

Lab 11

Research on Super-Netting, DHCP, VLAN & DNS

Lab 11 - Task

Task 1;

What is “DHCP, VLAN & DNS”, explain with Example (draw structure in cisco)

DHCP (Dynamic Host Configuration Protocol) is a network management protocol used to dynamically assign an IP address to any device, or node, on a network so it can communicate using IP. DHCP automates and centrally manages these configurations rather than requiring network administrators to manually assign IP addresses to all network devices. DHCP can be implemented on small local networks, as well as large enterprise networks.

DHCP assigns new IP addresses in each location when devices are moved from place to place, which means network administrators do not have to manually configure each device with a valid IP address or reconfigure the device with a new IP address if it moves to a new location on the network.

Versions of DHCP are available for use in IP version 4 (IPv4) and IP version 6 (IPv6). IPv6 became an industry standard in 2017 -- nearly 20 years after its specifications were first published. While the adoption rate of IPv6 was slow, more than 29% of Google users were making inquiries using IPv6 by July 2019.

How DHCP works

DHCP runs at the application layer of the TCP/IP stack. It dynamically assigns IP addresses to DHCP clients and allocates TCP/IP configuration information to DHCP clients. This information includes subnet mask information, default gateway IP addresses and domain name system (DNS) addresses.

DHCP is a client-server protocol in which servers manage a pool of unique IP addresses, as well as information about client configuration parameters. The servers then assign addresses out

of those address pools. DHCP-enabled clients send a request to the DHCP server whenever they connect to a network.

A **virtual local area network** (VLAN) is any broadcast domain that is partitioned and isolated in a computer network at the data link layer (OSI layer 2). In this context, virtual refers to a physical object recreated and altered by additional logic, within the local area network. Basically, a VLAN behaves like a virtual switch or network link that can share the same physical structure with other VLANs while staying logically separate from them. VLANs work by applying tags to network frames and handling these tags in networking systems, in effect creating the appearance and functionality of network traffic that, while on a single physical network, behaves as if it were split between separate networks. In this way, VLANs can keep network applications separate despite being connected to the same physical network, and without requiring multiple sets of cabling and networking devices to be deployed.

VLANs allow network administrators to group hosts together even if the hosts are not directly connected to the same network switch. Because VLAN membership can be configured through software, this can greatly simplify network design and deployment. Without VLANs, grouping hosts according to their resource needs the labor of relocating nodes or rewiring data links. VLANs allow devices that must be kept separate to share the cabling of a physical network and yet be prevented from directly interacting with one another. This managed sharing yields gains in simplicity, security, traffic management, and economy. For example, a VLAN can be used to separate traffic within a business based on individual users or groups of users or their roles (e.g. network administrators), or based on traffic characteristics (e.g. low-priority traffic prevented from impinging on the rest of the network's functioning). Many Internet hosting services use VLANs to separate customers' private zones from one other, allowing each customer's servers to be grouped in a single network segment no matter where the individual servers are located in the data center. Some precautions are needed to prevent traffic "escaping" from a given VLAN, an exploit known as VLAN hopping.

To subdivide a network into VLANs, one configures network

equipment. Simpler equipment might partition only each physical port (if even that), in which case each VLAN runs over a dedicated network cable. More sophisticated devices can mark frames through VLAN tagging, so that a single interconnect (trunk) may be used to transport data for multiple VLANs. Since VLANs share bandwidth, a VLAN trunk can use link aggregation, quality-of-service prioritization, or both to route data efficiently.

The **Domain Name System** (DNS) is a hierarchical and distributed name service that provides a naming system for computers, services, and other resources on the Internet or other Internet Protocol (IP) networks. It associates various information with domain names (identification strings) assigned to each of the associated entities. Most prominently, it translates readily memorized domain names to the numerical IP addresses needed for locating and identifying computer services and devices with the underlying network protocols. The Domain Name System has been an essential component of the functionality of the Internet since 1985.

The Domain Name System delegates the responsibility of assigning domain names and mapping those names to Internet resources by designating authoritative name servers for each domain. Network administrators may delegate authority over subdomains of their allocated name space to other name servers. This mechanism provides distributed and fault-tolerant service and was designed to avoid a single large central database. In addition, the DNS specifies the technical functionality of the database service that is at its core. It defines the DNS protocol, a detailed specification of the data structures and data communication exchanges used in the DNS, as part of the Internet protocol suite.