CONESTOGA

COURSE OUTLINE

Course Technology Infrastructure: Networking (2013-2014)

Code / Version INFO1380 (101)

Total Hours 45

Credits 3

PreRequisite(s)

CoRequisite(s)

Course Description

This course will provide the student with the knowledge to conduct meaningful dialogue with the network specialists who design, install and maintain the network within their organization. The student will be introduced to broad networking concepts including protocols, topologies, transmission media and security, using hands-on examples of networking issues.

PLAR Eligible: Yes

Course Outcomes

Successful completion of this course will enable the student to:

1. Relate hardware and protocols in a network to layers of the OSI Model and the TCP/IP model.
2. Discuss the physical topologies found in a network, explaining their relative advantages and disadvantages.
3. Use crimpers, punch-down tools and cable meters to create, test and troubleshoot network cabling.
4. Identify the hardware used in a network and the function of each, relative to its standing in the protocol stack.
5. Discuss wide area networking topologies and transmission methods.
6. Explain how addressing is structured and used in IPv4, including subnetting and inter-network communication.
7. Configure dynamic routing to show how it works and to demonstrate how it is self-healing.
8. Use users and groups to permit or deny access to files and folders on a server.
9. Configure and secure a wireless access point.
10. Use command-line tools to troubleshoot a network.
11. Explain mechanisms to protect a network from physical failure or malicious attacks.

Unit Outcomes

Successful completion of the following units will enable the student to:

1.0 Networks, Network Standards and the OSI Model

- 1.1 Discuss how networks are used to benefit businesses and individuals.
- 1.2 Differentiate between binary, digital and analogue systems, and explain how analogue systems can use digital sequences to transmit binary data.
- 1.3 Explain how letters and symbols can be conveyed in a binary system.
- 1.4 Explain why layering is required in the OSI model.
- 1.5 Identify and describe the purpose of each of the 7 layers of the OSI model.
- 1.6 Explain what encapsulation is and how it is used in the OSI model.

2.0 TCP/IP Protocol Stack

- 2.1 Relate layers in the TCP/IP protocol to the corresponding ones in the OSI model.
- 2.2 Explain how addressing and name resolution functions in a TCP/IP network.

2.3 Demonstrate the use of applications to help troubleshoot problems with TCP/IP such as ping, ipconfig or ifconfig.

2.4 Identify various applications and services commonly used in networks and argue which layer they pertain to.

3.0 Layer 1 – Physical

3.1 Describe the common physical topologies in LANs: bus, ring, star, star-bus and backbone.

3.2 List the devices that function at layer-1 and the functionality each provides in a network.

3.3 Give an example of baseband signalling and how media distances affect it through attenuation.

3.4 Identify the media (cabling) used in LANs (coax, twisted-pair, fibre), their grades (CAT5, 5e, 6), characteristics (plenum/riser, UTP, STP) and capabilities.

3.5 Define radio frequency interference (RFI) and electro-magnetic interference (EMI) and how to mitigate their effects.

3.6 Define a ground loop in STP and how to avoid it.

3.7 Make both straight-through and cross-over patch cables using twisted-pair and explain when each is used.

3.8 Use crimping and punch-down tools to wire the components of a structured wiring layout (patch cables, modular wall jacks, BIX panels).

3.9 Test and troubleshoot cables using cable meters.

4.0 Layer 2 – Data Link

4.1 List the devices at OSI layer-2 and describe how they use frame information such as the MAC address to make decisions.

4.2 Describe how layer-2 protocols such as token ring, Ethernet (CSMA/CD) and AppleTalk/wireless (CSMA/CA) control traffic flow on a LAN.

4.3 Define collision and broadcast domains and how layer-2 devices can improve traffic loads.

4.4 Describe how twisted-pair cabling and switches enable full-duplex transmission and how this can improve network transmission rates.

4.5 Explain the benefit of the spanning tree protocol in a multi-path environment.

4.6 Explain how port mirroring or spanning is used to monitor traffic.

4.7 Describe the advantages of PoE when deploying network devices, such as wireless bridges and access points.

5.0 Layer 3 – Network

5.1 List the devices that function at layer-3 and describe how they are used in conjunction with (and in contrast to) layer-2 devices.

5.2 Discuss what a VLAN is, its impact on LAN broadcasts and security, and why routers or layer-3 switches are required.

5.3 Describe how IPv4 addressing works:

5.3.1 Define the terms bit, byte, octet and hex.

5.3.2 Describe the major classes in IP addressing and why they were used.

5.3.3 Describe the function of the network mask and use it to subnet an IP address range.

5.3.4 Define and describe the use of private vs public subnets, reserved subnets and reserved addresses within a subnet.

5.3.5 Describe what a default gateway is used for and provide examples of how it is used in a network, along with the limitations on its IP address.

5.3.6 Describe what dynamic host configuration protocol (DHCP) provides to a network and how to configure a DHCP service.

5.3.7 Describe how the domain name service (DNS) functions on the Internet.

5.3.8 Contrast features of IPv6 to IPv4.

5.4 Give some examples of the layer-3 protocol ICMP.

5.5 Describe how each of the following commands would be used to troubleshoot an IP network: ping, tracert, ipconfig, arp, nslookup, route, netstat, hostname.

5.6 Use netsh to query, alter and deploy network settings: http://lantoolbox.com/articles/netsh-tips-and-tricks-for-network-administrator/

5.7 Describe how sniffers and scanners are used in a network to do troubleshooting or to hack traffic for malicious use.

6.0 Layer 4 – Transport

- 6.1 Differentiate between TCP and UDP protocols and provide examples when one or the other would be preferable.
- 6.2 Describe the need for TCP & UDP ports in a protocol stack, both at the source and destination.
- 6.3 Describe how network address translation (NAT) works in a network and how it provides rudimentary security when combined with stateful inspection.

7.0 Application Layer

- 7.1 List and describe the use of the common application-layer protocols such as HTTP, HTTPS, FTP, telnet, DNS, SMTP, SNMP, etc.
- 7.2 List and describe common services provided by servers, such as: firewall, database server, proxy server, file server, mail server, directory server, certificate server, web server, application/transaction server, RRAS server.
- 7.3 Describe how the port number is used by Port Address Translation (PAT, or NAT Overload) to allow multiple computers on a network to use one public address to access the Internet.
- 7.4 Use telnet to configure a router and TFPT to load or save its configuration.

8.0 Routing

- 8.1 Differentiate between link-state, distance-vector and hybrid routing protocols and identify the major ones.
- 8.2 Provide examples of where static or dynamic routing would be preferable.
- 8.3 Explain, using examples, how a mesh router topology is “self-healing”.
- 8.4 Program a Cisco router’s interfaces, routing protocols, and access control lists using IOS.

9.0 Wireless

- 9.1 Describe the evolution, capabilities and interoperability of the current Wi-Fi protocols 802.11a/b/g/n/ac.
- 9.2 Define SSID, how it’s used in a network and the implications of beaconing.
- 9.3 Differentiate between open and shared-key authentication based on their inherent security implications.
- 9.4 Discuss how the major wireless security protocols work, their strengths and their weaknesses (WEP, WPA, WPA2, RADIUS, TKIP).
- 9.5 Differentiate between an access point, a bridge and a repeater in a wireless infrastructure.
- 9.6 Discuss current trends in wide-area or metro-area wireless technologies.

10.0 Authentication & Access Control

- 10.1 Explain why encryption has become more important over time.
- 10.2 Describe how the major encryption mechanisms (VPN, PPTP, SSL, IPsec, L2TP) work and how algorithms like AES, DES/3DES and Diffie-Hellman contribute to them.
- 10.3 Create users and groups on a server and control their access to files and folders.

11.0 Threats & Security

- 11.1 Methodically classify network assets and the risks they are subject to.
- 11.2 Explain how to strengthen a network against intrusion using firewalls, IDS, DMZ, VLAN zones, subnets, etc.
- 11.3 Classify malware such as worms, viruses, spyware, adware, Trojans, logic bombs, etc. according to how they spread and the damage they can inflict.
- 11.4 Detail actions to minimise the exposure to malware and to deal with an infection.
- 11.5 Describe how to physically protect network assets and to reduce staff risks.
- 11.6 Plan backup and disaster recovery strategies.

12.0 Wide Area Networks (WAN)

- 12.1 Contrast a point-to-point protocol such as dial-up with TCP/IP.
- 12.2 Discuss pros and cons of a leased-line WAN to a shared (Internet) WAN.
- 12.3 Discuss the technological differences between WAN and LAN technologies such as packet-switched, circuit-switched, broadband multiplexing vs. baseband, etc.

12.4 Explain how analog technologies are used as a digital system to send binary data.

12.5 Describe the protocols and capabilities of various WAN technologies such as T1, SONET, ATM and frame-relay.

12.6 Explain how wireless technologies are becoming viable WAN or MAN media.

13.0 Troubleshooting

13.1 Discuss a formal methodology for troubleshooting network problems.

13.2 Describe some hardware and software tools used in troubleshooting networks.

13.3 List symptoms and common sources of network problems.

Required Student Resources

Lammle, Todd. Comp TIA Network+ Study Guide: Exam N10-005 (2). Sybex.

Optional Student Resources

Evaluation

The minimum passing grade for this course is 55 (D).

In order to successfully complete this course, the student is required to meet the following evaluation criteria:

Tests	60.00
In-class lab exercises	40.00
	100.00 %

A passing grade in both the test and quizzes/labs portion independently is required in order to attain standing in this course. If the student fails one or both portions, then the lowest failing mark is submitted.

Other

Conestoga College is committed to providing academic accommodations for students with documented disabilities. Please contact the Accessibility Services Office.

Prepared By Dave Turton

School Information Technology

Date 2014-01-02