COURSE NET3100: NETWORK MEDIA & DEVICES, SECURITY

Level: Advanced

Prerequisite: None

Description: Students develop an understanding of different connectivity strategies for linking computers and security devices in a local area network (LAN). They acquire knowledge of industry standards for network cables and gain practical experience through installing cabling, connectors and other hardware components.

Parameters: Designed to be delivered in conjunction with other intermediate and advanced level courses in computer networking systems. Schools have the option of delivering courses in conjunction with one or more project courses if they wish to extend learning and/or address other specific technologies.

Access to an appropriate computer work station, the Internet, networking hardware, software and tools, and consumable supplies.

Access to instruction from an individual with specialized knowledge and skills in computer networking.

Particular emphasis is placed on Institute of Electrical and Electronics Engineers (IEEE) standards for cabling, and on safe procedures for preparing and connecting network media and devices. Students model and assume personal responsibility for ethical behaviour in their use of networking technologies and in their access to electronic sources of information. They also demonstrate an understanding of industry-based policies regarding network use and security.

Supporting Course: NET2020: Workstation Technology & Operations

Outcomes: The student will:

1. **identify and describe the characteristics, standard names and applications for common network media and connectors**
   1.1 identify and describe the structural components and uses of major types of network cables including:
      1.1.1 coaxial; e.g., thick, thin
      1.1.2 twisted pair; e.g., unshielded, shielded
      1.1.3 fibre optic
   1.2 identify and describe the characteristics and uses of common media connectors including:
      1.2.1 registered jack 11 (RJ-11)
      1.2.2 registered jack 45 (RJ-45)
      1.2.3 attachment unit interface (AUI)
      1.2.4 British naval connector (BNC)
      1.2.5 small computer system interface (SCSI)
      1.2.6 single mode fibre optic connector; e.g., SC-type, ST-type

1.3 identify IEEE standards for Ethernet cabling including:
 1.3.1 bandwidth/speed
 1.3.2 transmission mode
 1.3.3 maximum segment length
 1.3.4 cable type

1.4 identify and describe categories for unshielded twisted pair cable defined by the Electronics Industries Alliance and the Telecommunications Industry Association

1.5 describe the media and function of network backbones and segments

1.6 explain the relationship between media type, connector and topology in a network environment

1.7 choose an appropriate cable type and connector to add a client, given a practical network scenario

2. identify and explain the purpose, features and basic operation of network hardware components

2.1 explain the purpose of hardware components in:
 2.1.1 connecting network devices
 2.1.2 boosting data signals
 2.1.3 determining data flow

2.2 demonstrate an understanding of the features, functionality and performance of basic hardware components including:
 2.2.1 network interface card
 2.2.2 hub
 2.2.3 repeater
 2.2.4 switch
 2.2.5 bridge
 2.2.6 router
 2.2.7 gateway
 2.2.8 wireless access point
 2.2.9 modem

3. demonstrate knowledge of cabling tools and demonstrate the ability to install network cabling, connectors and hardware components

3.1 identify layers of the open system interconnection (OSI) reference model at which specific hardware components operate

3.2 describe the features and functionality of power fault-tolerance hardware such as:
 3.2.1 surge suppressor
 3.2.2 power line conditioner
 3.2.3 uninterruptible power supply

3.3 choose an appropriate hardware component to use or replace an existing device, given a practical network scenario

3.4 physically install a network interface card and verify that the card is operational

3.5 demonstrate the correct use of cabling tools; e.g., wire crimper, punch down tool

3.6 demonstrate the appropriate use of basic test equipment including:
 3.6.1 media testers/certifiers
 3.6.2 crossover cables
 3.6.3 tone generators and probes; e.g., fox and hound
 3.6.4 optical testers

3.7 demonstrate the proper sequence of steps to crimp and test Ethernet cable

3.8 select the appropriate cabling tool and test equipment, given a practical cabling task

4. demonstrate established laboratory procedures and safe work practices

4.1 demonstrate procedures for compliant installation of:

4.1.1 jacks and outlets

4.1.2 cable and structured cable runs

4.1.3 patch panels and patch cords

4.1.4 network cards

4.1.5 a wired or wireless connection

4.2 demonstrate the appropriate use of test equipment in checking for:

4.2.1 continuity

4.2.2 proper grounding

4.2.3 correct cable termination

4.3 create a proposal for a new or refit cabling project

4.4 design, build and troubleshoot a small Ethernet network

5. identify the fundamental principles of networks

5.1 describe basic networking concepts including:

5.1.1 addressing

5.1.2 bandwidth

5.1.3 status indicators

5.1.4 protocols; e.g., Internet Protocol Suite (TCP/IP) including Internet Protocol (IP), classful subnet, Internetwork Packet Exchange/Sequenced Packet Exchange (IPX/SPX) including network basic input/output system

5.1.5 full-duplex, half-duplex

5.1.6 cabling; e.g. twisted pair, coaxial cable, fibre optic, RS-232, USB, IEEE 1394/Firewire

5.1.7 networking models including peer-to-peer and client/server

5.2 identify names, purposes and characteristics of the common network cables including:

5.2.1 plenum/PVC

5.2.2 unshielded twisted pair (UTP); e.g., CAT3, CAT5/5e, CAT6

5.2.3 shielded twisted pair (STP)

5.2.4 fibre; e.g., single-mode and multi-mode

5.3 identify names, purposes and characteristics of network connectors; e.g., RJ-45, RJ-11, ST/SC/LC, MT-RJ

5.4 identify names, purposes and characteristics (e.g., definition, speed, connections) of the following technologies for establishing connectivity:

5.4.1 LAN/Wide Area Network (WAN)

5.4.2 Integrated Services Digital Network (ISDN)

5.4.3 broadband; e.g., Digital Subscriber Line (DSL), cable, satellite

5.4.4 dial-up

5.4.5 wireless standards, all 802.11

5.4.6 infrared

5.4.7 Bluetooth

5.4.8 cellular

5.4.9 Voice over Internet Protocol (VoIP)

6. identify the fundamental principles of security

6.1 identify names, purposes and characteristics of hardware and software security including:

6.1.1 hardware deconstruction/recycling

6.1.2 smart cards/biometrics; e.g., key fobs, cards, chips, scans

6.1.3 authentication technologies; e.g., password, biometrics, smart cards

6.1.4 malicious software protection; e.g., viruses, Trojans, worms, spam, spyware, adware, grayware

6.1.5 software firewalls
6.1.6 file system security; e.g., file allocation table (FAT)32 and Windows NT File System (NTFS)

6.2 identify names, purposes and characteristics of wireless security including:
6.2.1 wireless encryption; e.g., Wired Equivalent Privacy (WEP), Wi-Fi Protected Access (WPA), client configuration
6.2.2 access points; e.g. disable Dynamic Host Configuration Protocol (DHCP)/use static IP, change service set identifiers (SSID) from default, disable SSID broadcast, Media Access Control (MAC) filtering, change default user name and password, update firmware, firewall

6.3 identify names, purposes and characteristics of data and physical security
6.3.1 data access; e.g., basic local security policy
6.3.2 encryption technologies
6.3.3 backups
6.3.4 data migration
6.3.5 data/remnant removal
6.3.6 password management
6.3.7 locking work station; e.g., hardware, operating system

6.4 describe the importance and process of incidence reporting

6.5 recognize and respond appropriately to social engineering situations

6.6 install, configure, upgrade and optimize hardware, software and data security including:
6.6.1 Basic Input/Output System (BIOS)
6.6.2 smart cards
6.6.3 authentication technologies
6.6.4 malicious software protection
6.6.5 data access; e.g., basic local security policy
6.6.6 backup procedures and access to backups
6.6.7 data migration
6.6.8 data/remnant removal

6.7 implement software security preventive maintenance techniques such as installing service packs and patches and training users about malicious software prevention technologies

6.8 diagnose and troubleshoot hardware, software and data security issues including:
6.8.1 BIOS
6.8.2 smart cards, biometrics
6.8.3 authentication technologies
6.8.4 malicious software
6.8.5 file system; e.g., FAT32, NTFS
6.8.6 data access; e.g., basic local security policy
6.8.7 backup
6.8.8 data migration

7. demonstrate basic competencies

7.1 demonstrate fundamental skills to:
7.1.1 communicate
7.1.2 manage information
7.1.3 use numbers
7.1.4 think and solve problems

- 7.2 demonstrate personal management skills to:
  - 7.2.1 demonstrate positive attitudes and behaviours
  - 7.2.2 be responsible
  - 7.2.3 be adaptable
  - 7.2.4 learn continuously
  - 7.2.5 work safely
- 7.3 demonstrate teamwork skills to:
  - 7.3.1 work with others
  - 7.3.2 participate in projects and tasks

8. create a transitional strategy to accommodate personal changes and build personal values

- 8.1 identify short-term and long-term goals
- 8.2 identify steps to achieve goals