| **DEPARTMENT OF CSE**  **CTY Project Work In collaboration with HPE** | |
| --- | --- |
| **Project Title** | **Auto locate servers in a Network** |
| **Student Team** | Ansha Prashanth 1BM20CS018  Chethan Kumar K 1BM20CS034  H Vidyasagar 1BM20CS053  MD Suraj Kumar 1BM20CS079  Shashanka G 1BM20CS147 |
| **Faculty Mentor** | * Rekha G S (Assistant Professor) * Dr. Manjunath D R (Assistant Professor) |
| **Review for the**  **Period** | 13-1-23 to 27-1-23 |
| **Task Given** | Understanding Servers Hardware (Good to look at HPE ProLiant Servers [documentation](https://www.hpe.com/us/en/servers/proliant-servers.html)). Understand different models.  Understand networking concepts: Ethernet, Subnet, Ping, TCP/IP/UDP, DHCP, ICMP, Routing protocols, tcpdump (Source internet)  Understanding Linux: Choose [CentOS](https://www.centos.org/). CentOS network interfaces, IP address (IPV4 and IPV6), routing table. |
| **Difficulties Faced** | None |
| **Libraries Used** | None |
| **Github Link for**  **the code:** | None |
| **Code:** None | |

| **Server Hardware** | Understanding server hardware involves familiarizing yourself with the various components that make up a server and how they work together to provide computing power, storage, and networking capabilities.  Some of the key components of a server include:   * Processor: The brain of the server, responsible for executing instructions and performing calculations. * Memory: This is where the server stores data that it is currently using or processing. * Storage: Servers typically have one or more hard drives or solid-state drives (SSDs) for storing data and software. * Network interface card (NIC): This component allows the server to connect to a network and communicate with other devices. * Power supply: Provides power to the server's components. * Chassis: The physical structure that houses and protects the server's components. * Cooling system: Servers generate a significant amount of heat and require a cooling system to prevent overheating. * Management features: Some servers come with built-in management features such as a remote management controller, which allows you to manage the server remotely.   Understanding how these components work together and the different options available for each component can help you choose the right server hardware for your needs. It is also important to consider the form factor, rack-mount, tower, blade and microserver, of the server depending on the data center space and the number of servers you need to deploy.  It is also important to keep in mind that some servers may have additional components or specialized hardware designed for specific workloads, such as GPU or FPGA acceleration.  The hardware of different server models :   * File servers: File servers typically have large storage capacity and may have multiple hard drives or solid-state drives (SSDs) for storing files. They may also have redundant power supplies and cooling systems to ensure high uptime. * Web servers: Web servers may have multiple processors and a large amount of memory to handle the high number of requests from users. They may also have multiple NICs for connecting to different networks * Database servers: Database servers may have specialized processors and memory optimized for handling large amounts of data. They may also have multiple NICs for connecting to different networks and specialized storage for storing and retrieving data quickly. * Mail servers: Mail servers may have multiple processors and a large amount of memory to handle the high number of email messages. They may also have specialized storage for storing and retrieving messages quickly. * Application servers: Application servers may have multiple processors and a large amount of memory to handle the high number of requests from users. They may also have specialized storage for storing and retrieving data quickly. * Virtual servers: Virtual servers typically have a high-performance host server that runs a virtualization software and multiple virtual servers are created on top of it. * Cloud servers: Cloud servers are hosted by a third-party provider and the hardware configuration may vary depending on the provider. They are typically accessed over the internet. * High-Performance Computing servers: High-performance computing servers typically have multiple processors, a large amount of memory and storage, and specialized hardware such as GPU or FPGA acceleration, to perform complex calculations and process large amounts of data quickly. |
| --- | --- |

| **Networking concepts:** | Ethernet: Ethernet is a widely used networking standard that specifies how data is transmitted over a network. It defines the physical and data link layers of the OSI model, and is used to connect devices such as computers, servers, and switches.  Subnet: A subnet is a smaller network that is created by dividing a larger network into multiple smaller networks. This allows for better organization and control of network resources, as well as increased security.  Ping: Ping is a simple utility that allows you to check the connectivity and response time of a networked device. It works by sending a small packet of data to the target device, and measuring the time it takes for the device to respond.  TCP/IP: Transmission Control Protocol/Internet Protocol (TCP/IP) is the most widely used networking protocol on the internet. It is responsible for routing data packets between networks, and for providing a reliable, error-free data transfer.  UDP: User Datagram Protocol (UDP) is an alternative to TCP/IP, which is used for sending data packets over a network. Unlike TCP/IP, UDP is a connectionless protocol, which means that it does not establish a connection before sending data.  DHCP: Dynamic Host Configuration Protocol (DHCP) is a networking protocol used to automatically assign IP addresses to devices on a network. This allows devices to communicate with each other without the need for manual configuration.  ICMP: Internet Control Message Protocol (ICMP) is used to send error messages and operational information about network conditions. It is typically used by the ping utility to check connectivity and response time.  Routing protocols: Routing protocols are used to determine the best path for data packets to travel from one network to another. Common routing protocols include OSPF, BGP, and EIGRP.  tcpdump: Tcpdump is a command-line tool used to capture and analyze network traffic. It can be used to troubleshoot network issues, capture packets for analysis, and monitor network activity.  These networking concepts are important to understand to manage, troubleshoot and optimize the performance of a network. Additionally, they are widely used in the industry and are an important part of the curriculum of networking and IT related careers. |
| --- | --- |

| **Linux (CentOS):** | CentOS is a popular distribution of Linux, which is based on Red Hat Enterprise Linux (RHEL). It is known for its stability, security, and compatibility with enterprise-level environments.  Network interfaces: In CentOS, network interfaces are represented by network devices such as eth0, eth1, etc. These interfaces can be managed using the ifconfig command, which allows you to view, configure, and troubleshoot network interfaces. For example, you can use the command "ifconfig eth0" to view the current settings for the eth0 interface.  IP address: An IP address is a unique numerical label assigned to each device connected to a computer network that uses the Internet Protocol for communication. In CentOS, you can view the IP address of a network interface using the command "ifconfig eth0" and it will display the IPV4 address. To view IPV6 address use "ifconfig eth0" and it will show the IPV6 address. |
| --- | --- |
| **Servers and Networks** | There are several methods that can be used to discover and identify servers on a network:  **IP address scanning**: This involves sending a ping or other type of network packet to a range of IP addresses in order to identify which ones are in use by servers. Once an IP address responds, additional information can be gathered about the server using other tools such as port scanning.  **Hostname resolution**: This method involves using DNS or other name resolution protocols to convert hostnames to IP addresses. This can be used to identify servers that have registered hostnames on the network.  **Network protocol analysis**: This method involves capturing and analyzing network traffic to identify servers based on the protocols they are using. For example, servers using the SMB protocol may indicate that they are file servers.  **SNMP**: Simple Network Management Protocol is a standard protocol used for network management. It can be used to query network devices for information about their status, configuration, and performance.  **Active Directory**: If the network is using Active Directory, it can be used to discover and identify servers that are joined to the domain.  **There are several ways to automatically retrieve the serial number of a server during the first connection to a network:**   1. **Use a script:** A script can be run on the server during the initial setup or first boot that retrieves the serial number from the BIOS or firmware and then reports it to a centralized management system. 2. **Use a network management tool:** Many network management tools have the ability to automatically discover new devices on the network and retrieve information about them, including the serial number. These tools can be configured to run automatically during the initial connection of a new device. 3. **Use an inventory management software:** Some inventory management software can automatically detect new devices on a network, retrieve information about them and store the information in a database. This information can then be accessed and used to identify the device. 4. **Use Remote Management Controller (ILO, iDRAC, etc) :** Many servers have a built-in Remote Management Controller that can be accessed over the network. These controllers often provide information about the server including its serial number. 5. **Use an agent software:** Some servers have an agent software that can be installed on them, this software will periodically check-in to a central management server and report the server information, including the serial number.   Flow Diagram Using Script To Receive Server Information: |

| **References** | * <https://www.tecmint.com/commands-to-collect-system-and-hardware-information-in-linux/> * <https://sid-500.com/2018/05/14/get-serial-numbers-of-all-domain-computers-by-using-windows-powershell/> * <https://en.wikipedia.org/wiki/CentOS> * <https://wiki.centos.org/Documentation> |
| --- | --- |