

CST-502 : Advanced Networking

First Semester

Text Book : INTERNETWORKING WITH TCP/IP PRINCIPLES, PROTOCOLS, AND ARCHITECTURE (Vol 1, 6th Edition; Douglas E. Comer)

Period : 23 periods for 15 weeks (4 periods/week) (Lecture + Lab)

Course Description

Internetworking with TCP/IP course is to provide the TCP/IP Internet from the viewpoint of a single host, showing the protocols a host contains and how they operate. It also covers the Internetworking concept and architectural model, Internet addressing, Multi-Protocol Label Switching, Network virtualization, Application level services available in the Internet (including network management), network security, and the Internet of Things.

Course Objectives

Upon completing this module, you should be able to:

- Calculate and assign the IPv4 and IPv6 addresses in your site
- Understand the technology using switching with IP
- Discuss the network virtualization and NAT
- Debate the policy of network security and packet filtering of firewall

Upon completing of this course, students should be able to understand the internet abstraction, the notion of protocol layering, the basics of Internet addressing and forwarding, transport protocols and network security.

Assessment Plan for the Course

Paper Exam:	30%
Attendance:	5%
Test/ Quiz:	5%
Lab:	5%

Lab Test:

5%

No.	Chapter	Page	Detail Lecture Plan
	Chapter 3 Internetworking Concept And Architectural Model	35-42	
1.	3.1 Introduction		
2.	3.2 Application-Level Interconnection		
3.	3.3 Network-Level Interconnection		
4.	3.4 Properties Of The Internet		
5.	3.5 Internet Architecture		
6.	3.6 Interconnection Of Multiple Networks With IP Routers		
7.	3.7 The User' View		
	Chapter 5 Internet Addressing	69-97	
8.	5.1 Introduction		
9.	5.2 Universal Host Identifiers		
10.	5.3 The Original IPv4 Classful Addressing Scheme		
11.	5.4 Dotted Decimal Notation Used With IPv4		
12.	5.5 IPv4 Subnet Addressing		
13.	5.6 Fixed Length IPv4 Subnets		
14.	5.7 Variable-Length IPv4 Subnets		
15.	5.8 Implementation Of IPv4 Subnets With Masks		
16.	5.9 IPv4 Subnet Mask Representation And Slash Notation		
17.	5.10 The Current Classless IPv4 Addressing Scheme		
18.	5.11 IPv4 Address Blocks And CIDR Slash Notation		
19.	5.12 A Classless IPv4 Addressing Example		
20.	5.13 IPv4 CIDR Blocks Reserved For Private Networks		
21.	5.14 The IPv6 Addressing Scheme		
22.	5.15 IPv6 Colon Hexadecimal Notation		
23.	5.16 IPv6 Address Space Assignment		
24.	5.17 Embedding IPv4 Addresses In IPv6 For Transition		
25.	5.18 IPv6 Unicast Addresses And /64		

No.	Chapter	Page	Detail Lecture Plan
26.	5.19 Ipv6 Interface Identifiers And MAC Addresses		
27.	5.20 IP Addresses, Hosts, And Network Connections		
28.	5.21 Special Addresses		
29.	5.22 Weaknesses In Internet Addressing		
30.	5.23 Internet Address Assignment And Delegation Of Authority		
	Chapter 16 Label Switching, Flows, And MPLS	353-365	
31.	16.1 Introduction		
32.	16.2 Switching Technology		
33.	16.3 Flows And Flow Setup		
34.	16.4 Large Networks, Label Swapping, And Paths		
35.	16.5 Using Switching With IP		
36.	16.6 IP Switching Technologies And MPLS		
37.	16.7 Labels And Label Assignment		
38.	16.8 Hierarchical Use Of MPLS And A Label Stack		
39.	16.9 MPLS Encapsulation		
40.	16.10 Label Semantics		
41.	16.11 Label Switching Router		
42.	16.12 Control Processing And Label Distribution		
43.	16.13 MPLS And Fragmentation		
44.	16.14 Mesh Topology And Traffic Engineering		
	Chapter 19 Network Virtualization: VPNs, NATs, And Overlays	399-411	
45.	19.1 Introduction		
46.	19.2 Virtualization		
47.	19.3 Virtual Private Networks (VPNs)		
48.	19.4 VPN Tunneling And IP-in-IP Encapsulation		
49.	19.5 VPN Addressing And Forwarding		
50.	19.6 Extending VPN Technology To Individual Hosts		
51.	19.7 Using A VPN With Private IP Addresses		
52.	19.8 Network Address Translation (NAT)		
53.	19.9 NAT Translation Table Creation		
54.	19.10 Variant Of NAT		
55.	19.11 An Example Of NAT Translation		
56.	19.12 Interaction Between NAT And ICMP		

No.	Chapter	Page	Detail Lecture Plan
	Chapter 29 Internet Security And Firewall Design (IPsec, SSL)	605-620	
57.	29.1 Introduction		
58.	29.2 Protecting Resources		
59.60.	29.3 Information Policy		
61.	29.4 Internet Security		
62.	29.5 IP Security (IPsec)		
63.	29.6 IPsec Authentication Header		
64.	29.7 Security Association		
65.	29.8 IPsec Encapsulating Security Payload		
66.	29.9 Authentication And Mutable Header Fields		
67.	29.10 IPsec Tunneling		
68.	29.11 Required Security Algorithms		
69.	29.12 Secure Socket Layer (SSL and TLS)		
70.	29.13 Firewalls And Internet Access		
71.	29.14 Multiple Connections And Weakest Links		
72.	29.15 Firewall Implementation And Packet Filters		
73.	29.16 Firewall Rules And The 5-Tuple		
74.	29.17 Security And Packet Filter Specification		
75.	29.18 The Consequence Of Restricted Access For Clients		
76.	29.19 Stateful Firewalls		
77.	29.20 Content Protection And Proxies		
78.	29.21 Monitoring And Logging		
	Practical		
79.	Point-to-Point GRE Tunneling		
80.	Basic Site-to-Site IPsec VPN		
	Lab Assessment I		
81.	Configuring Port Address Translation (PAT)		
82.	Basic Configuration of Cisco ASA Firewall		
	Lab Assessment II		