**Course Competency**

**Competency 1:** The student will demonstrate understanding knowledge of computer network concepts by:

1. Explaining the purposes and uses of ports and protocols.
2. Explaining devices, applications, protocols and services at their appropriate OSI layers.
3. Explaining the concepts and characteristics of routing and switching.
4. Configuring the appropriate IP addressing components, for a given scenario.
5. Comparing and contrast the characteristics of network topologies, types and technologies.
6. Implement the appropriate wireless technologies and configurations, for a given scenario.
7. Summarizing cloud concepts and their purposes.
8. Explaining the functions of network services.
9. Describing proper procedures for the handling, safeguarding and disposal of computer equipment.
10. Describing the management of computer systems and peripherals following institutional protocol.

**Learning Outcomes**

- Numbers / Data
- Information Literacy
- Ethical Issues
- Computer / Technology Usage

**Competency 2:** The student will demonstrate an understanding of network infrastructure by:
<table>
<thead>
<tr>
<th>Competency 1: The student will demonstrate an understanding of network administration by:</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Deploying the appropriate cabling solution, for a given scenario.</td>
</tr>
<tr>
<td>2. Determine the appropriate placement of networking devices on a network and install/configure them, for a given scenario.</td>
</tr>
<tr>
<td>3. Comparing and contrasting the use of networking services and applications.</td>
</tr>
<tr>
<td>4. Explaining the purposes and use cases for advanced networking devices.</td>
</tr>
<tr>
<td>5. Explaining the purposes of virtualization and network storage technologies.</td>
</tr>
<tr>
<td>6. Comparing and contrasting various network types (including WAN, PAN, LAN, WLAN) and technologies.</td>
</tr>
<tr>
<td>7. Installing and configuring networking services and applications.</td>
</tr>
<tr>
<td>8. Differentiating between common network topologies.</td>
</tr>
<tr>
<td>10. Comparing the use of different protocols to accomplish routing tasks.</td>
</tr>
<tr>
<td>11. Explaining the purpose of Virtual LANs (VLANs).</td>
</tr>
<tr>
<td>12. Describing supervisory control and data acquisition (SCADA) systems and critical infrastructures.</td>
</tr>
<tr>
<td>13. Describing the Internet of Things (IoT).</td>
</tr>
</tbody>
</table>

Competency 3: The student will demonstrate an understanding of network operations by:

| 1. Using appropriate documentation and diagrams to manage the network, for a given scenario. |
| 2. Comparing and contrasting business continuity and disaster recovery concepts. |
| 3. Explaining common scanning, monitoring and patching processes and summarize their expected outputs. |
| 4. Using remote access methods, for a given scenario. |
| 5. Identifying policies and best practices. |

Updated Spring 2021
6. Differentiating between appropriate monitoring tools based on a given scenario.
7. Analyzing metrics and reports from monitoring and tracking performance tools based on a given scenario.
8. Choosing appropriate resources to support configuration management based on a given scenario.
10. Installing and applying patches and updates based on given scenario.
11. Discuss the managed services approach to network management.

**Competency 4**: The student will demonstrate an understanding of network security by:

1. Identifying the purposes of physical security devices.
2. Explaining authentication and access controls.
3. Securing a basic wireless network, for a given scenario.
4. Identifying common networking attacks.
5. Implementing network device hardening, for a given scenario.
6. Explaining common mitigation techniques and their purposes.
9. Implementing network hardening techniques based on a given scenario.
11. Installing and configuring a basic firewall based on a given scenario.
12. Explaining the purpose of various network access control models.

**Competency 5**: The student will demonstrate an understanding of network troubleshooting and tools by:
1. Explaining the network troubleshooting methodology.
2. Using the appropriate tool, for a given scenario.
3. Implementing the appropriate network troubleshooting methodology for common wired connectivity and performance issues, for a given scenario.
4. Implementing the appropriate network troubleshooting methodology for common wireless connectivity and performance issues, for a given scenario.
5. Implementing the appropriate network troubleshooting methodology for common network service issues, for a given scenario.
6. Implementing the appropriate network troubleshooting methodology for common cabling issues, for a given scenario.

**Competency 6:** The student will demonstrate an understanding of industry standards, practices, and network theory by:

1. Implementing the appropriate policies or procedures based on a given scenario.
2. Selecting appropriate safety practices to address specific treats.
3. Installing and configuring equipment in the appropriate location using best practices.
4. Discussing change management procedures.

**Course Competency 7:** The student will demonstrate an understanding of network communications by:

1. Describing the basic concepts of telecommunications and data communications.
2. Explaining the use of binary numbers to represent instructions and data. Converting decimal, binary, and hexadecimal numbers and performing binary arithmetic.
3. Interpreting the different classes of IP addresses and the public and private address ranges. Defining IPv6 Networking Suite.
<table>
<thead>
<tr>
<th>Competency 1:</th>
<th>The student will demonstrate an understanding of network user support and professional development skills by:</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Instructing users on login and security procedures, network organization, resource locations, and acceptable use and download policies.</td>
<td></td>
</tr>
<tr>
<td>2. Discussing employee rights regarding network use, privacy, security, safety, and other network policies.</td>
<td></td>
</tr>
</tbody>
</table>

4. Explaining the functions of subnets. Performing subnetting of the various network classes.
5. Identifying the function of routers, gateways, and other devices that perform path determination and packet switching. Identifying advanced routing algorithms and protocols.
6. Explaining the purpose of Network Address Translation (NAT) and Port Address Translation (PAT).
7. Explaining data units at each layer of the Open Systems Interconnection (OSI) model, including bits, frames, packets, and segments.
8. Identifying source and destination addresses of data units at each layer of the OSI model, including Media Access control (MAC) and Internet Protocol (IP) addresses.
9. Explaining the process of data encapsulation and transmission.
10. Differentiating the functions of Local Area Network (LAN) hardware protocols including Ethernet, token ring and Fiber Distributed Data Interface (FDDI). Comparing LAN software protocols such as TCP/IP, User Datagram Protocol (UDP/IP), Internetwork Packet Exchange/Sequenced Packet Exchanged (IPX/SPX), AppleTalk and network Basic Input/Output System (NetBEUI).
11. Identifying technical issues related to network performance including load, bandwidth, latency, jitter, collision and broadcast domains, and security.
12. Identifying Application protocols such as SMTP, HTTP, VoIP, SSH, etc.

Updated Spring 2021
3. Describing appropriate appearance and professional behavior for a business environment.
4. Identifying organizational computing and network workplace competencies.
5. Communicating effectively with individuals who lack a technical background.