Student: Man Fu Lei

Student Number: 32065409

Unit Name: Network Switching

Submission Date: May 15th, 2015

**Network Design**

**Design a network model for five labs in Murdoch University**

#### Group Members

|  |  |
| --- | --- |
| **Name** | **Student Number** |
| Man Fu Lei | 32065409 |
| Bhuwan Gautam | 32361689 |
| Khalid Alsaeed | 31054964 |
| Vishwas Patel | 32497706 |

#### Table of Content

[1 Introduction 1](#_Toc418875256)

[1.1 The Authorization 1](#_Toc418875257)

[1.2 The Purpose 1](#_Toc418875258)

[1.3 The Scope 1](#_Toc418875259)

[1.4 Terms of Reference 1](#_Toc418875260)

[1.5 Acknowledgements 1](#_Toc418875261)

[2 Method 2](#_Toc418875262)

[2.1 Field Observation 2](#_Toc418875264)

[2.2 Packet Tracer 2](#_Toc418875265)

[2.3 Group discussion 2](#_Toc418875268)

[3 Modelling 3](#_Toc418875269)

[3.1 List of Labs 3](#_Toc418875271)

[3.2 VLAN Structure 3](#_Toc418875272)

[3.3 IP Addressing 5](#_Toc418875273)

[4 Design 6](#_Toc418875274)

[4.1 Access Layer 7](#_Toc418875276)

[4.2 Distribution Layer 7](#_Toc418875277)

[4.3 Core Layer 9](#_Toc418875278)

[4.4 Other Features 9](#_Toc418875279)

[5 Recommendation 10](#_Toc418875280)

[6 Conclusions 11](#_Toc418875281)

[7 Appendices 12](#_Toc418875282)

[8 List of References 20](#_Toc418875286)

[9 Glossary 21](#_Toc418875287)

[10 Index 23](#_Toc418875288)

#### Table of Tables

[Table 1 - List of labs modelled 3](#_Toc418864322)

[Table 2 - VLAN models 5](#_Toc418864323)

#### Executive Summary

Murdoch University has many computer labs. Five of them need to be modelled as a network design. These computer labs typically don't contain many computers and they are all connected to a network mostly consisting of switches. During the design real commands are input into the Cisco Packet Tracer to test if the configurations are feasible. Test was also run to simulate the communication among different hosts and host from the Internet. After fully testing, this report shows the list of labs modelled in the project, the structure used to model the five labs and the addressing scheme for the model. It also explained the decisions made during designing the model from access layer to core layer. A part of the initial configuration commands are provided in the Appendices.

# Introduction

## The Authorization

In week 9 the author was assigned a task to model a part of the Murdoch University computer lab network. The assignment requires to model five laboratories from Murdoch University. Three of them are ECL2.044, ECL2.039 and a lab from Loneragan building. The other two must consist of one from the ECL building and the other from somewhere outside the ECL building. The designed model will be represented as a Cisco Packet Tracer file.

## The Purpose

The purpose of this report is to design a network model including IP addressing schemes as well as explanations on the decisions made during the design process.

## The Scope

This report contains two parts: modelling and design. The modelling part includes the list of labs the author chose to model, the Virtual Local Area Network (VLAN) structure of the five labs and the IP addressing scheme based on the structure. The design part includes design outline and explanation on the three-layer architecture: access layer, distribution layer and core layer. Part of the initial configuration commands representing each layer will be placed in the Appendices. The labs are all connected to the network with cables so no wireless knowledge is involved. Only the VLAN structure and the IP addressing are needed to be modelled for the labs.

## Terms of Reference

This report is prepared for readers with medium networking knowledge equivalent to the level of Cisco Certified Network Associates (CCNA) 4. Labs refer to the computer labs connecting to the campus network with Ethernet cables. Cisco Packet Tracer is a piece of software which can simulate process of network communication. This project used Packet Tracer 6.0.2.0052 student version. This report should be reviewed with the Packet Tracer file uploaded by the author. If referencing this report, please include all the authors’ names.

## Acknowledgements

The author wants to thank these people who helped us a lot during the project:

Aubrey Adams*, Murdoch University, Tutor*

Terry Koziniec *Murdoch University, Unit Coordinator*

# Method



## Field Observation

The author went to the five labs and started the computers to determine the IP addressing schemes and the VLAN structure.

## Packet Tracer

The author used Packet Tracer to design the network model and test if the configurations meet the requirements.



## Group discussion

The author discussed possible technologies that can be used in the design with the group members to find out the best solution.

# Modelling



## List of Labs

The following table lists the labs modelled and their addressing schemes according to the numbers of hosts:

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Name** | **Location** | **Network** | **Prefix Length** | **Default Gateway** | **Number of Hosts** |
| ECL2044/2039 | ECL Building | 134.115.153.0 | 26 | 134.115.153.1 | 16+19=35 |
| Loneragan3032 | Loneragan Building | 134.115.128.0 | 26 | 134.115.128.1 | 28 |
| ECL2046 | ECL Building | 134.115.156.0 | 26 | 134.115.156.1 | 15 |
| GCL1 | Near Library | 134.115.156.0 | 26 | 134.115.156.1 | 33 |

Table - List of labs modelled

## VLAN Structure

The topology used in the design is like:

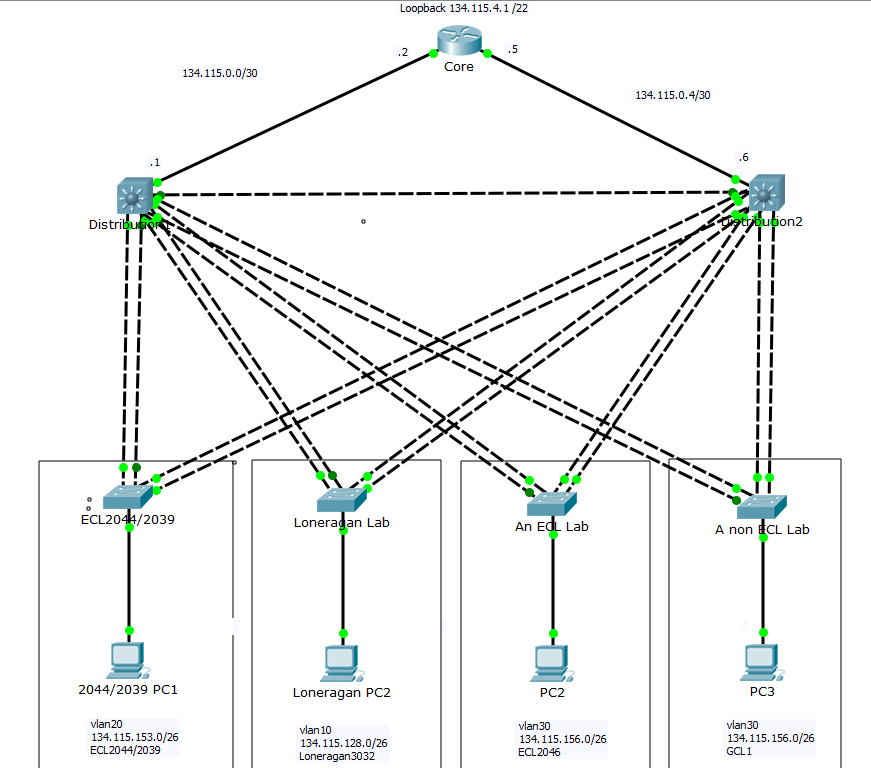


Figure - Design topology

According to the subnets these labs belong to, the VLAN structure should use a mixed model. The Loneragan lab and the ECL2044/2039 should use local VLAN because they belong to subnets that are different from that of the other two labs. The benefit of using local VLAN is that the access switches don't need to be configured with other VLANs they are not directly connected to. In this case traffic for different VLANs won't flood the switches all the time so that performance can be enhanced. The local VLAN also sets up a physical boundary to the computers inside the labs. The benefit of local VLAN is making the traffic flow more deterministic so that failure can be isolated into the switch block. It is also scalable because when there is new lab a new access switch can be added into the topology with a new subnet assigned to its access ports.

The GCL1 and ECL2046 should use end-to-end VLAN because they are in the same subnet but are separated from each other far away. If local VLAN is used more switches and cables are needed to group these two labs together. End-to-end VLAN is suitable for geographically dispersed network so that computers stay in the same VLAN even if they are in the other room. Because all computers in each of the labs are in the same subnet each switch only needs to be configured with that VLAN for access ports. Traffic between these two labs can also avoid being routed so that latency is reduced and routing resource is not wasted. It is also scalable because new computers can be introduced into any of the two labs easily without changing any other configuration.

The mixed model can be fault tolerant because all access switches have redundant links to either of the distribution layer switches. It is also maintainable because the local VLAN design can isolate the failure and the end-to-end VLAN design is only for one subnet so the failure can also be easily detected.

## IP Addressing

The subnet mask for all five labs is 255.255.255.192.

ECL2044 has 19 hosts and ECL2036 has 16 hosts. They are in the same subnet 134.115.153.0 with a gateway 134.115.153.1. With a block size of 64 there can be 62 usable addresses. After three addresses are taken away by the two distribution layer switches and the virtual gateway, there are 59 addresses usable. Given the room size of these two labs, there can be most 50 computers so it should be enough to have 26 as the prefix.

Loneragan3032 has 28 hosts. If the block size is set to 32, even if there are 30 usable addresses, it won't be enough because the gateways are using at least three addresses. So the block size should be 64. After three addresses are used by the gateways, there are 59 addresses usable. It should be enough for new computers coming into this room.

ECL2046 has 15 hosts and GCL1 has 33 hosts. Totally they have 48 hosts. With a block size of 64, there are still 59-48=11 usable addresses for new hosts. It should be enough for new computers brought by the lecturers for both classrooms. Given the room sizes of these two rooms, there can’t be more than 10 computers that can be added into these rooms.

An additional VLAN used for management and troubleshooting is created with a subnet assigned too. The following table shows the VLANs and their addressing:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **VLAN Number** | **Name** | **Network** | **Prefix** | **Default Gateway** |
| 10 | Loneragan3032 | 134.115.128.0 | 26 | 134.115.128.1 |
| 20 | ECL2044/2039 | 134.115.153.0 | 26 | 134.115.153.1 |
| 30 | GCL1/ECL2046 | 134.115.156.0 | 26 | 134.115.156.1 |
| 99 | Management | 134.115.1.0 | 24 | 134.115.1.1 |

Table - VLAN models

# Design

The design is outlined here and will be briefly explained.

* All links, devices and VLANs are given names and descriptions to make future design and maintenance easier.
* For the design model no console password is setup and the line console timeout is set to zero for only testing purposes. Logging synchronous is also enabled to make the network administrator free of mistaking inputs.
* For remote management, it is more secure to use Secure Shell (SSH) than telnet because the traffic can be encrypted. All devices are configured with domain name, crypto-graphical keys with 1024 bits and a username with password that is not encrypted yet for testing reason. The privilege level of the user is zero. Only SSH is accepted for Virtual Teletype (VTY) line as incoming traffic. The username and password will be used for SSH authentication. Privileged mode password is set up to allow remote management for different devices using SSH.
* The addressing scheme for each VLAN is that Distribution1 and Distribution2 use the second and the third usable addresses while the first usable addresses for each VLAN are reserved for the virtual gateways. The access switches will use the third to sixth usable addresses in management VLAN.
* All interfaces connecting to switches and the core router will be assigned bandwidths according to their interface types and the duplex type is set to full. These are configured as trunk ports manually so that they are trunk ports regardless of neighbors’ modes. They are also configured as non-negotiated so that no Dynamic Trunking Protocol (DTP) frame is generated and the neighbor switches must configure their trunk ports manually.
* There are three VLANs created on each switches other than data VLANs. A parking VLAN for interfaces not used, the management VLAN for troubleshooting and the native VLAN. All unused ports are assigned the parking VLAN and shutdown manually to avoid security violation using these ports. The native VLAN is consistent on all switches which is not any of the data VLANs to prevent VLAN hopping attack.
* The spanning tree mode is configured as Rapid per VLAN Spanning Tree (Rapid PVST+) to allow fast convergence of the whole switched network.
* Redundant cables between any two devices are configured as ether-channel to maximize the usage of bandwidths of these links. The channel protocol is Link Aggregation Control Protocol (LACP) which is Institute of Electrical and Electronics Engineers (IEEE) standard so that new switches from different vendors can accommodate the ether-channel to the distribution switches too. The interfaces must be shutdown first before configuring the ether-channel to prevent possible problems.
* All port-channels are configured as trunk ports manually and their native VLAN is consistent with that of the physical links. They are also configured as non-negotiate so that trunk ports must be configured manually. The distribution layer switches use 802.1Q trunking protocol which is IEEE standard to provide compatibility with the access layer switches.
* The VLAN Trunking Protocol (VTP) mode on all switches are configured as transparent mode so that none of them will affect others’ VLAN configuration and if new switches are introduced they won’t be affected either.



## Access Layer

* Because VTP is disabled by configuring as transparent mode, each access switch has its own set of data VLANs. None of them will be affected by other switches or affecting others’ VLAN configuration.
* Ports connected to hosts are configured as access ports manually to disable dynamic negotiation of trunk ports to prevent rogue switches or routers from negotiating trunk ports. These ports are assigned the VLANs the labs belong to so that hosts connecting to these ports will automatically obtain an IP address from Dynamic Host Configuration Protocol (DHCP) server that makes the hosts in that subnet.
* Access ports are configured with edge port feature for rapid PVST+ to allow them to enter forwarding mode directly so that clients can have immediate connectivity to the network after starting up. This feature also blocks data if a switch is connected to the port.
* Access ports are also configured with Bridge Protocol Data Unit (BPDU) Guard feature so that if users plug in new switches to these ports they will be in Error-disabled state and shut down until administrative intervention. This can prevent the Spanning-tree topology from being changed.
* Every access switch is given a default gateway which is a virtual address of the First Hop Redundancy Protocol (FHRP) group to allow failover. Each access switch is configured with only the data VLAN it is connected to so that traffic for other VLANs are pruned.
* The hosts are configured to use DHCP as means to obtain IP addresses so that when new hosts are introduced they can be free of manual configuration of IP addresses, subnet masks and default gateways. The Domain Name Service (DNS) server can also be configured automatically but for the model it is unnecessary to do so.
* Most traffic for the labs is for communicating between these labs and hosts outside the campus network. So the access switches should use source Media Access Control (MAC) address based load balancing in Ether-channel because they don't need to control the traffic received from the Ether-channel ports. They only need to control those being forwarded onto the Ether-channels and when several computers are sending traffic to the others this load-balancing method can evenly distribute the traffic onto the links in the port-channel. (Understanding Ether-Channel Load Balancing and Redundancy on Catalyst Switches, 2007)
* The port security is configured on access ports on all the access switches to prevent MAC table flooding attack. The maximum allowed number of hosts is set to 64 which is the same as the block size of all the subnets to allow more computers to be introduced into the labs. This is based on the assumption that the computers in each lab are connected to a hub connected to the switch's access port.

## Distribution Layer

* The two distribution layer switches are configured with all the VLANs to provide inter-VLAN routing and first hop redundancy. Routing is enabled on these switches.
* The trunking encapsulation protocol is 802.1Q which is IEEE standard providing compatibility with the access switches and switches manufactured by other vendors.
* The ports connecting to the core router are configured as routed ports with IP addresses assigned so that the links between distribution layer and core layer are routed because the router isn't aware of the VLANs.
* The root bridges of the four VLANs are distributed onto the two distribution layer switches. One is also the backup root bridge for the other in case of failure of the other switch. Traffic for different VLANs can be load balanced in this way.
* Hot Standby Redundancy Protocol (HSRP) is configured on all the data VLANs and the management VLAN to maintain availability in the case of failure on each of the distribution layer switches. The active routers for the VLANs are also distributed evenly onto the two switches by giving them corresponding priorities for load balancing. Switches with higher priorities can failback as the active routers too if they are up again by configuring them with pre-empt.
* A DHCP server is created for each data VLAN and they are distributed onto the two switches to provide load balancing. The first three addresses of the DHCP pool are excluded to avoid possible IP address conflict which delays the process of assigning IP addresses. The default gateways are set to the virtual IP addresses of the HSRP groups in different VLANs to provide first hop redundancy.
* Cisco Express Forwarding (CEF) is enabled as distributed mode which enables fast routing and switching by relieving the route processor from processing routing information.
* The link between the two distribution layer switches is configured as switch link because it can be free of routing for traffic travelling throughout the switched network. If there are thousands of packets travelling between the two switches every second the network latency for packets to go through the route processor and then the Application Specific Integrated Circuit (ASIC) is significant. So it is better to use switched network to avoid wasting CPU resources.
* Links connecting the distribution layer switches and the access layer switches are configured with spanning-tree root guard to prevent the access switches from becoming root bridges for any of the VLANs. The root bridge should be either of the distribution layer switches to provide fast network switching.
* The spanning-tree root bridge, DHCP server and the default active router in HSRP are on the same switch for a specific VLAN to shorten the network latency for the traffic from that VLAN.
* Open Shortest Path First (OSPF) is configured on both switches to exchange dynamic routing information with the core router. OSPF has the shortest convergence time and is IEEE standard so it is preferred. The area number is chosen as zero for modelling purpose only. Only directly connected network will be advertised so the wildcard masks are specified as such.
* The distribution switches should use destination MAC address based load balancing in Ether-channel because they only need to balance the load from the hosts outside the campus to the labs. Different hosts inside the same lab can be delivered with traffic balanced on the links in the same channel when traffic comes from the outside. The XOR method for load balancing should not be used either for MAC address or IP address because only the last bit will be used for XOR operation and if by accident many hosts in the same lab use the IP addresses or MAC address with the same last bit the load balancing is not working.

## Core Layer

* A loopback interface is created for testing purposes.
* OSPF advertises all directly connected networks to propagate and receive the routes to different networks.

## Other Features

Other technologies not supported in Packet Tracer including uplink fast and backbone fast are not compatible with Rapid PVST+. For FHRP it is also possible to use Virtual Router Redundancy Protocol (VRRP) and Gateway Load Balancing Protocol (GLBP). Though VRRP is IEEE standard which provides compatibility with products from other vendors and GLBP can provide better load balancing, HSRP is better because its convergence time is shortest which provides seamless network access to the clients. By assigning different priorities to the groups on different switches it also achieves the goal of load balancing.

# Recommendation

The author recommends network administrators to adopt this network model as a candidate for future network design because it has been fully tested to have met all the requirements. This report is a documentation of the design so it should be reviewed if the model were to be used. Protocols of public standard are preferred when designing the network. Redundancy, load balancing, fast convergence and scalability are crucial to network design.

# Conclusions

This report explained the five labs modelled during the project, the reasons for the structure chosen for the VLANs and the IP addressing of the network design. It also described the outline of the design including technologies used in access, distribution and core layers. Features not supported by Packet Tracer may not be compatible or good enough to be chosen in the design.

# Appendices



#### Distribution1 Configuration Commands

hostn Distribution1

lin c 0

exec-t 0

logg s

exi

ip domain-n lab.com

cryp ke ge rs

1024

usern admin pas cisco

lin v 0 4

logi l

tr in ss

ena se cisco

vt m tran

vl 5

na ParkingVLAN

vl 10

na Loneragan3032

vl 20

na ECL2039/2044

vl 30

na GCL1/ECL2046

vl 99

na Management

vl 100

na NativeVLAN

int vl10

ip add 134.115.128.2 255.255.255.192

int vl20

ip add 134.115.153.2 255.255.255.192

int vl30

ip add 134.115.156.2 255.255.255.192

int vl99

ip add 134.115.1.2 255.255.255.0

int r f0/1-2

des To ECL2044/2039

spe 100

dup ful

int r f0/3-4

des To Loneragan3032

spe 100

dup ful

int r f0/5-6

des To ECL2046

spe 100

dup ful

int r f0/7-8

des To GCL1

spe 100

dup ful

int g0/1

des To Core

spe 1000

dup ful

int g0/2

des To Distribution2

spe 1000

dup ful

exi

ip routi

int r f0/1-8, g0/2

sw tr en d

sw m tr

sw tr n vl 100

sw non

int g0/1

no sw

ip add 134.115.0.1 255.255.255.252

no sh

int r f0/9-24

sw m ac

sw ac vl 5

sh

exi

spa m rap

spa vl 10,99 r p

spa vl 20,30 r s

int vl10

sta 1 ip 134.115.128.1

sta 1 pri 150

sta 1 pre

int vl20

sta 1 ip 134.115.153.1

sta 1 pri 100

sta 1 pre

int vl30

sta 1 ip 134.115.156.1

sta 1 pri 100

sta 1 pre

int vl99

sta 1 ip 134.115.1.1

sta 1 pri 150

sta 1 pre

exi

ip dhc ex 134.115.128.1 134.115.128.3

ip dh po vlan10-dhcp

netw 134.115.128.0 255.255.255.192

def 134.115.128.1

exi

ip cef dis

int r f0/1-8

spa g r

sh

int r f0/1-2

channel-g 1 mo ac

int r f0/3-4

channel-g 2 mo ac

int r f0/5-6

channel-g 3 mo ac

int r f0/7-8

channel-g 4 mo ac

exi

port-chan loa dst-mac

int p1

sw tr en d

sw m tr

sw tr n vl 100

sw non

int p2

sw tr en d

sw m tr

sw tr n vl 100

sw non

int p3

sw tr en d

sw m tr

sw tr n vl 100

sw non

int p4

sw tr en d

sw m tr

sw tr n vl 100

sw non

router osp 1

net 134.115.128.0 0.0.0.63 a 0

net 134.115.153.0 0.0.0.63 a 0

net 134.115.156.0 0.0.0.63 a 0

net 134.115.1.0 0.0.0.255 a 0

net 134.115.0.0 0.0.0.3 a 0

int r f0/1-8

no sh

#### ECL2044/2039 Configuration Commands

hostn ECL2044/2039

lin c 0

exec-t 0

logg s

exi

ip domain-n lab.com

cryp ke ge rs

1024

usern admin pas cisco

lin v 0 4

logi l

tr in ss

ena se cisco

vtp m tr

vl 5

na ParkingVLAN

vl 20

na ECL2039/2044

vl 99

na Management

vl 100

na NativeVLAN

int vl99

ip add 134.115.1.4 255.255.255.0

int r f0/21-22

des To Distribution1

int r f0/23-24

des To Distribution2

exi

int r f0/21-24

dup ful

spe 100

sw m tr

sw tr n vl 100

sw non

int r f0/2-20,g0/1-2

sw m ac

sw ac vl 5

sh

int f0/1

sw m ac

sw ac vl 20

spa portfa

spa bp en

sw port

sw port max 64

exi

spa m ra

ip default-g 134.115.1.1

int r f0/21-24

sw tr al vl 20,99,100

sh

int r f0/21-22

channel-g 1 m ac

int r f0/23-24

channel-g 2 m ac

exi

port-chan loa src-mac

int p1

sw m tr

sw tr n vl 100

sw non

int p2

sw m tr

sw tr n vl 100

sw non

int r f0/21-24

no sh

#### Core Configuration Commands

hostn Core

lin c 0

exec-t 0

logg s

exi

ip domain-n lab.com

cryp ke ge rs

1024

usern admin pas cisco

lin v 0 4

logi l

tr in ss

ena se cisco

int g0/0

ip add 134.115.0.2 255.255.255.252

spe 1000

dup ful

no sh

int g0/1

ip add 134.115.0.5 255.255.255.252

spe 1000

dup ful

no sh

int l0

ip add 134.115.4.1 255.255.252.0

exi

router os 1

netw 134.115.0.0 0.0.0.3 a 0

netw 134.115.0.4 0.0.0.3 a 0

netw 134.115.4.0 0.0.3.255 a 0

# List of References

Understanding EtherChannel Load Balancing and Redundancy on Catalyst Switches. (2007) In *Cisco.com*. Retrieved May 14, 2015 from <http://www.cisco.com/c/en/us/support/docs/lan-switching/etherchannel/12023-4.html>

# Glossary

**Packet Tracer:** A network simulation program that allows students to experiment with network behavior

**Virtual Local Area Network**: Has the same attributes as a physical local area network (LAN), but it allows for end stations to be grouped together more easily even if they are not on the same network switch

**Access layer**: Where host computers and end users connect to the network

**Distribution layer**: Includes LAN-based routers and layer 3 switches

**Core layer**: Considered the backbone of the network and includes the high-end switches and high-speed cables such as fiber cable

**Cisco Certified Network Associates**: An associate-level Cisco Career certification

**Ethernet**: The most widely-installed local area network (LAN) technology

**Local VLAN**: VLANs grouped in the basis of geographic locations of computers

**End-to-end VLAN**: Computers are grouped as the same VLAN regardless of their physical locations

**Secure Shell**: A cryptographic (encrypted) network protocol for initiating text-based shell sessions on remote machines in a secure way

**Telnet**: An application protocol used on the Internet or local area networks to provide a bidirectional interactive text-oriented communication facility

**Virtual Teletype**: A command line interface that enables users to connect to the daemon using the Telnet protocol

**Duplex**: A point-to-point system composed of two connected parties or devices that can communicate with one another in both directions

**Dynamic Trunking Protocol**: A proprietary networking protocol developed by Cisco Systems for the purpose of negotiating trunking on a link between two VLAN-aware switches, and for negotiating the type of trunking encapsulation to be used

**Spanning Tree**: A network protocol that ensures a loop-free topology for any bridged Ethernet local area network

**Link Aggregation Control Protocol**: Provides a method to control the bundling of several physical ports together to form a single logical channel

**Institute of Electrical and Electronics Engineers**: World's largest association of technical professionals with more than 400,000 members in chapters around the world

**VLAN Trunking Protocol**: A Cisco proprietary protocol that propagates the definition of Virtual Local Area Networks (VLAN) on the whole local area network

**Dynamic Host Configuration Protocol**: A standardized network protocol used on Internet Protocol (IP) networks for dynamically distributing network configuration parameters

**Bridge Protocol Data Unit**: Frames that contain information about the Spanning tree protocol

**First Hop Redundancy Protocol**: A computer networking protocol which is designed to protect the default gateway used on a subnetwork by allowing two or more routers to provide backup for that address

**Domain Name Service**: An Internet service that translates domain names into IP addresses

**802.1Q**: The networking standard that supports virtual LANs (VLANs) on an Ethernet network

**Hot Standby Redundancy Protocol**: A Cisco proprietary redundancy protocol for establishing a fault-tolerant default gateway

**Cisco Express Forwarding**: An advanced layer 3 switching technology used mainly in large core networks or the Internet to enhance the overall network performance

**Application Specific Integrated Circuit**: A microchip designed for a special application, such as a particular kind of transmission protocol

**Open Shortest Path First**: Uses a link state routing algorithm and falls into the group of interior routing protocols, operating within a single autonomous system

**Virtual Router Redundancy Protocol**: Eliminates the single point of failure inherent in the static default routed environment

**Gateway Load Balancing Protocol**: A Cisco proprietary protocol that attempts to overcome the limitations of existing redundant router protocols by adding basic load balancing functionality

# Index

8

802.1Q, 6, 8, 22

A

Access layer, V, 1, 6, 8

Active router, 8

Application Specific Integrated Circuit, 8, 22

ASIC. *See* Application Specific Integrated Circuit

B

Backbone fast, 9

BPDU. *See* Bridge Protocol Data Unit

Bridge Protocol Data Unit, 7, 21

C

CCNA

Cisco Certified Network Associates, 1

CEF. *See* Cisco Express Forwarding

Cisco

Certified Network Associates, 1, 21

Packet Tracer, V, 1

Cisco Express Forwarding, 8, 22

Core layer, V, 1, 8

Crypto-graphical key, 6

D

DHCP. *See* Dynamic Host Configuration Protocol

Distribution layer, 1, 4, 5, 6, 7, 8

DNS. *See* Domain Name Service

Domain name, 6

Domain Name Service, 7, 22

DTP

Dynamic Trunking Protocol, 6

Duplex, 6

Dynamic Host Configuration Protocol, 7, 21

Dynamic Trunking Protocol, 6, 21

E

End-to-end VLAN, 4

Ether-channel, 6

Ethernet, 1, 21, 22

F

FHRP. *See* First Hop Redundancy Protocol

First Hop Redundancy Protocol, 7, 22

G

Gateway Load Balancing Protocol, 9, 22

GLBP. *See* Gateway Load Balancing Protocol

H

Hot Standby Redundancy Protocol, 8, 22

HSRP. *See* Hot Standby Redundancy Protocol

I

IEEE. *See* Institute of Electrical and Electronics Engineers

Institute of Electrical and Electronics Engineers, 6, 21

Inter-VLAN routing, 7

L

LACP. *See* Link Aggregation Control Protocol

Link Aggregation Control Protocol, 6, 21

Load balancing

destination MAC address based, 8

source MAC based, 7

XOR, 8, 9

Local VLAN, 4

Loopback interface, 9

M

Mode

distributed, 8

forwarding, 7

O

Open Shortest Path First, 8, 22

OSPF. *See* Open Shortest Path First

P

Port-channel, 6

Privilege level, 6

R

Rapid per VLAN Spanning Tree, 6

Rapid PVST+. *See* Rapid per VLAN Spanning Tree

Root bridge, 8

S

Secure Shell, 6, 21

SSH

Secure Shell, 6

State

Error-disabled, 7

T

Three-layer architecture, 1

U

Uplink fast, 9

V

Virtual gateway, 5

Virtual Local Area Network, 1, 21

Virtual Router Redundancy Protocol, 9, 22

Virtual Teletype, 6, 21

VLAN. *See* Virtual Local Area Network

hopping, 6

management, 6, 8

native, 6

parking, 6

VLAN Trunking Protocol, 6, 21

VRRP. *See* Virtual Router Redundancy Protocol

VTP. *See* VLAN Trunking Protocol

VTY. *See* Virtual Teletype