CNP - Certified Network Principles

Course Overview

This course covers network principles. Topics covered include networking fundamentals, wireless LANs, security principles, network planning, and more.

Course Introduction	5m
Course Introduction	
Chapter 1 - The Desktop Lifecycle	1h
Introduction to Network Fundamentals	
Overview	
Section 1: Basics of Networking	
What is a Network?	
Network Integration	
Networking Components	
Networking Components (cont.)	
Networking Components (cont.)	
Networking Components (cont.)	
Networking Components (cont.)	
Logical Infrastructure Design Notes	
Networking Challenges	
Section 2: Classifying Networks	
Important Definition	
The Different Types of Networks	
Explaining the Different Types of Networks	
Explaining the Different Types of Networks	
Explaining the Different Types of Networks	
Network Topology	
Different Network Topologies	
Section 3: Network Models	
What is the Purpose of a Reference Model?	
7 Layers of the OSI Model	
Explaining the 7 layers of the OSI Model	
TCP/IP Reference Model	
The Explanation of the 4 TCP/IP Layers	
Section 4: Troubleshooting Process	
Troubleshooting General Methodology	
What are the Best Practices for Successful Network Ethernet Troubleshooting?	
Network+ Troubleshooting Problem	
Troubleshooting Techniques	
Troubleshooting Techniques	
Troubleshooting Techniques	
Troubleshooting Techniques	
Troubleshooting Techniques	

Troubleshooting Techniques
Network Troubleshooting Tools
Review

Chapter 2 - The Physical Networking Fundamentals 1h 34m

The Physical Networking Fundamentals
Course Outline
Overview
Section 1: Connection Technologies
What is a Physical Network?
Connection Technologies
Ethernet
Signaling and Modulating
Baseband vs. Broadband
Network Bandwidth
Multiplexing
Data Link Layer
Network Interface Controller (NIC)
Channel Access
Multiple Access Techniques
MAC Address
Computer to Computer Connections
Addressing Methods
Ethernet Frame
Section 2: Network Devices
Types of Networking Devices
Layer 1 Devices
Layer 2 Device
Switches
Layer 3 Device
Network Repeater
Network Modem
Section 3: Copper Media
Electrical Interference
Types of Copper Media
UTP vs. STP
UTP Categories
Twisted-Pair Connectors
Wiring Standard
Centralized Connections
Centralized Connections
RS-232
Termination Tools
COAX Cable
Different Types of COAXIAL Cables
Cable Testing Tools
Troubleshooting Copper Cables
Section 4: Optical Media
Optical Fibers
Fiber Types

Fiber Types
Fiber Types
Wavelength-Division Multiplexing (WDM)
Up to 200GB Technology
Fiber Optical Connectors
Fiber Optical Connectors
Fiber Optical Standards
Equipment
Troubleshooting Fiber
Section 5: Ethernet Standards
The Evolution of Ethernet
Power over Ethernet (POE)
Standard Ethernet Code
Exam Relevant Standards
Advanced Options
Review

Chapter 3 - TCP/IP Primer 3h 9m

TCP/IP Primer
Course Outline
Overview
Section 1: IP Addressing
Binary Numbering
IP Address
IPv4 Address Scheme
What makes up an IP Address?
Classful Addressing
Classless Addressing
Special IPv4 Addresses
Classful Addressing
Classless Addressing
Special IPv4 Addresses
Subnetting
IPv6 Addressing
Drawbacks of IPv6
Typical IPv6 Address
IPv6 Address Scopes
Multicast Addresses
IPv6 Migration Strategies
Address Resolution
Physical Address Resolution
ARP Requests
ARP
Physical Address Resolution IPv6
Domain Name System (DNS)
Domain Names
DNS Servers
DNS Server Database Resource Records
DNS Server Database Resource Records
Address Assignment

Automating Dynamic IP Assignment
DHCPv4/v6 Common Features
DHCPv4 Leasing Process
DHCPv6 Leasing Process
Virtual IP Addresses
IP Address Management (IPAM)
Section 2: Core Protocols
IP Packets
IPv4 Packet Structure
IPv6 Packet Structure
ICMP
TCP/IP protocols
TCP Connections
Establishing a Connection
Sliding windows
UDP Connections
Section 3: Network Ports and Applications
Network Ports
The Different Port Ranges
Common Ports
Common Ports (continued)
Common Ports (continued)
Application Protocols
Email Protocols
Remote Access Protocols
Resource Sharing Protocols
TCP/IP Tools
Review

Chapter 4 - Connecting Networks, Internet, and WAN Technologies 1h 46m

Connecting Networks, Internet, and WAN Technologies
Course Outline
Overview
Section 1: Switching
What is a Switching Loop?
Switching Loop Effects on Network Performance
Activating a Blocked Port
Spanning Tree Protocol (STP)
Spanning Tree Protocol (STP)
Spanning Tree Protocol (STP)
Spanning Tree Protocol (STP)
Spanning Tree Protocol (STP)
Spanning Tree Replacements
How To Avoid Switching Loop
Spanning Tree Replacements
About VLANs
VLAN Trunking
Switch Management
Section 2: Routing
Routing Tables

Route Commands
Remote Routes
Exterior/Interior Gateway Protocol
Exterior Gateway Protocol (EGP)
NAT Methods
NAT Methods (continued)
Port Address Translation (PAT)
NAT and IPv6
Section 3: Internet Connections
The History of Internet Access
Technologies
Demarcation Points
Dialup Access
Integrated Services for Digital Network (ISDN)
Two ISDN options
DSL
Cable Broadband
Fiber Optics Internet
Multiple Approaches for Fiber Optics
Wireless Internet Access
Cellular Connection
Two Mobile Networks
Internet Access
ISP Troubleshooting Tools
Internal and External Connectivity Errors
Section 4: WAN Infrastructure
Circuit vs. Packet Switching
Virtual Circuits
T and E Carriers
Optical Carriers
Point-to-Point Protocol
Packet Switched WANs
Frame Relay
Asynchronous Transfer Mode
UNI and NNI
ATM Cells
Review

Chapter 5 - Wireless LANs 42m

Wireless LANs
Course Outline
Overview
Section 1: Wireless Networks
Radio Broadcasts
Managing Bandwidth
Narrowband Transmission
Spread Spectrum Encoding Methods
MIMO and MUMIMO
Devices in Wireless Networks
Wireless Bridge

Wireless Topology

Wireless Topology

Scaling Technology

Scaling Technology

Section 2: Wireless LAN Standards

Wi-Fi Networks

Frequency Bands

Early Wi-Fi Standards

Current Wi-Fi Standards

Standards Comparison

Local Wireless Technologies

Local Wireless Technologies (continued)

Local Wireless Technologies (continued)

Bluetooth

Wireless Connectivity

Radio Performance Factors

Radio Performance Factors

Review

Chapter 6 - Security Principles 2h 3m

Security Principles

Course Outline

Overview

Section 1: Goals and Threats

What is Information Security?

What is Information Security?

Defense in Depth

CIA Triad

Confidentiality Controls

Integrity Controls

Availability Controls

Risk Based Definitions

Classify Controls by the Actions

Control Types

Types of Threats

Attack Vectors

Password Cracking Techniques

Social Engineering Techniques

Phishing Information

Malware

Types of Malware

More Malware Spyware and Adware

What is a Botnet?

Ransomware

Stealthing: Rootkit

Network Probes

Spoofing

Redirection

DoS

DDoS

Packet Sniffers
Passive Sniffing
Active Sniffing
Active Sniffing Methods
Man-in-the-Middle (MitM)
ARP Cache Poisoning
ARP Normal Operation
ARP Cache Poisoning
Attacking Wireless
DOS: Deauth/ Disassociation Attack
Attacking Bluetooth
Section 2: Digital Security
Encryption
Symmetric Cryptography – Use of Secret Keys
Symmetric Encryption
Symmetric Keys
Asymmetric Cryptography
Asymmetric Encryption
When to Use Which Key?
Asymmetric
http://ijcscn.com/Documents/Volumes/vol5issue1/ijcscn2015050103.pdf
Hashing Algorithms
Data Integrity Mechanisms
AAA Process
Authentication
Strong Authentication
Access Control Mechanisms
Biometric System Types
Passwords and PINs
One-Time Password Authentication
Synchronous Token (Hardware or Software Token)
Asynchronous Token Device (Hardware or Software Token)
Cryptographic Keys
Memory Cards
Smart Card
Digital Certificates (Public Key Certificates)
Section 3: Transport Encryption
SSL/TLS Hybrid Encryption
SSH Security Protocol
E-mail Standards
Secure E-mail Standard
Encryption Protocols
Wireless Security Wired Equivalent Privacy
Wireless Security Wi-Fi Protected Access
Wireless Security 802.11i - WPA2
WPA and WPA2 Mode Types
Wireless Security WPA3
Wi-Fi Protected Setup
Authentication
Virtual Private Network (VPN)

Virtual Private Network Technologies
What is a Tunneling Protocol?
Tunneling Protocols – PPTP
Tunneling Protocols – L2TP
Tunneling Protocols – IPSec
IPSec – Network Layer Protection
IPSec Key Management
IPSec Handshaking Process
SAs in Use
IPSec is a Suite of Protocols
IPSEC Datagrams
Review

Chapter 7 - Defending the Network 2h 9m

Defending the Network
Course Outline
Overview
Section 1: Network Security Components
Bastion Host
Devices Work at Different Layers
Access Control Lists
Switch Security Features
Firewalls
Firewall – First Line of Defense
Firewall Types – Packet Filtering
Firewall Types – Proxy Firewalls
Firewall Types – Circuit-Level Proxy Firewall
Firewall Types – Application-Layer Proxy
Firewall Types – Stateful
Firewall Types – Dynamic Packet-Filtering
Firewall Types – Kernel Proxies
Layer 7 Firewall
Content Filtering
Network Access Control (NAC)
Design
Firewall Placement
Firewall Architecture Types – Screened Host
Firewall Architecture Types – Multi- or Dual-Homed
Firewall Architecture Types – Screened Subnet
DMZ
IDS – Second Line of Defense
IPS – Last Line of Defense?
IDS / IPS
NIDS / NIPS
HIDS / HIPS
HIPS
Unified Threat Management
Unified Threat Management (UTM)
UTM Product Criteria
Malware Defenses

Data Loss Prevention (DLP)
Data Loss Prevention (DLP)
Data Loss Prevention (DLP)
Data Loss Prevention (DLP)
Surveillance Systems
Intrusion Sensors
Securing Mobile Devices
Secure Entryways
Section 2: Network Authentication Systems
Terms Used
Terms Used
Single Sign-on Technology
Windows Account Types
PPP
Authentication Protocols – PAP, CHAP, MS-CHAP
Authentication Protocol – EAP
Authentication Protocol – EAP
Remote Centralized Administration
RADIUS Characteristics
RADIUS
TACACS+ Characteristics
What is Kerberos?
Important Note
Dependencies
Kerberos Components
Keys used in Authentication
Keys used in Authentication (cont.)
Tickets
Tickets (cont.)
Login Process
Message 1: Authentication Service Request
Message 2: Authentication Service Reply
Message 3: Ticket-Granting Service Request
Message 4: Ticket-Granting Service Reply
Delegation
802.1X
802.1X Three Main Components
Section 3: Hardening the Network
Defense in Depth
Data Security Lifecycle
Data Discovery
Data Classification
Data Classification Categories
Typical Security Measures
Data Protection Policies
Data Deletion
Application Security
Secure Coding Principles
Patch Management
Security Updates

Host Firewall Settings
Securing Hosts
Securing Hosts
Securing the Internal Network
Securing the Perimeter Network
Create or Promote Cyber Security Culture
What is a Vulnerability Assessment (VA)?
Typical Vulnerability Assessment Process
Vulnerability Scanners
What is a Penetration Test?
Security Troubleshooting
Review

Chapter 8 - Network Technology Boom 1h 5m

Network Technology Boom
Course Outline
Overview
Section 1: Network Expansion
Today's Networks
VoIP
VoIP Components
VoIP Protocols
SIP Trunks
Streaming Media
Industrial Control Systems
Industrial Control Systems
Industrial Control Systems
What makes IoT Unique?
IoT Devices
DAS
NAS
SAN
SAN Architecture
SAN Architecture
Quality of Service
QoS
802.1p Classes
Differentiated Services
Differentiated Services
Section 2: Virtual and Cloud Networks
Virtualization Definition
How Does Virtualization Work?
What is a Virtual Machine (VM)?
What is a Hypervisor?
Type 1 and Type 2 Hypervisors
Why Virtualize? Commonly Cited Benefits
Virtualization Benefits
vSwitch Terminology
vSwitch Terminology
Connectivity

Vmware vSphere 6.x Virtual Switches
vSwitch Connections
vSwitch Routing
What is a Software Defined Datacenter?
Network and Communications in the Cloud
Cloud Networking – VXLAN
Cloud Computing Defined
NIST Five Essential Characteristics
NIST Three Service Models
SaaS Pros and Cons
PaaS Pros and Cons
IaaS Pros and Cons
NIST Four Deployment Models
Cloud Computing Characteristics
Cloud Computing Benefits
Security Risks Most Commonly Cited
Cloud Access Security Broker (CASB)
Review

Chapter 9 - Day to Day Networking 1h 29m

Day to Day Networking
Course Outline
Overview
Section 1: Network Monitoring and Optimization
Monitoring Tools
Network Analyzer Wireshark
Network Analyzer Tasks
Protocols – SNMP
SNMP
Syslog
System Logs
SIEM
Metrics / Performance
Optimizing Performance
Load Balancer
Load Balancer Configurations
Proxy Servers
Proxy Servers
Section 2: Network Fault Tolerance and Recovery
Availability and Recovery
Availability and Recovery
Reliability and Recovery Terminology
Reliability and Recovery Terminology
Redundancy
Power Management
Site Strategies
DR Site Strategies
DR Site Strategies
DR Site Strategies
DR Site Strategies

Backup Types
Backup Security
Creating Backup Policies
Section 3: Responding to Network Security Incidents
Security Events
What is an Incident?
Security Incident
Indication of Compromise
Incident Response Goals
Incident Response Goals
Six Step Approach to Incident Handling
Preparation Phase
Identification Basic Steps
Identification and Initial Response
Containment
Containment Goals
Eradication
Eradication Goals
Recovery Goals
Follow-up Goals
Review

Chapter 10 - Network Planning 36m

Network Planning
Course Outline
Overview
Section 1: Network Policy Design
About Policy
Recommendations for Policy
Policy Examples
Acceptable Use Policies
Passwords
Implement General Password Policies that Work!
Consider Something Better
Mobile Device Policies
Remote Access Policies
Human Resource Policies
Regulatory Compliance
Business Agreements
Section 2: Network Installation
Network Documentation
Network Diagrams
Logical Infrastructure Design Notes
Network Requirements
Network Installation
Rack Systems
Organizing Components
Section 3: Maintenance and Upgrades
Controlling How Changes Take Place
Change Control Process

Requesting Changes
Change Control Steps
Software Changes
Review

Total Duration: 15h 39m