Pract 7

1. Implement EtherChannel 2. Tune and Optimize EtherChannel Operations

Background Info:

EtherChannel is a port link aggregation technology or port-channel architecture used primarily on Cisco switches. It allows grouping of several physical Ethernet links to create one logical Ethernet link for the purpose of providing fault-tolerance and high-speed links between switches, routers and servers. An EtherChannel can be created from between two and eight active Fast, Gigabit or 10-Gigabit Ethernet ports, with an additional one to eight inactive (failover) ports which become active as the other active ports fail. EtherChannel is primarily used in the backbone network, but can also be used to connect end user machines.

Using an EtherChannel has numerous advantages, and probably the most desirable aspect is the bandwidth. Using the maximum of 8 active ports a total bandwidth of 800 Mbit/s, 8 Gbit/s or 80 Gbit/s is possible depending on port speed. This assumes there is a traffic mixture, as those speeds do not apply to a single application only. It can be used with Ethernet running on twisted pair wiring, single-mode and multimode fiber.

Pract 8

OSPF Implementation 1. Implement Single-Area OSPFv2 2. Implement Multi-Area OSPFv2 3. OSPFv2 Route Summarization and Filtering 4. Implement Multiarea OSPFv3

Background info:

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.

Single Area OSPF

• All routers contained in one area • Called the backbone area • Known as Area 0 • Used in smaller networks with few routers

Multi Area OSPF

• Designed using a hierarchical scheme • All areas connect to area 0 • More commonly seen with numerous areas around area 0 (like a daisy or aster) • Routers that connect area 0 to another area is known as an Area Border Router (ABR) • Used in large networks • Multiple areas reduces processing and memory overhead • A failure in one area does not affect other areas

Pract 9

Implement BGP Communities 1. Implement MP-BGP 2. Implement eBGP for IPv4 3. Implement BGP Path Manipulation

Background Info:

BGP is the protocol that makes the Internet work by enabling data routing. when someone submits data via the Internet, BGP is responsible for looking at all of the available paths that data could travel and picking the best route, which usually means hopping between autonomous systems.

MP-BGP:

The normal version of BGP (Border Gateway Protocol) only supported IPv4 unicast prefixes. Nowadays we use MP-BGP (Multiprotocol BGP) which supports different addresses like IPv4 unicast, IPv4 multicast, IPv6 unicast, IPv6 multicast

MP-BGP is also used for MPLS VPN where we use MP-BGP to exchange the VPN labels. For each different "address" type, MP-BGP uses a different address family.

eBGP:

EBGP is used between autonomous systems. It is used and implemented at the edge or border router that provides inter-connectivity for two or more autonomous system. It functions as the protocol responsible for interconnection of networks from different organizations or the Internet.

Pract 10

Implement IPsec Site-to-Site VPNs 1. Implement GRE over IPsec Site-to-Site VPNs 2. Implement VRF Lite

Background Info:

Internet Protocol Security, commonly known as IPsec is a method of encrypting packets that makes VPNs possible. Using a suite of protocols, IPsec can authenticate and encrypt data passing over Internet Protocol networks

A site-to-site virtual private network (VPN) is a connection between two or more networks, such as a corporate network and a branch office network. Many organizations use site-to-site VPNs to leverage an internet connection for private traffic as an alternative to using private MPLS circuits.

GRE over IPsec

GRE is an encapsulation protocol and it can't encrypt the data, so we take the help of IPsec for getting the encryption job done.

GRE over IPsec can be configured in two modes, GRE IPsec Tunnel Mode and
GRE IPsec Transport Mode

VRF-lite is a feature that enables a service provider to support two or more VPNs, where IP addresses can be overlapped among the VPNs. VRF-lite uses input interfaces to distinguish routes for different VPNs and forms virtual packet-forwarding tables by associating one or more Layer 3 interfaces with each VRF.

Pract 11

Simulating SDN with 1. OpenDaylight SDN Controller with the Mininet Network Emulator 2. OFNet SDN network emulator

Background info:

OpenDaylight is an open source SDN controller / framework, hosted by the Linux Foundation. It's one of the more popular (open source) SDN controllers at the moment.

One of the southbound interface protocols it supports is OpenFlow. To test OpenDaylight, we'll need some switches that support OpenFlow.

You could buy some hardware that supports OpenFlow but a great alternative is Mininet.

Mininet allows you to run a virtual network on your own computer with devices that support OpenFlow.

OFNet is a new software-defined network (SDN) emulator that offers functionality similar to the Mininet network emulator and adds some useful tools for generating traffic and monitoring OpenFlow messages and evaluating SDN controller performance.

Pract 12

Simulating OpenFlow Using MININET

Background info:

OpenFlow (OF) is considered one of the first software-defined networking (SDN) standards.

It originally defined the communication protocol in SDN architectures that enabled the SDN controller to directly interact with the forwarding plane of network devices such as switches and routers, both physical and virtual (hypervisor-based), so it can better adapt to changing business requirements.

To work in an OF environment, any device that wants to communicate to an SDN controller must support the OpenFlow protocol. Through this interface, the SDN controller pushes down changes to the switch/router flow-table allowing network administrators to partition traffic, control flows for optimal performance, and start testing new configurations and applications.