Minor Project- Report

Aug-2021-22

Course Faculty: Swapna Racherla Course Name & code: Computer Networks & 19CS5DCCNW

Semester: V-C Date:17/01/22

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| TITLE OF THE PROJECT | Client Server Architecture using Cisco Packet Tracer | | | |
|  |  | | | |
| STUDENT NAME | P R Sai Rahul | Pavan Patel G S | Vamsi Krishna P | Preetish Ranjan |
| USN | 1DS19CS107 | 1DS19CS111 | 1DS19CS113 | 1DS19CS118 |
| INDIVIDUAL  CONTRIBUTION | Implementation of DNS, SMTP , POP3 protocols | Implementation of RIP,FTP protocols | Implementation of WEP protocol and whole network topology | Implementation of OSPF,DHCP protocols |
| **GUIDE** | **Course Coordinator:** Swapna Racherla  **Lab Incharge:** Deepak G, Suman M | | | |
|  |  | | | |
| PROJECT ABSTRACT: | Generalization/Inheritance is a feature in network topology that **allows access control entry for an object whose network routes are being configured to be propagated to other objects**. This project shows how students(clients) in an organization get access to multiple (here two) objects while the sub-departments get access to their respective objects.  **To make sure the servers are accessed by genuine users, sniffers are implemented** through which we can keep a track of MAC addresses of the Systems accessing the servers.  The below topology which was implemented for one organization with sub departments is expanded through a router and is connected to another organization which implements the same concept. The complete topology as mentioned above could be considered as a server organization. This server organization provides information regarding the organization to its clients through 2 information servers. In the client-side network wireless end users are added which is implemented in the real  Case scenarios. | | | |
| PLATFORM USED  (H/W & S/w tools to be used | Cisco Packet Tracer | | | |
|  |  | | | |
| Introduction  +  UI Screenshots | Client - Server architecture: Architecture of a computer network in which many clients (remote processors) request and receive service from a centralized server (host computer). Client computers provide an interface to allow a computer user to request services of the server and to display the results the server returns.  This project is about designing a topology that implements generalization property where objects from two LANs (departments) is being accessed by a super LAN, along with communication between the three LANs.  Consider a college network scenario which consists of two branch departments. For example, from DSCE, we are considering the branches as CSE and ISE. We have implemented both intra and inter networking. There are several devices connected within each department(**intranetworking**) and the two departments are interconnected using a router(**internetworking**).  This project also implements client server architecture topology where the server provides information about its environment to the client(students), here we can consider an organization as a server and the clients as the students, the organization provides the information regarding its nature of academics through servers which can be accessed by the students. The students interact amongst themselves and with their servers in a well-established and fast network.    Server side:  Client side:      Outside the client-server network:    Protocols implemented:   1. **DNS**   The **Domain Name System** (**DNS**) is the hierarchical and [decentralized](https://en.wikipedia.org/wiki/Decentralised_system" \o "Decentralised system) naming system used to identify computers, [services](https://en.wikipedia.org/wiki/Internet" \l "Applications_and_services" \o "Internet), and other resources reachable through the [Internet](https://en.wikipedia.org/wiki/Internet" \o "Internet) or other [Internet Protocol](https://en.wikipedia.org/wiki/Internet_Protocol" \o "Internet Protocol) (IP) networks. The [resource records](https://en.wikipedia.org/wiki/Domain_Name_System" \l "Resource_records" \o "Domain Name System) contained in the DNS associate [domain names](https://en.wikipedia.org/wiki/Domain_name" \o "Domain name) with other forms of information. These are most commonly used to map human-friendly domain names to the numerical [IP addresses](https://en.wikipedia.org/wiki/IP_address" \o "IP address) computers need to locate services and devices using the underlying [network protocols](https://en.wikipedia.org/wiki/Communication_protocol" \o "Communication protocol), but have been extended over time to perform many other functions as well.  In our project, DNS has been implemented on the server side. We have two departments, CSE and ISE. We have Server0 which is accessible by every PC in both departments and Server1 which is accessible only by ground floors of both the departments. Server0 is the student portal and Server1 contains the data of the examination department.  “student” is the domain name given to the student portal (Server0). So, the student form is accessible by every PC in both the departments.    “quiz” is the domain name given to the DNS implemented for Server1. It is accessible only by PCs in the ground floors of both departments. So, when we try to access it from PC0 which is on second floor of CSE department, it should not be allowed.    Now if we consider a PC in the ground floor of any department, say PC2, it should be able to access both “student” and “quiz”.      We have also added **Sniffers** to monitor network traffic by examining streams of data packets that flow between computers on the network as well as between networked computers and the larger Internet. Using sniffers, we can keep a track of the devices accessing the server. For example, in the previous image PC2 has accessed “quiz”. So now in IP header of Sniffer1(which is connected to Server1) under GUI, HTTP we can see the IP address of the end user who has accessed Sniffer1, i.e., IP address of PC2.     1. **RIP**   **Routing Information Protocol (RIP)** is a distance-vector routing protocol. Routers running the distance-vector protocol send all or a portion of their routing tables in routing-update messages to their neighbors.  We have implemented RIP in both the departments. The implementation for one of the routers, Router0, has been shown below:     1. **WEP**   ***Wired Equivalent Privacy* (WEP)** is a security protocol, specified in the [IEEE](https://whatis.techtarget.com/definition/IEEE-Institute-of-Electrical-and-Electronics-Engineers) Wireless Fidelity ([Wi-Fi](https://searchmobilecomputing.techtarget.com/definition/Wi-Fi)) standard, 802.11b. That standard is designed to provide a wireless local area network (WLAN) with a level of security and privacy comparable to what is usually expected of a wired [LAN](https://www.techtarget.com/searchnetworking/definition/local-area-network-LAN).  We have implemented WEP on the client side, with a number of wired and wireless devices. We have used an access point to create a WLAN.  Access  Point:    A Wireless end user(tablet):       1. **DHCP**   ***Dynamic Host Configuration Protocol*** (DHCP) is a client/server protocol that automatically provides an Internet Protocol (IP) host with its IP address and other related configuration information such as the subnet mask and default gateway.  We have implemented DHCP outside the client-server network (in the external organization).    Assigning IP to a end user using DHCP:       1. **OSPF**   ***Open Shortest Path First* (OSPF)** is a link-state routing protocol that was developed for IP networks and is based on the Shortest Path First (SPF) algorithm. OSPF is an Interior Gateway Protocol (IGP). In an OSPF network, routers or systems within the same area maintain an identical link-state database that describes the topology of the area. Each router or system in the area generates its link-state database from the link-state advertisements (LSAs) that it receives from all the other routers or systems in the same area and the LSAs that itself generates. An LSA is a packet that contains information about neighbors and path costs. Based on the link-state database, each router or system calculates a shortest-path spanning tree, with itself as the root, using the SPF algorithm.  We have implemented OSPF outside the client-server network (in the external organization).     1. **FTP**   The term ***file transfer protocol* (FTP)** refers to a process that involves the transfer of files between devices over a network. The process works when one party allows another to send or receive files over the internet. Originally used as a way for users to communicate and exchange information between two physical devices, it is now commonly used to store files in the [cloud](https://www.investopedia.com/terms/c/cloud-computing.asp), which is usually a secure location that is held remotely.  Say we want to send a file from PC2(CSE department) to Laptop0(Client side) using Server0:  First, we enable FTP service in Server0.    Then we connect to Server0 from PC2 using FTP and upload a file.    Next, we connect to Server0 from Laptop0 and then get the file from Server0 using FTP.    To check if the file has been uploaded to Server0, use “dir” command.    Now open the file from Laptop0.     1. **SMTP & POP3**   SMTP also known as ***Simple Mail Transfer Protocol***, is part of the application layer of the TCP/IP protocol which is primarily used by following a process called "store and forward". SMTP moves email on and across networks based on Mail Transfer Agent (MTA) to send communication to the right computer and email.  On other hand POP3, which is an abbreviation for ***Post Office Protocol 3***, is again a protocol used for receiving email. Much like the physical version of a post office clerk, POP3 receives and holds email for an individual until they pick it up.  Say we want send a mail from PC2(CSE department) to PC10(client side) using Server0:  First, we enable SMTP and POP3 services in Server0.    Now to send a mail from PC2, go to the Email section and configure the mail.    Next, click on the compose mail option, enter the details and click on “Send”.    Now go to email section on PC10 and click on “Receive”. Double click on the received mail to open it. | | | |
|  |  | | | |
| Design |  | | | |
|  |  | | | |
| Project Source Code Link (Github/ Google DRive) | https://github.com/BruceKP6/Cisco-Packet-Tracer | | | |
|  |  | | | |
| Conclusion /FUTURE ENHANCEMENT | * Introducing ***more protocols*** in the client server model.(eg: STP) * **Add more end users** in both organisations and as well as in clients. * To introduce ***subnetting*** within a organisation. * To ***extend the client topology*** to homes,hostels,etc. of the students and introduce   Wireless home routers in them. | | | |
|  |  | | | |