

CNIT R144: COMPTIA NETWORK+ FUNDAMENTALS AND CERTIFICATION PREPARATION

Originator

alynch

College

Oxnard College

Discipline (CB01A)

CNIT - Computer Networking/IT

Course Number (CB01B)

R144

Course Title (CB02)

CompTIA Network+ Fundamentals and Certification Preparation

Banner/Short Title

CompTIA Network+ Fundamentals

Credit Type

Credit

Start Term

Fall 2021

Formerly

ENGT R144

Catalog Course Description

The CompTIA Network+ certification is an internationally recognized validation of the technical knowledge required of foundation-level IT network practitioners. A student who successfully completes this course should have the knowledge and hands-on skills necessary to design, install, manage, and troubleshoot a network infrastructure for both wired and wireless networks. This course will also cover network security basics. Students who successfully complete this course should be prepared for the CompTIA Network+ certification. CompTIA certification voucher discounts are available to all CNIT program students.

Taxonomy of Programs (TOP) Code (CB03)

0708.10 - *Computer Networking

Course Credit Status (CB04)

D (Credit - Degree Applicable)

Course Transfer Status (CB05) (select one only)

B (Transferable to CSU only)

Course Basic Skills Status (CB08)

N - The Course is Not a Basic Skills Course

SAM Priority Code (CB09)

C - Clearly Occupational

Course Cooperative Work Experience Education Status (CB10)

N - Is Not Part of a Cooperative Work Experience Education Program

Course Classification Status (CB11)

Y - Credit Course

Educational Assistance Class Instruction (Approved Special Class) (CB13)

N - The Course is Not an Approved Special Class

Course Prior to Transfer Level (CB21)

Y - Not Applicable

Course Noncredit Category (CB22)

Y - Credit Course

Funding Agency Category (CB23)

Y - Not Applicable (Funding Not Used)

Course Program Status (CB24)

1 - Program Applicable

General Education Status (CB25)

Y - Not Applicable

Support Course Status (CB26)

N - Course is not a support course

Field trips

May be required

Faculty notes on field trips; include possible destinations or other pertinent information

Possible destinations would be an IT shop, IT managed service provider, or a public sector managed network.

Grading method

Letter Graded

Alternate grading methods

Credit by exam, license, etc.

Does this course require an instructional materials fee?

No

Repeatable for Credit

No

Is this course part of a family?

No

Units and Hours

Carnegie Unit Override

No

In-Class

Lecture

Minimum Contact/In-Class Lecture Hours

52.5

Maximum Contact/In-Class Lecture Hours

52.5

Activity

Laboratory

Minimum Contact/In-Class Laboratory Hours

52.5

Maximum Contact/In-Class Laboratory Hours

52.5

Total in-Class**Total in-Class****Total Minimum Contact/In-Class Hours**

105

Total Maximum Contact/In-Class Hours

105

Outside-of-Class**Internship/Cooperative Work Experience****Paid****Unpaid****Total Outside-of-Class****Total Outside-of-Class****Minimum Outside-of-Class Hours**

105

Maximum Outside-of-Class Hours

105

Total Student Learning**Total Student Learning****Total Minimum Student Learning Hours**

210

Total Maximum Student Learning Hours

210

Minimum Units (CB07)

4

Maximum Units (CB06)

4

Student Learning Outcomes (CSLOs)**Upon satisfactory completion of the course, students will be able to:**

- | | |
|---|--|
| 1 | List the 7 layers of the OSI computer networking model and place networking hardware and protocols at the correct corresponding OSI layer. |
| 2 | Successfully troubleshoot a networking problem using TCP/IP utilities including ipconfig, ping, and tracert. |
| 3 | Complete a CompTIA Network+ certification simulation exam with an 80% or higher score to demonstrate preparedness for the actual CompTIA Network+ certification. |

Course Objectives**Upon satisfactory completion of the course, students will be able to:**

- | | |
|---|--|
| 1 | Explain the function of common networking protocols such as TCP, IP, DNS, DHCP, SMTP, and POP3. |
| 2 | Identify commonly used TCP and UDP default ports such as FTP, TELNET, DHCP, HTTP, and HTTPS. |
| 3 | List the address ranges for Class A, B, and C IPv4 addresses and the associated default subnet mask. |
| 4 | Summarize the benefits of the IPv6 IP address structure over IPv4. |
| 5 | Build a LAN that is connected to the Internet using an integrated service router (ISR). |

- 6 Harden a network using port filtering, IP and MAC address filtering, time-of-day restrictions, keyword restrictions, and stateless packet filtering.
- 7 Configure a wireless network using the appropriate 802.11 standard and wireless security protocol.
- 8 Build a straight-through cable using the EIA/TIA568A standard with the appropriate cabling hand tools.
- 9 Punch down UTP cable on a block using the 110 hand tool.
- 10 Test cables and end-to-end connectivity using a cable tester.
- 11 Identify common IPv4 and IPv6 routing protocols.
- 12 List the key elements of physical layer topologies such as bus, star, extended star, mesh, hybrid mesh, point-to-point, and point-to-multipoint.
- 13 Categorize WAN technology types and properties such as frame relay, T1/E1, DSL, Cable, FIOS, ISDN, PSTN, OC-x, and satellite.
- 14 Explain the function of each layer of the OSI model.
- 15 Create a baseline measurement for network performance using a packet capture program.
- 16 Write filters to capture only specific protocol traffic using a packet capture program.
- 17 Troubleshoot common network problems using TCP/IP utilities such as PING, TRACERT, IPCONFIG, ARP, NSLOOKUP, and NETSTAT.
- 18 Differentiate between the different methods of performing user authentication such as Kerberos, RADIUS, TACACS+, 802.1x, EAP, CHAP, MS-CHAP.
- 19 Identify common PC and network security threats and mitigation techniques for viruses, worms, Trojan horses, denial-of-service attacks, spamware, and spyware.
- 20 Summarize the key elements of a security policy for the network infrastructure and the most effective methods for training users on the policy.
- 21 List the key characteristics of cellular service options including 3G, 4G, and 5G.

Course Content

Lecture/Course Content

1. Networking Protocols
 - a. Ethernet
 - b. TCP/IP
 - c. DHCP, DNS, FTP, TELNET, HTTP, HTTPS,SMTP, POP3, IMAP4
2. IP Addressing
 - a. IPv4 and IPv6
 - b. Subnet Mask
 - c. Subnetting
 - d. Broadcast domain
 - e. Network address translation (NAT)
 - f. Port address translation (PAT)
 - g. IPv6 link-local, global, and multicast addresses
3. Cabling
 - a. UTP, STP, fiber optic, and coaxial
 - b. Straight-through cable, crossover cable, rollover cable
 - c. EIT/TIA 568 standards
 - d. Category 5, 5e, 6, 6a, and 7 cables
 - e. Crosstalk
 - f. Data jacks, patch panel, punch down blocks
 - g. Cable stripper, RJ-45 crimper, 110 punch down tool, cable tester
4. Network Devices
 - a. Repeater, hub, and access-point (AP)
 - b. Bridge and switch
 - c. Router
 - d. Integrated service router (ISR)
5. Physical Layer Topologies
 - a. Bus
 - b. Star and extended star

- c. Mesh and hybrid mesh
 - d. Point-to-point and multipoint
6. OSI Model
 - a. Physical layer, data link layer, network layer
 - b. Transport layer, session layer, presentation layer, application layer
 - c. TCP/IP model versus the OSI model
 - d. Troubleshooting using the OSI model
 7. WAN Types
 - a. POTS and PSTN
 - b. ADSL and SDSL
 - c. FIOS and OC-x
 - d. Satellite and WiMAX
 - e. Cable
 8. TCP/IP Utilities
 - a. PING and TRACERT
 - b. IPCONFIG and IPCONFIG/ALL
 - c. NSLOOKUP
 - d. ARP
 - e. NETSTAT and NBTSTAT
 9. Packet Sniffing & Protocol Analyzing
 - a. Wired and wireless networks
 - b. Wireshark application
 - c. Baseline measurements
 - d. Protocol analysis
 - e. Password sniffing and vulnerability analysis
 10. Authentication Protocols
 - a. Kerberos
 - b. RADIUS and TACACS
 - c. EAP and LEAP
 - d. SLIP and PAP
 - e. CHAP and MS-CHAP
 - f. 802.1x
 11. Malware
 - a. Virus, worm, Trojan horse
 - b. Spyware and spamware
 - c. Rootkit
 - d. AV programs
 - e. AV definitions and updates
 12. Firewall
 - a. MAC and IP based
 - b. Port filter
 - c. URL, time-of-day, and keyword restrictions
 - d. IDS and IPS
 - e. Stateful packet inspection (SPI)
 - f. External threats and mitigation techniques
 13. Security Policy
 - a. Backups
 - b. Cold site, warm site, hot site
 - c. Acceptable use
 - d. Vulnerability analysis and threat detection
 - e. Training
 14. Wireless Networking
 - a. IEEE 802.11a,b,g,n, ac, & ax
 - b. Antenna types
 - c. Wireless security
 - d. WEP, WPA, WPAII, IEEE 802.11i
 - e. PSK vs Enterprise mode
 15. Cellular Wireless

- a. Frequencies
- b. Speed
- c. Standards
 - i. 3G
 - ii. 4G
 - iii. 5G
- d. Radiation
- e. Interference

Laboratory or Activity Content

1. Cabling
 - a. Make an Ethernet straight-through cable
 - b. Make an Ethernet crossover cable
 - c. Punch down cable into a data jack with 110 tool
 - d. Test out cable with a cable tester
2. Create a LAN
 - a. Cable computers, switch, and router
 - b. Configure IP address settings including IP address, subnet mask, gateway, and DNS server
 - c. Configure firewall to permit/deny specific network traffic
 - d. Verify connectivity using ping command
3. Create a wireless LAN
 - a. Configure a wireless router to support an 802.11n or higher wireless network
 - b. Configure SSID, channel, and administrator password on the wireless router
 - c. Select WPAII encryption and create a secure passphrase
 - d. Implement a MAC address filter
 - e. Adjust power levels on the transceiver to control signal propagation
 - f. Configure a host to connect to SSID and enter the appropriate WPAII passphrase to connect host to wireless router
4. TCP/IP Utilities
 - a. Use ping to verify connectivity
 - b. Use tracert to view the path a packet takes from source to destination
 - c. Use ipconfig and ipconfig/all to gather IP addressing information
 - d. Use netstat to verify current TCP/UDP connections
 - e. Use nslookup to view DNS server information
5. Security
 - a. Configure port security on a switch
 - b. Configure host based firewall to permit or deny specific programs
 - c. Configure advanced host based firewall to permit or deny specific protocol traffic
 - d. Configure access-control lists on a router to control source to destination network traffic and permit or deny based on port number
 - e. Utilize Anti-Virus software to update and perform scans at regular intervals
 - f. Analyze output of AV scans for malware
 - g. Utilize heuristic based AV software and analyze results
6. Updates and Patching
 - a. Utilize Windows Update feature to schedule OS updates to occur at regular intervals
 - b. Utilize Windows Update to patch specific 3rd party applications
 - c. Patch applications with the most recent updates using manufacturer websites
 - d. Utilize Windows to update drivers from specific manufacturers
 - e. Patch drivers using manufacturer websites
 - f. Roll back drivers that are causing system issues
7. Cellular
 - a. Bandwidth tests of the various standards in a specific location
 - b. Comparison of cellular bandwidth vs WiFi bandwidth
 - c. Wireless hotspot configuration and analysis of network performance
 - d. Security

Methods of Evaluation

Which of these methods will students use to demonstrate proficiency in the subject matter of this course? (Check all that apply):

Problem solving exercises
Skills demonstrations
Written expression

Methods of Evaluation may include, but are not limited to, the following typical classroom assessment techniques/required assignments (check as many as are deemed appropriate):

Computational homework
Essays
Group projects
Individual projects
Laboratory activities
Laboratory reports
Objective exams
Oral presentations
Projects
Problem-Solving Assignments
Problem-solving exams
Quizzes
Reports/papers
Research papers
Skills demonstrations

Instructional Methodology

Specify the methods of instruction that may be employed in this course

Audio-visual presentations
Computer-aided presentations
Collaborative group work
Class activities
Class discussions
Distance Education
Demonstrations
Field trips
Group discussions
Guest speakers
Instructor-guided use of technology
Internet research
Laboratory activities
Lecture
Role-playing
Small group activities

Describe specific examples of the methods the instructor will use:

1. Instructor will use publisher-provided PowerPoints to lecture on CompTIA Network+ course topics.
2. The instructor will introduce labs and demonstrate lab solutions where appropriate.
3. The instructor may summarize current IT events or trends in the IT industry and ask students questions regarding the information that was shared.
4. Small group activities related to researching and reporting out recently released networking devices and the operating systems associated with the intermediary devices.
5. The instructor will illustrate some of the more challenging multiple-choice questions and performance-based questions that students may experience on the CompTIA Network+ certification.

Representative Course Assignments

Writing Assignments

1. Students are required to answer reflection questions at the end of their lab activities to demonstrate that they grasp the material in the lab and to see if they can relate their knowledge to a new networking scenario. An example of this would be for a student to configure an access-control list on a router and then summarize the effect of the ACL on the network and how the ACL may improve network utilization and security.

- Discussion forums may be utilized using the course learning management system. An example would be for a student to respond to a question explaining why it may be better to use a layer 3 switch in a given networking scenario instead of a switch and a router.

Critical Thinking Assignments

- Evaluation of a security vulnerability on a network when specific ports are open and then write specific recommendations to mitigate the risk while still allowing necessary traffic.
- Students will evaluate the technology needs of a fictitious company and determine a solution that best meets the needs of the customer. For example, a company is currently managing their own datacenter but they would like to know the advantages and disadvantages of moving from on-premise to cloud. The student will perform an objective analysis and evaluation of the situation and provide a recommendation based on their best judgement.

Reading Assignments

- Students are required to read and study the information in the assigned chapter of the book in between classes in order to be prepared for the lecture and classroom activities. A typical reading activity would be for the students to read the chapter on IP addressing so that they are prepared to configure devices with the proper IPv4 and IPv6 address settings.
- Students are required to perform reading from assigned support websites such as www.comptia.org (<http://www.comptia.org>), www.arin.net (<http://www.arin.net>), www.cisco.com, www.ietf.org (<http://www.ietf.org>), www.juniper.com, and www.sans.org (<http://www.sans.org>).
- In preparation for lab activities, students may be required to read a portion of a product manual from select manufacturers and interpret diagrams to configure the network devices with either the GUI or CLI.

Skills Demonstrations

- Students will properly cable and configure a LAN, harden the network devices with the proper configuration, and implement an IP addressing scheme using DHCP.
- Students will implement layered wireless LAN security including adjusting the power levels to control signal propagation, MAC address filtering, WPA2-Personal, WPA2-Enterprise, SSID cloaking, and RADIUS user authentication.

Other assignments (if applicable)

- Students are required to complete hands-on activities using a network simulation program outside of class hours. An example of an activity would be for a student to configure a LAN with a hub and then configure a LAN with a switch and run the simulation comparing performance of the LAN with each device and summarizing the difference between how a hub and switch handle network traffic.
- In order to prepare for the CompTIA Network+ certification, students will be required to answer certification preparation questions and take a CompTIA Network+ simulated exam.

Outside Assignments

Representative Outside Assignments

- Students will be required to read the assigned CompTIA Network+ curriculum to be properly prepared for the lecture, class activities, and lab activities.
- Students need to complete simulated labs from the courseware as part of their grade in the class and to be properly prepared for the CompTIA Network+ certification at the end of the semester.
- Students will be assigned Network+ certification prep questions and performance-based simulated labs that will help prepare them for success on the final exam and the CompTIA Network+ certification.

Articulation

C-ID Descriptor Number

ITIS 150

Status

Aligned

Comparable Courses within the VCCCD

CNSE M01 - Networking Fundamentals

Equivalent Courses at other CCCs

College	Course ID	Course Title	Units
Hancock College	EL 106	Networking Essentials 1	3

District General Education**A. Natural Sciences****B. Social and Behavioral Sciences****C. Humanities****D. Language and Rationality****E. Health and Physical Education/Kinesiology****F. Ethnic Studies/Gender Studies****CSU GE-Breadth****Area A: English Language Communication and Critical Thinking****Area B: Scientific Inquiry and Quantitative Reasoning****Area C: Arts and Humanities****Area D: Social Sciences****Area E: Lifelong Learning and Self-Development****Area F: Ethnic Studies****CSU Graduation Requirement in U.S. History, Constitution and American Ideals:****IGETC****Area 1: English Communication****Area 2A: Mathematical Concepts & Quantitative Reasoning****Area 3: Arts and Humanities****Area 4: Social and Behavioral Sciences****Area 5: Physical and Biological Sciences****Area 6: Languages Other than English (LOTE)****Textbooks and Lab Manuals****Resource Type**

Textbook

Description

Lammle, Todd. CompTIA Network+ Study Guide (4th ed.). Sybex, 2018

Resource Type

Software

Description

Wireshark Protocol Analyzer

Resource Type

Other Instructional Materials

Description

TestOut Network+ Certification Prep Software.

Resource Type

Websites

Description

<http://www.comptia.org>

Distance Education Addendum**Definitions****Distance Education Modalities**

Hybrid (51%–99% online)

Hybrid (1%–50% online)

100% online

Faculty Certifications

Faculty assigned to teach Hybrid or Fully Online sections of this course will receive training in how to satisfy the Federal and state regulations governing regular effective/substantive contact for distance education. The training will include common elements in the district-supported learning management system (LMS), online teaching methods, regular effective/substantive contact, and best practices.

Yes

Faculty assigned to teach Hybrid or Fully Online sections of this course will meet with the EAC Alternate Media Specialist to ensure that the course content meets the required Federal and state accessibility standards for access by students with disabilities. Common areas for discussion include accessibility of PDF files, images, captioning of videos, Power Point presentations, math and scientific notation, and ensuring the use of style mark-up in Word documents.

Yes

Regular Effective/Substantive Contact**Hybrid (1%–50% online) Modality:**

Method of Instruction	Document typical activities or assignments for each method of instruction
Asynchronous Dialog (e.g., discussion board)	Topics will be presented for discussion with the opportunity to provide commentary and feedback on fellow student responses.
E-mail	Email will be used for individual interaction between professor and student, to send group email reminders of deadlines, to inform of upcoming course content.
Face to Face (by student request; cannot be required)	Face to face with students will take place at student request to discuss specific questions, issues, or concerns.
Video Conferencing	Zoom or comparable video conferencing software to lecture on course content, demonstrate lab assignments, answer student questions in real time, and provide student assistance on anything that is course related.
Other DE (e.g., recorded lectures)	Any real-time instruction will be recorded and available to students through the LMS.

Hybrid (51%–99% online) Modality:

Method of Instruction	Document typical activities or assignments for each method of instruction
Asynchronous Dialog (e.g., discussion board)	Topics will be presented for discussion with the opportunity to provide commentary and feedback on fellow student responses.
E-mail	Email will be used for individual interaction between professor and student, to send group email reminders of deadlines, to inform of upcoming course content.

Face to Face (by student request; cannot be required)	Face to face with students will take place at student request to discuss specific questions, issues, or concerns.
Video Conferencing	Zoom or comparable video conferencing software to lecture on course content, demonstrate lab assignments, answer student questions in real time, and provide student assistance on anything that is course related.
Other DE (e.g., recorded lectures)	Any real-time instruction will be recorded and available to students through the LMS.
100% online Modality:	
Method of Instruction	Document typical activities or assignments for each method of instruction
Asynchronous Dialog (e.g., discussion board)	Topics will be presented for discussion with the opportunity to provide commentary and feedback on fellow student responses.
E-mail	Email will be used for individual interaction between professor and student, to send group email reminders of deadlines, to inform of upcoming course content.
Video Conferencing	Zoom or comparable video conferencing software to lecture on course content, demonstrate lab assignments, answer student questions in real time, and provide student assistance on anything that is course related.
Other DE (e.g., recorded lectures)	Any real-time instruction will be recorded and available to students through the LMS.

Examinations

Hybrid (1%–50% online) Modality

Online
On campus

Hybrid (51%–99% online) Modality

Online
On campus

Primary Minimum Qualification

COMPUTER INFORMATION SYS

Additional local certifications required

CompTIA Network+. This course is preparing students for the CompTIA Network+ certification so the instructor needs to hold this certification.

Review and Approval Dates

Department Chair

09/12/2020

Dean

09/14/2020

Technical Review

09/23/2020

Curriculum Committee

09/23/2020

Curriculum Committee

11/25/2020

CCCCO

MM/DD/YYYY

Control Number

CCC000319826

DOE/accreditation approval date

MM/DD/YYYY