I'm not a bot

Web server is a combination of two words; web and server. The web is an information system known through its URL. While a server means to serve. So it is a place on the internet where information is stored and served by the clients. A web server is also called an HTTP server. The HTTP server is software that understands the URL and delivers the contents requested by the clients. Moreover, the popular protocol HTTP or HTTPS is used to transfer webpages from a web server or HTTP server to the client's browser. There are two versions of the hypertext transfer protocol. HTTP transfers webpages without encryption, while HTTPS uses encryption. HTTP server is a combination of hardware and software. Through this software and hardware, we translate and browse all the data and information. The webpages or websites that we visit while browsing, is stored within this server. There are four important types: It is the most popular web server on the internet. Apache Foundation developed it in 1995. It works on all OS platforms such as Windows, Linux, Mac OS, etc. Moreover, It is an open source and Nearly 60% of websites are hosted on it. You can change it according to your needs by adding the module. It has greater flexibility than the other web servers, due to which it has a greater number of users. Microsoft developed an Internet Information Service or IIS in 1995. It has the same features as Apache, but it is not open source as Apache. We can't add a new module in IIS, so we can't change it according to our needs. NGINX is a popular web server and was developed in 2004. It's the same as Apache. Moreover, It handles 7.5% of the domain hosting. Additionally, Hosting companies prefer it. Developers created light-speed in 2003. It is the fourth most popular web server in the world. With a high-performance ratio, Normally it is used in commercial usage. We will use the following lab topology for the web or HTTP server. First, assign the IP address to the Router interface and PCs. Subsequently, assign 192.168.1.10/24 to the server. Open the server. Follow the numbers 1,2 and 3. Click on edit at the 3rd number. Make some changes in the "index.html" file. Additionally, the yellow highlighted color are changes we have made to it. Open PC1 and click on the Desktop tab. Next, click on the web browser and write the IP address of the webserver to browse it. It browsed successfully. Next, go to PC11 on the other side of the network or the Router. Keep practicing and perfecting your CCNA skills! Discover more CCNA labs on our practice pages. A Domain Name System server (DNS server) plays a crucial role in mapping the hostname of a network device to its corresponding IP address. Typically, computers use the IP address of a device to identify the device in a network. However, IP addresses can be challenging for humans to remember. DNS helps to associate a recognizable hostname of a device with its IP address. This enables humans to reach the device using its name rather than its numerical IP address. Here's a brief overview of how DNS works: When a host device attempts to reach a device in the network or a device on the internet, such as "youtube.com," the host device initiates a DNS request to the DNS server to discover the IP address associated with "youtube.com." The DNS server responds to the host device with the IP address "youtube.com." Subsequently, the host device can directly send packets to "youtube.com" using the IP address obtained from the DNS server. In this post, I will show you how to configure a DNS server on Cisco Packet Tracer. DNS servers used by host devices can be configured manually or learned using DHCP. In this demonstration, I will show you how to configure a DNS server manually. Related Post ALSO READ: How to Configure Native VLAN on Cisco RouterNetwork Topology The network topology we will be making use of in this post is shown below. As you can see, it comprises a DNS server, a host device representing Youtube.com, a router, two-layer switches, and other PCs. In this demonstration, we will configure the DNS server to have a record of all the host devices in the network so that all the host devices can be reached using their host names. How to Configure DNS Server Here are steps to configure DNS server; Step 1: Assign IP address to the server Just like other host devices need an IP address to be identified on a network, the server also needs an IP address to be identified on the network. As labeled in the network diagram, the IP address of the server should be 192.168.2.3, and the default gateway IP address should be 192.168.2.1. Then Assign IP address to the interface; ALSO READ: Standard Numbered ACL Configuration in Packet Tracer Step 2: Add DNS records. Open the "Services" tab to add the DNS records. To add a record, you need the hostname and the IP address of the network device for which you want to map. As shown above, I have added an entry to map the IP address 192.168.2.2 to the name "youtube.com" in the DNS record. The steps to do so have been highlighted in the image above. Follow the above steps to add other records to the DNS server. Note: A record is for IPV4 address while AAA record is for IPV6 address Step 3: Configure the interface of the router Enter the following commands to assign an IP address to the interfaces of the router as labeled above. Router>enable Router#configure terminal Router(config)#hostname R0 R0(config)#interface g0/0/0 R0(config-if)#ip address 192.168.1.1 255.255.255.0 R0(config-if)#no shutdown R0(config-if)#interface g0/0/1 R0(config-if)#ip address 192.168.2.1 255.255.255.0 R0(config-if)#no shutdown Step 4: Configure the host devices Configure the default gateway and the DNS server on each of the host devices. The default gateway should be the IP address of the interfaces of the router the PC is connected to, and the DNS server IP is the IP address of the DNS server. ALSO READ: How To Configure Dynamic Routing In Cisco Packet Tracer Then configure the fastethernet0 interface of the PC. Repeat the above step for each of the hosts in the network. Step 5: Test the configuration You can confirm that the configuration is working by sending a Ping packet to a host using the hostname configured in the DNS record. Related Post I am a passionate Networking Associate specializing in Telecommunications. With a degree in Electronic engineering, I possess a strong understanding of electronic systems and the intricacies of telecommunications networks. I gained practical experience and valuable insights working for a prominent telecommunications company. Additionally, I hold certifications in networking, which have solidified my expertise in network architecture, protocols, and optimization. Through my writing skills, I aim to provide accurate and valuable knowledge in the networking field. Connect with me on social media using the links below for more insights. You can contact me using or connect with me using any of the social media account linked below Cisco Packet Tracer as the name suggests, is a tool built by Cisco. This tool provides a network simulation to practice simple and complex networks. As Cisco believes, the best way to learn about networking is to do it. The main purpose of Cisco Packet Tracer is to help students learn the principles of networking with hands-on experience as well as develop Cisco technology specific skills. Since the protocols are implemented in software only method, this tool cannot replace the hardware Routers or Switches. Interestingly, this tool does not only include Cisco products but also many more networking devices. Using this tool is widely encouraged as it is part of the curriculum like CCNA, CCENT where Faculties use Packet Trace to demonstrate technical concepts and networking systems. Students complete assignments using this tool, working on their own or in teams. Engineers prefer to test any protocols on Cisco Packet Tracer before implementing them. Also, Engineers who would like to deploy any change in the production network prefer to use Cisco Packet Tracer to first test the required changes and proceed to deploy if and only if everything is working as expected. This makes the job easier for Engineers allowing them to add or remove simulated network devices, with a Command line interface and a drag and drop user interface. You can download the tool from by clicking on the Packet Tracer graphic and selecting the appropriate OS package, then you are good to play with it. This course will help you kick start using the tool: . Workspace : Logical - Logical workspace shows the logical network topology of the network the user has built. It represents the placing, connecting and clustering virtual network devices. Physical - Physical workspace shows the graphical physical dimension of the logical network. It depicts the scale and placement in how network devices such as routers, switches and hosts would look in a real environment. It also provides geographical representation of networks, including multiple buildings, cities and wiring closets. Key Features: Unlimited devices E-learning Customize single/multi user activities Interactive Environment Visualizing Networks Real-time mode and Simulation mode Self-paced Supports majority of networking protocols International language support Cross platform compatibility A web server is like a computer that uses an HTTP (Hyper Text Transfer Protocol) and many other protocols. it responds when a client makes a request over the World Wide Web. The main work of the web server is to show website content that is processed, and stored, in the webserver to deliver the webpages to the user. The Web server also uses SMTP (Simple Mail Transfer Protocol) for sending mail and FTP (File Transfer Protocol) for file transfer and storage. Installation Process Of Packet Tracer Click Here Steps of Deploying a Web server:Step 1: After Installation Open Packet Tracer. Step 2: Implementation- Click End Devices and Then Select PC The Drag Into them In the Screen. Result After This: Step 3: Again Click End Devices And After that click on a server. Drag Into Screen Result: Step 4: Connect each other with a wire for this click-on connection. Step 5: After Click On this Click on the PC and other hand click on a server. Like This Configuration:Step 1: Double-Click On PC0 and Click on Desktop Then Go to IP Configuration Step 2: Then Set the IP that you want to give. Step 3: Double-Click on Server0. Then Click on IP Configuration and Set the IP for the web server. Step 4: Set the IP Address to identify the web address. Step 5: Now go to Services and add some HTML code to check whether the server is working or not HTML Page Title

Welcome To GFG

Default code has been loaded into the Editor. Add this code and save it Step 6: Go to PC0 Click on Desktop and then open Web Browser. Step 7: Remember the IP that we are given to the web server enter the same ip to the address bar. click on go This is how you can create a web server. A web server is a server that delivers a webpage to a user when requested using a browser. When we surf the internet, we are actually making a request to a web server for a web page or file. A web server uses two basic protocols to render its service: HTTP/HTTPS and a DNS service. HTTP/HTTPS is a protocol used to send or receive data between a website and a browser. On the other hand, the Domain Name System (DNS) is a service that resolves a hostname (domain name) into an IP address. Normally, a web server is identified with an IP address over the internet; however, remembering this IP address for each website a user visits poses challenges. Hence, DNS helps to mitigate this by mapping the IP address of a website/web server to a human-readable name that users can use to surf on the website. In Packet Tracer simulation software, one can simulate a network that allows a user to access a web server using HTTP/HTTPS requests and plain domain names. In this post, I will show you how to Configure a Web Server in Packet Tracer. Related Post Network topology The network topology we will be making use of in this post is shown below. As you can see, it is a point-to-point connection between a PC (which will serve as the client) and server. I decided to make this very simple to reduce complications in configuration. In this demonstration, we will Enable both DNS service and the HTTP/HTTPS service on the server. As we know, the server in packet tracer is a multipurpose server; hence, we can use it for DNS and HTTP services. Here is a video on how to configure a web Server in packet tracer; How to Configure a Web Server in Packet Tracer Here are steps to Configure a Web Server in Packet Tracer; Step 1: Configure the Interface IP addresses For both PC0 and the web server to communicate, we need to assign an IP address to their interfaces. As we have labeled, PC0 has 192.168.1.2 as the interface IP address and 192.168.1.1 as the DNS server IP address. The webserver, on the other hand, has 192.168.1.1 as the interface IP address and 192.168.1.1 as the DNS server IP address. ALSO READ: How to Configure Trunk Port on Cisco Switch Packet Tracer Step 2: Enable DNS service on the Webserver For the server in our topology to serve a webpage, when requested with a domain name instead of an IP address, we need to enable DNS service and add a DNS record. In the above image, we made the IP address; 192.168.1.1 which is the IP address of the webserver to resolve to netizzan.com. We have detailed post on how to configure DNS in cisco packet tracer. Step 3: Enable HTTP service on the webserver HTTP/HTTPS allows a client to send and receive data (a webpage) between the webserver and the client's browser. To Enable HTTP service on the webserver, go to services>HTTP Step 4: Create the Webpage As shown in the image above, we have up to five default webpages that can be served by the webserver. Those are created by Cisco; you can customize them or delete them. In this demonstration, I will delete every other webpage except "index.html.". I will edit the index.html with the following code; Welcome to Netizzan body { font-family: Arial, sans-serif; text-align: center; margin: 50px; } h1 { color: #007BFF; } Welcome to Netizzan The best networking blog. In the client-server model, a server is a computer or device that provides a service or function to another device, known as a client. Essentially, the server's job is to give the client what it asks for, whether that's a webpage, a file, or any other resource. The client and server communicate over a network to exchange information as you can remember from part 1, sometimes we use WI-FI or sometimes we use cables.Let's break it down with a simple example: think of Google. Google has thousands of servers all over the world, and when you use your laptop to search for something, your device is the client, and the server is the one responding with search results. You're accessing a service hosted on their server over the internet.What's a Server?A server is just a computer that provides something, like information, a service, or a file. Servers are not always just one computer — there can be thousands of them, like Google's servers, which are responsible for giving you search results or storing your emails. Servers are always ready to give you what you ask for, as long as they understand the request.You can also turn your laptop into a server. For example, if you share a file with someone, your laptop becomes the server because it's providing the file to another device (the client).How Servers Listen to Requests: PortsOkay, let's make it even simpler. Think of a server like a person who speaks multiple languages. But instead of speaking to you directly, the server listens for specific languages (or protocols) based on the port number you send your request to. Each port is like a different language or channel, and the server knows how to respond based on which "language" you speak.Different Ports for Different ThingsPort 80 (HTTP) is like speaking English. If you want to access a regular website, you're speaking "English," and the server listens to you in English. This is how most websites are accessed.Port 443 (HTTPS) is like speaking a more formal, secure version of English. If you want to access a secure website(one with encryption, like when you log into your bank account), you're speaking "secure English," and the server listens to that.Ports 20 and 21 (FTP) are like speaking File Transfer Language. If you want to send or receive files (like downloading or uploading something), the server is tuned to listen to FTP language on these ports.Why Do We Need These Doors (Ports)?Imagine you're listening to a radio station, but the station is only broadcast in certain languages (just like how a server listens on different ports). You have to tune into the right station (port) to understand the language being spoken.For example:If you tune into port 80, it's like you're asking for a regular website in English (HTTP).If you tune into port 443, it's like you're asking for a secure website in secure English (HTTPS).If you tune into ports 20 and 21, it's like you're asking to transfer files in File Transfer Language (FTP).Each port is a different language. The server listens for different languages depending on the type of service you want. Just like how you'd speak English to get a general conversation, and speak a formal language to get something secure, the server uses the right port to understand what you're asking for.Breakdown:Ports = LanguagesDifferent ports = Different servicesSpeak the right language (port) = Get the right serviceHow Does This All Work?When you use the internet, your computer is like a client. It's asking for something, like a website. But to get what you want, the server needs to know exactly what you're asking for. So, it listens for these requests on different ports.Port 80: If you just want to browse a website, you send your request to port 80 (HTTP).Port 443: If you want a secure connection, you send your request to port 443 (HTTPS).So, when you type a website address in your browser, you're basically knocking on the right door (port 80 or 443), and the server opens it and sends you the website you asked for. That's how it works. Your computer just knows which door to knock on based on what you're trying to do.Ok one more time for Example:Imagine you're at a restaurant (the client) and you want some food (the request). You tell the waiter (the server) what you want. The waiter goes to the kitchen (the server's resources) to get your order. The kitchen has many "stations" (just like ports) — one for making burgers, one for making pizzas, and one for desserts. The waiter goes to the right station (or port) to get what you ordered. Then, the waiter brings it to you at your table. The server does the same thing for your computer.This is the basic idea of the client-server model — your device asks a server for something, and the server sends it back through the correct "door" (port).Let's break this down step by step and build a simple network to see how a client and server work together. We'll also see how a client can also act as a server. To help understand this, we'll use a diagram to visualize the setup.Step 1: Setting Up the DevicesPC (Client): This is the device that will ask for a service. It could be a laptop or desktop.Server: This is a different device that provides a service, such as a website, file, or app.In our case:The PC will request something from the server.The server will respond with the requested resource, such as a webpage or a file.How Do We Get These Two Devices to Talk?Okay, so now we've got our two devices (let's say a PC and a server), but they can't just talk to each other out of thin air. We need something to make that connection happen. That "something" is what we call a medium. In the old days, to get two computers to talk directly, we needed a crossover cable. It's a special type of cable that's made to connect two devices directly without needing a router or switch. So, a crossover cable is just a special kind of Ethernet cable that connects the sending pins of one device to the receiving pins of the other.The Ethernet Ports and the Green LightNow, once you plug that crossover cable into the Ethernet ports of your PC and server, something cool happens: you should see a green light on the ports. This green light is your signal that tells you the devices are connected. It's like turning on the power to a device — now they can send data back and forth. Okay, so why do we even need this cable? Here's the thing: without a medium (like a cable or Wi-Fi), your devices can'ttalk. It's like trying to send a letter without an envelope. The cable is the envelope that holds the letter and makes sure it gets to the right place.The Ethernet cable is like the pipe that lets all the data flow. No pipe? No data. Simple as that.The Basics of MAC AddressesSo, imagine you're trying to get a message from one device to another, like sending an email from your laptop to a server. But before any communication can happen, each device needs a name to be identified. This "name" is called a MAC address.A MAC address is like a unique ID card for your device on the network. It's built into your Network Interface Card (NIC), which is the part of your computer or phone that lets it connect to a network (either wired with Ethernet or wireless with Wi-Fi).Every device connected to a network, like a PC or a phone, has its own MAC address, and no two devices should have the same one. It's made up of 12 hexadecimal characters, which are just numbers and letters, like this: 00:1A:2B:3C:4D:5E.How Does It Work?When your PC wants to talk to another device (like a server), it sends a message with the MAC address of the device it wants to talk to. This ensures that the message goes to the right place, just like sending a letter to a specific address.For example:Your laptop's MAC address might be 00:1A:2B:3C:4D:5E.The server's MAC address might be 00:5F:6G:7H:8I:9J.Each device knows who it is because of its MAC address, and this helps it know where to send and receive data on the network.Why Do We Need MAC Addresses?Think of a network as a bunch of houses (devices), and the MAC address is the address on each house. When data gets sent through the network, it needs to know which house it's going to. So, each device uses its MAC address to identify itself to the network, ensuring the data goes to the right device.Now, We Need an IP AddressOkay, now that we've got our devices physically connected with the cable, there's still one more important thing we need: an IP address. Without an IP address, your devices would basically be lost in the digital world, like not having a home address for your house. The IP address is how devices identify each other on a network, like a phone number for your computer or server.What's an IP Address?An IP address (Internet Protocol address) is like the address of your device on a network. It lets devices know where to send data. If you send a letter, you need an address to get it to the right person, right? Same thing with an IP address. Typically, your Internet Service Provider (ISP) will give you an IP address when you connect to the internet. This is done automatically through a system called DHCP — it stands for Dynamic Host Configuration Protocol.How Does DHCP Work?When you connect your device to the network (like plugging your laptop into Wi-Fi), DHCP automatically assigns it an IP address. This is a dynamic process, meaning it can change. It doesn't stay the same forever (unless you set it to be static, but we'll get into that later). It hands out IP addresses to devices on the network, so they can talk to each other. It's like a network manager that assigns a seat to every device at the table so that everyone knows where to sit and can communicate with each other.Without an IP address, your device wouldn't be able to communicate with other devices or access the internet. The IP address is like a digital address that helps the data find its way to you. So, when you type a website address into your browser, it's actually asking for that website's IP address to get the information back to your device.So, in our network, we don't have a router. Normally, a router would give out IP addresses automatically (thanks to DHCP), but since we don't have one, we need to manually configure our IP addresses for our devices. This is something you wouldn't usually have to do, but since we're doing this in Packet Tracer, we have to manually assign the IP addresses to make sure everything works.Verifying Connectivity: The Ping TestNow that we've set up our IP addresses on both the PC and Server, we need to test if they can actually communicate with each other. This is where the ping comes in.The ping command is like saying, "Hey, are you there?" to another device on the network. If the other device is online and reachable, it replies back with a "Yes, I'm here!" message. It's a simple way to check if the devices are connected and can talk to each other.Checking Services on the ServerNow that we know we have IP connectivity between the PC and the server (thanks to our ping test), let's move on to the next step: checking the services running on the server.The server can offer different types of services to the client, like:DNS (Domain Name System): Resolves domain names to IP addresses.Email: Allows sending and receiving emails.FTP (File Transfer Protocol): Used for transferring files.HTTP (HyperText Transfer Protocol): The protocol used for web browsing.Now, let's focus on HTTP, which is used for web pages.If everything is set up correctly, you should see a simple web page load up. This page is served to you by the server via the HTTP service.This means that the server is listening on port 80 (the default port for HTTP), and when you access the server via the browser, it delivers the web page.How Does It Work?HTTP is the service that lets web pages be served. When you type an address in your browser, your PC (the client) sends a request to the server, asking for a page.The server, which is running the HTTP service on port 80, listens for incoming requests. When it receives your request, it sends back the web page you asked for.Recap:HTTP Service: The server listens on port 80 for requests from clients (like your PC).When you type in the browser, your PC sends an HTTP request to the server, and the server responds by serving a web page.Client-Server Model: The server provides services (like serving a web page) to the client. A web server is like a computer that uses an HTTP (Hyper Text Transfer Protocol) and many other protocols. it responds when a client makes a request over the World Wide Web. The main work of the web server is to show website content that is processed, and stored, in the webserver to deliver the webpages to the user. The Web server also uses SMTP (Simple Mail Transfer Protocol) for sending mail and FTP (File Transfer Protocol) for file transfer and storage. Installation Process Of Packet Tracer Click Here Steps of Deploying a Web server:Step 1: After Installation Open Packet Tracer. Step 2: Implementation- Click End Devices and Then Select PC The Drag Into them In the Screen. Result After This: Step 3: Again Click End Devices And After that click on a server. Drag Into Screen Result: Step 4: Connect each other with a wire for this click-on connection. Step 5: After Click On this Click on the PC and other hand click on a server. Like This Configuration:Step 1: Double-Click On PC0 and Click on Desktop Then Go to IP Configuration Step 2: Then Set the IP that you want to give. Step 3: Double-Click on Server0. Then Click on IP Configuration and Set the IP for the web server. Step 4: Set the IP Address to identify the web address. Step 5: Now go to Services and add some HTML code to check whether the server is working or not HTML Page Title

Welcome To GFG

Default code has been loaded into the Editor. Add this code and save it Step 6: Go to PC0 Click on Desktop and then open Web Browser. Step 7: Remember the IP that we are given to the web server enter the same ip to the address bar. click on go This is how you can create a web server. DHCP is a network management protocol used in networks to dynamically assign IP addresses and other network configuration information like default gateway, mask, DNS server address, etc. It is an application layer protocol. In this article, we will know about DHCP server configuration using Cisco Packet Tracer. Steps to Configure and Verify DHCP Server in Cisco Packet Tracer:Step 1: First, open the cisco packet tracer desktop and select the devices given below: S.NODeviceModel-NameUnit1.PCPC52.SwitchPT-Switch23.RouterPT-Router14.ServerServer-PT1Now create a network topology as shown below the image.Use an Automatic connecting cable to connect the devices with others.Step 2: Configure the Server with IPv4 address and Subnet Mask according to the Data given above. To assign an IP address in Server, click on Server-PT.Then, go to desktop and IP configuration and there you will find IPv4 configuration.Add IPv4 address, subnet mask, and Default Gateway.ParametersAddress valueIPv4 Address172.168.10.2Subnet Mask255.255.255.0Default-Gateway172.168.10.12. Assigning IP address using the ipconfig command. We can also assign an IP address with the help of a command.Go to the command prompt of the serverThen, type ipconfig (if needed)example: ipconfig 172.168.10.2 255.255.255.0 172.168.10.1Step 3: Configuring the DHCP server. To configure the DHCP server first, Click on Server then, Go to services.Click on DHCP and turn on the services and, configure the DHCP server with the help of the data given below.Delete the default values of Start IP Address and subnet Mask then save the info.Create two new pools.POOL1 and POOL2 and fill the data as shown in the images below. Step 4: Configuring Router with IPv4 Address and Subnet Mask. IP Addressing Table for Router: S.NODeviceInterfaceIPv4 AddressSubnet Mask1.router0FastEthernet0/0172.168.10.1255.255.255.0FastEthernet0/1192.168.10.1255.255.255.0To assign an IP address in router0, click on router0.Then, go to config and then Interfaces, and make sure to turn on the ports.Then, configure the IP address in FastEthernet according to IP addressing Table.Fill IPv4 address and subnet mask.Step 5: Configuring the PCs and changing the IP configuration. To assign an IP address in PC0, click on PC0.Then, go to desktop and IP configuration and there you will find IPv4 configuration.Change its state from static to DHCP.It will automatically fetch the data and configure itself.Repeat the same procedure with other PCs to configure them thoroughly.Output: You can also refer to the articles DHCP server and Working of Dynamic Host Configuration Protocol for more details. To simulate the internet, we have to configure the server endpoint available in the packet tracer. This server has the capability to provide web service. Download We have two hosts that will be able to access the internet via an ISP router. Our internal network is connected to the ISP router. The interface of the internal router which is connected to the ISP router has been given public IP address. This is static IP that has been configured on the interface. ISP router is further connected to the Google web server so after the successful configuration of our network, we should be able to access the google.com How to configure the web server We have to open services and click on HTTP service. This service is enabled by default and we can see that server is hosting some files already. These files are present by default and when we point the web browser to this server, this server will serve the web page to our browser. We have configured this server as a Google web server and it is serving a Google web page. To change the content of the webpage, we have to edit the index file present in the web server. For testing purposes, we can copy the source code of any side that you want the webserver to show and paste it into the index file. After saving the file, the web server will show sites according to the source code. Now, we can test the web server by opening the browser on the PC and pointing it to the server. We have to enter the IP address of the web server in the URL and press enter. If everything is configured properly then we should see the browser loading the webpage successfully. Before opening the browser, we must make sure that the connectivity of the server is fine. Download the lab and test the Google web server and if you want the server to host any other site then change the index file present on the server. This lab is the smaller presentation of a big network like the internet. This is the way how the internet works however there are thousands of routers and servers connected forming a huge network. You can try adding more servers with different sites and accessing those sites on the browser of the PC.