

Network configurations



**ASSIGN
BUSTER**

Standardized Configurations across the Network Replace with DeVry

NETW206: Introduction to Switching Submitted Your professor's name

Date: Current date

Standardized configurations across the network

A Virtual LANs otherwise known as a VLANs which are usually defined within switches, are broadcast domain that control broadcast, multicast, and unicast within a device in layer 2. They are placed on specific ports to restrict access. One VLAN cannot communicate with the other. For them to communicate, a router needs to be installed. A VLAN is important in that it addresses issues of security by restricting access to the sensitive information, it eliminates the need of purchasing additional expensive network equipment, and it also increase the performance of the network by supporting multiple broadcast domain, hence reduces the issues of traffic.

The VLANs are going to be defined in our Cisco catalyst 4300-X series switch in the VLAN Trunking Protocol (VTP). After the creation of the VLANs, there is the creation of ports. The VLANs are created using numbers and the numbers are in two ranges for the creation, that is:

1-1000 For the Normal Range

1025-4096 For the Extended Range,

To configure VLAN, the following steps are to be followed:

Configuration of the VTP- VTP is a procedure that enables the Cisco switches to maintain the consistency of the database for the purpose of trunking. It facilitates easier administration of the VLANs.

Then we create the VLANs- As stated earlier, VLANs are created using numbers. The extended VLANs are presently supported on the switches that run on the COS software edition 6. 1 or greater.

<https://assignbuster.com/network-configurations/>

The creation of the solution template helps in the design of a standard modular network solutions. This solution template handles the issue of all non-standard, non device-specific configuration, for instance VLAN configuration, routing protocols, spanning tree parameters, among others (Lammle, 2011).

For achieving standard hostname, a naming system should be used, e. g the Network Information Systems, Domain Name System, among others.

There are three privileges levels in a router:

privilege level 1 which is for the non-privileged (prompt is router>), the default level for logging in

privilege level 15 which is for the privileged (prompt is router#), the level after going into enable mode

privilege level 0 which is seldom used, but includes 5 commands: disable, enable, exit, help, and logout.

These privileges are assigned with the TACACS+ and the RADIUS servers.

The Secure Shell otherwise known as SSH is a secure network protocol for the Cisco devices compared to telnet. Our Cisco switch can be setup to access the SSH by following the steps below:

First we configure the hostname command,

Configure the DNS domain,

Generate the SSH key to be used,

Enable SSH transport support for the virtual type terminal (vty).

Ideally, authentication protocols like the RADIUS, LDAP, TACACS+, among others provide a means to verify a legitimate user. These protocols are used to prevent those that are not supposed to access the out-of-band management ports. IP address filtering and authentication can also be

<https://assignbuster.com/network-configurations/>

employed. One can also opt to use Password Manager Pro which provides a centralized repository for that stores all of passwords securely and facilitates easy administration (Ohio, 2011).

References

Lammle, T. (2011). CCNA: Cisco Certified Network Associate study guide (Exam 640-802).

Indianapolis, Ind: Wiley Pub.

Ohio. (2011). LAN/WAN access and distribution layer switches. Columbus:

Enterprise IT

Architecture & Policy, Investment and Governance Division.