Revised 1/2018

NOVA COLLEGE-WIDE COURSE CONTENT SUMMARY
ITN 208 – PROTOCOLS AND COMMUNICATIONS TCP/IP (4 CR.)

Course Description

Centers on providing an understanding of the TCP/IP suite and the details of its implementation. The details of implementation are treated by discussing IP addressing, the structure of frames and protocol headers that enable communication between two computers. Discusses IP routing, tunneling, SNMP, and security. Lecture 4 hours per week.

General Course Purpose

This course provides a comprehensive foundation in understanding the family of TCP/IP protocols, which are the essence of how majority of devices communicate today over the LAN and WAN networks, including the Internet. Students will be able to capture and interpret network traffic using a protocol analyzer. Most current or future IT professionals should know about these protocols, especially network engineers, network administrators, security analysts, network forensic analysts and many others. Information is this course provides foundation for most networking related industry certifications, like Network+, Security+, CCNA and many others.

Course Prerequisites/Corequisites

Prerequisite: ITN 100 or ITN 101. Students must be able to read and write at a college level.

Course Objectives

Upon completion of this course, the student will be able to:

a) Understand the function of the essential TCP/IP protocols used today in wide and local area networks.
b) Use software protocol analyzer to capture and network traffic
c) Interpret network traffic captured with protocol analyzer in the context of the learned protocols.
d) Troubleshoot basic network problems including.
e) Understand, recognize and prevent common security issues of TCP/IP protocols.

Major Topics to be Included:

a) TCP/IP overview
b) OSI and Internet networking models
c) Protocol Analysis
d) Addressing
e) Routing - RIP, OSPF
f) Network diagnosis and control - ICMP
g) Interface configuration - DHCP
h) Name Resolution - DNS
i) Transport protocols - TCP, UDP
j) Transition from IPv4 to IPv6
k) Network Security

Student Learning Outcomes:

1. TCP/IP overview
   1.1. Describe TCP/IP's origins.
   1.2. Explain the basic packet structure.
   1.3. Explain the process of protocol encapsulation.
   1.4. Explain the purpose of various fields in packet headers.
   1.5. Describe the process of TCP/IP standardization (RFC)
   1.6. Explain the differences between v4 and v6
2. OSI and Internet networking models
   2.1. Describe the OSI and Internet networking models.
   2.2. Explain the difference between the models.
   2.3. Link the TCP/IP functions to the model layers.
3. Protocol Analysis
   3.1. Describe the purpose and basic functions of protocol analysis
   3.2. Understands how protocol analyzer works and how to deploy it.
   3.3. Use protocol analyzer Wireshark.
4. Addressing
   4.1. Describe IP addressing.
   4.2. Explain and compare the difference between v4 and v6 addressing
   4.3. Explain the difference between public and private addresses.
   4.4. Explain conventional class-full and classless (CIDR) addressing.
   4.5. Explain and apply subnetting and designs.
   4.6. Explain supernetting designs.
5. Routing - RIP, OSPF
   5.1. Explain the mechanics of IP routing,
   5.2. Classify exterior and interior routing protocols.
   5.3. Describe and compare RIP and OSPF routing protocols.
   5.4. Explain and compare the difference between v4 and v6 routing.
   5.5. Use network protocol analyzer to decode routing protocol packets.
6. Network diagnosis and control – ICMP
   6.1. Explain the basics of the Internet Control Message Protocol (ICMP) and the roles it plays on networks.
   6.2. Explain how Path MTU Discovery operates.
   6.3. Understand the general differences between ICMPv4 and ICMPv6
   6.4. Use network protocol analyzer to decode routing protocol packets.
   6.5. Able to use utilities PING, PATHPING, TRACEROUTE to troubleshoot.
7. Interface configuration – DHCP
   7.1. Describe the basic DHCP services.
   7.2. Explain the DHCP Discovery, renewal, and release processes
   7.3. Describe the difference between broadcast, unicast and multicast.
   7.4. Describe relay agent communications.
   7.5. Use network protocol analyzer to decode DHCP protocol packets.
   7.6. Describe Neighbor Discovery in IPv6 and how it compares to ARP in IPv4
8. Name Resolution – DNS
   8.1. Describe name resolution protocols DNS and LLMNR.
   8.2. Describe how forward and reverse mapping works.
   8.3. Describe different type of DNS servers.
   8.4. Use network protocol analyzer to decode DNS protocol packets.
   8.5. Able to use utilities NBTSTAT, NETSTAT and NSLOOKUP to troubleshoot.
9. Transport protocols - TCP, UDP
   9.1. Explain the differences between connectionless and connection-oriented transport mechanisms.
   9.2. Understand the three way handshake procedure.

9.3. Compare transport protocols in v4 and v6.
9.4. Use network protocol analyzer to decode TCP and UDP protocol packets.

10. Transition from IPv4 to IPv6
    10.1. Describe the various methods that allow IPv4 and IPv6 networks to interact.
    10.2. Explain how an IPv6 transition address works
    10.3. Describe the different tunneling configuration types and their device interactions
    10.4. Explain IPv6 deployment requirements and considerations.
11. Network Security
    11.1. Explain basic concepts and principles for maintaining computer and network security.
    11.2. Recognize key security weaknesses in TCP/IP architecture and how to prevent them.
    11.3. Explain how VPN protocols work.
    11.4. Explain how basic types of firewalls work.

Required Time Allocation per Topic

In order to standardize the core topics of ITN 208 so that a course taught at one campus is equivalent to the same course taught at another campus, the following student contact hours per topic are required. Each syllabus should be created to adhere as closely as possible to these allocations. Of course, the topics cannot be followed sequentially. Many topics are taught best as an integrated whole, often revisiting the topic several times, each time at a higher level. There are normally 60 student-contact-hours per semester for a four credit course. (This includes 15 weeks of instruction and does not include the final exam week so 15* 4 = 60 hours. Sections of the course that are given in alternative formats from the standard 16 week section still meet for the same number of contact hours.) The final exam time is not included in the time table. The category, Other Optional Content, leaves ample time for an instructor to tailor the course to special needs or resources.

Topic:	**Time in Hours:**	**Percentages:**
TCP/IP overview	2	3%
OSI and Internet networking models	2	3%
Protocol Analysis	6	10%
Addressing	4	7%
Routing - RIP, OSPF	4	7%
Network diagnosis and control - ICMP	4	7%
Interface configuration - DHCP	6	10%
Name Resolution - DNS	6	10%
Transport protocols - TCP, UDP	6	10%
Transition from IPv4 to IPv6	4	7%
Network Security	6	10%
Other optional content	4	7%
Exams and quizzes	6	10%
Total:	**60**	**100%**