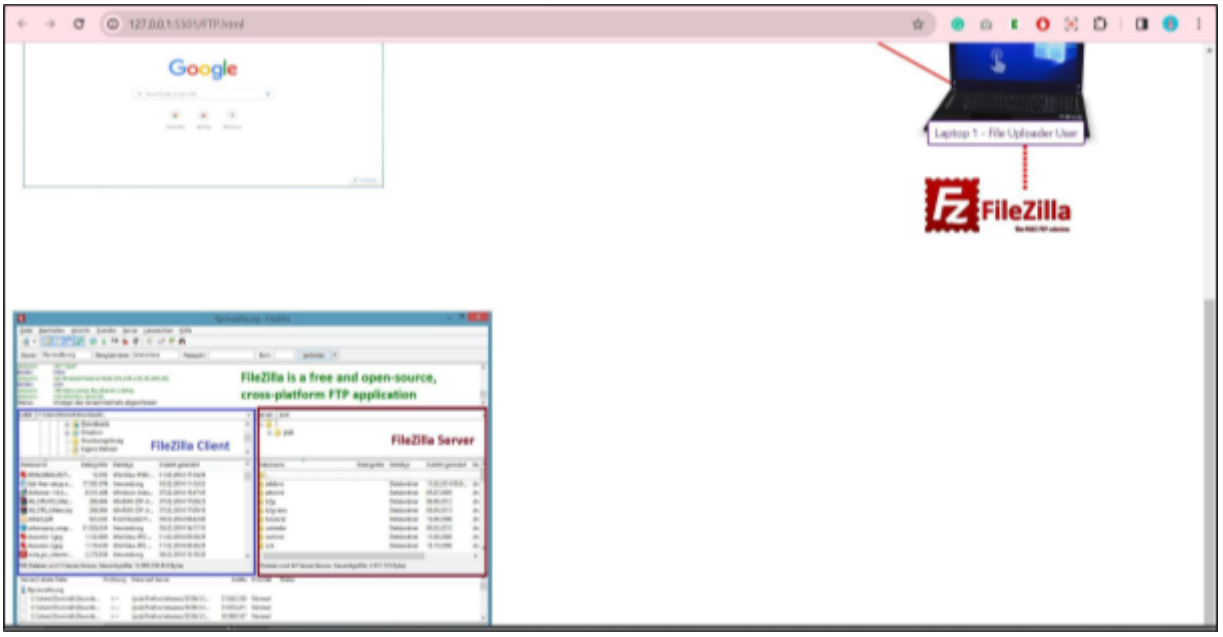
2. Click on FileZilla FTP Application Logo

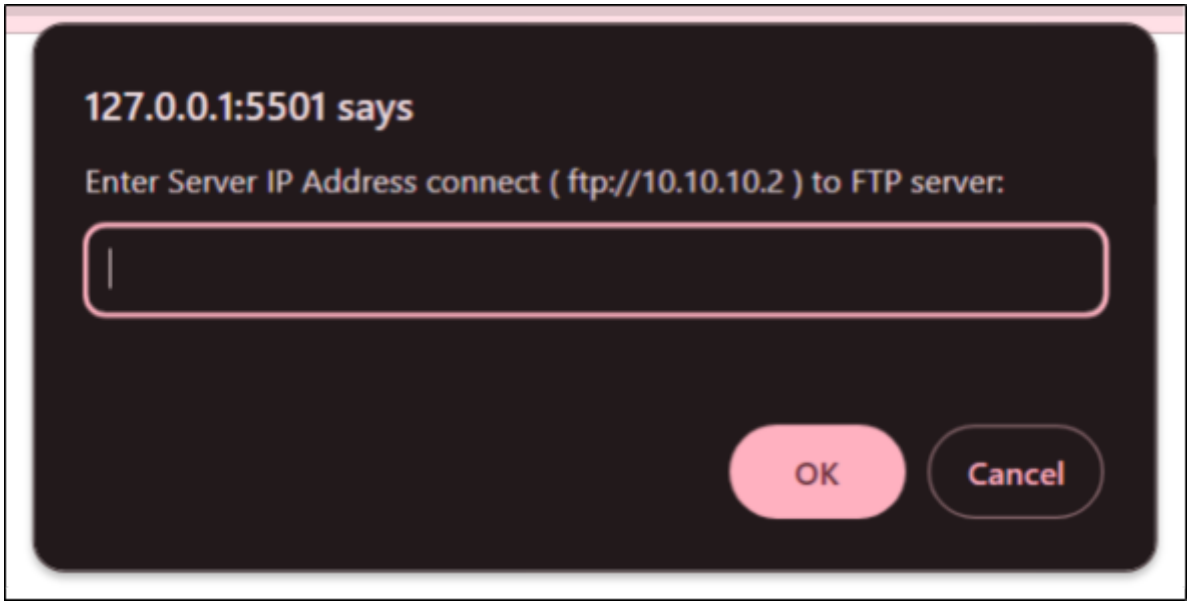
2.1 It will display something like this



After Reading it Click “Ok”.

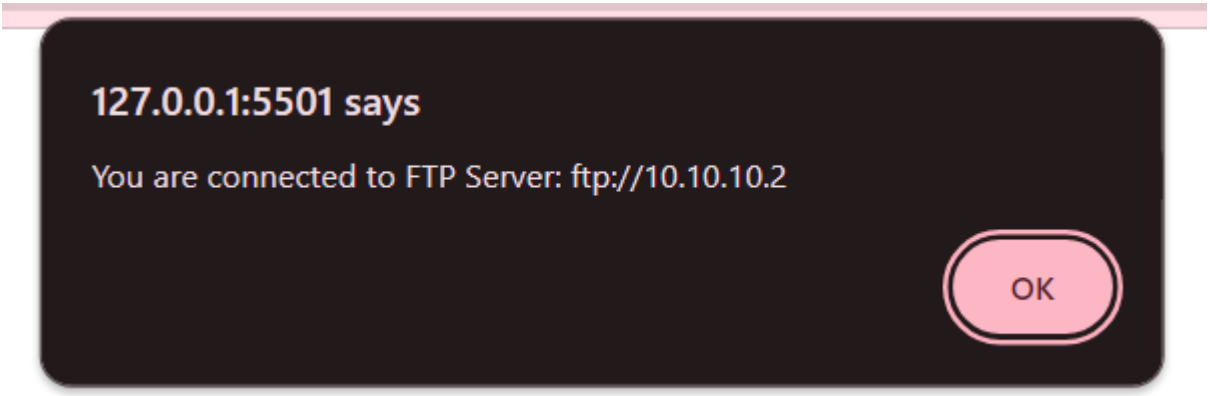
Now Scroll Down you will see image like this





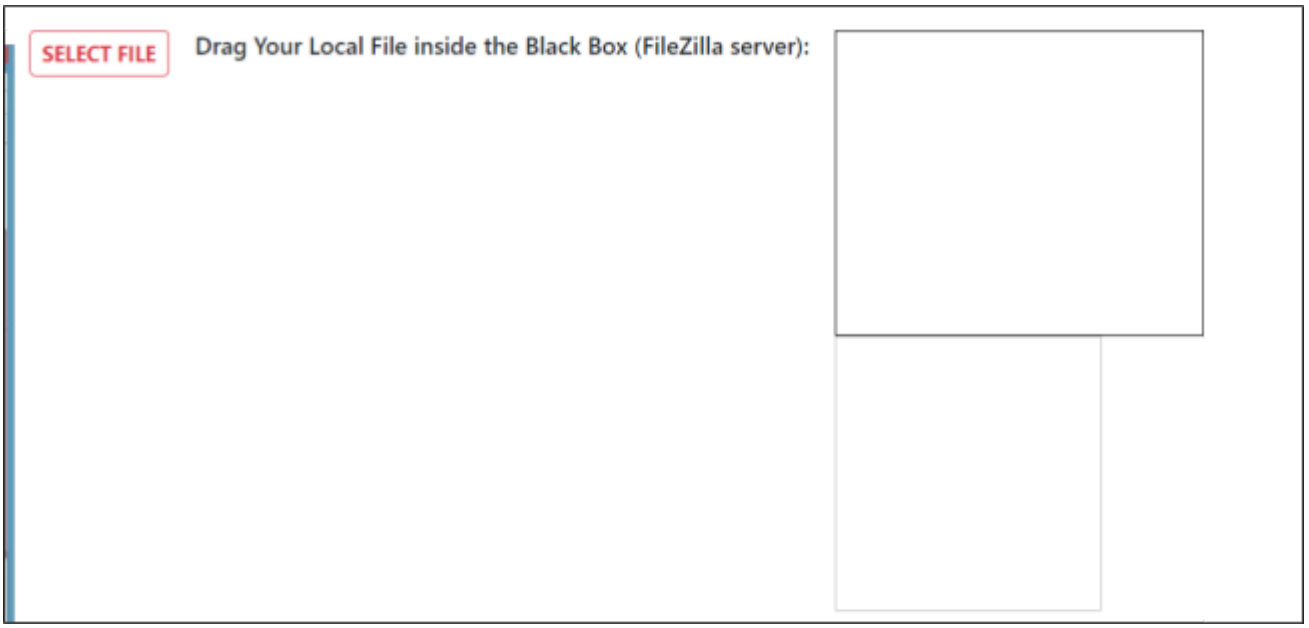
2.2 Enter there out FTP Server IP Address which we saw on first step ftp://10.10.10.2

2.3 Then it will prompt after entering correct IP Address



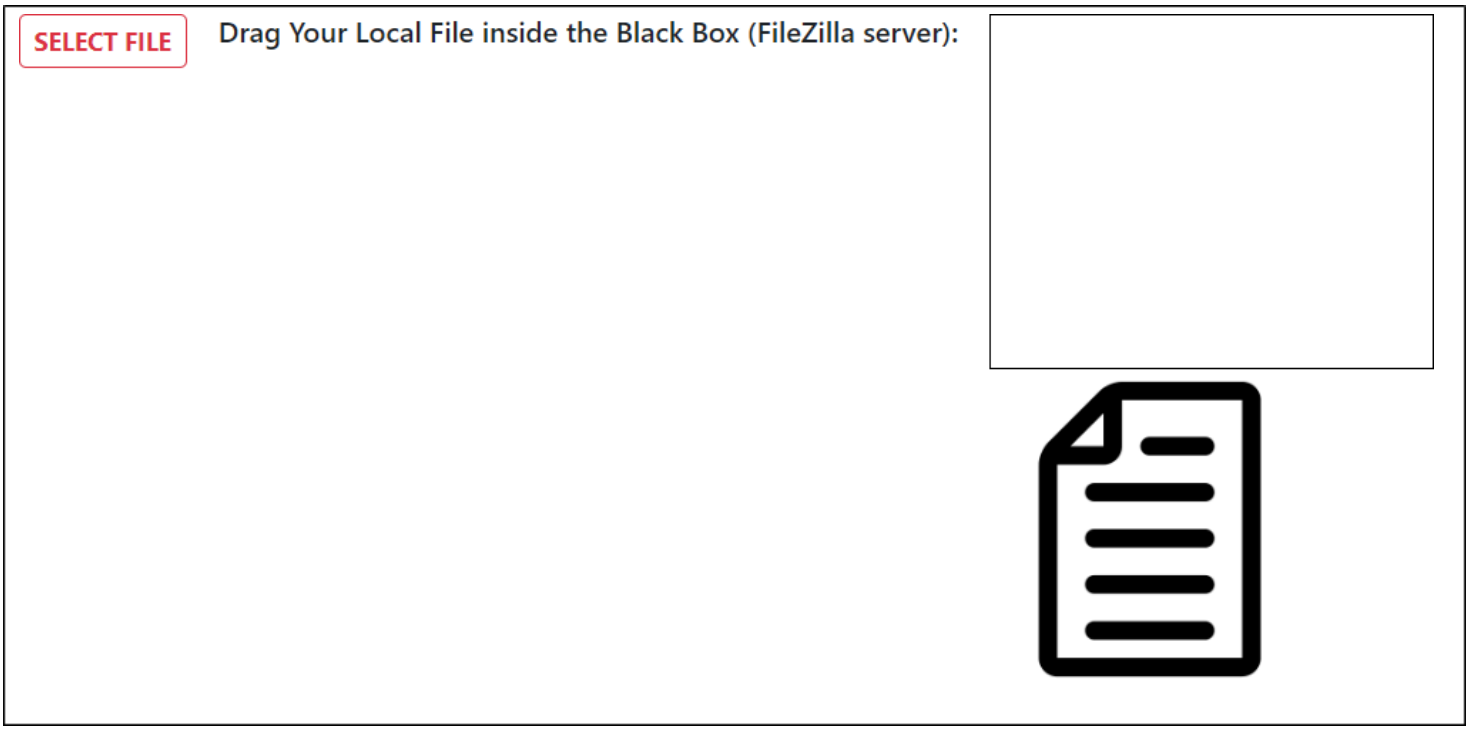
Click “Ok”

Now you will get a few things to upload your local file to the FTP Server. It shows FileZilla Application is used to upload files from your local file that represent FileZilla Client where you see your local files and then you can drag those to FileZilla Server.



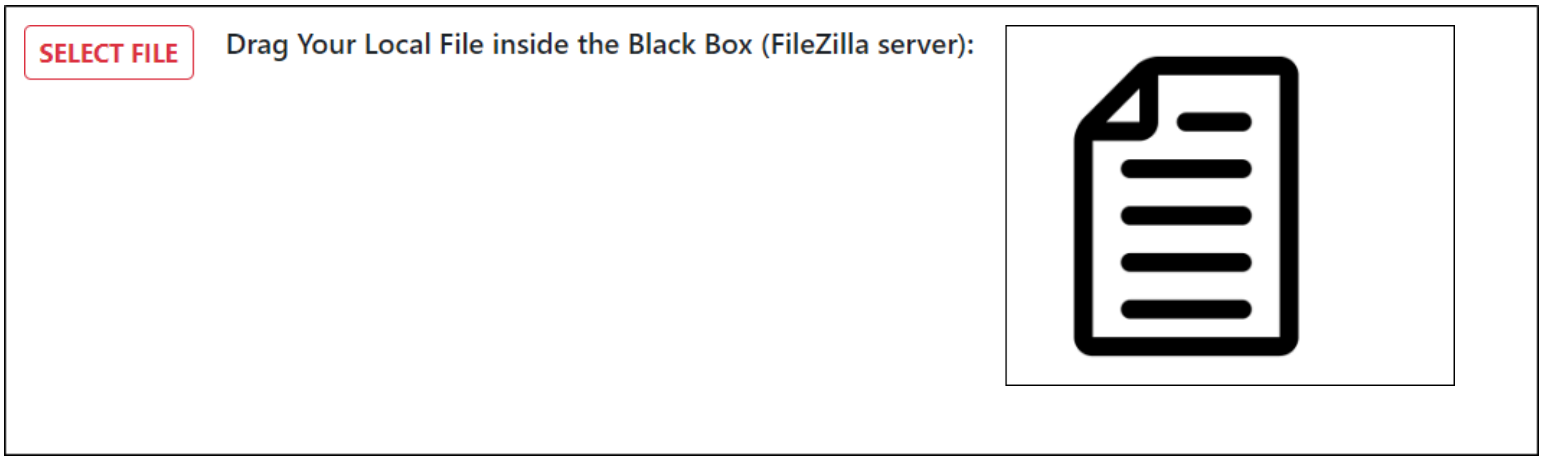
Click on the “SELECT FILE” red color button and select any file from your computer.

After selecting any one file it will look like this: you have selected one file from your local files.

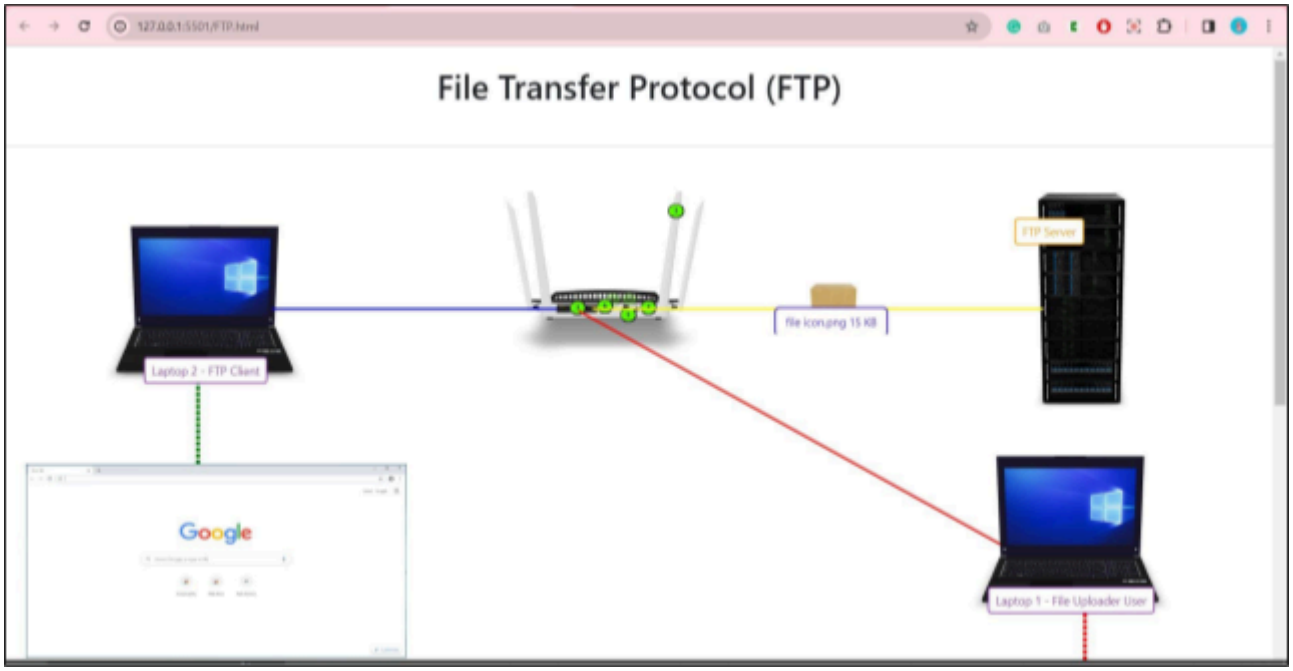


Drag that file into black box using mouse pointer

It Will look like this something



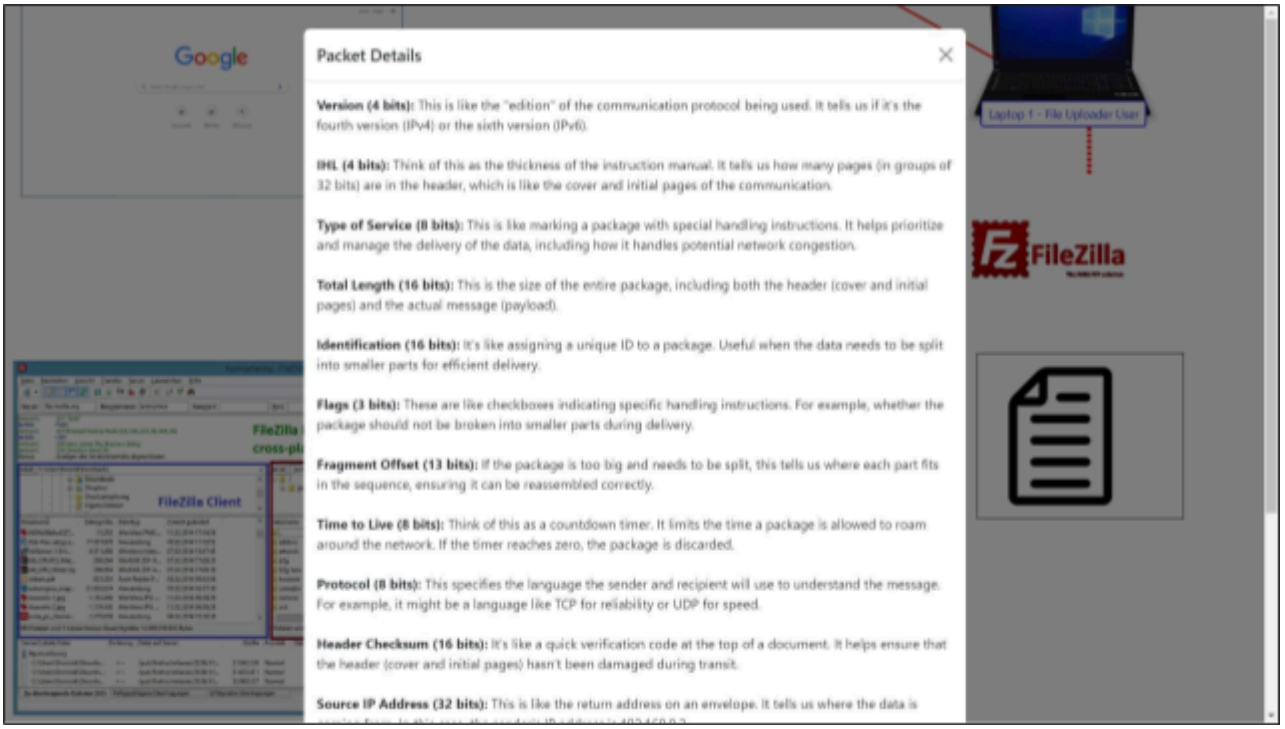
After a process of uploading of file will start in packets by packets

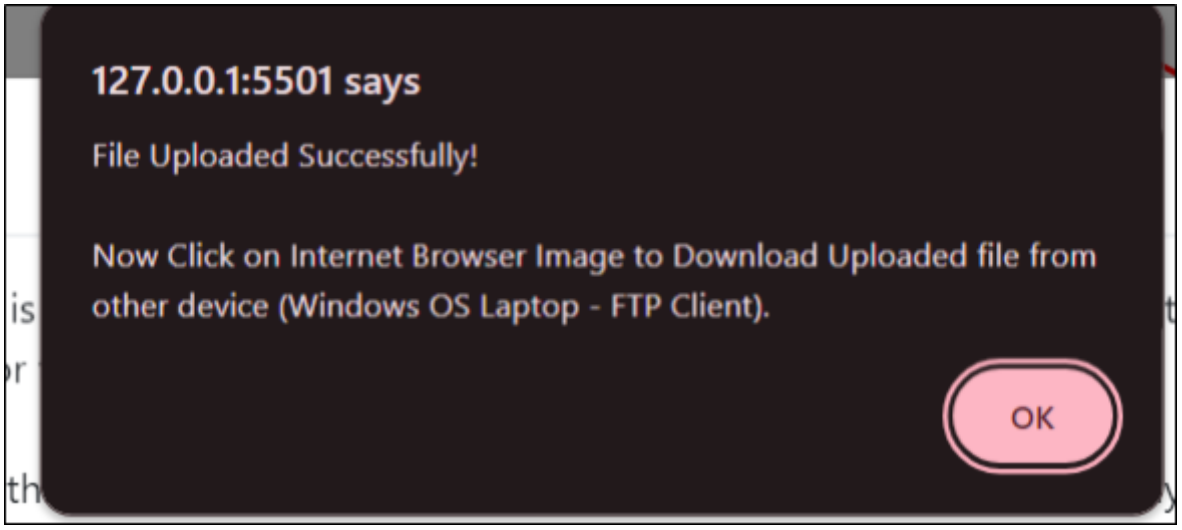


You can see your file name and file size.

Click on the file name then you will see how the file is transferred in packets with packet details you can read.

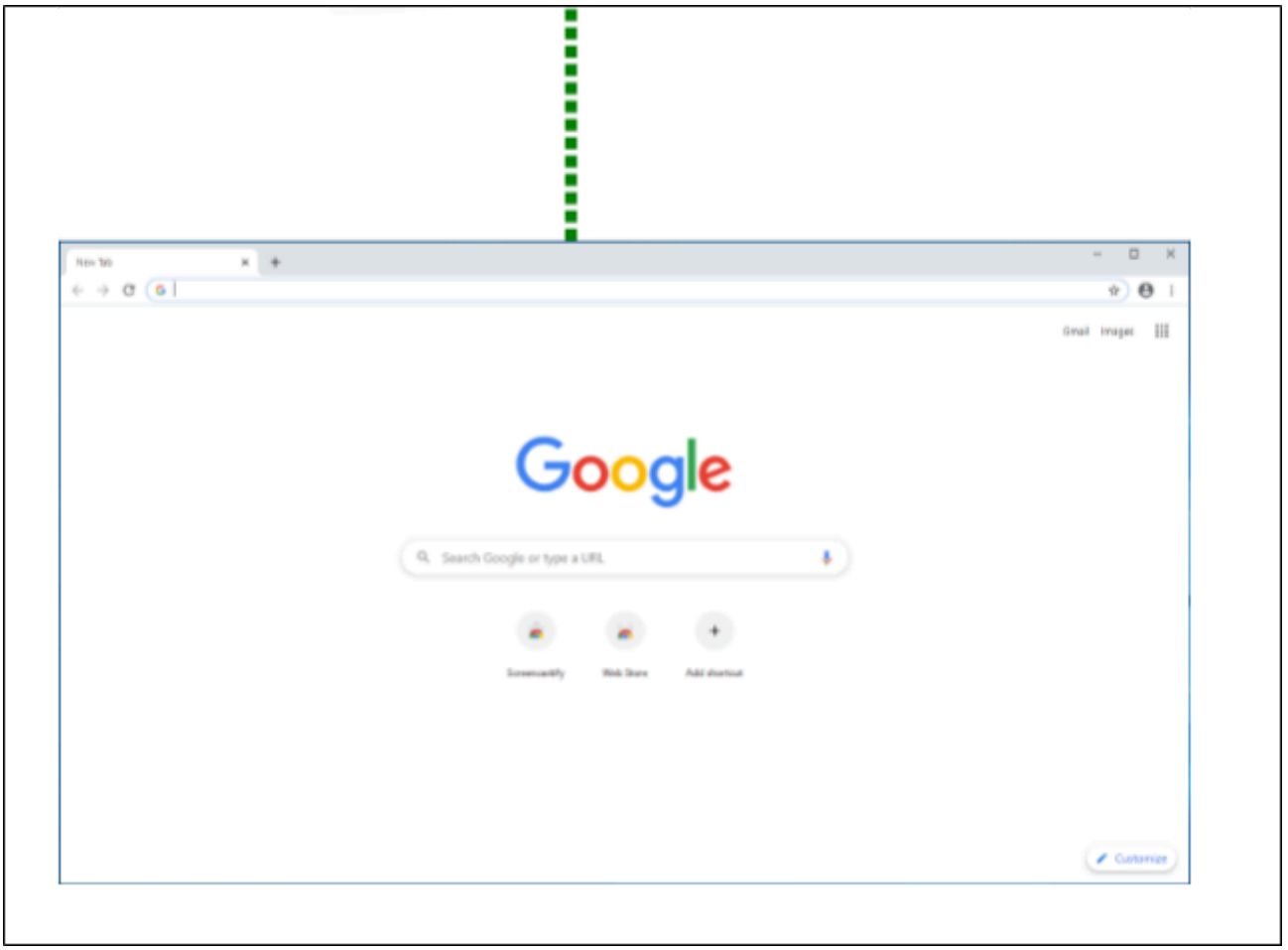
You will get a message that file has been uploaded successfully



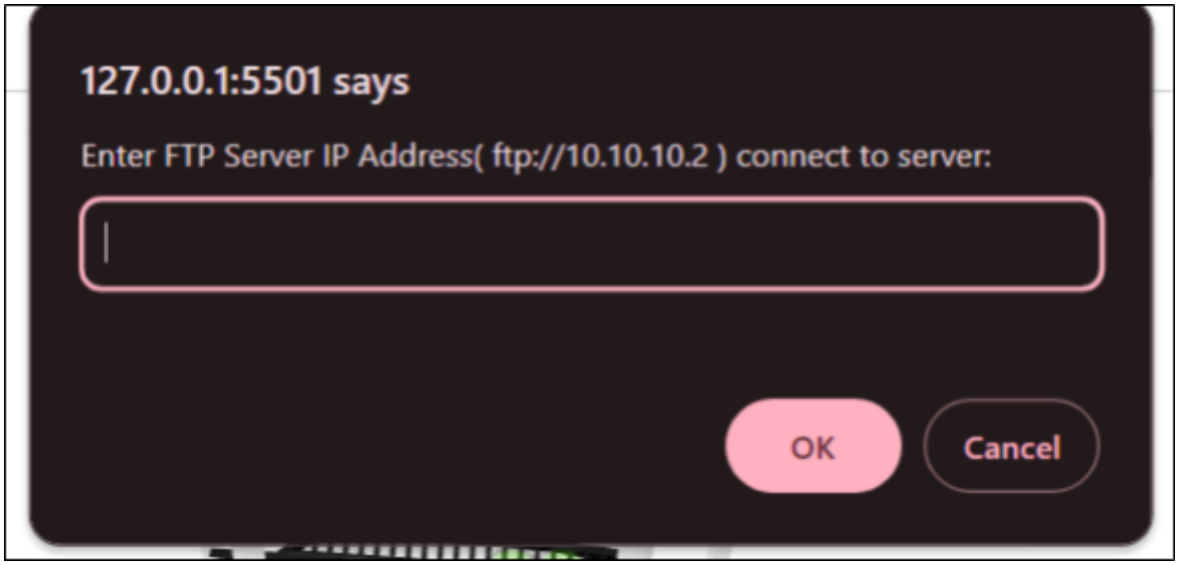


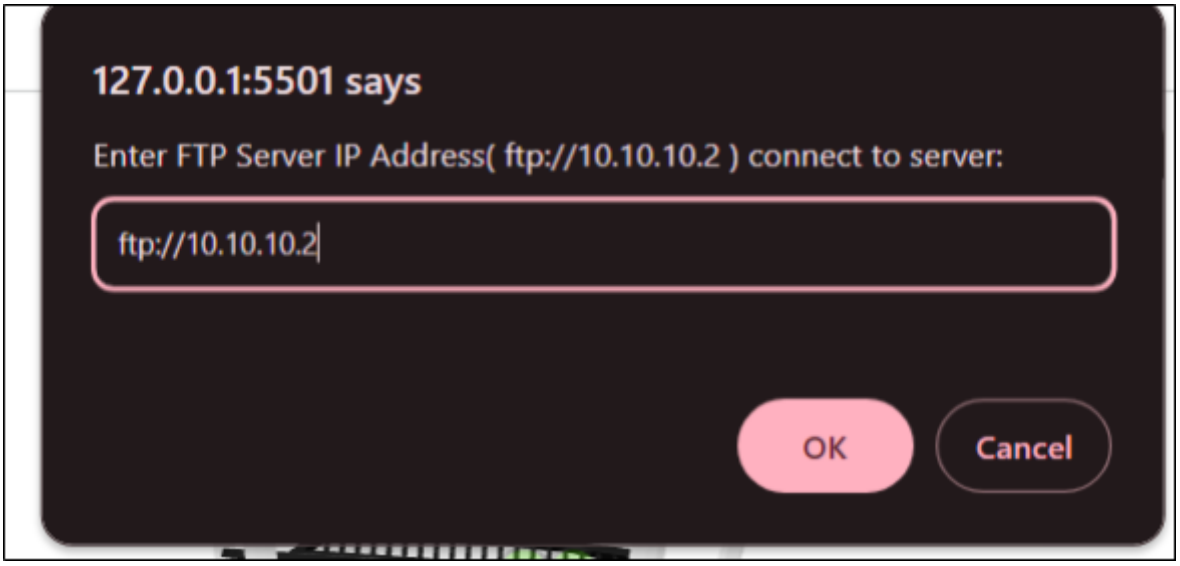
Next Part is to download a file which has been uploaded on server from another device using the same IP Address.

Click on the image shown below to download the file.

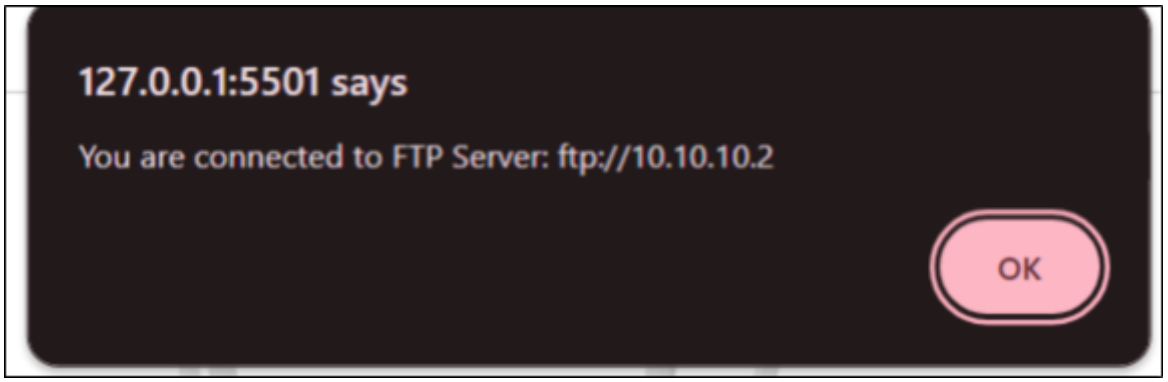


You will get a message to enter Server IP Address enter there ftp://10.10.10.2 to get that file.

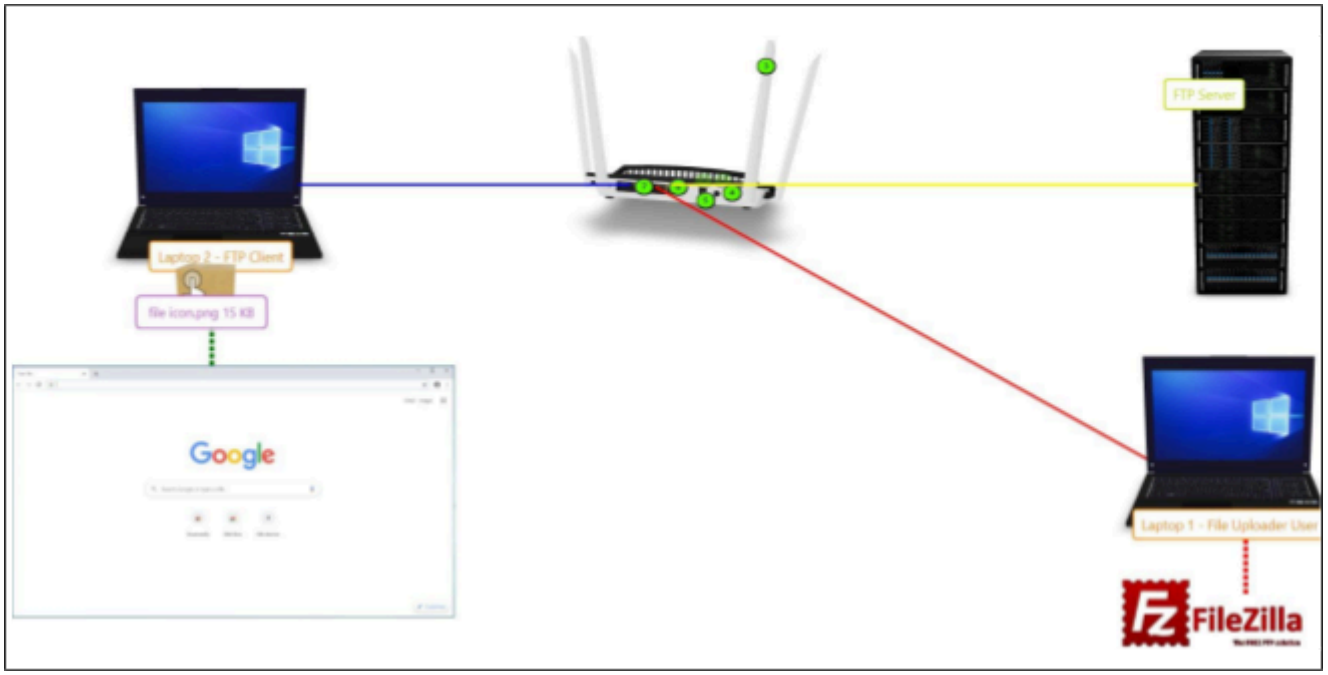


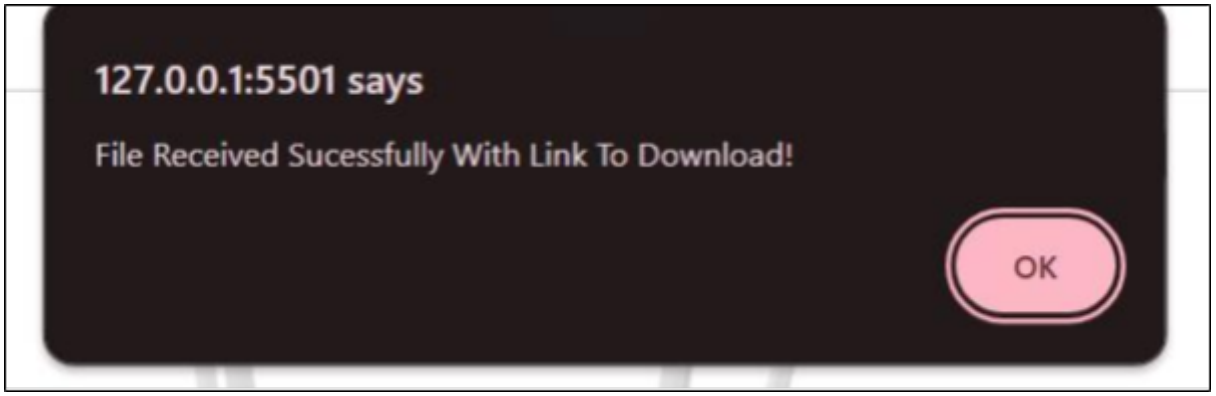


You get a successful message that you're connected to FTP Server.

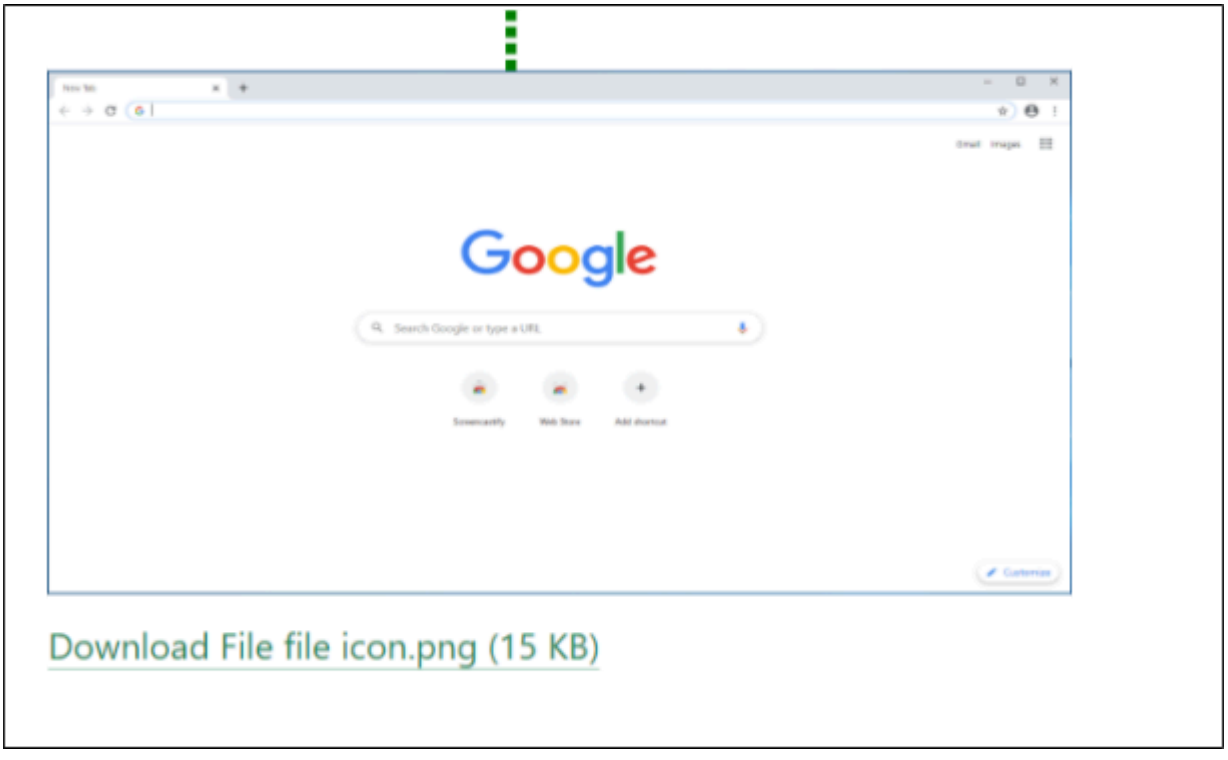


Now your file will start downloading to other device Laptop 2 - FTP Client



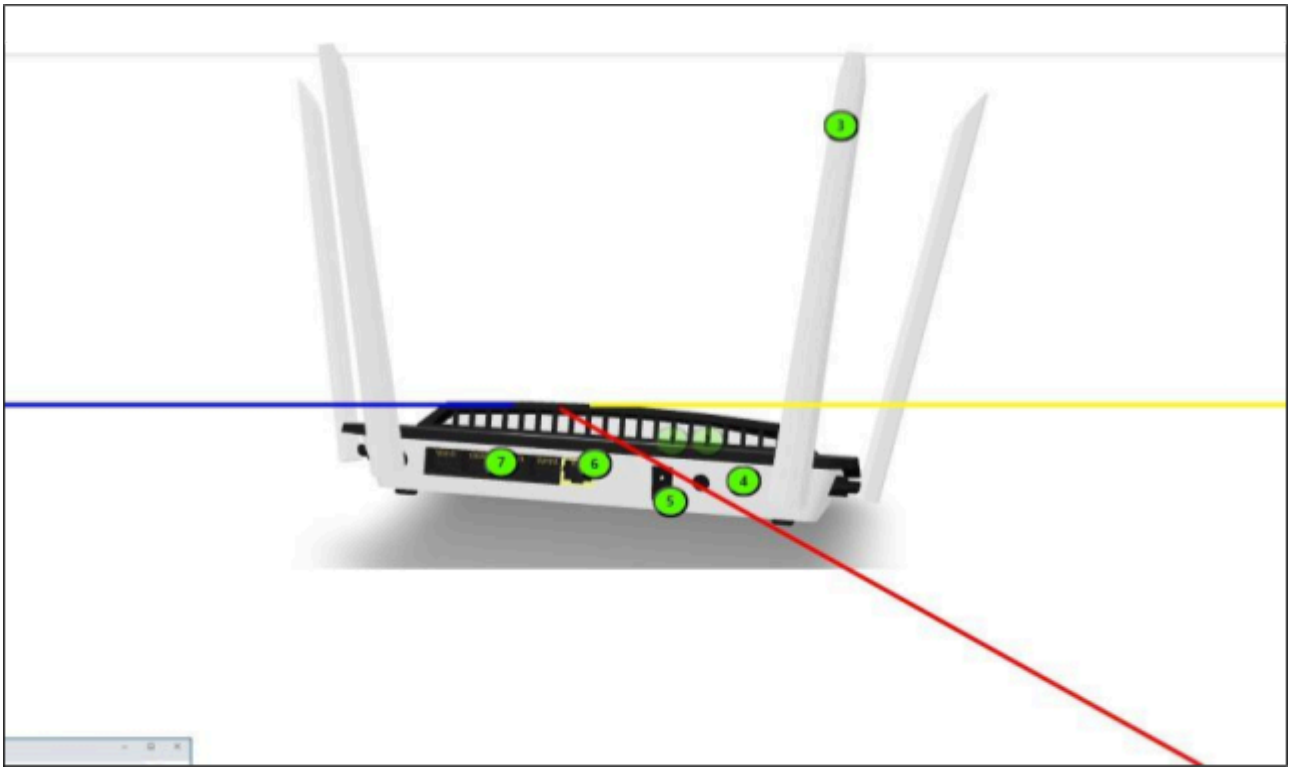


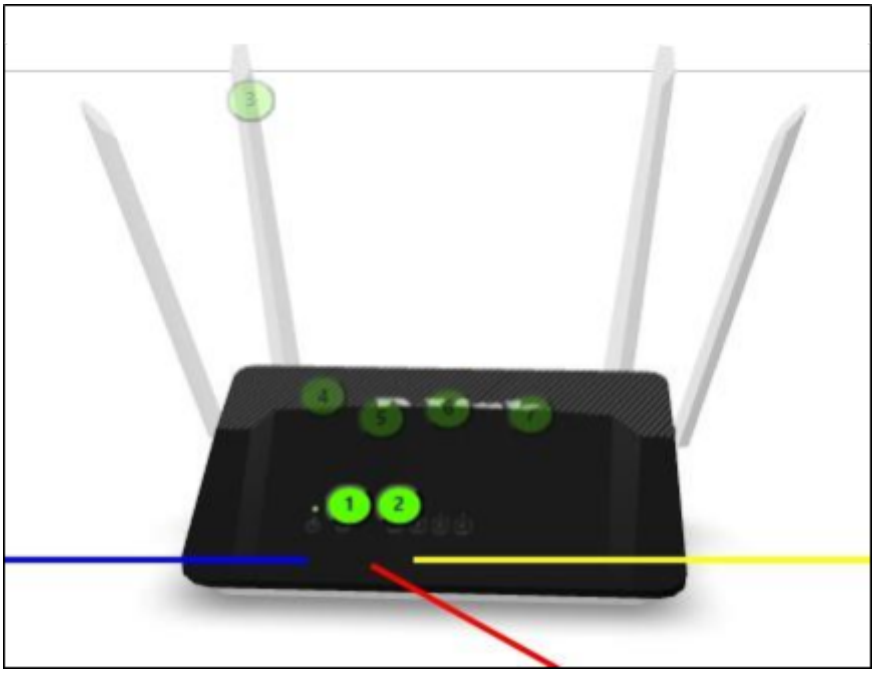
You will get the link of File Received Successfully. Now Click on the Green Color link to download the file to your device. This is how FTP works in the real world shown similarly in Augmented Reality.



You can explore more in AR not till file transferring only!! You can view how the router looks and zoom in with the mouse.

Click on green circles to know the parts of Router.





WAN/Internet Port

Connect modem or transceiver to link home network to internet.

Okay

Address Resolution Protocol

Introduction:

The Address Resolution Protocol (ARP) is a fundamental protocol used in computer networks to map IP addresses to physical MAC addresses within a local network segment. Its primary function is to facilitate communication between devices by resolving IP addresses to MAC addresses, which are necessary for data transmission at the link layer of the OSI model.

Aim and Objective:

The aim of ARP is to provide a method for dynamically resolving IP addresses to MAC addresses within a local network, enabling efficient and reliable communication between devices. Its objectives include:

- Address Resolution: ARP aims to resolve the mapping between IP addresses and MAC addresses to facilitate communication between devices on the same network segment.
- Efficiency: ARP aims to operate efficiently by minimizing network traffic and overhead associated with address resolution.
- Dynamic Updates: ARP allows for dynamic updates of the ARP cache, ensuring that changes in network topology or device configurations are reflected accurately.

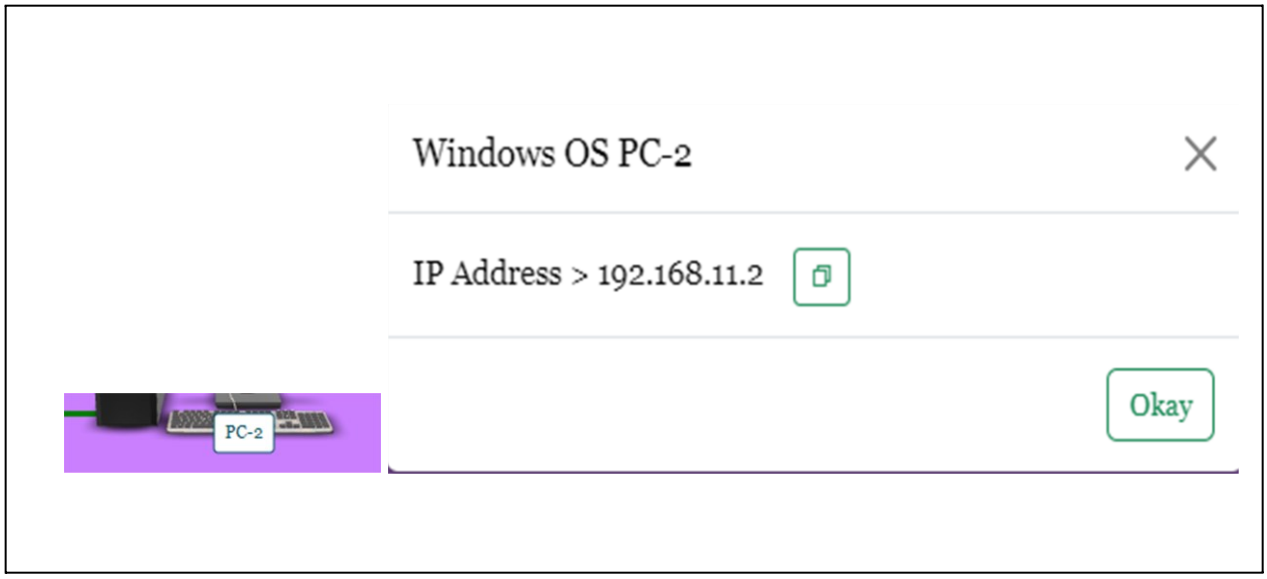
Steps Involved in Address Resolution Protocol:

- ARP Request: When a device needs to communicate with another device on the same network segment and does not have the MAC address of the destination device, it broadcasts an ARP request packet containing the IP address it wishes to resolve.
- ARP Reply: The device with the corresponding IP address specified in the ARP request responds with an ARP reply packet containing its MAC address.
- ARP Caching: Upon receiving the ARP reply, the requesting device stores the IP-to-MAC mapping in its ARP cache to facilitate future communication with the same device. This caching mechanism helps to reduce ARP traffic and improve network efficiency.
- Address Resolution: With the IP-to-MAC mapping stored in its ARP cache, the requesting device can now encapsulate the data packets with the correct destination MAC address, enabling direct communication with the destination device.

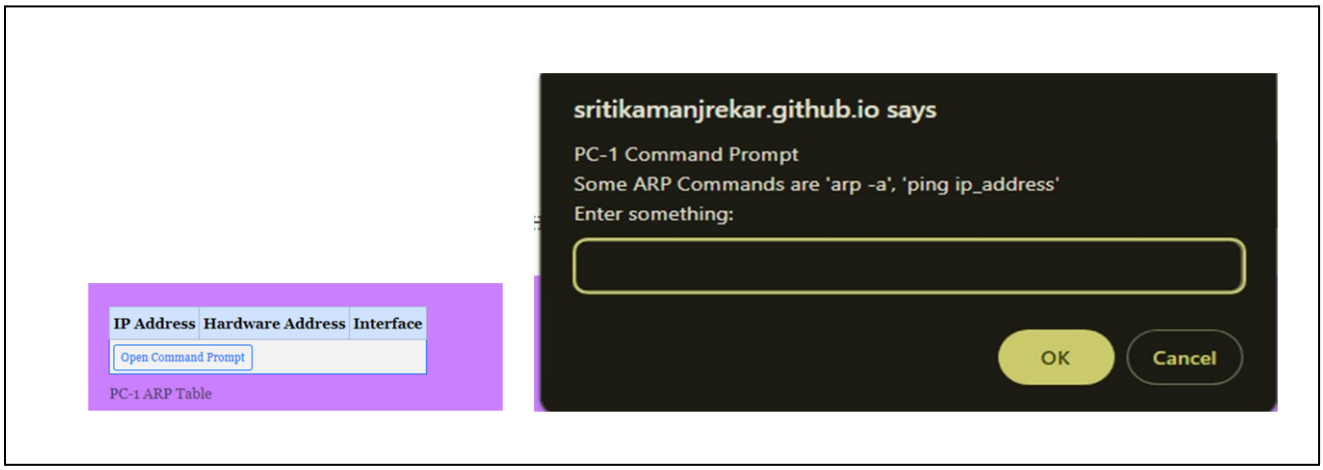
Conclusion:

In conclusion, the Address Resolution Protocol (ARP) plays a crucial role in enabling communication between devices on the same network segment by dynamically resolving IP addresses to MAC addresses. By facilitating efficient address resolution and maintaining an ARP cache, ARP helps optimize network performance and reliability. It serves as a fundamental component of modern networking protocols, ensuring seamless connectivity within local networks.

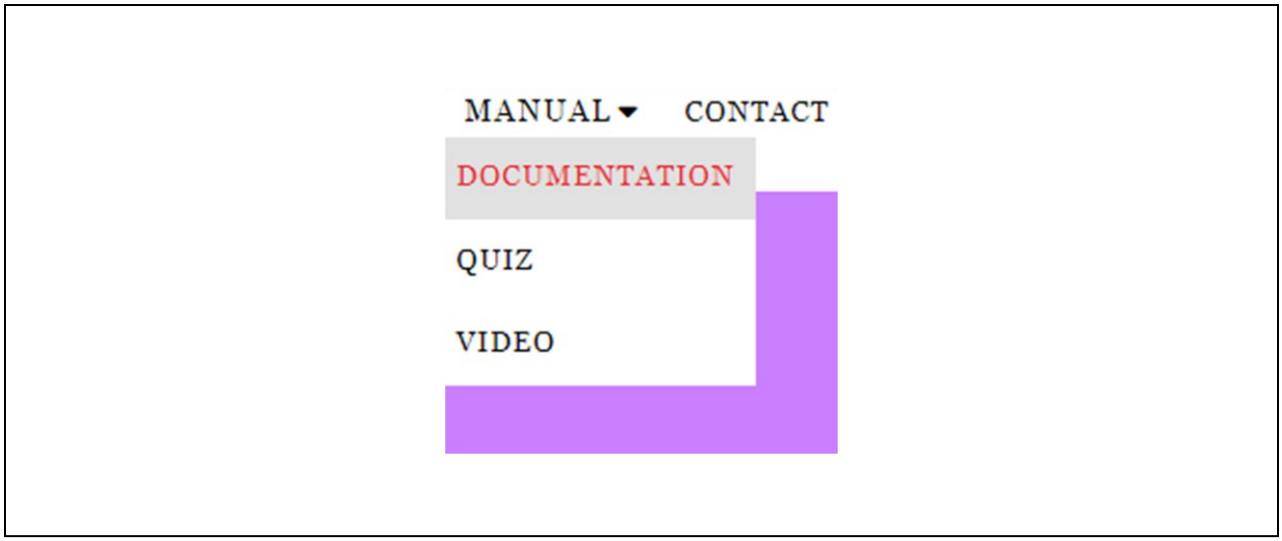
1. If you want know IP & MAC Address of any PC you can click on blue square as shown below:



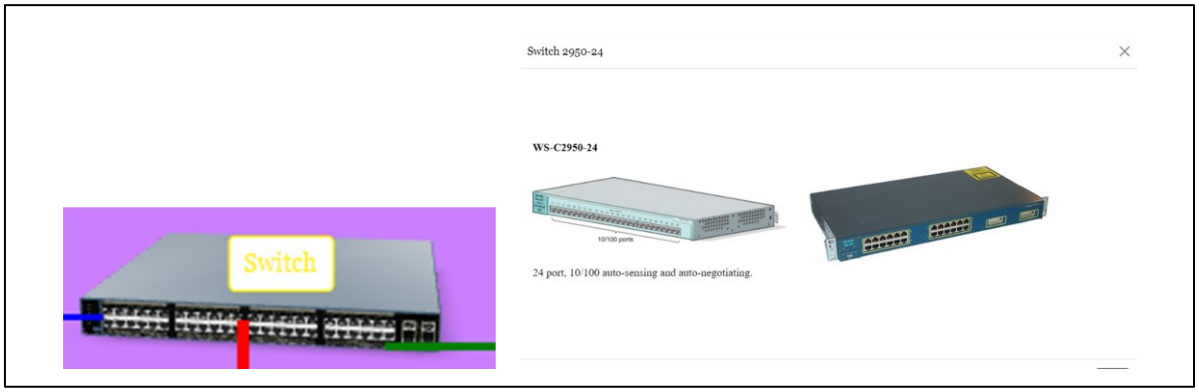
2. Let's start performing ARP in AR World!!! Click on "Open Command Prompt" button of any PC:



3. Click on “Explore ARP Magic” to view Presentation on ARP :

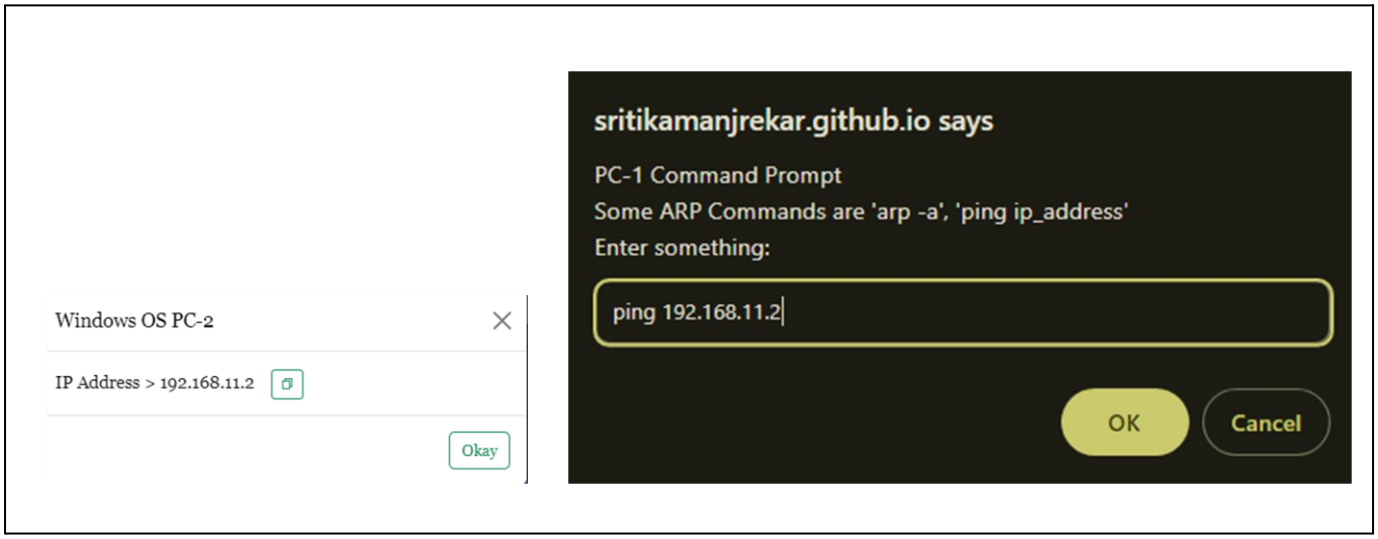


4. Click on “Switch” to view Switch Details:



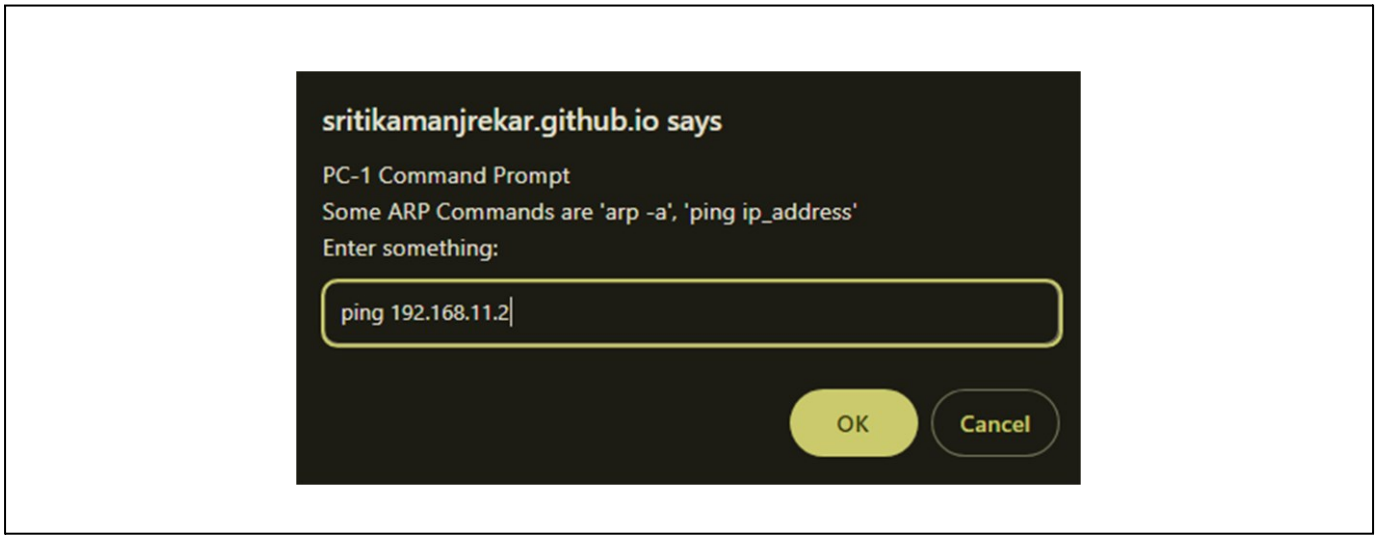
5. Click on wire colors “Red”/”Blue”/”Green” to view wire details:

6. Enter “ping IP_Address” of PC of which you want to know MAC Address

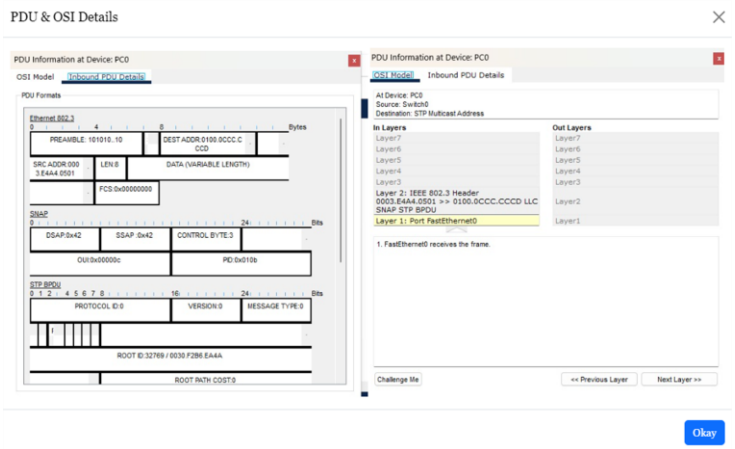


For now let’s enter IP Address of PC-2 which is 192.168.11.2

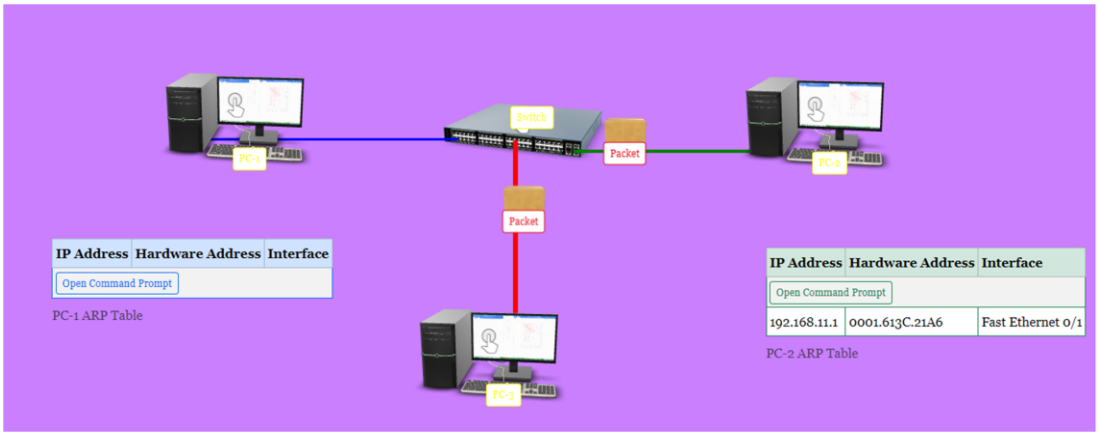
7. Now Click on OK then the magic AR World will begin the packet will start simulating



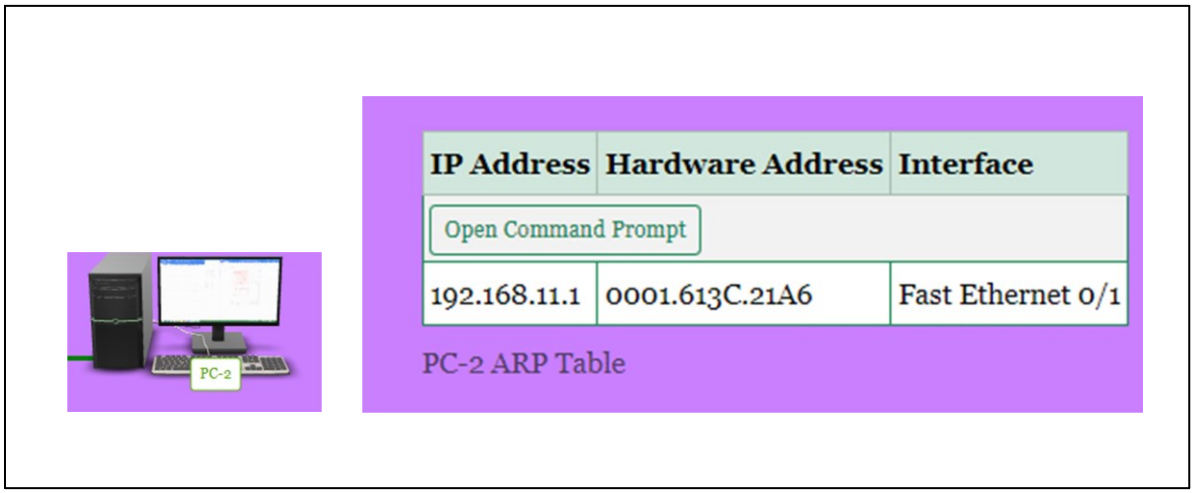
8. When you click on Packet Label you will get details of what is there inside the Packet when it goes from PC-1 to PC-2, PC-3 to search for that IP Address



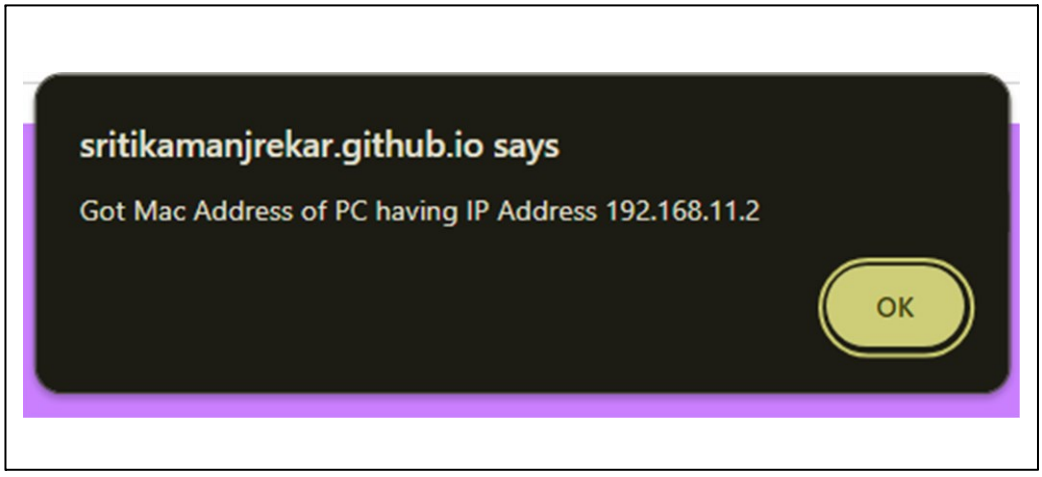
9. PC-1 sends a ping to all PC's whichever PC matches that ping IP Address sends Acknowledgement and also stores PC-1 IP Address and MAC Address in their ARP table.



10. PC-2 stores IP Address, MAC Address, Interface in their ARP Table of PC-1.



11. You will get an alert message like this: “Got MAC Address” means communication between PC-1 to respective PC with IP Address 192.168.11.2 is completed.



12. You will observe that after clicking on OK the PC-1 ARP table shows IP Address, MAC Address, Interface of PC-2.

IP Address	Hardware Address	Interface
Open Command Prompt		
192.168.11.2	0030.A333.03CB	Fast Ethernet 0/1

PC-1 ARP Table

This way you can get the MAC Address of any PC when you know only one thing that is an IP Address and this is how it works in Real World also.

Bonus!!!

You can also zoom in network devices with mouse to look around to take a look

Reverse Address Resolution Protocol

Introduction:

Reverse Address Resolution Protocol (RARP) is a networking protocol used to obtain an IP address from a known MAC address. Unlike ARP, which resolves IP addresses to MAC addresses, RARP resolves MAC addresses to IP addresses. RARP is primarily utilized in diskless workstation environments where devices need an IP address to boot and initialize network services.

Aim and Objective:

The aim of RARP is to enable diskless workstations or devices without pre-configured IP addresses to obtain their IP addresses dynamically based on their MAC addresses. The objectives of RARP include:

- Dynamic IP Address Assignment: RARP aims to dynamically assign IP addresses to devices based on their MAC addresses, simplifying network administration and configuration management.

- Bootstrapping: RARP facilitates the bootstrapping process for diskless workstations by providing them with the necessary IP configuration information to initialize network services and communicate on the network.

Steps Involved in Reverse Address Resolution Protocol:

- RARP Request: A diskless workstation sends a broadcast RARP request packet onto the network, containing its MAC address and indicating its need for an IP address.

- RARP Server Response: A RARP server on the network receives the broadcast RARP request and checks its configuration database for the MAC address. Once found, the RARP server responds with a unicast RARP reply packet containing the corresponding IP address for the requesting MAC address.

- IP Configuration: Upon receiving the RARP reply packet, the diskless workstation configures its network interface with the assigned IP address, subnet mask, default gateway, and other network parameters included in the RARP reply.

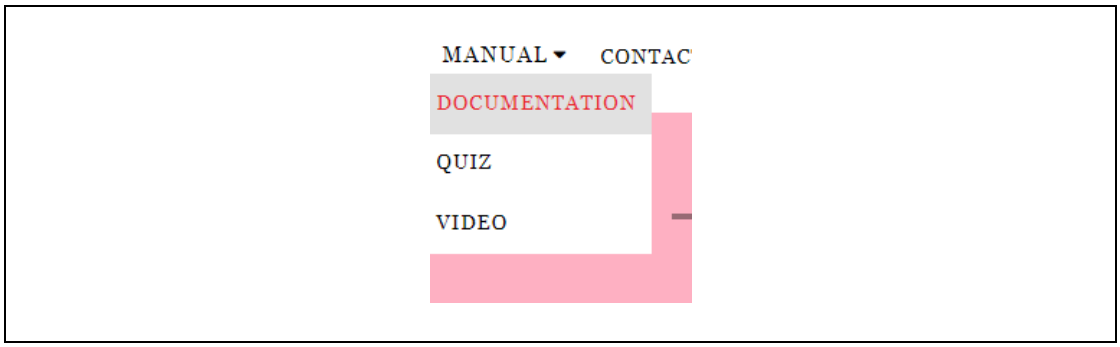
- Network Communication: With the IP address configured, the diskless workstation can now participate in network communication, including the ability to boot from a remote server, access network resources, and perform other network-related tasks.

Conclusion:

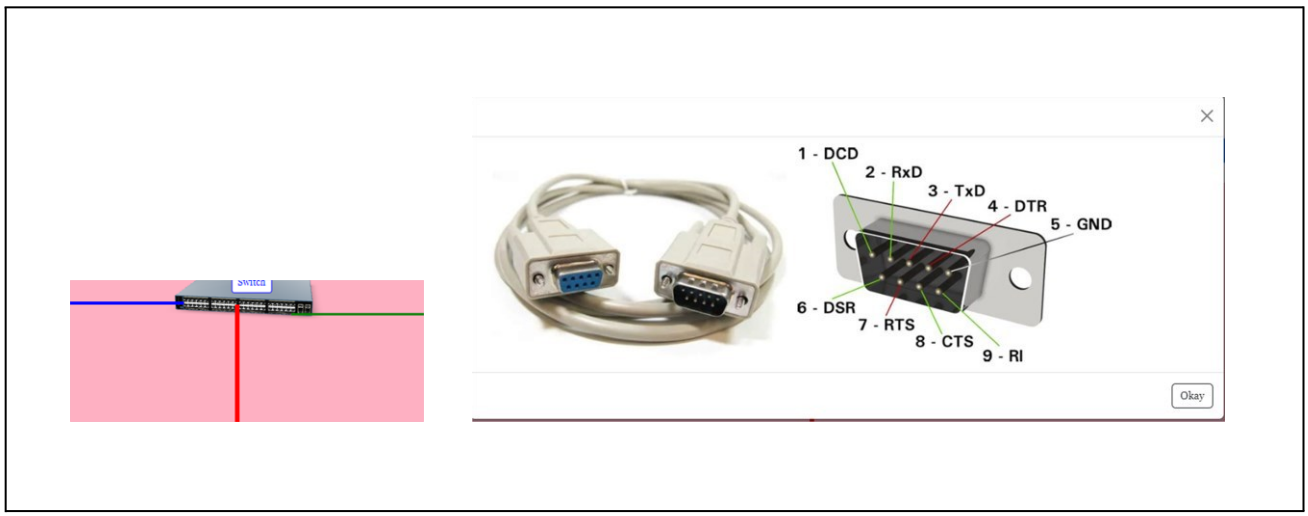
Reverse Address Resolution Protocol (RARP) provides a mechanism for diskless workstations and devices without pre-configured IP addresses to obtain their IP configuration dynamically based on their MAC addresses. By enabling dynamic IP address assignment, RARP simplifies network administration and facilitates the bootstrapping process for devices operating in diskless environments. While RARP has been largely replaced by more advanced protocols like DHCP (Dynamic Host Configuration Protocol), it remains a fundamental concept in understanding network address assignment mechanisms.

1. If you want know MAC Address of any PC you can click on blue square as shown below:

2. Click on “Manual” to view Presentation on RARP topic:

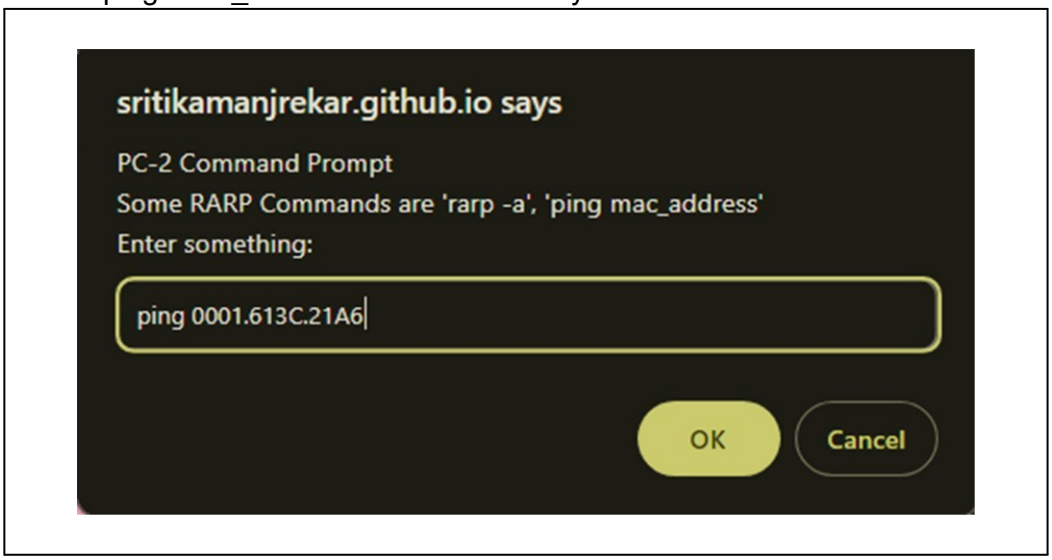


3. Click on wire colors “Red”/” Blue”/” Green” to view wire details:



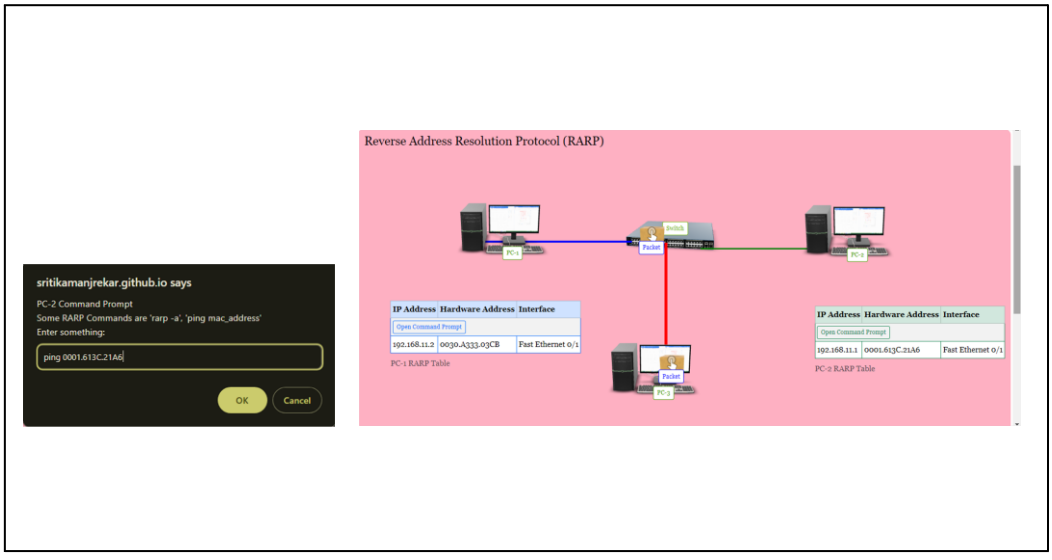
4. Let’s start performing RARP in AR World!!! Click on “Open Command Prompt” button of any PC:

5. Enter “ping MAC_Address” of PC of which you want to know IP Address

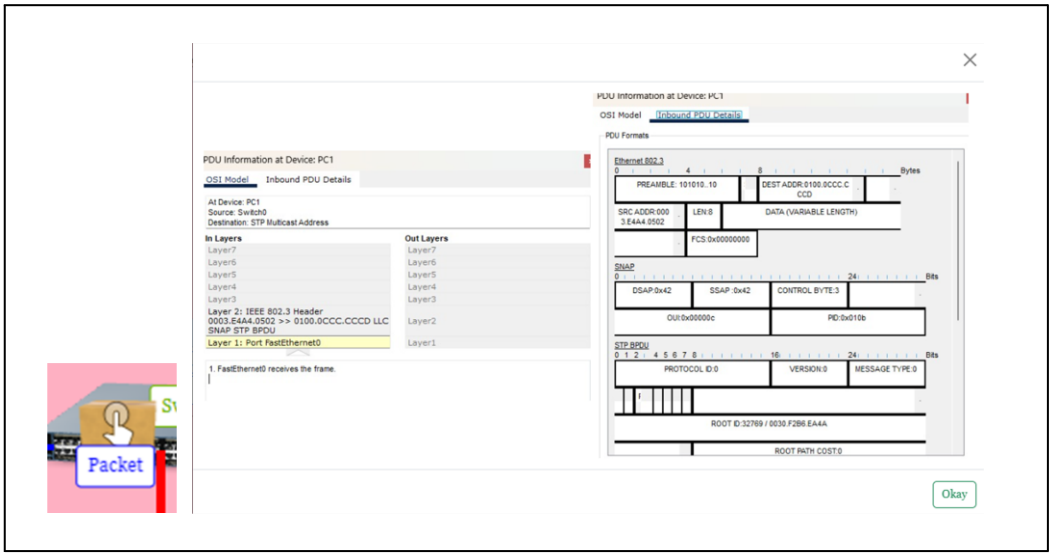


6. For now let’s enter MAC Address of PC-1 which is 0001.613C.21A6

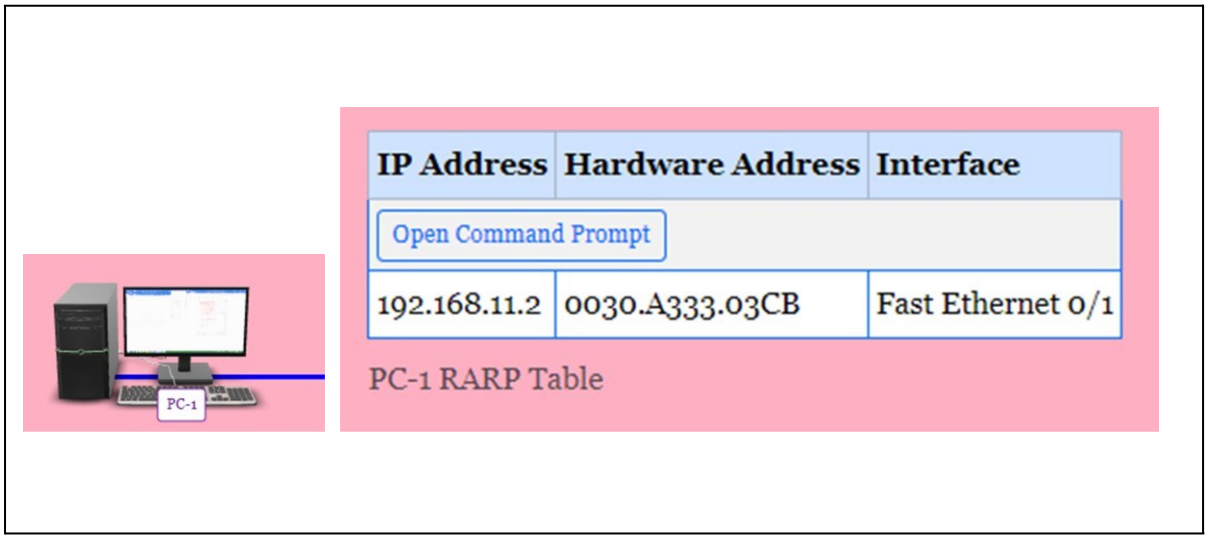
7. Now Click on OK then the magic AR World will begin the packet will start simulating



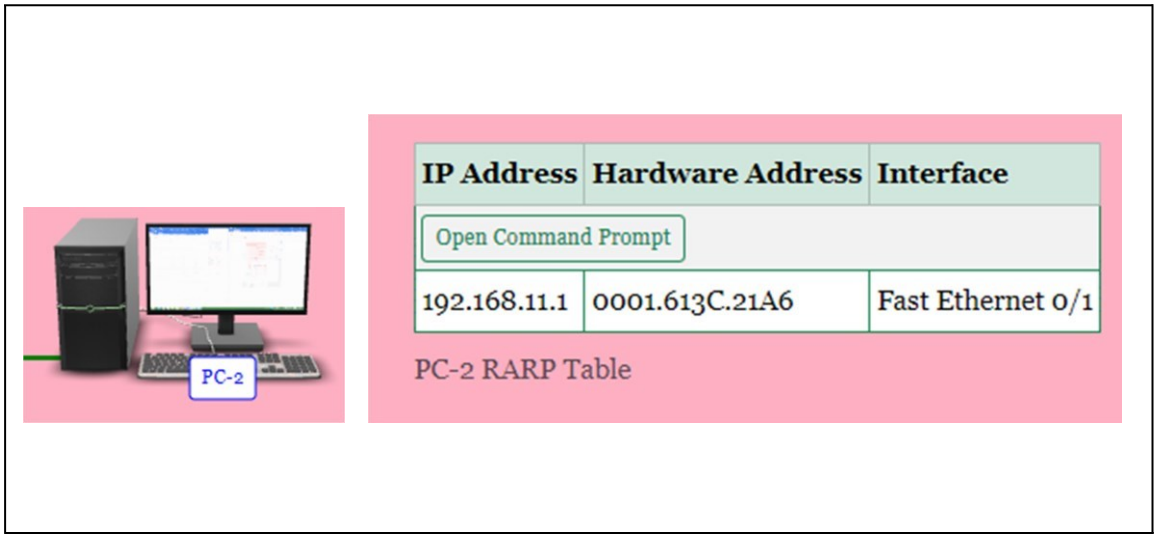
8. When you click on Packet Label you will get details of what is there inside the Packet when it goes from PC-1 to PC-2, PC-3 to search for that MAC Address



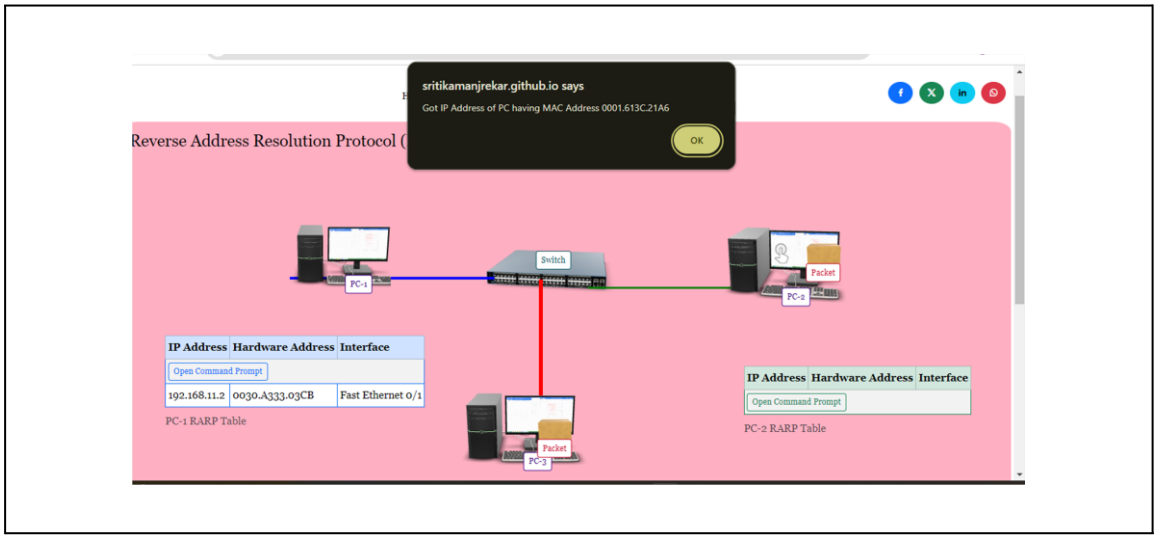
9. PC-1 sends a ping to all PC's whichever PC matches that ping MAC Address sends Acknowledgement and also stores PC-1 MAC Address and IP Address in their RARP table.



10. PC-2 stores IP Address, MAC Address, Interface in their RARP Table of PC-1.



11. You will get an alert message like this: “Got MAC Address” means communication between PC1 to respective PC with IP Address is completed.



This way you can get the IP Address of any PC when you know only one thing that is an MAC Address and this is how it works in Real World also.

Bonus!!!

You can also zoom in network devices with mouse to look around to take a look

HyperText Transfer Protocol

Introduction:

Hypertext Transfer Protocol (HTTP) is an application protocol used for distributed, collaborative, hypermedia information systems. It is the foundation of data communication for the World Wide Web, enabling the exchange of text, images, videos, and other multimedia content between web servers and clients.

Aim of HTTP:

The primary aim of HTTP is to facilitate the retrieval and display of resources on the World Wide Web. It defines how messages are formatted and transmitted, allowing web browsers to communicate with web servers and retrieve web pages and other content.

Objectives of HTTP:

- Interoperability: HTTP aims to ensure interoperability between different systems and platforms, allowing clients and servers developed by different vendors to communicate effectively.

- Efficiency: HTTP strives to optimize the transfer of data over the network by minimizing latency and maximizing throughput, thus improving the user experience during web browsing.

- Flexibility: HTTP provides a flexible framework for the exchange of various types of data, including text, images, videos, and structured documents, enabling the development of diverse web applications.

- Security: While not originally designed with security in mind, modern versions of HTTP (such as HTTPS) incorporate encryption and authentication mechanisms to enhance the security of data transmission over the web.

Steps in HTTP Communication:

- Client Request: A client (typically a web browser) sends an HTTP request to a server to retrieve a specific resource (e.g., a web page) identified by a Uniform Resource Identifier (URI).

- Server Processing: The server receives the HTTP request and processes it, determining the appropriate response based on the requested resource and any additional parameters provided in the request.

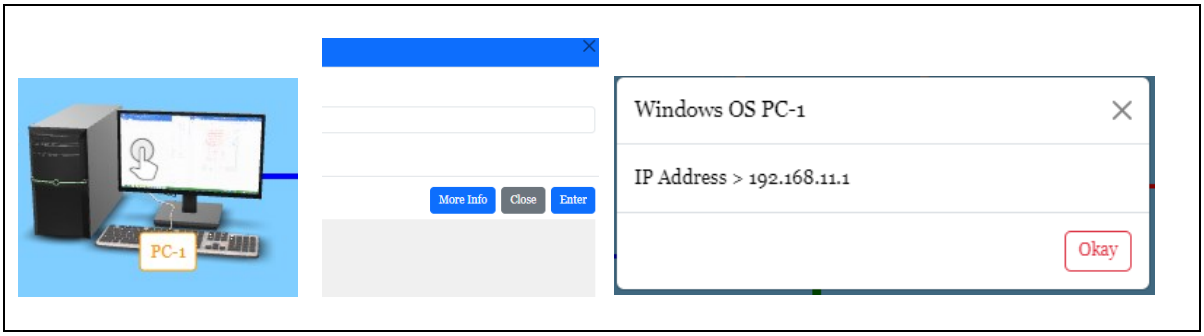
- Resource Retrieval: If the requested resource is available and accessible, the server retrieves it and prepares an HTTP response containing the requested resource along with relevant metadata (e.g., HTTP headers).

- Response Transmission: The server sends the HTTP response back to the client, which then processes the response and renders the retrieved resource (e.g., displays a web page in the browser).

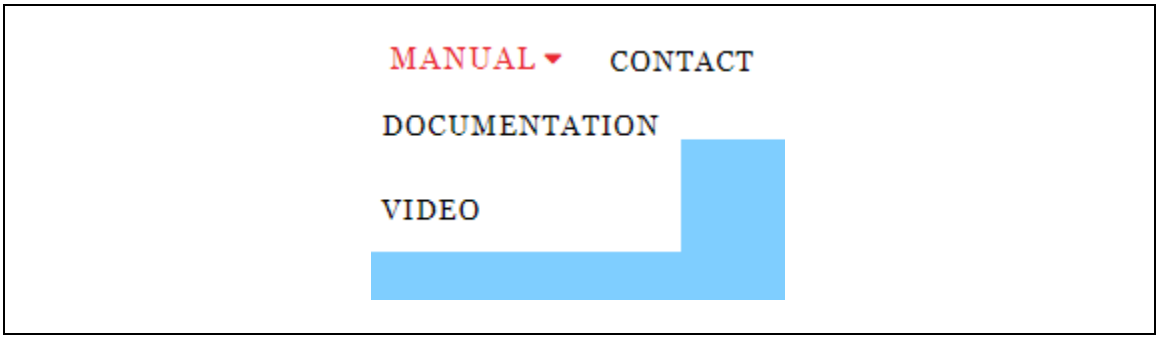
Conclusion

In conclusion, HTTP is a foundational protocol for communication on the World Wide Web, enabling the exchange of hypermedia content between clients and servers. By adhering to its principles of interoperability, efficiency, flexibility, and security, HTTP facilitates seamless and secure data transmission over the internet, powering the modern web browsing experience.

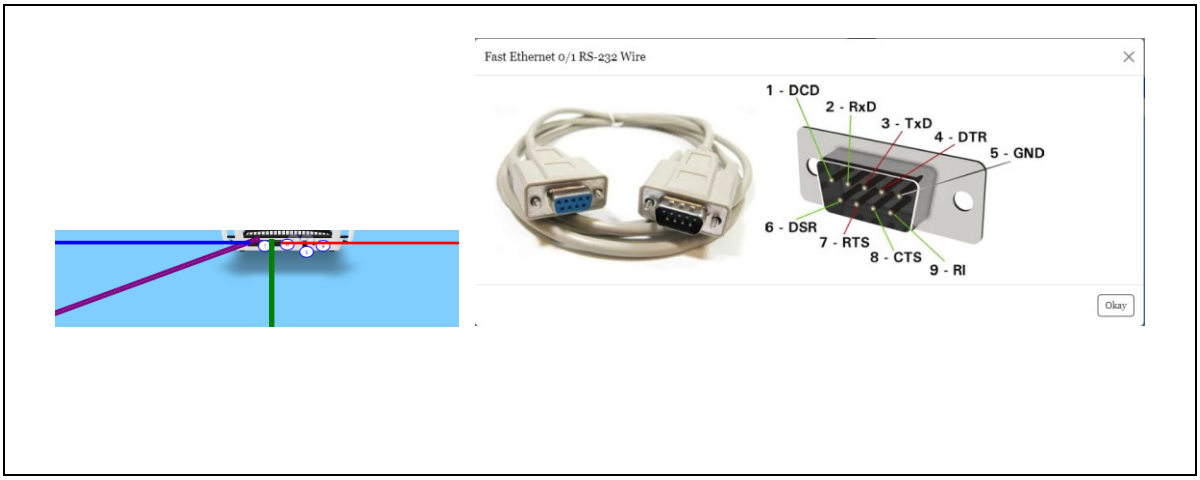
1. If you want know IP Address of any PC's "more info" you can click on blue square as shown below:



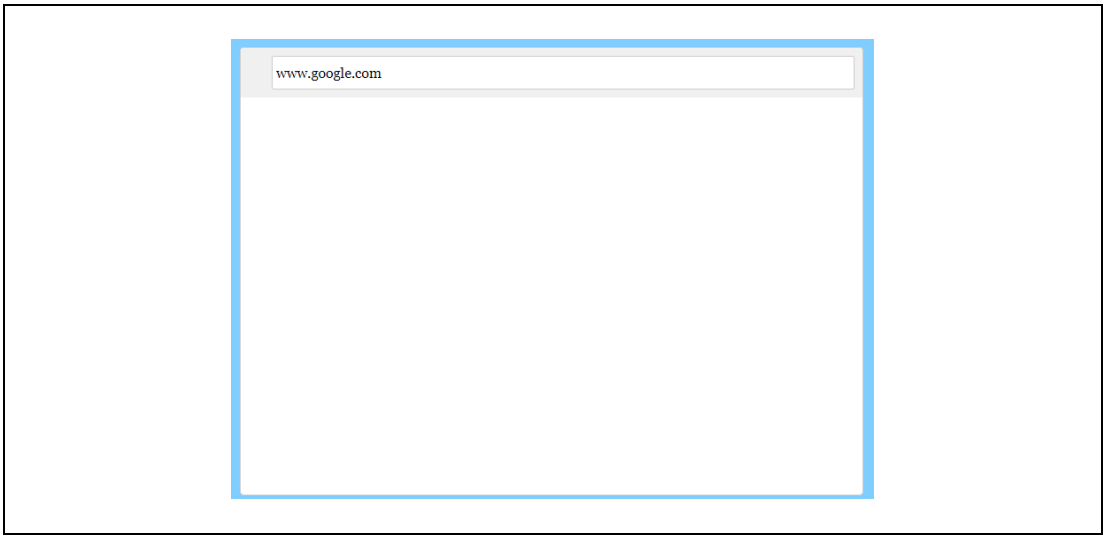
2. Click on "Manual" to view Presentation on HTTP topic:



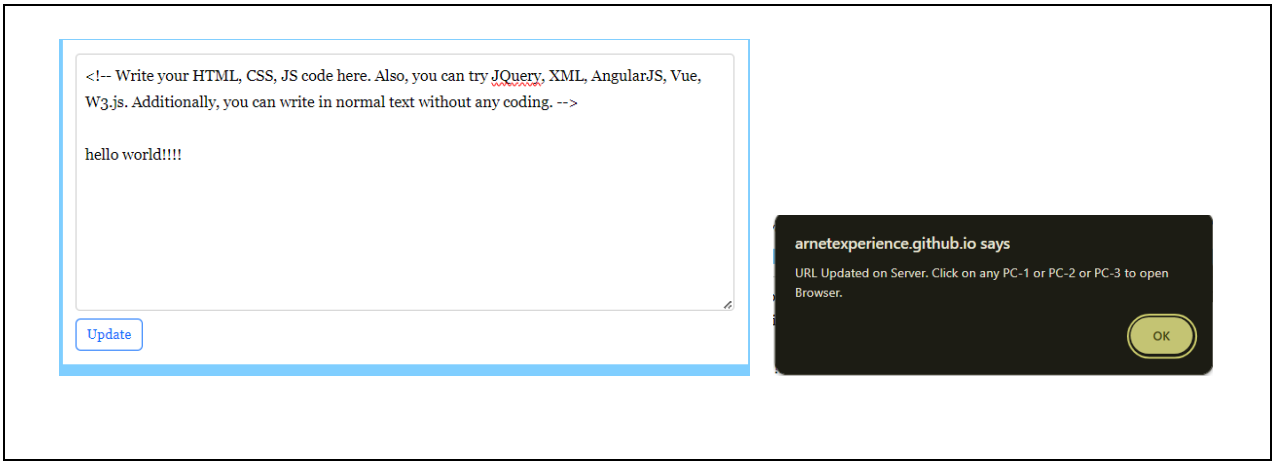
3. Click on wire colors "Red"/" Blue"/" Green" to view wire details:



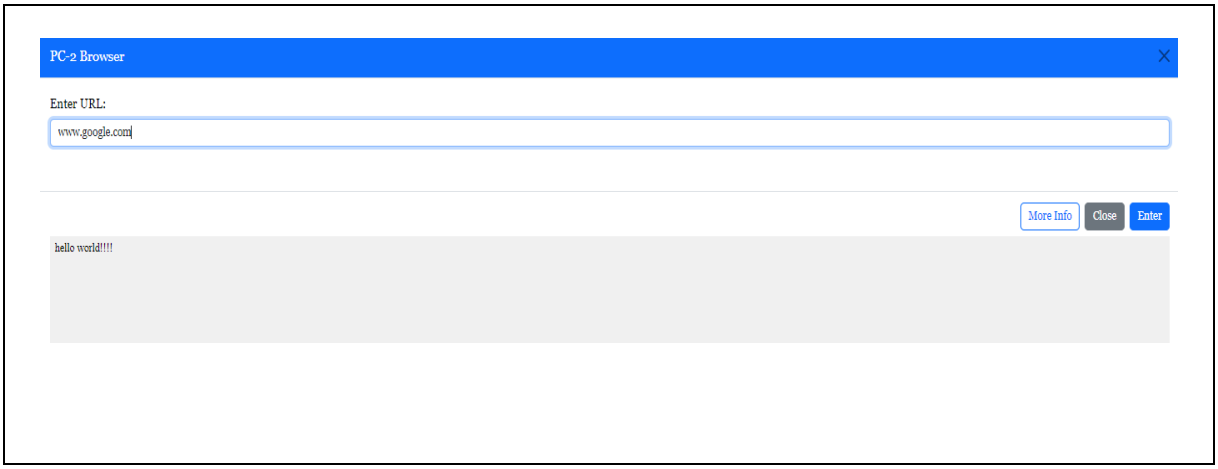
4. Go to the command prompt and set the URL to update on the server for example “www.google.com”



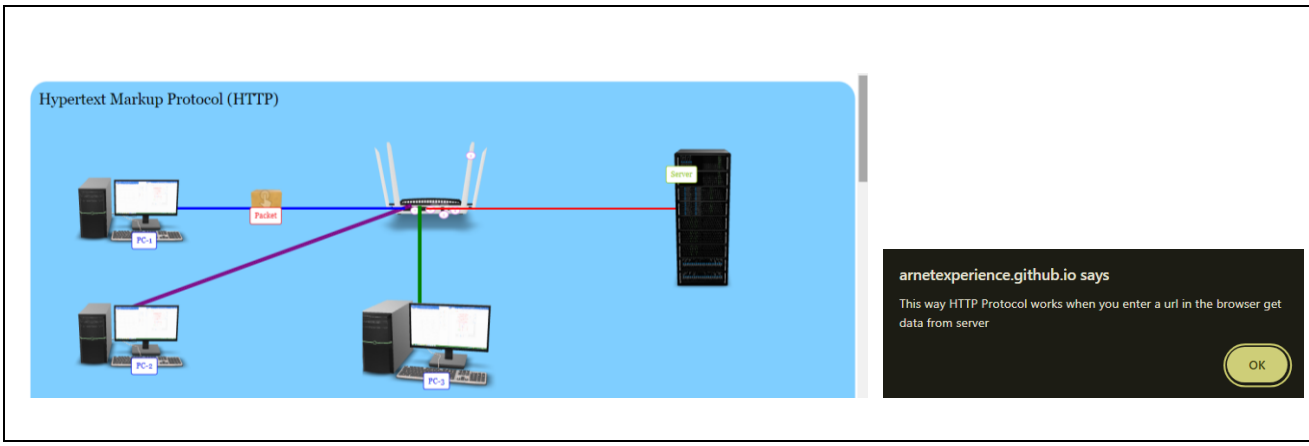
5. Write your HTML, CSS, JS code here in the given below and click on update



6. Click on the PC and enter the set URL to see the message



7. Now you will see that packet are moving



Bonus!!! You can also zoom in network devices with mouse to look around to take a look

Simple Mail Transfer Protocol

Introduction:

Simple Mail Transfer Protocol (SMTP) is a communication protocol used to transmit electronic mail (email) messages between servers and clients over a network. SMTP is a fundamental component of internet email transmission, enabling the exchange of emails reliably and efficiently.

Aim of SMTP:

The primary aim of SMTP is to provide a standardized method for the transmission of email messages across networks. It ensures that emails are delivered securely, reliably, and in a timely manner to their intended recipients.

Objectives of SMTP

- Reliability: SMTP aims to ensure that email messages are reliably delivered to their destinations without loss or corruption.
- Interoperability: SMTP facilitates interoperability among different email systems and platforms, enabling communication between users regardless of their email service providers.
- Security: SMTP includes mechanisms for authentication and encryption to enhance the security of email transmission, protecting sensitive information from unauthorized access.
- Efficiency: SMTP is designed to efficiently handle the transmission of email messages, optimizing network resources and minimizing latency.

Steps in SMTP Transmission

- Connection Establishment: The sending SMTP server establishes a connection with the recipient's SMTP server.
- Handshake: A handshake process occurs between the sending and receiving servers to negotiate parameters for the email transmission.
- Message Transfer: The sending server transmits the email message to the receiving server using a series of commands defined by the SMTP protocol.

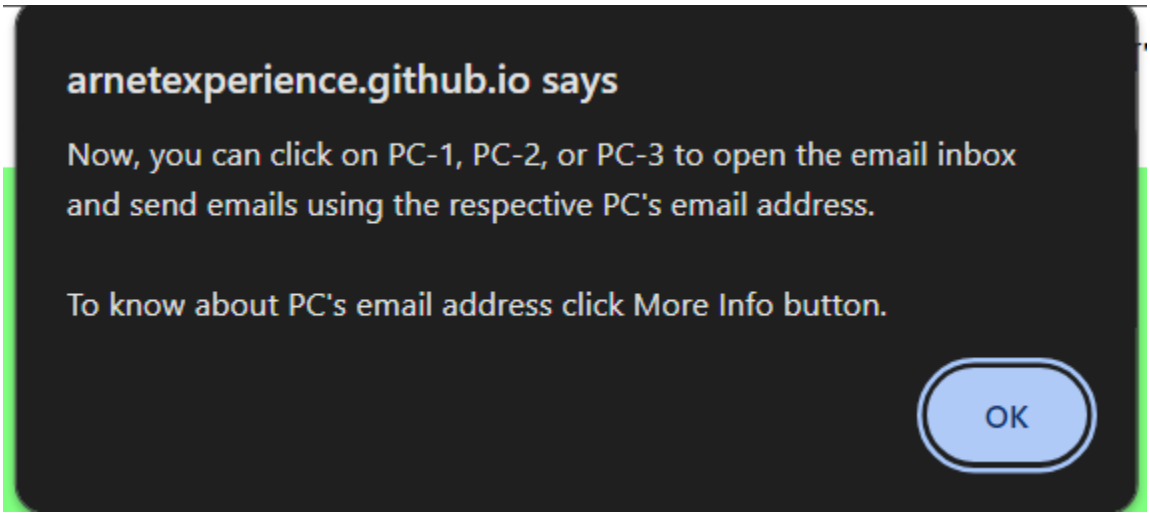
- Message Delivery: The receiving server processes the incoming email message and stores it in the recipient's mailbox for retrieval.

Conclusion:

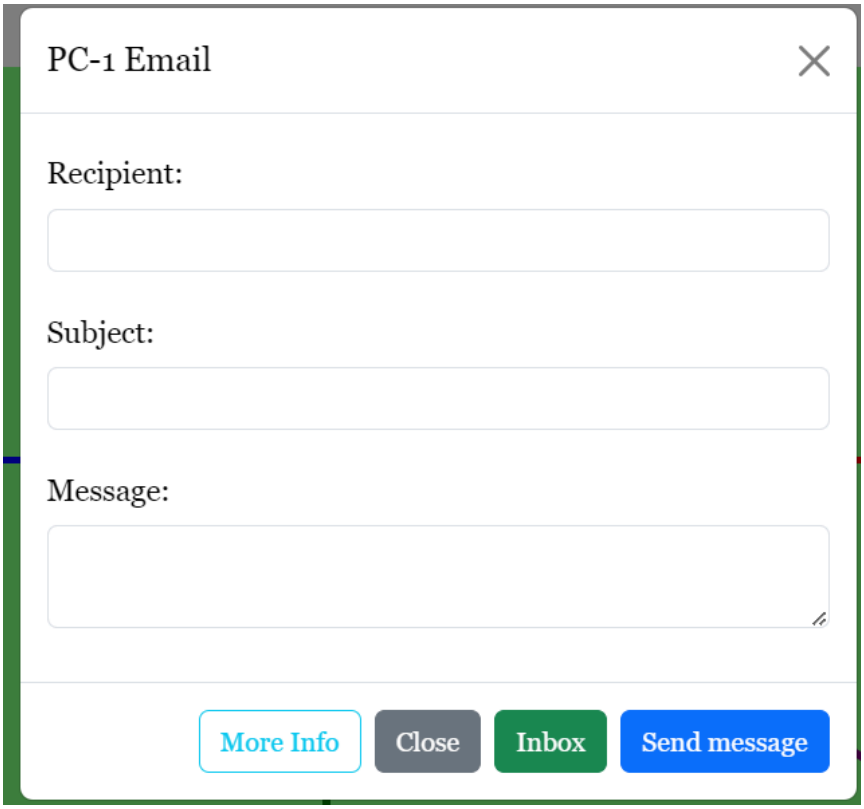
In conclusion, SMTP plays a crucial role in the transmission of email messages across the internet, providing a standardized and reliable method for exchanging electronic communications. By adhering to its principles of reliability, interoperability, security, and efficiency, SMTP enables seamless communication between users and ensures the integrity and confidentiality of email transmission.

How to Perform:

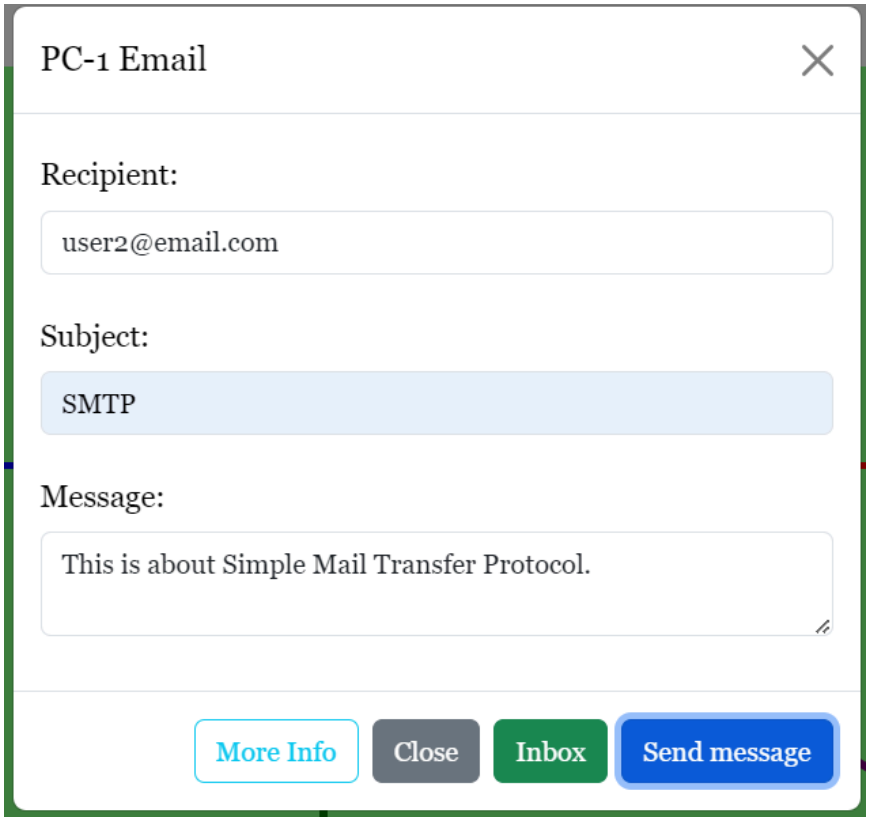
1) Click on any PC to open the email inbox and send emails using the respective PC's email address.



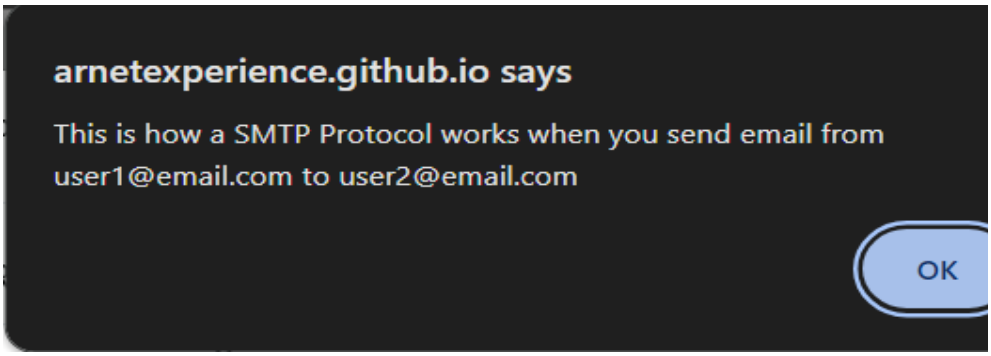
2) Say, clicked on PC-1, then
Enter Recipient email, subject, message as shown in figure,



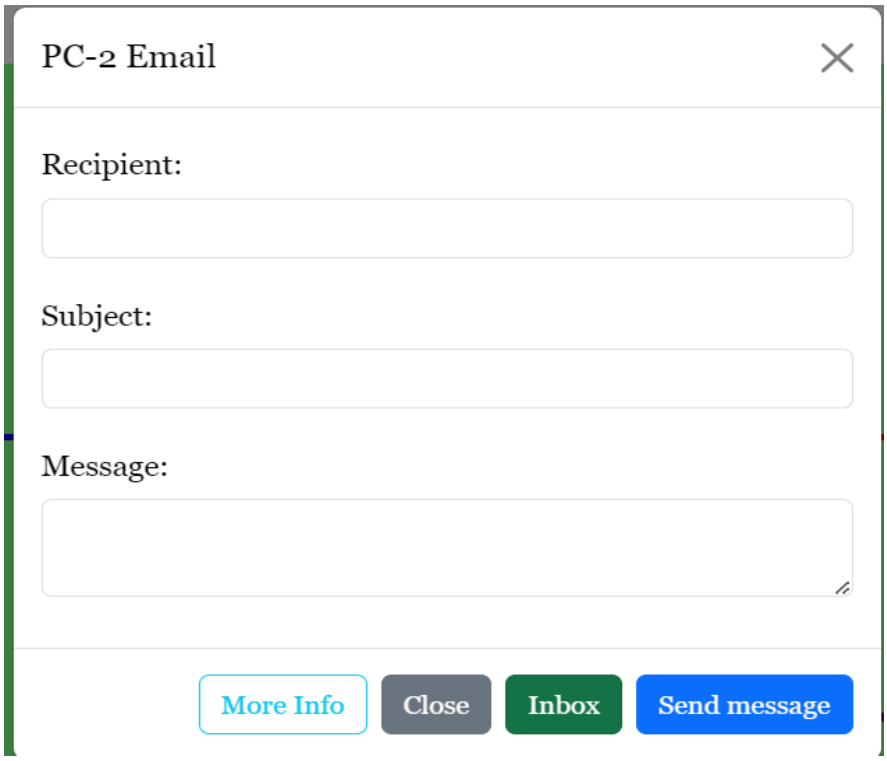
Click on Send Message Button, after packets will transfer



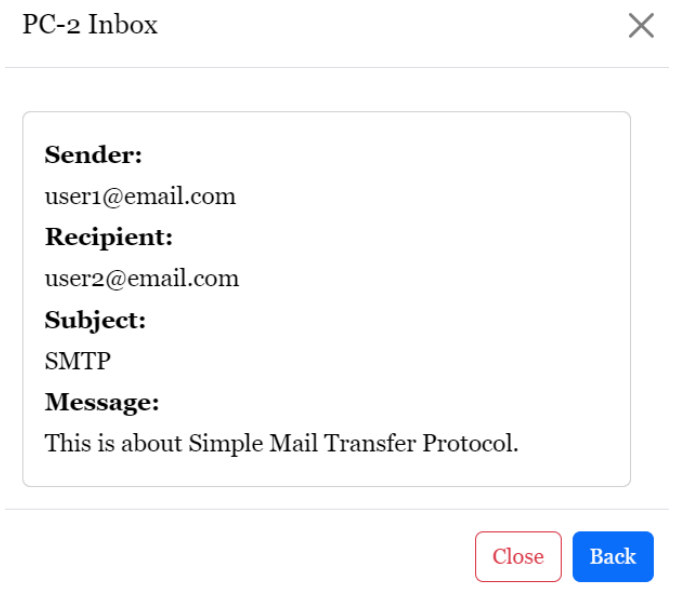
3) Pop-up message like this will be received.



4) Click on Inbox button



5) The Message sent by PC-1 will be display here



6) Click on Server to know it's IP Address and Domain Name

Secure Shell Protocol

Introduction

Secure Shell (SSH) protocol is a cryptographic network protocol for operating network services securely over an unsecured network. Its primary application is for remote login to computer systems by users. SSH provides a secure channel over an unsecured network by using a client-server architecture, connecting an SSH client application with an SSH server.

Aim

The aim of this document is to provide a comprehensive understanding of the SSH protocol, covering both practical usage and theoretical underpinnings. This includes the objectives, procedural steps, and concluding remarks on its importance and implementation.

Objectives

1. Understand the fundamental principles of SSH protocol.
2. Learn the theoretical concepts behind SSH security mechanisms.
3. Gain practical knowledge on how to use SSH for secure communication.
4. Understand the configuration and management of SSH servers and clients.
5. Appreciate the importance of SSH in network security and its application in various scenarios.

Theory

1. Principles of SSH Protocol

- Encryption: SSH uses strong encryption to protect the data being transmitted over the network. The most common algorithms include AES (Advanced Encryption Standard) and RSA (Rivest-Shamir-Adleman).
- Authentication: SSH provides robust authentication mechanisms to verify the identities of the client and server. Methods include password-based, key-based, and more advanced mechanisms like two-factor authentication.
- Integrity: To ensure data integrity, SSH employs hashing algorithms like SHA-2 to verify that data has not been altered during transmission.

- Forward Secrecy: Ensures that session keys are not compromised even if the private key of the server or client is compromised in the future.

2. Components of SSH

- SSH Client: The software that initiates the connection.
- SSH Server: The software that accepts and manages the connection.
- SSH Daemon: The background process running on the server that handles incoming SSH connections.
- SSH Keys: Pairs of cryptographic keys used for securing communications and authenticating the parties involved.

3. SSH Key Management

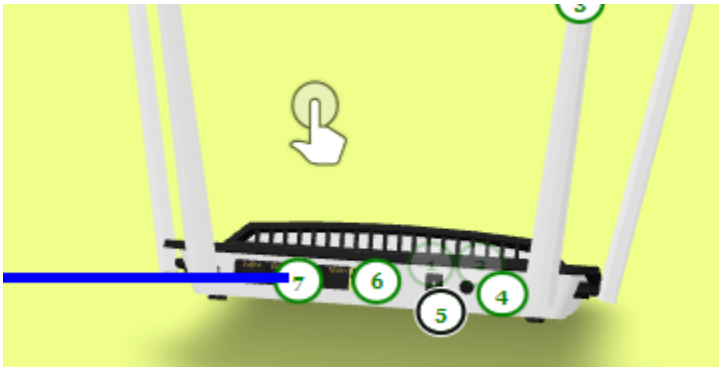
- Public/Private Key Pair: The public key is shared, while the private key is kept secret. They are used for establishing a secure connection.
- Key Generation: Tools like `ssh-keygen` are used to create key pairs.
- Key Storage: Keys are typically stored in `~/.ssh/` directory with permissions set to ensure security.

Conclusion

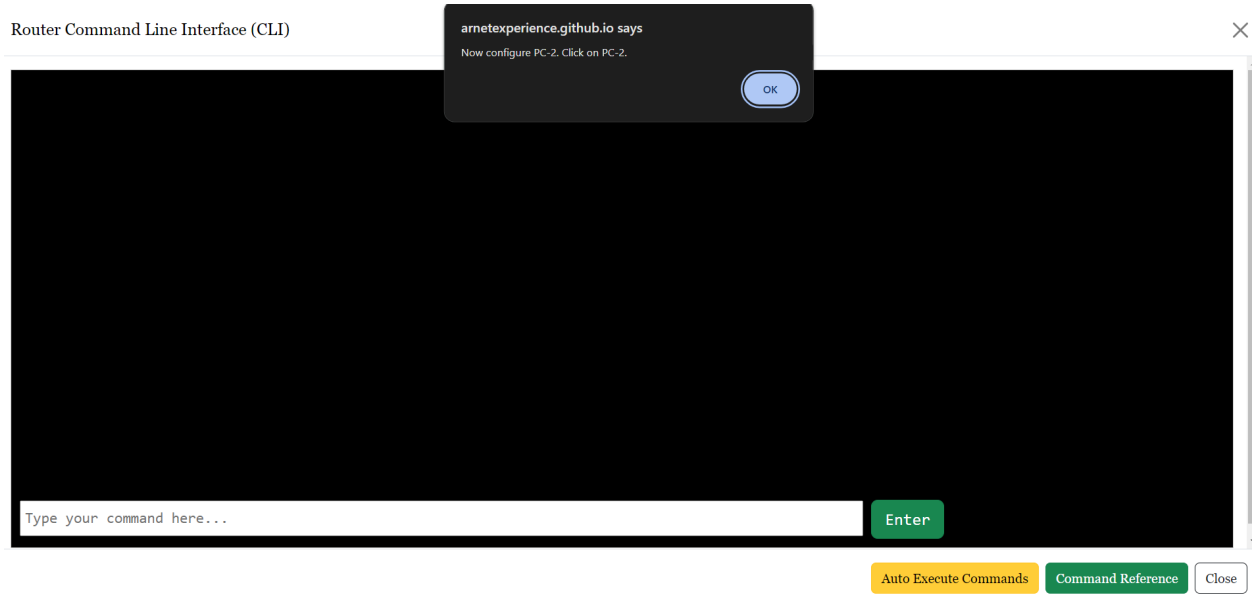
SSH is an essential protocol for secure communication over unsecured networks. Its robust encryption, authentication, and integrity mechanisms ensure the confidentiality and security of data. Practical knowledge of SSH, from key generation to configuring the SSH daemon, is crucial for network administrators and anyone involved in managing secure communications.

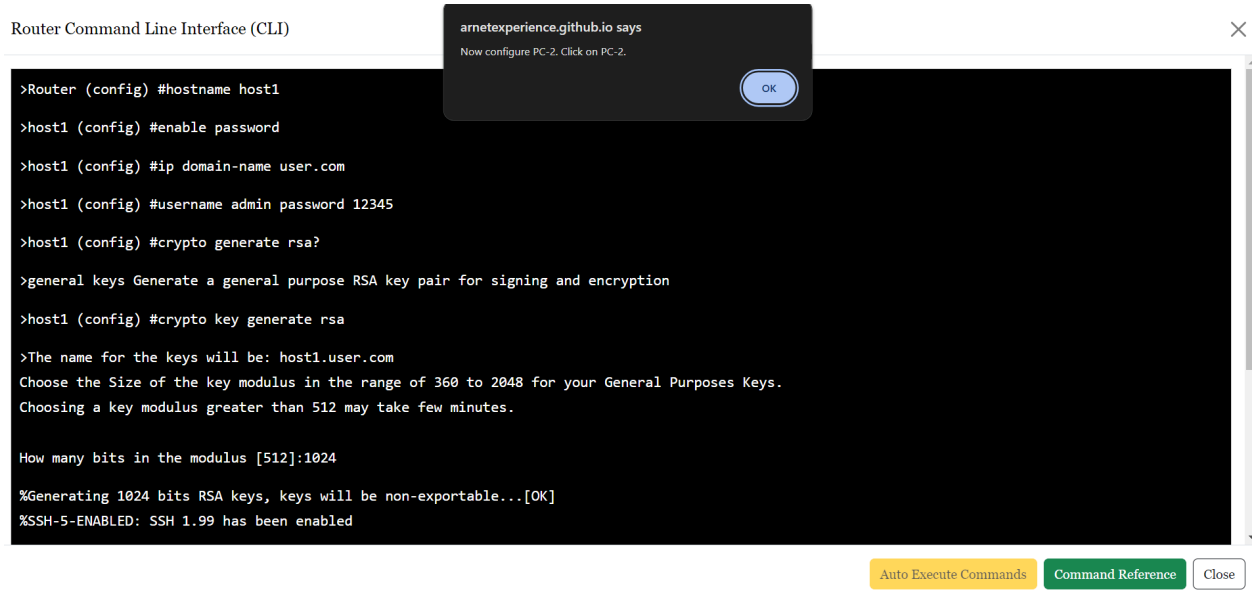
By understanding both the theoretical aspects and practical implementations of SSH, users can effectively secure remote connections and manage networked systems with confidence. The ongoing advancements and updates to SSH protocols and tools underscore the importance of staying informed and vigilant in maintaining network security.

1) Click on router's button number 6 and open CLI



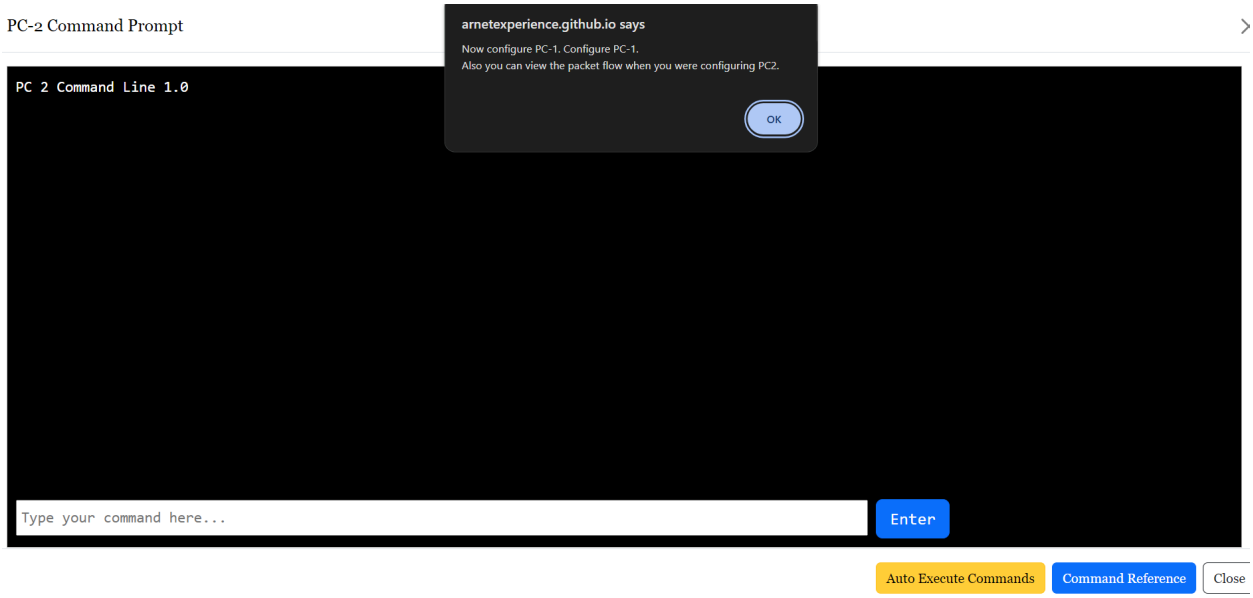
2) Click on auto execute command, you can also execute command one by one





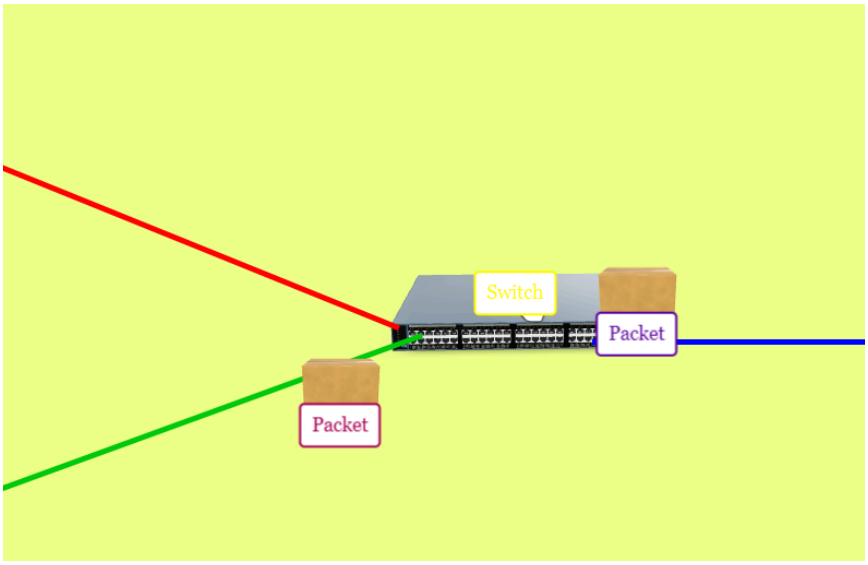
3) Now click on PC2, open command prompt

4) Auto execute command, you can also execute commands one by one

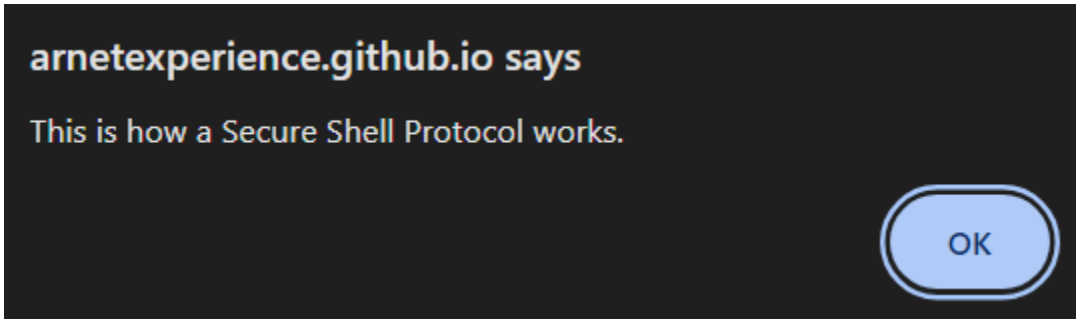



```
PC 2 Command Line 1.0
>ssh -l Admin 192.168.10.1

>Password:12345

host1>en

Password:12345

host1 #conf t

host1(config) #hostname PC2-SSH

PC2-SSH(config) #
```

5) Now packets will start flowing PC's to router and router to PC's



6) After the operation is successfully completed, you will get a pop-up message



Bonus!!! You can zoom in and zoom out the devices and also can read about each in detail.

Border Gateway Protocol

Introduction:

The Border Gateway Protocol (BGP) is an exterior gateway protocol used to facilitate inter-domain routing on the Internet. It is the protocol used between autonomous systems (ASes) to exchange routing information and make decisions about the best paths for routing traffic between networks.

Aim of BGP:

The primary aim of BGP is to enable the exchange of routing information between different autonomous systems while ensuring scalability, stability, and policy control in Internet routing. BGP allows networks to make informed decisions about the best routes for reaching destinations across the Internet.

Objectives of BGP:

- Inter-Domain Routing: BGP facilitates the exchange of routing information between different autonomous systems, allowing networks to learn about reachable destinations and their corresponding paths.

- Path Selection: BGP enables networks to select the best paths for routing traffic based on policies, preferences, and network characteristics such as path length, bandwidth, and reliability.

- Traffic Engineering: BGP supports traffic engineering by allowing networks to influence the flow of traffic through the network based on policies and preferences, optimizing resource utilization and network performance.

- Route Aggregation: BGP enables the aggregation of routing information to reduce the size of routing tables and improve scalability in the Internet routing infrastructure.

Steps in BGP Operation:

- Neighbor Establishment: BGP routers establish neighbor relationships with other BGP routers in neighboring autonomous systems to exchange routing information.

- Route Advertisement: BGP routers advertise routes to their neighbors by sending BGP update messages containing information about reachable destinations and their corresponding paths.

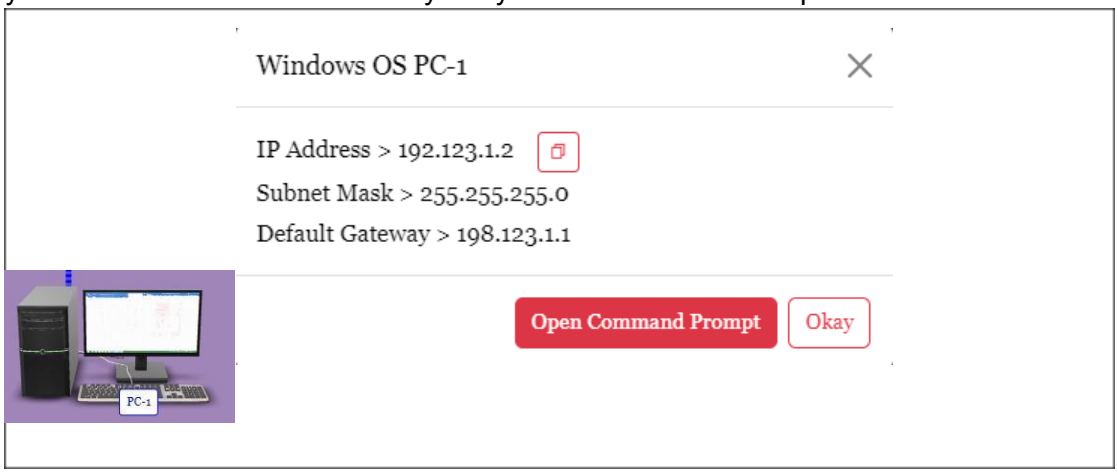
- Route Selection: BGP routers use a set of criteria, including policies, preferences, and attributes such as path length, to select the best routes for reaching each destination.

- Route Propagation: BGP routes are propagated throughout the Internet, with routers making forwarding decisions based on the best routes learned through BGP updates.

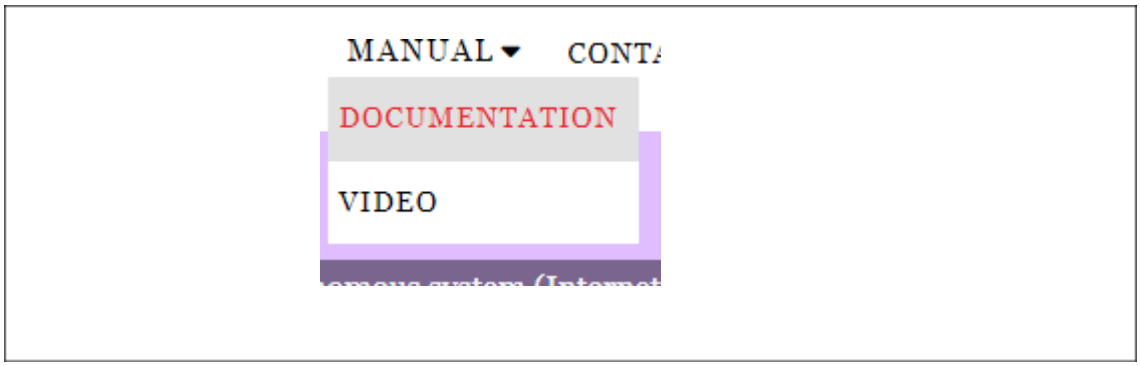
Conclusion:

In conclusion, BGP is a critical protocol for inter-domain routing on the Internet, enabling the exchange of routing information between autonomous systems and the selection of optimal paths for routing traffic. By providing scalability, stability, and policy control in Internet routing, BGP plays a crucial role in ensuring the efficient and reliable operation of the global Internet infrastructure.

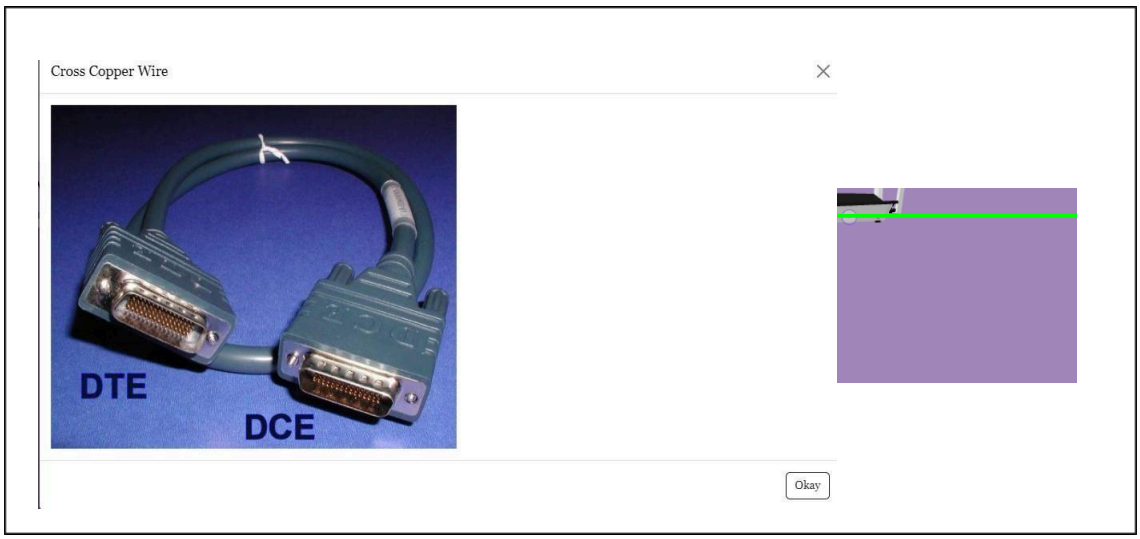
1. If you want know IP Address of any PC you can click on blue square as shown below:



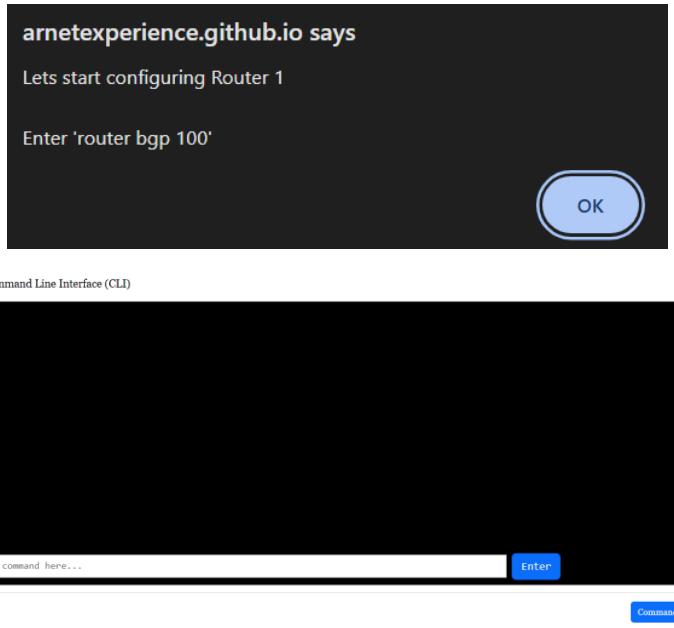
2. Click on “Manual” to view Presentation on BGP topic:



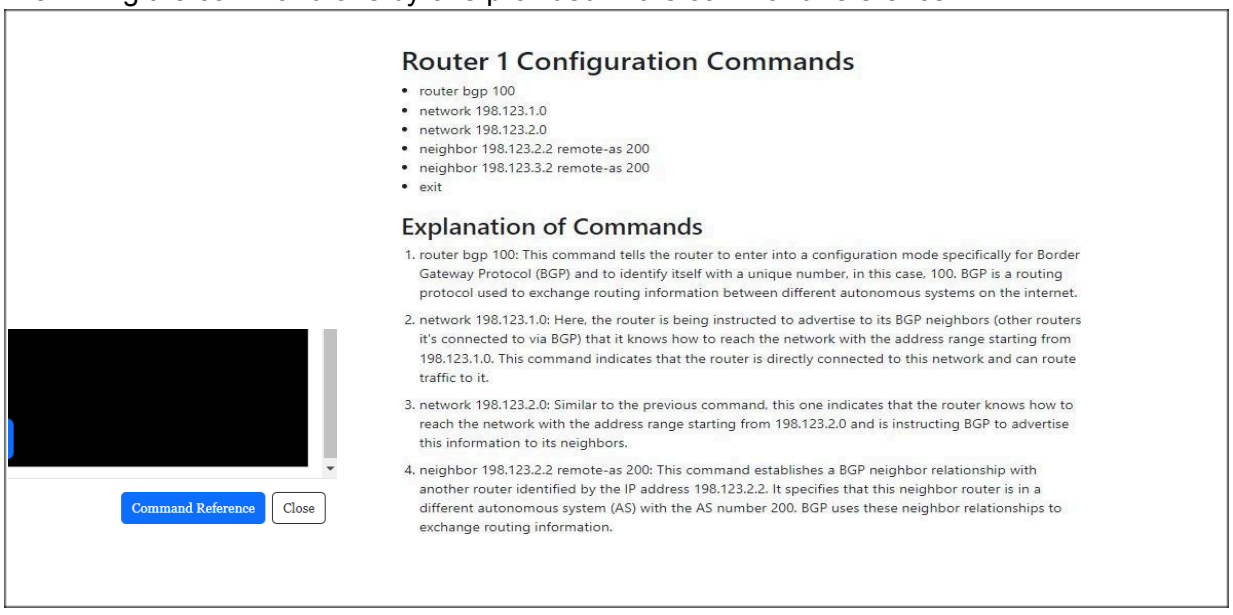
3. Click on wire colors “Red”/” Blue”/” Green” to view wire details:



4. Let’s start performing BGP in AR World!!! To configure Router 1 and Router 2 Click on “BUTTON-2 of router” :

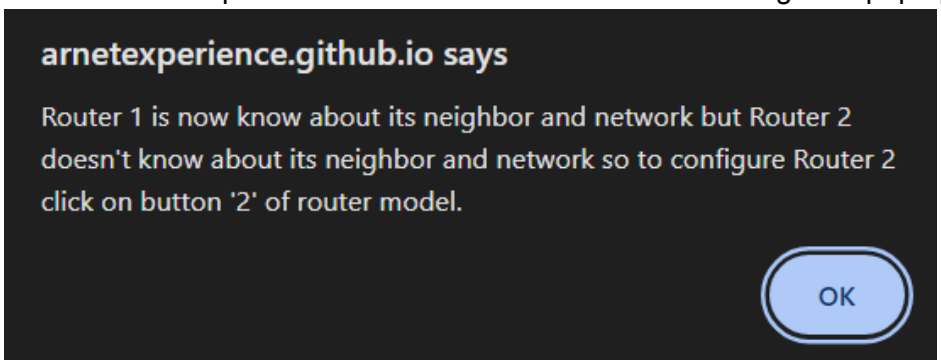


5. Ping the command one by one provided in the command reference



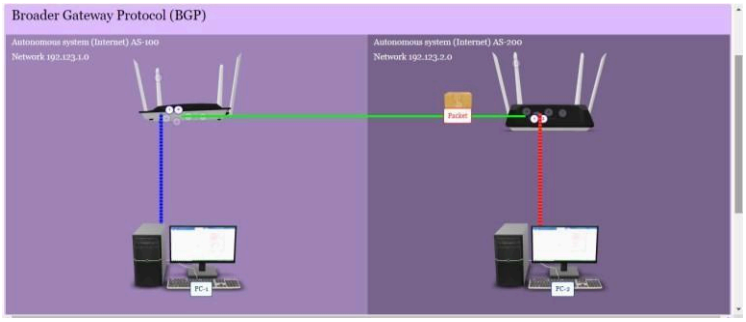
6. After performing all the command you will get message that all the network are connected to router

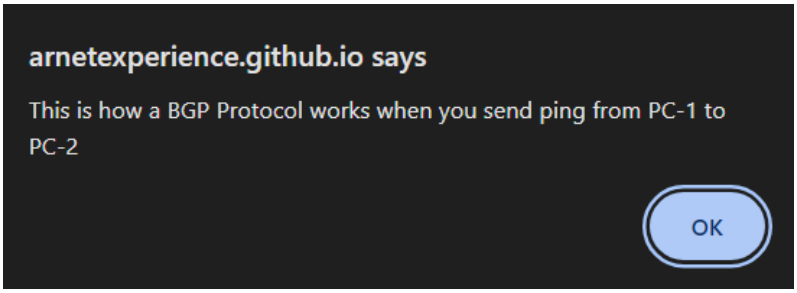
7. Follow the same process for Router 2 . after that this message will pop up



8. Open the command prompt of any pc and paste the ip address of that pc and close the window to see packet transfer

9. These how packet are transferred once the packet transformation is completed you will get a pop up message of “this is how BGP protocol work.





Bonus!!! You can also Zoom in network devices with a mouse to look around to take a look.

Dynamic Host Configuration Protocol

Introduction:

The Dynamic Host Configuration Protocol (DHCP) is a network management protocol used to dynamically assign IP addresses and other network configuration parameters to devices on a network. DHCP simplifies the administration of IP addressing by automating the process of IP allocation, thus reducing configuration errors and minimizing network downtime.

Aim of DHCP:

The primary aim of DHCP is to automate and streamline the assignment of IP addresses and network configuration parameters within a network infrastructure. By dynamically allocating IP addresses and other settings to devices as they connect to the network, DHCP ensures efficient utilization of IP address space and simplifies network administration.

Objectives of DHCP:

- Efficient IP Address Management: DHCP aims to efficiently manage IP address allocation within a network, ensuring that IP addresses are assigned dynamically and reused when devices are no longer connected.

- Centralized Network Configuration: DHCP centralizes the management of network configuration parameters such as IP addresses, subnet masks, default gateways, and DNS servers, reducing the need for manual configuration on individual devices.

- Reduced Configuration Errors: By automating the assignment of network configuration parameters, DHCP helps to minimize configuration errors and inconsistencies, improving network reliability and stability.

- Scalability: DHCP supports the dynamic allocation of IP addresses across large-scale networks, enabling efficient scaling to accommodate varying numbers of devices and network growth.

Steps in DHCP Operation:

- DHCP Discovery: When a device (client) connects to the network, it sends out a DHCP discovery broadcast message to locate a DHCP server.

- DHCP Offer: DHCP servers on the network receive the discovery message and respond with a DHCP offer message, which includes an available IP address and other configuration parameters.

- DHCP Request: The client selects one of the offered IP addresses and sends a DHCP request message to the chosen DHCP server, confirming its intention to use the offered configuration.

- DHCP Acknowledgment: The DHCP server that receives the request message sends a DHCP acknowledgment (ACK) message back to the client, confirming the lease of the IP address and providing the client with the assigned configuration parameters.

- Configuration Renewal: Periodically, the client initiates a DHCP lease renewal process to extend the lease duration or request a new IP address if necessary.

Conclusion:

In conclusion, DHCP plays a crucial role in simplifying and automating IP address management within network infrastructures.
By dynamically allocating IP addresses and network configuration parameters to devices, DHCP improves efficiency, reduces configuration errors, and enhances scalability in network environments.

Click on Documentation to read about DHCP, to know your knowledge about the topic click on Quiz and click on video to check how it works.

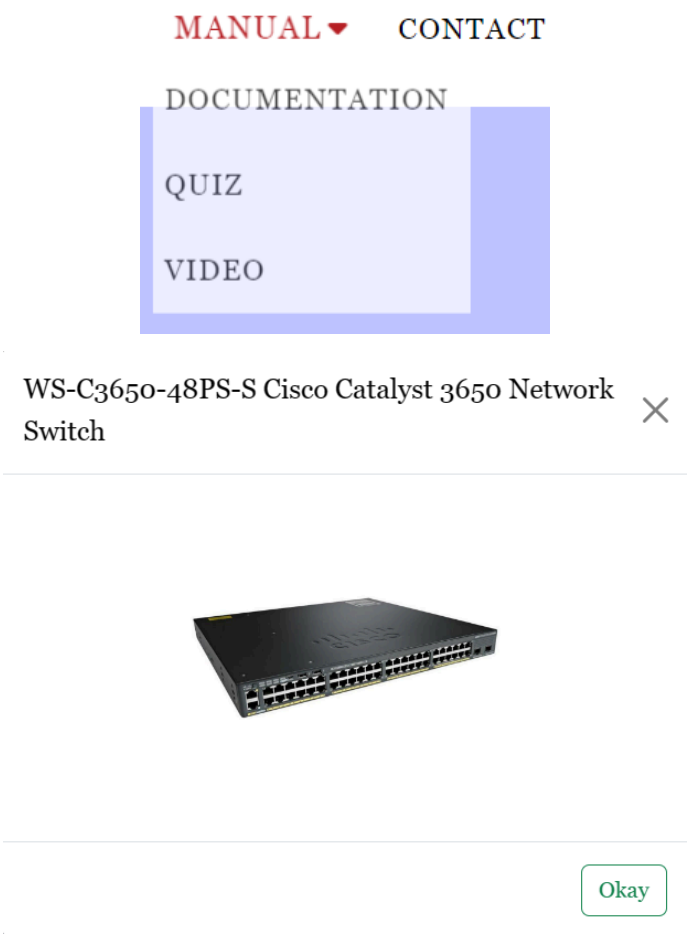


Fig. Rotable Network switch

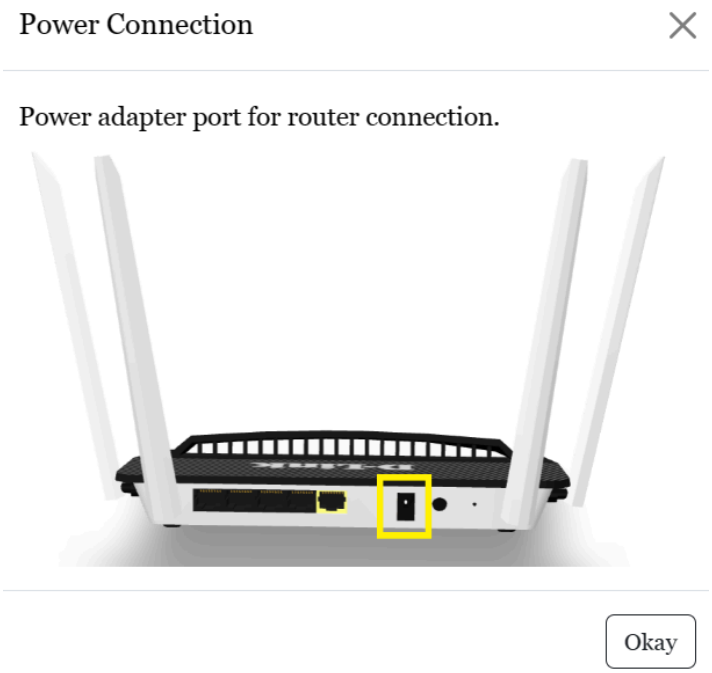


Fig. Power Connection

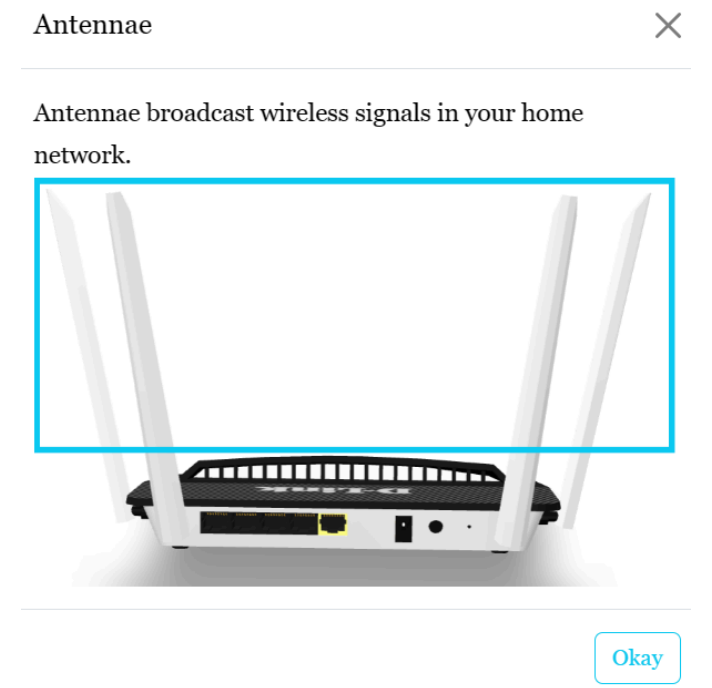


Fig. Antennae

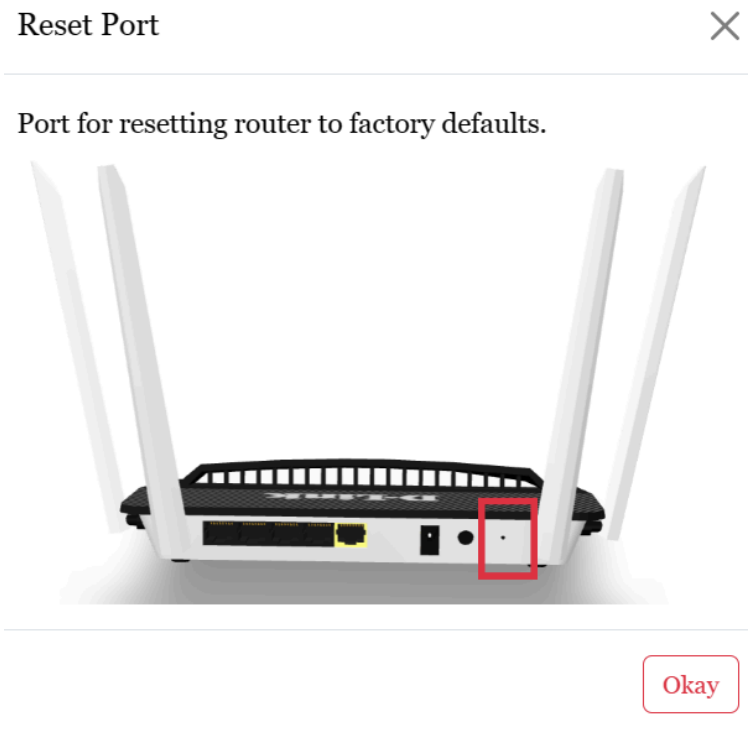


Fig. Reset Port

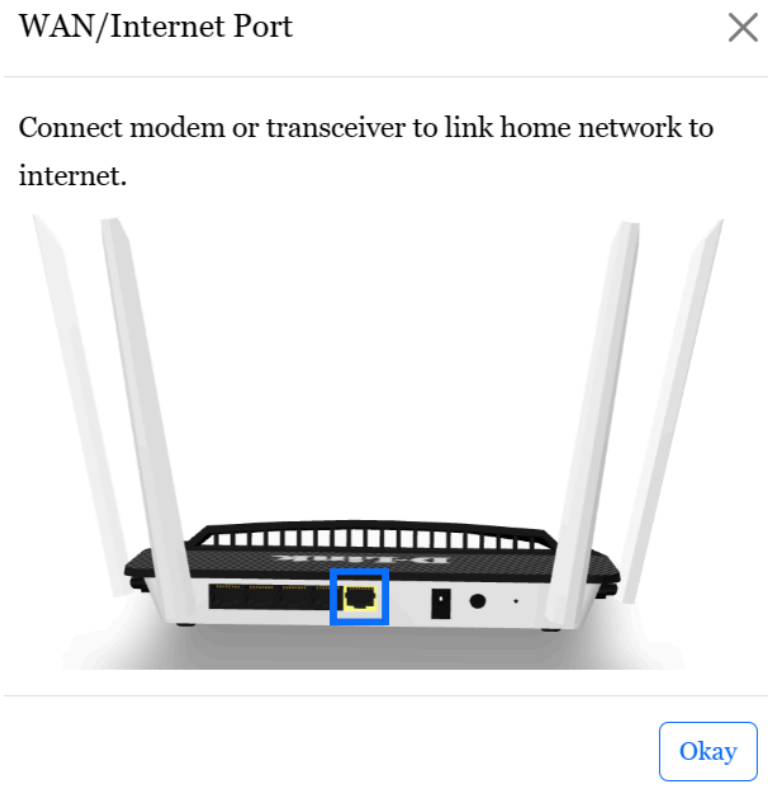


Fig. WAN/Internet Port

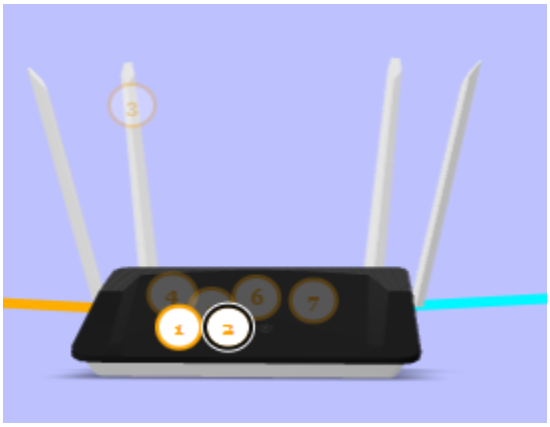
LAN Ports

Ports for wired devices on home network without wireless capability.

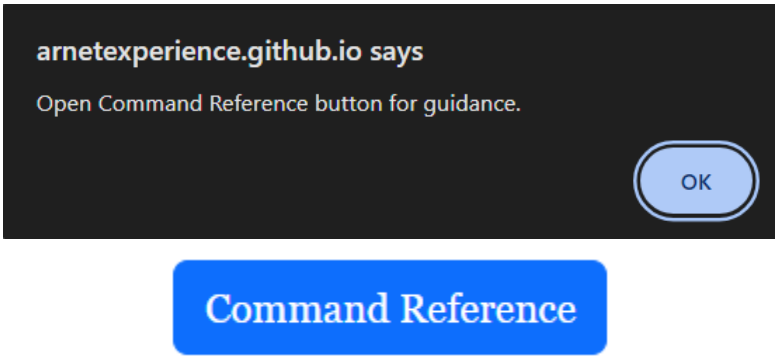
Okay

Fig. LAN Port

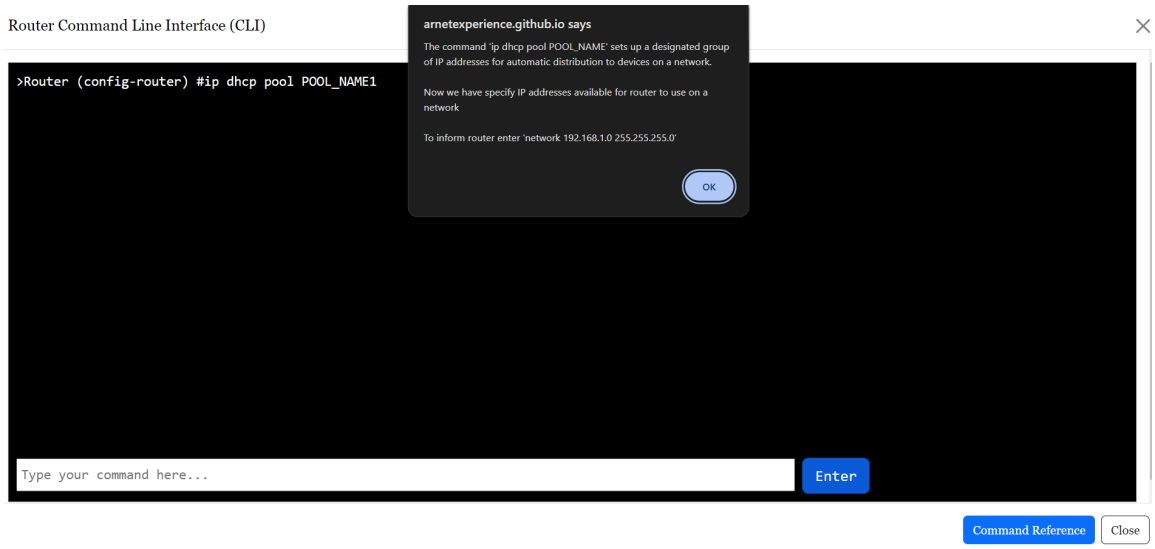
Click on Button number 2 of Router and Open CLI (Command Line Interface)

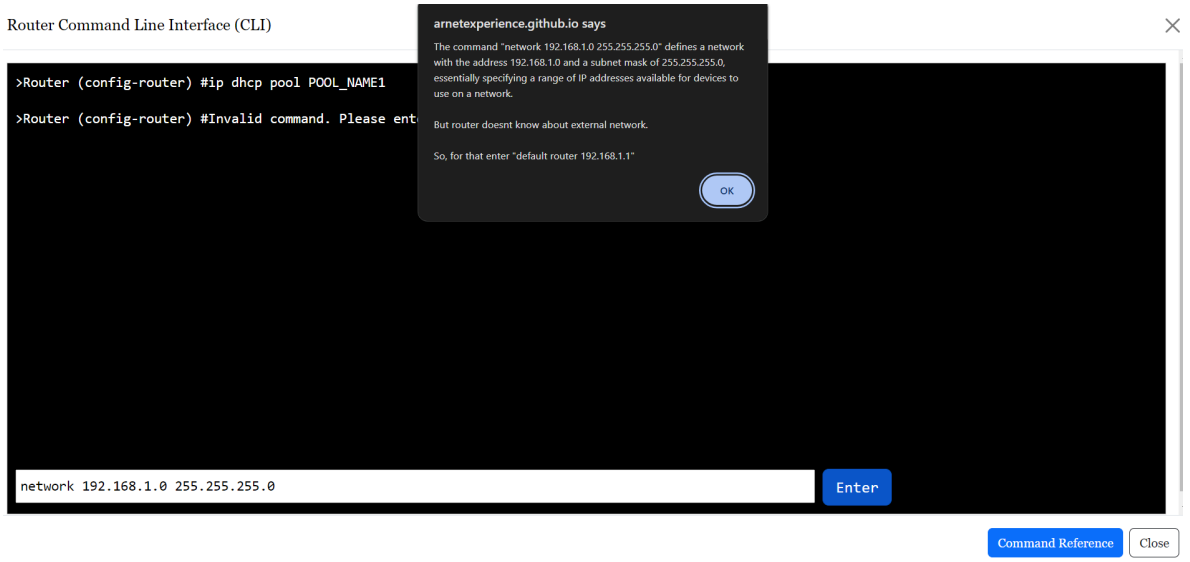


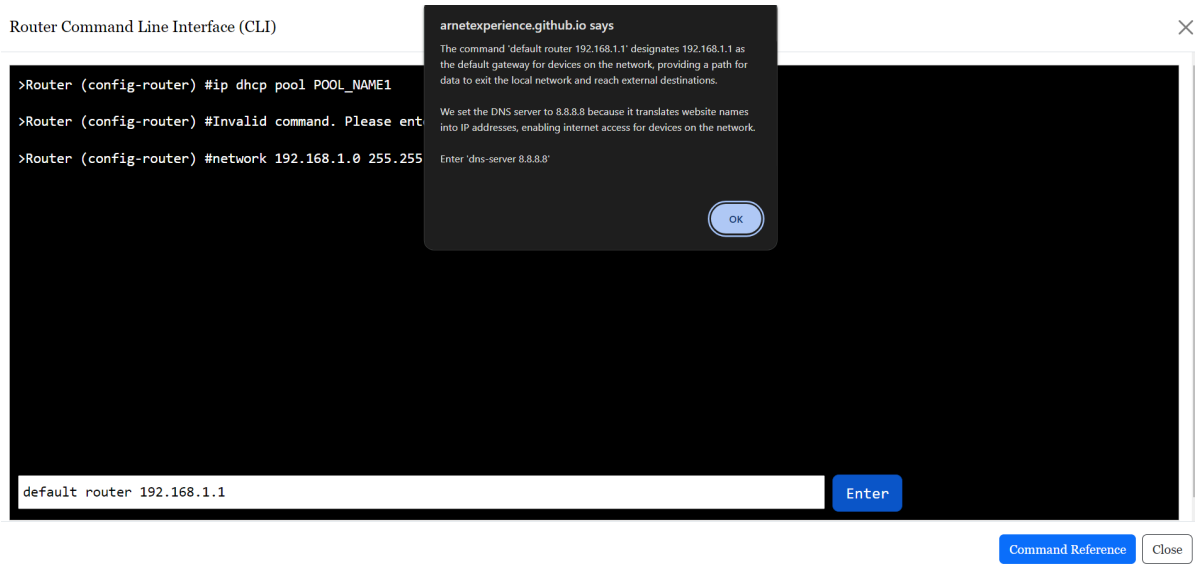
Click Ok

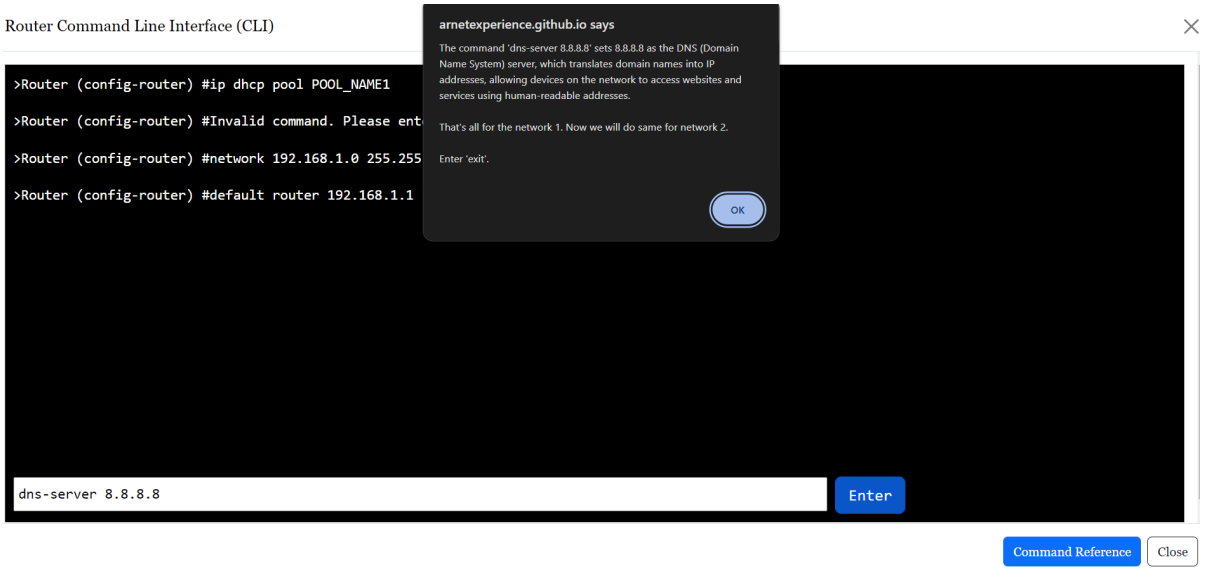


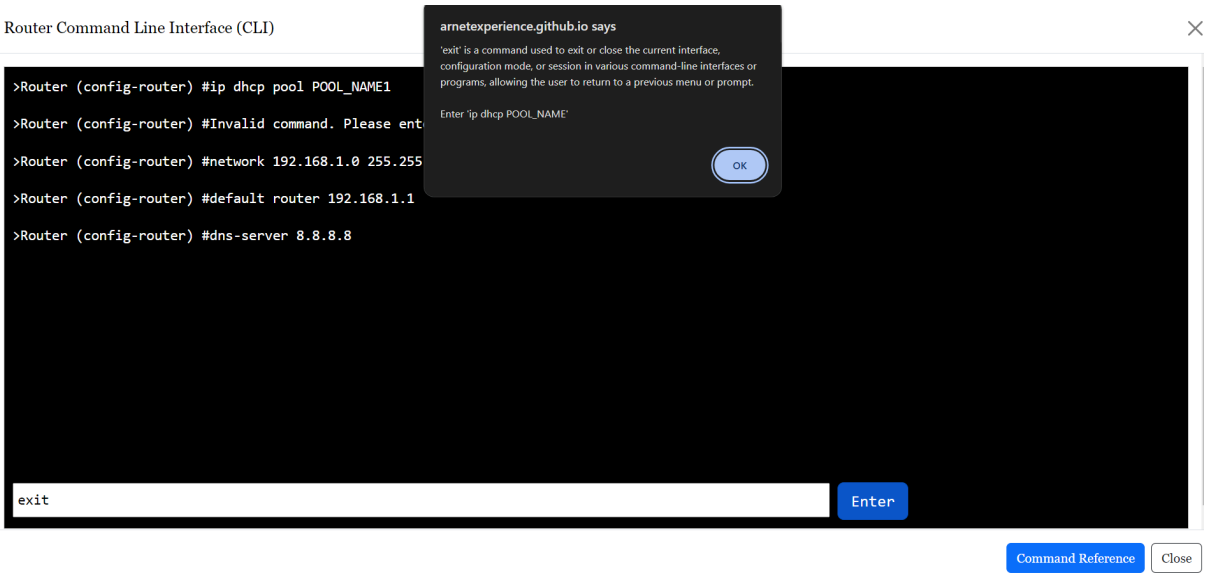
Enter one by one Configuring Pool for network 1




Router Command Line Interface (CLI)
arnetexperience.github.io says
The command "network 192.168.1.0 255.255.255.0" defines a network with the address 192.168.1.0 and a subnet mask of 255.255.255.0, essentially specifying a range of IP addresses available for devices to use on a network.
But router doesnt know about external network.
So, for that enter "default router 192.168.1.1"
OK
>Router (config-router) #ip dhcp pool POOL_NAME1
>Router (config-router) #Invalid command. Please ent
network 192.168.1.0 255.255.255.0
Enter
Command Reference
Close


Router Command Line Interface (CLI)
arnetexperience.github.io says
The command 'default router 192.168.1.1' designates 192.168.1.1 as the default gateway for devices on the network, providing a path for data to exit the local network and reach external destinations.
We set the DNS server to 8.8.8.8 because it translates website names into IP addresses, enabling internet access for devices on the network.
Enter 'dns-server 8.8.8.8'
OK
>Router (config-router) #ip dhcp pool POOL_NAME1
>Router (config-router) #Invalid command. Please ent
>Router (config-router) #network 192.168.1.0 255.255
default router 192.168.1.1
Enter
Command Reference
Close

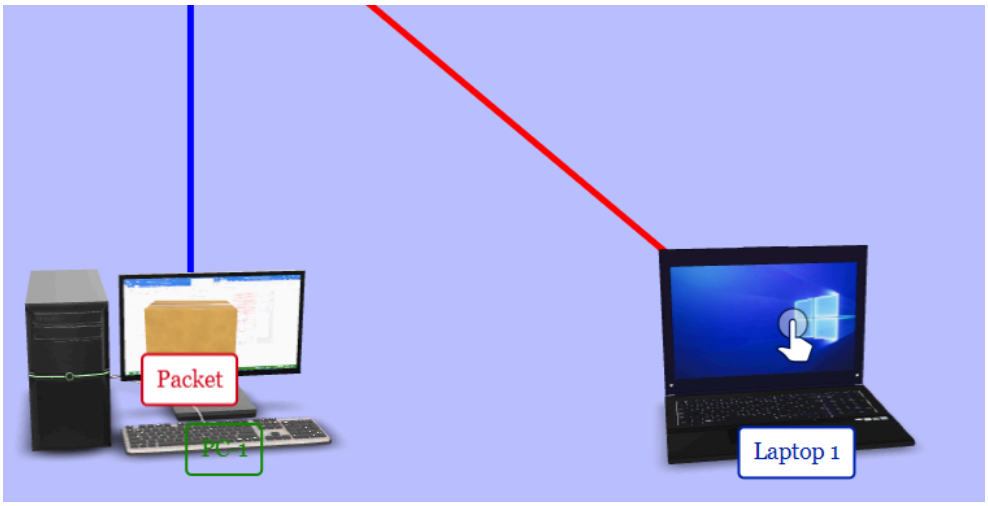




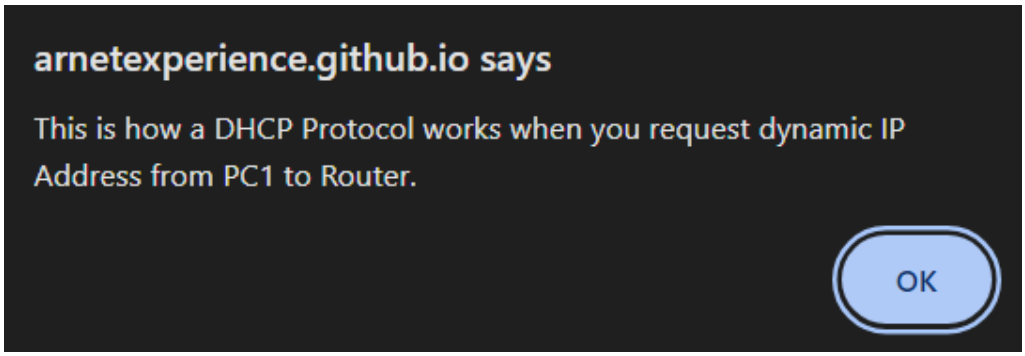
Similarly, enter the Configuring Pool for network 2 then close.

Click on PC1 then DHCP to know the IP Address,

Packets will start moving from PC1 to router.



You will get a pop-up message after the operation is successful.



Similarly, We can perform for PC2 or Laptop1 to Router or Laptop2 to Router.

Local Area Network (LAN)

Aim:

To design, implement, and manage a Local Area Network (LAN) that efficiently supports the communication needs of an organization within a limited geographical area such as a building or campus.

Objectives:

1. Facilitate Resource Sharing: Allow users to share resources such as files, printers, and applications.
2. Enhance Communication: Enable effective communication through emails, instant messaging, and video conferencing.
3. Improve Data Management: Centralize data storage and backup to enhance data security and management.
4. Increase Efficiency: Optimize network performance and ensure quick data access and transfer within the organization.
5. Scalability: Ensure the network can be expanded easily to accommodate future growth.

Theory:

A Local Area Network (LAN) is a network that connects computers and other devices within a limited area such as a residence, school, laboratory, or office building. A LAN is typically characterized by high data transfer rates, small geographic range, and lack of need for leased telecommunication lines.

Key Components of LAN:

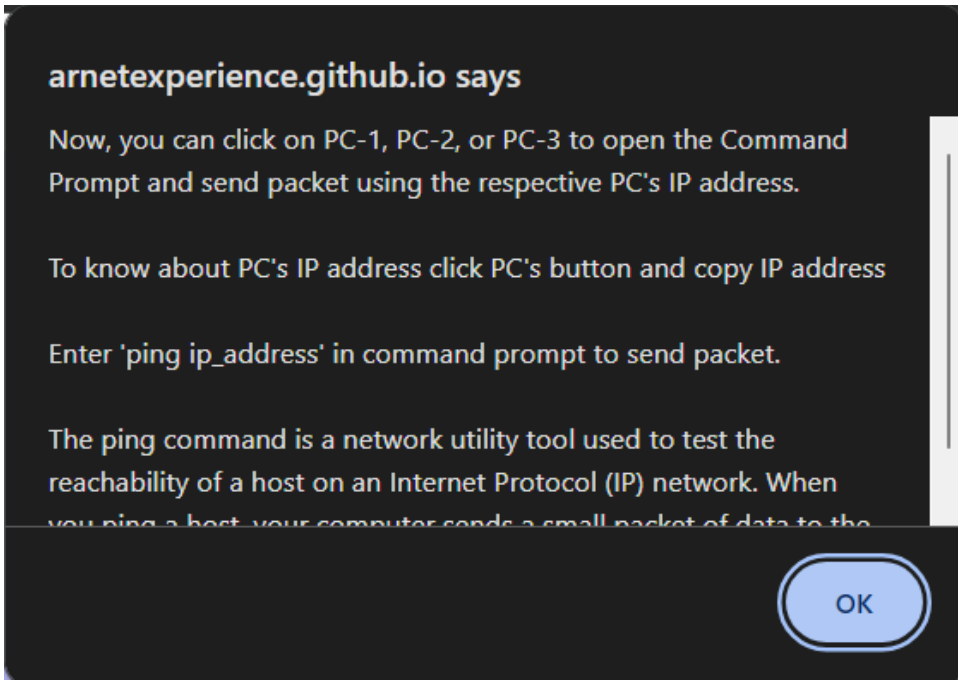
1. Network Interface Cards (NICs): Hardware that allows computers to connect to the network.
2. Switches: Devices that filter and forward network packets.
3. Routers: Devices that route data between different networks.
4. Cabling and Connectors: Physical media like Ethernet cables (Cat5, Cat6) that connect devices.

5. Wireless Access Points (WAPs): Devices that allow wireless devices to connect to the network.
6. Servers: Centralized computers that provide resources and services to networked devices.

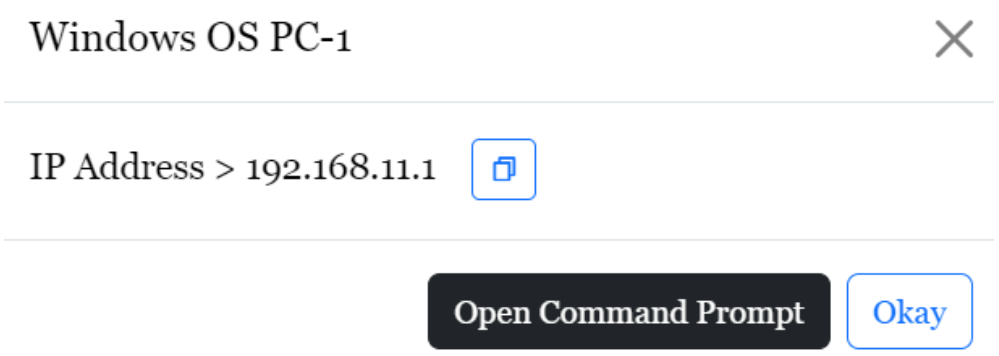
Conclusion:

A well-designed and implemented Local Area Network (LAN) significantly enhances the operational efficiency of an organization by facilitating seamless communication, resource sharing, and data management.

1) To know how to start implementation read the message carefully.



2) Now click on any of given PC and copy IP address



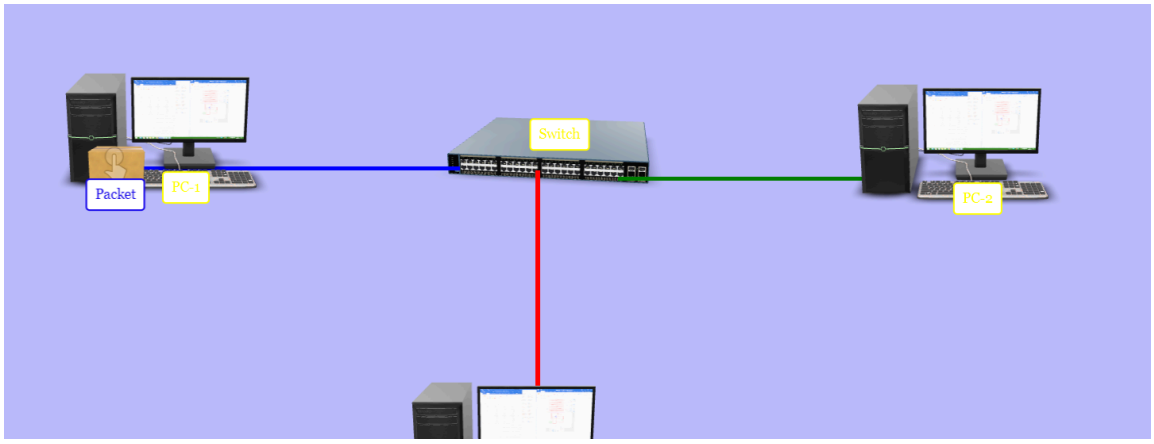
3) Click on another PC open command prompt and enter ping ip_address

PC-2 Command Prompt

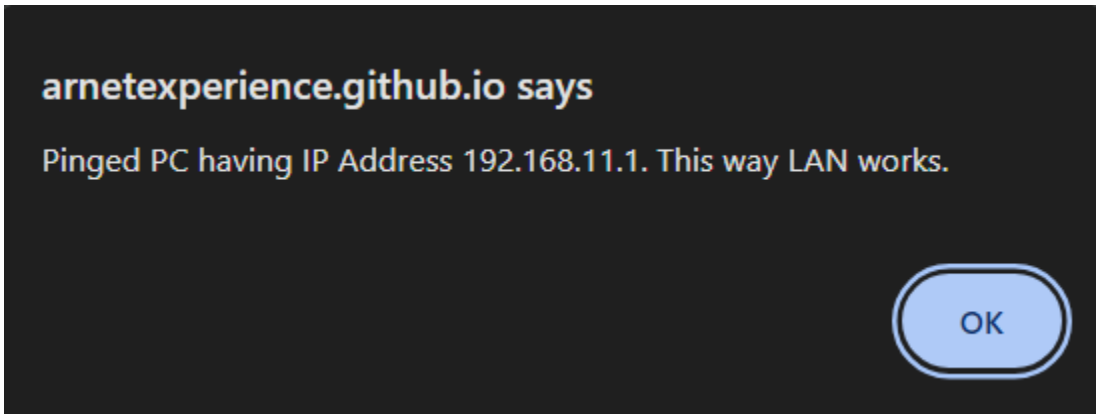
```
PC 2 Command Line 1.0
>ping 192.168.11.1

Pinging 192.168.11.1 with 32 bytes of data:

Reply from 192.168.11.1: bytes=32 time=1ms TTL=127
Reply from 192.168.11.1: bytes=32 time<1ms TTL=127
Reply from 192.168.11.1: bytes=32 time=1ms TTL=127
Reply from 192.168.11.1: bytes=32 time<1ms TTL=127

Ping statistics for 192.168.11.1:
 Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
Minimum = 0ms, Maximum = 1ms, Average = 0ms
```

Type your command here... Enter

4) Close command prompt and observe packets transferring from Pc 2 to PC 1



5) Now you will see a pop-up message.



Virtual Local Area Network (VLAN)

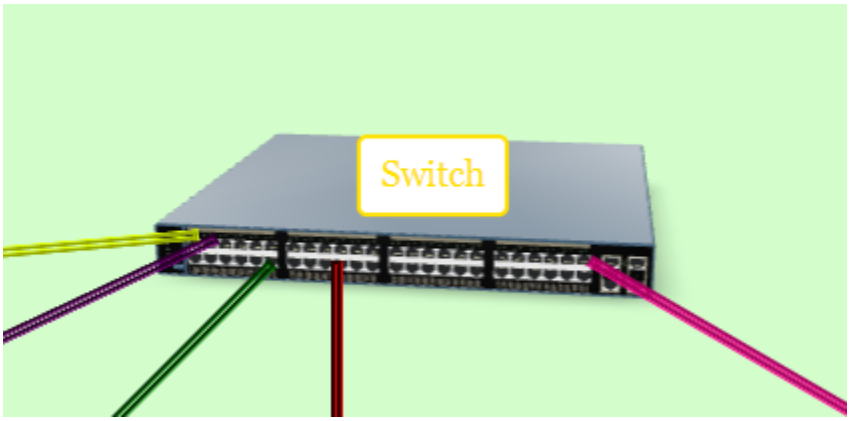
Aim:
The aim of this document is to provide a comprehensive understanding of File Virtual Local Area Network (VLAN), focusing on its theoretical foundations and practical implementations. This includes defining VLAN, explaining its objectives, detailing the steps for its configuration, and concluding with its benefits and considerations.

Objectives
To understand the concept and significance of VLANs in network management.

Definition
A Virtual Local Area Network (VLAN) is a subnetwork that can group together collections of devices from different physical LANs. VLANs improve network efficiency and security by segmenting a larger network into smaller, isolated segments. This allows for better management and utilization of bandwidth and provides additional security by isolating sensitive data.

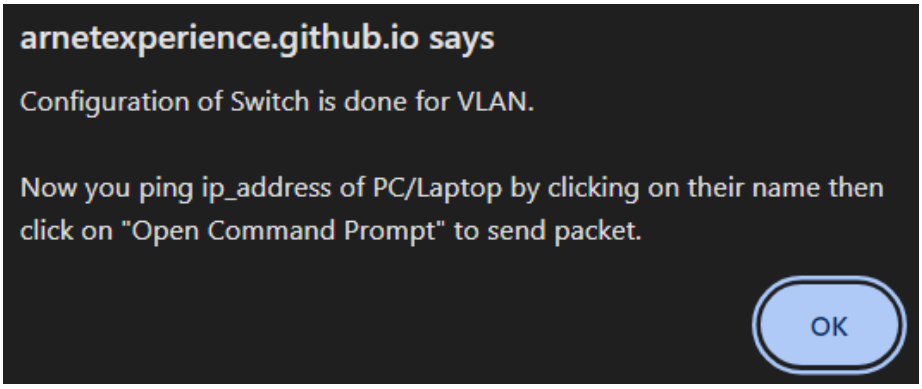
Conclusion
The implementation of VLANs in a network offers significant benefits in terms of efficiency, security, and manageability. By logically segmenting a physical network into smaller, isolated segments, VLANs help in reducing broadcast traffic, enhancing security, and providing flexibility in network design.

1) Click on switch button and open command line interface,

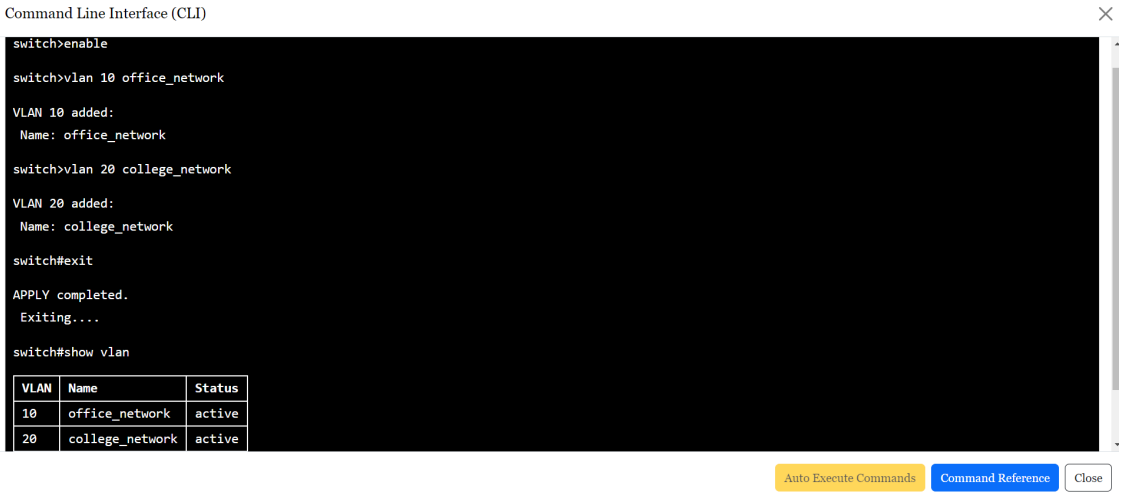


WS-C3650-48PS-S Cisco Catalyst 3650 Network Switch

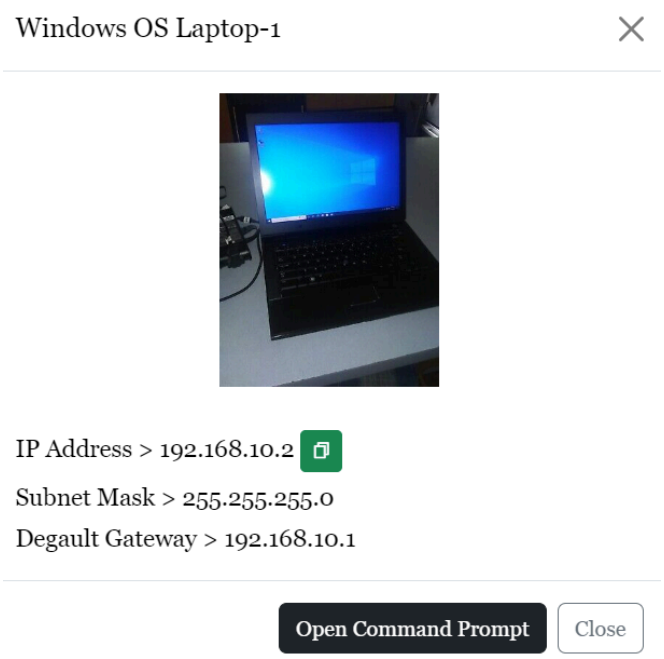
Open CLI Okay



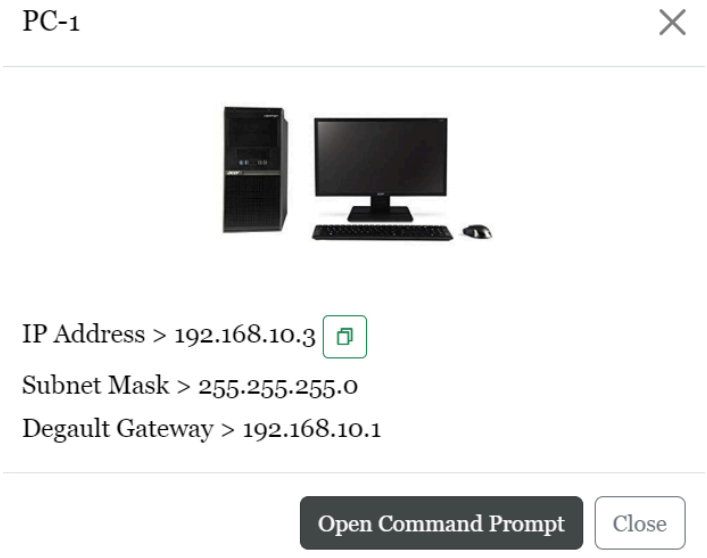
2) Auto execute commands or you can also execute commands one by one.



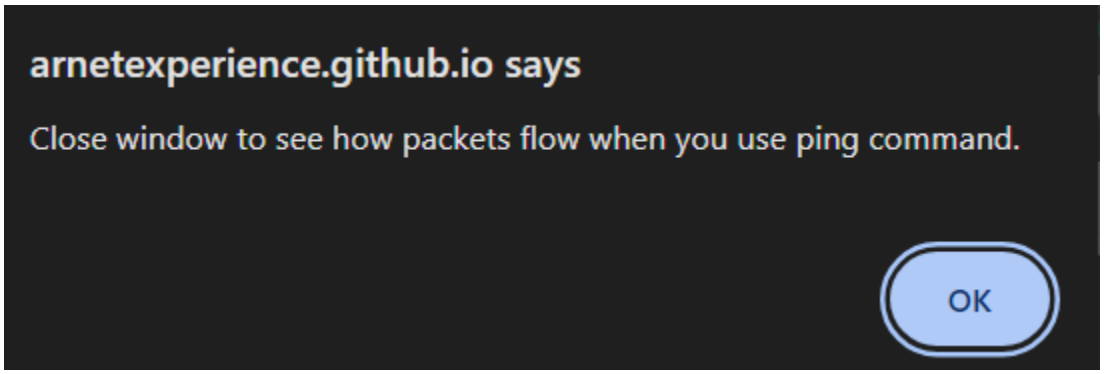
3) Click on any laptop or PC and copy IP address



4) Click on another PC or laptop and open CLI and paste the IP address of previous laptop/PC



5)



6) Packets will move from switch to laptop and PC to router, after successful completion of simulation you will get a pop-up message.