Virginia Western Community College
ITN 101
Introduction to Network Concepts

Prerequisites
None

VCCS Course Description
Provides instruction in networking media, physical and logical topologies, common networking standards and popular networking protocols. Emphasizes the TCP/IP protocol suite and related IP addressing schemes, including CIDR. Includes selected topics in network implementation, support and LAN/WAN connectivity.

Semester Credits: 3
Lecture Hours: 3

Required Materials
Textbook
- Network+ Guide to Networks 10th Edition by Jill West, Cengage, 9798214012780

Other Required Materials:
None

VCCS COURSE OUTCOMES
- Compare peer-to-peer and client–server network models.
- Identify types of applications and protocols used on a network.
- Describe various networking hardware devices and the most common physical topologies.
- Compare the seven layers of the OSI model.
- Explain best practices for safety when working with networks and computers.
- Apply the seven-step troubleshooting model for troubleshooting network problems.
- Describe the roles of various network and cabling equipment in commercial buildings and work areas.
- Maintain network documentation.
- Manage assets on a network.
- Investigate MAC addresses.
- Configure TCP/IP settings on a computer, including IP address, subnet mask, default gateway, and DNS servers.

- Identify the ports of several common network protocols.
- Describe domain names and the name resolution process.
- Use command-line tools to troubleshoot common network problems.
- Describe the functions of core TCP/IP protocols.
- Secure network data and transmissions using encryption protocols.
- Configure remote access connections between devices.
- Employ various TCP/IP utilities for network discovery and troubleshooting.
- Explain basic data transmission concepts.
- Describe various types of network cables and their related connectors.
- Compare the benefits and limitations of various networking media.
- Apply the appropriate tool to troubleshoot common cable problems.
- Describe characteristics of wireless transmissions.
- Explain 802.11 standards.
- Plan a Wi-Fi network.
- Secure a Wi-Fi network.
- Troubleshoot a Wi-Fi network.
- Describe how to configure and manage switches in physical network architecture.
- Explain forms of virtualization technologies on a network.
- Summarize cloud characteristics, models, and connectivity options.
- Explain the roles of automation and orchestration in network management.
- Explain the purposes of network segmentation.
- Apply subnetting to network devices.
- Configure VLANs.
- Describe networking and segmentation options in the cloud.
- Compare WAN connectivity technologies.
- Explain how routers manage internetwork communications.
- Describe ways to secure WAN connections.
- Troubleshoot common WAN connection problems.
- Identify people, technology, and malware security risks to a network.
- Increase network security through risk assessment and management.
- Implement device hardening techniques.
- Describe security policies and physical security that help secure a network.
- Explain how authentication, authorization, and accounting work together to help secure a network.
- Compare authentication technologies.
- Explain how network security is evolving to meet the needs of modern, distributed networks.
- Use appropriate tools to collect data about the network.
- Explain methods to optimize network performance.
- Identify best practices for incident response and disaster recovery.

Note to Instructors

This course maps to the CompTIA Network+ certification

TOPICAL DESCRIPTIONS

Chapter	Topic

01 Introduction to Networking	• Networking Models
	  ○ Peer-to-Peer Network Model
	  ○ Client-Server Network Model
	• Network Services
	  ○ Network Protocols
	• Network Hardware
	  ○ LANs and Their Hardware
	  ○ Routers and LANs
	  ○ MANs and WANs
	• The Seven Layer OSI Model
	  ○ Application Layer
	  ○ Presentation Layer
	  ○ Session Layer
	  ○ Transport Layer
	  ○ Network Layer
	  ○ Data Link Layer
	  ○ Physical Layer
	  ○ Protocol Data (PDU)
	  ○ Summary of How the Layers Work Together
	• Safety Procedures and Policies
	  ○ Emergency Procedures
	  ○ Safety Precautions
	• Troubleshooting Networking Problems
	  ○ Troubleshooting Example

02 Infrastructure and Documentation	• Components of Structured Cabling
	  ○ From Demarc to a Workstation
	  ○ Cabling
	  ○ Monitoring the Environment and Security
	• Network Documentation
	  ○ Network Diagrams
	  ○ Operating Procedures
	  ○ Inventory Management
	  ○ Labeling and Naming Conventions
	  ○ Business Documents
	• Asset Managements
	  ○ Anticipating Failure
	  ○ Life Cycle Management
	  ○ Change Management

03 Addressing	• Addressing Overview

	• MAC Addresses
	• IP Addresses
	  ○ IPv4 Addresses
	  ○ IPv6 Addresses
	• Ports and Sockets
	  ○ Port Types
	• Domain Names and DNS
	  ○ Namespace Databases
	  ○ Name Servers
	  ○ Resource Records in a DNS Database
	  ○ DNS Server Software
	• Troubleshooting Address Problems
	  ○ Troubleshooting Tools
	  ○ Common Network Issues

04 Protocols	• TCP/IP Core Protocols
	  ○ TCP (Transmission Control Protocol)
	  ○ UDP (User Datagram Protocol)
	  ○ IP (Internet Protocol)
	  ○ ICMP (Internet Control Message Protocol)
	  ○ ARP (Address Resolution Protocol)
	  ○ Neighbor Discovery
	  ○ Ethernet
	• Encryption Protocols
	  ○ Encryption
	  ○ SSL (Secure Sockets Layer) and TLS (Transport Layer Security)
	  ○ IPsec (Internet Protocol Security)
	• Remote Access Protocols
	  ○ Remote File Access
	  ○ Terminal Emulation
	  ○ VPNs (Virtual Private Networks)
	• Troubleshooting Network Issues
	  ○ Troubleshooting Tools
	  ○ Solving Common Network Problems

05 Cabling	• Transmission Basics
	  ○ Frequency, Bandwidth, and Throughput
	  ○ Transmission Flaws
	  ○ Duplex, Half-Duplex, and Simplex
	• Copper Cable
	  ○ Coaxial and Twinaxial Cable
	  ○ Coaxial Cable
	  ○ Twisted-Pair Cable
	  ○ STP (Shielded Twisted Pari)

	○ UTP (Unshielded Twisted Pair) ○ Comparing STP and UTP ○ Cable Pinouts ○ Ethernet Standards for Twisted-Pair Cable ○ PoE (Power over Ethernet) • Fiber-Optic Cable ○ SMF (Single Mode Fiber) ○ MMF (Multimode Fiber) ○ Fiber Connectors ○ Fiber Transceivers ○ Ethernet Standards for Fiber-Optic Cable • Cable Troubleshooting Tools ○ Toner and Probe Kit ○ Cable Continuity Tester ○ Cable Performance Tester ○ OPM (Optical Power Meter)
06 Wireless Networking	• Characteristics of Wireless Transmissions ○ The Wireless Spectrum ○ Channel Management ○ Antennas ○ Signal Propagation • 802.11 WLAN Standards ○ IEEE 802.11 Frames ○ Wi-Fi Access Method ○ Wi-Fi Association ○ Wireless Topologies ○ Band Steering • Implementing a Wi-Fi Network ○ Determine the Design ○ Configure Wi-Fi Connectivity Devices ○ Configure Wi-Fi Clients • Wi-Fi Networking Security ○ Historical Context: WEP (Wireless Equivalent Privacy) ○ Historical Context: WPA (Wi-Fi Protected Access) ○ WPA2 (Wi-Fi Protected Access, Version 2) ○ WPA3 (Wi-Fi Protected Access, Version 3) ○ WPA Security ○ Other Security Configurations ○ Security Threats to Wi-Fi Networks • Troubleshooting Wi-Fi Networks ○ Wi-Fi Network Tools

	○ Avoid Pitfalls
07 Network Architecture	• Physical Architecture ○ Types of Switches ○ Switch Port Security ○ Switch Path Management ○ Hierarchical Design ○ Network Availability and Redundancy • Virtual Architecture ○ Hypervisors ○ VM Network Connection Types ○ Pros and Cons of Virtualization ○ NFV (Network Functions Virtualization) ○ SDN (Software-Defined Networking0 • Cloud Architecture ○ Cloud Characteristics ○ Cloud Services Models ○ Cloud Deployment Models ○ Connecting to Your Cloud ○ Cloud Services • Automating Networks ○ Automation and Orchestration ○ Source Control
08 Network Segmentation	• Why Segment Networks ○ Benefits of Segmentation ○ OT (Operational Technology) ○ SAN (Storage Area Network) • Subnetting ○ How Subnets Work ○ How Subnet Masks Work ○ Subnet Mask Tables ○ Implementing Subnets on a Network ○ Network Services across Subnets ○ VLSM ○ Subnets in IPv6 • VLANs ○ Switch Port Configuration ○ VLANs and Subnets ○ Switch Virtual Interfaces ○ Types of VLANs ○ VLAN Maintenance ○ VXLAN (Virtual Extensions Local Area Network) • Cloud Networking

	○ Network Spaces in the Cloud ○ Cloud at the Edge
09 Wide Area Networking	• WAN Connectivity ○ WANs versus LANs ○ WAN Connection Service Options ○ Cloud Connectivity Options ○ SD-WAN ○ Wireless WANs • Routing Protocols ○ Types of Routers ○ Routing Tables ○ Routing Protocols to Determine Best Paths ○ Interior and Exterior Gateway Protocols ○ Routing Redundancy • Securing WAN Connections ○ ACLs (Access Control Lists) ○ Proxy Servers ○ Firewalls ○ Cloud Security Technologies • Troubleshooting WAN Connections ○ Internet Connectivity Issues ○ Interface Problems ○ Routing Issues
10 Risk Management	• Security Risks ○ Types of Risks ○ People Risks ○ Technology Risks ○ Malware Risks • Risk Assessment and Management ○ Assessment Types ○ Attack Simulations ○ Scanning Tools ○ Intrusion Detection and Prevention ○ Honeypots and Honeynets • Device Hardening ○ Updates and Security Patches ○ Services and Protocols ○ Administrative Credentials ○ Anti-Malware Software ○ Switch Security Configurations ○ Asset Disposal
11 Access Control	• Security and Users ○ Security Policies

	○ Physical Prevention Methods ○ Physical Detection Methods • AAA (Authentication, Authorization, and Accounting) ○ Authentication ○ Authorization ○ Accounting • Authentication Technologies ○ SSO (Single Sign-On) ○ Directory Services ○ Third-Party IdPs (Identity Providers) • Modernizing Network Security ○ Zero Trust Security ○ SASE (Security Access Service Edge)
12 Performance and Recovery	• Collect Network Data ○ Environmental Monitoring ○ Traffic Monitoring Tools ○ Cloud Observability • Manage Network Traffic ○ Performance Baselines ○ Bandwidth Management ○ Flow Control ○ Congestion Control ○ QoS (Quality of Service) Assurance • Plan Response and Recovery Strategies ○ Incident Response ○ Data Preservation ○ Disaster Recovery Planning ○ Disaster Recovery Contingencies ○ Power Management ○ Backup Systems

TITLE IX STATEMENT

ADA STATEMENT