CPNT 219 - Introduction to Networks

Course Description:

This course introduces learners to network terminology, devices, standards, and different networking protocols. Learners will gain a practical understanding on how networks operate and how to build small networks using different network devices and implement Internet Protocol (IP).

3 Credits

Time Guidelines:

The standard instructional time for this course is 75 hours.

Course Assessment:

Quizzes	5%
Assignments	35%
Project	35%
Final Exam	25%
Total:	100%

Other Course Information:

Learner Engagement:

In order to be successful, the learner is expected to be engaged in learning activities for a total of 9 to 12 learning hours per course per week, which includes both in-class and out-of-class time.

SAIT Policies and Procedures:

For information on the SAIT Grading Scale, please visit policy AC 3.1.1 Grading Progression Procedure, found on the SAIT Academic Policies and Procedures page: https://www.sait.ca/about-sait/administration/policies-and-procedures

For information on SAIT Academic Policies, please visit: www.sait.ca/about-sait/administration/policies-and-procedures/academic-student

Optional Reference Publication(s):

Kozierok, C. (2005). *The TCP/IP Guide: A Comprehensive, Illustrated Internet Protocols Reference*. No Starch Press.

Course Learning Outcome(s):

1. Describe advances in modern networking technology.

   Objectives:

1.1 Explain how networks affect our daily lives.

1.2 Explain how different devices are used in a network.

1.3 Explain how network representations are used in network topologies.

1.4 Explain how area networks connect to the internet.

1.5 Describe the four basic requirements of a reliable network.

2. Configure initial settings on network devices.

Objectives:

2.1 Explain how to access a Cisco IOS device for configuration purposes.

2.2 Explain how to navigate Cisco IOS software to configure network devices.

2.3 Describe the command structure of Cisco IOS software.

2.4 Explain how devices communicate across network media.

2.5 Configure a host device with an IP address.

2.6 Demonstrate how to verify connectivity between two end devices.

3. Explain how network protocols enable devices to access network resources.

Objectives:

3.1 Describe the rules required to successfully communicate in a network.

3.2 Explain why protocols are necessary in network communication.

3.3 Explain the purpose of adhering to a protocol suite.

3.4 Explain the role of standards organizations in establishing protocols for network interoperability.

3.5 Explain how the TCP/IP model and the OSI model are used to facilitate standardization in the communication process.

3.6 Explain how data encapsulation allows data to be transported across the network.

3.7 Explain how local hosts access local resources on a network.

4. Explain how the physical layer supports communications across data networks.

Objectives:

4.1 Describe the function of the physical layer in the network.

4.2 Describe the characteristics of the physical layer.

4.3 Identify the essential components of copper cabling.

4.4 Explain how UTP (unshielded twisted pair) cable is used in Ethernet networks.

4.5 Describe the advantages of fibre optic cabling over other media.

4.6 Demonstrate how to connect devices using wired and wireless media.

5. Explain how media access control in the data link layer supports communication across networks.

Objectives:

5.1 Calculate numbers between decimal, binary and hexadecimal systems.

5.2 Describe the purpose and function of the data link layer in preparing communication for transmission on specific media.

5.3 Compare the characteristics of media access control methods on WAN and LAN topologies.

5.4 Describe the characteristics and functions of the data link frame.

6. Explain how Ethernet operates in a switched network.

Objectives:

6.1 Relate Ethernet sublayers to frame fields.

6.2 Describe the components of an Ethernet MAC address.

6.3 Explain how a switch builds its MAC address table and forwards frames.

6.4 Describe switch forwarding methods available on Layer 2 switch ports.

7. Explain how routers use network layer protocols and services to enable end-to-end connectivity.

Objectives:

7.1 Explain how the network layer uses IP protocols for reliable communications.

7.2 Explain the role of the major header fields in the IPv4 packet.

7.3 Explain the role of the major header fields in the IPv6 packet.

7.4 Explain how network devices use routing tables to direct packets to a destination network.

7.5 Explain the function of fields in the routing table of a router.

7.6 Configure initial settings on a Cisco IOS router.

7.7 Configure two active interfaces on a Cisco IOS router.

7.8 Configure devices to use the default gateway.

8. Explain how address protocols enable communication on a network.

Objectives:

8.1 Compare the roles of MAC addresses and IP addresses.

8.2 Describe the purpose of ARP (address resolution protocols).

8.3 Describe the operation of IPv6 ND (neighbour discovery).

9. Calculate an IPv4 subnetting scheme to efficiently segment a network.

Objectives:

9.1 Describe the structure of an IPv4 address.

9.2 Explain types of IPv4 addresses.

9.3 Calculate IPv4 subnets.

9.4 Explain how to create a flexible addressing scheme using variable length subnet masking (VLSM).

9.5 Demonstrate how to implement a VLSM addressing scheme.

10. Implement an IPv6 addressing scheme.

    Objectives:

        10.1 Explain the need for IPv6 addressing.

        10.2 Compare types of IPv6 network addresses.

        10.3 Explain how to configure static global unicast and link-local IPv6 network addresses.

        10.4 Explain how to configure global unicast addresses dynamically.

        10.5 Configure link-local addresses dynamically.

        10.6 Identify IPv6 addresses.

        10.7 Demonstrate how to implement a subnetted IPv6 addressing scheme.

11. Use tools to test network connectivity.

    Objectives:

        11.1 Explain how ICMP (Internet Control Message Protocol) is used to test network connectivity.

        11.2 Use ping to test network connectivity.

        11.3 Use traceroute utilities to verify a network's path.

12. Compare the operation of transport layer protocols in supporting end-to-end communication.

    Objectives:

        12.1 Explain the purpose of the transport layer in managing the transmission of data in end-to-end communication.

        12.2 Explain characteristics of the TCP (Transmission Control Protocol).

        12.3 Explain characteristics of the UDP (User Datagram Protocol).

        12.4 Explain how transport layer protocols use port numbers.

        12.5 Explain how TCP session establishment and termination processes facilitate reliable communication.

        12.6 Explain how TCP protocol data units are transmitted and acknowledged to guarantee delivery.

        12.7 Describe the UDP client processes to establish communication with a server.

13. Explain the operation of application layer protocols in supporting end-user applications.

    Objectives:

        13.1 Explain how the application layer, session layer and presentation layer work together to provide network services to end-user applications.

        13.2 Explain how end-user applications operate in a peer-to- peer network.

        13.3 Explain how web and email protocols operate.

        13.4 Explain how DNS (domain name system) and DHCP (dynamic host configuration protocol) operate.

        13.5 Explain how FTP (file transfer protocol) operates.

14. Configure network devices with hardening features to enhance security.

    Objectives:

14.1 Explain why basic security measures are necessary on network devices.

14.2 Identify security vulnerabilities.

14.3 Identify general mitigation techniques.

14.4 Configure network devices hardening features to mitigate security threats.

15. Implement a network design on a small network.

Objectives:

15.1 Identify devices used in small networks.

15.2 Identify the protocols and applications used in small networks.

15.3 Explain how a small network serves as the basis of larger networks.

15.4 Use the output of the ping and tracert (traceroute) commands to verify connectivity and establish relative network performance.

15.5 Use host and IOS commands to acquire information about the devices in a network.

15.6 Describe common network troubleshooting methodologies.

15.7 Troubleshoot issues with devices in a network.