1. Project Title

Network design for a software development organization

1. Abstract

A network was designed for a software development organization that categorized the network into three departments. The method used to design the network included creating VLAN with Cisco routers and switches that provided various authority and access to the departments. The process was carried out in the command line interface of the Cisco routers and switches. The task was successfully completed and provided different levels of authority to each department for internet access and inter-departmental communication.

1. Project Scope

This kind of systems can be used in wide variety of institutions where communication between departments is necessary. Since this system also divides the authority over internet access it is essential in organizations that do not require internet access. Production companies, private institutions, government offices, educational institutions and various other fields can implement this system.

1. Network Requirements

The project is used to create VLANs to divide the authority among the departments whilst having the freedom to communicate. This type of system has the following requirements:

1. Cisco Packet Tracer
2. Cisco Switches
3. Cisco Router of Model No: 1841
4. Putty
5. Working PCs or Laptops
6. Connection Cables
7. Feasibility Study
   1. Technical Feasibility

A VLAN is a group of devices on one or more LANs that are configured to communicate as if they were attached to the same wire, when in fact they are located on a number of different LAN segments. The system is setup and network is configured by a CCNA graduate. Any problem that may arise in the system is to be dealt by trained professionals or individuals possessing expertise in the respective field.

* 1. Economic Feasibility

The VLANs can be configured in any system and the cost ranges according to the size of the network or the specifications required in the network.

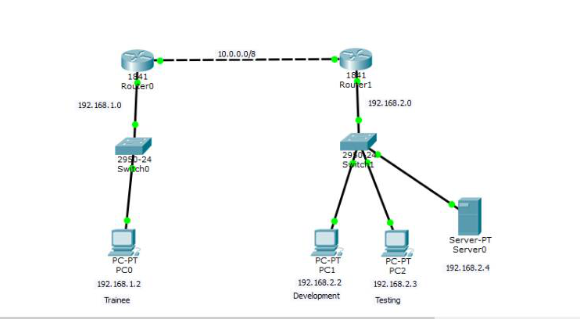
* 1. Operational Feasibility

The VLAN setup can be done with proper configuration in the CLI mode. Depending upon the size and requirements of the network, the system can be modified and implemented as per the necessity of the institution. Trained specialists are required to operate and supervise the established system.

1. Project Details
   1. Working Procedure

Cisco provides basic traffic filtering capabilities with access control lists (also referred to as access lists). Access lists can be configured for all routed network protocols (IP, AppleTalk, and so on) to filter the packets of those protocols as the packets pass through a router. Access lists filter network traffic by controlling whether routed packets are forwarded or blocked at the router's interfaces. Your router examines each packet to determine whether to forward or drop the packet, on the basis of the criteria you specified within the access lists. Access lists can allow one host to access a part of your network and prevent another host from accessing the same area.

* 1. Network Diagram



* 1. Commands/Codes

A. Configuring Router0

1. To configure FastEthernet 0/0

Router>enable

Router#configure terminal

Enter configuration commands, one per line. End with CNTL/Z.

Router(config)#interface FastEthernet0/0

Router(config-if)#ip address 192.168.1.1 255.255.255.0

Router(config-if)#no shutdown

Router(config-if)#

%LINK-5-CHANGED: Interface FastEthernet0/0, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0, changed state to up

Router(config-if)#exit

2. To configure FastEthernet 0/1

Router(config)#interface FastEthernet0/1

Router(config-if)#ip address 10.0.1.1 255.0.0.0

Router(config-if)#

Router(config-if)#exit

Router(config)#interface FastEthernet0/1

Router(config-if)#no shutdown

Router(config-if)#

%LINK-5-CHANGED: Interface FastEthernet0/1, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1, changed state to up

Router(config-if)#exit

B. Configuring Router1

1. To configure FastEthernet 0/0

Router>enable

Router#configure terminal

Enter configuration commands, one per line. End with CNTL/Z.

Router(config)#interface FastEthernet0/0

Router(config-if)#ip address 192.168.2.1 255.255.255.0

Router(config-if)#no shutdown

Router(config-if)#

%LINK-5-CHANGED: Interface FastEthernet0/0, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0, changed state to up

Router(config-if)#exit

2. To configure FastEthernet 0/1

Router(config)#interface FastEthernet0/1

Router(config-if)#

Router(config-if)#exit

Router(config)#interface FastEthernet0/1

Router(config-if)#ip address 10.0.1.2 255.0.0.0

Router(config-if)#no shutdown

Router(config-if)#

%LINK-5-CHANGED: Interface FastEthernet0/1, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1, changed state to up

Router(config-if)#exit

C. RIP Protocol

1. In Router0

Router(config)#router rip

Router(config-router)#network 192.168.1.0

Router(config-router)#network 10.0.0.0

Router(config-router)#

Router(config-router)#end

Router#copy running-config startup-config

Destination filename [startup-config]?

Building configuration...

[OK]

Router#

%SYS-5-CONFIG\_I: Configured from console by console

2. In Router1

Router(config)#router rip

Router(config-router)#network 192.168.2.0

Router(config-router)#network 10.0.0.0

Router(config-router)#

Router(config-router)#end

Router#copy running-config startup-config

Destination filename [startup-config]?

Building configuration...

[OK]

Router#

%SYS-5-CONFIG\_I: Configured from console by console

D. ACL for port 80 (www)

(In Router0)

Router#configure ter

Enter configuration commands, one per line. End with CNTL/Z.

Router(config)#

Router(config)#access-list 100 deny tcp host 192.168.1.2 host 192.168.2.4 eq 80

Router(config)#access-list 100 permit ip any any

Router(config)#in fa 0/0

Router(config-if)#ip access-group 100 in

Router(config-if)#

Router#

%SYS-5-CONFIG\_I: Configured from console by console

Router#configure ter

1. Conclusion

In the project we used CISCO packet tracer to design, analyze and test the system by creating VLANs and Access lists. The requirements of the system were met and concluded such that it could easily be implemented in real life systems if need be. The ACL provided a list of members in the system to be filtered for the internet access. The establishment of VLANs ensured division of departments and also allowed communication both within and among the departments.

1. Future Enhancements

The network flow can be designed to perform better with the use of modern tools.