

**NETWORKING 2**  
**Course Code 5311**  
**(COURSE NAME CHANGES TO “ADVANCED NETWORKING” IN 2016-17)**

**COURSE DESCRIPTION:** Advanced Networking is designed to provide students with classroom, laboratory, and hands-on experience in current and emerging networking technologies. Upon successful completion of the course sequence within the networking major, students will be able to seek employment or further their education and training in the information technology field.

The networking student will benefit most from the curriculum if he or she possesses a strong background in reading, math, and problem-solving skills.

Instruction is based on mastery of industry domains including advanced network architecture; advanced network operations; advanced network security; advanced network troubleshooting; industry standards, advanced practices, and advanced network theory; and workplace readiness and leadership skills. In addition, instruction and training are provided for the proper care, maintenance, and use of networking software, tools, and equipment.

Particular emphasis is given to the use of critical thinking skills and problem-solving techniques.

**OBJECTIVE:** Given the essential classroom and work-based learning experiences, the student will be able to perform the following advanced competencies.

**PREREQUISITE(S):** Networking Fundamentals (5310)

**COURSE CREDIT:** 1 or 2 Carnegie units

**RECOMMENDED GRADE LEVEL:** 10-12

**A. SAFETY**

1. Review school safety policies and procedures.
2. Review classroom safety rules and procedures.
3. Review safety procedures for using equipment in the classroom.
4. Identify major causes of work-related accidents in office environments.
5. Demonstrate safety skills in an office/work environment.

**B. STUDENT ORGANIZATIONS**

1. Identify the purpose and goals of a Career and Technology Student Organization (CTSO).
2. Explain how CTSOs are integral parts of specific clusters, majors, and/or courses.
3. Explain the benefits and responsibilities of being a member of a CTSO.
4. List leadership opportunities that are available to students through participation in CTSO conferences, competitions, community service, philanthropy, and other activities.

5. Explain how participation in CTSOs can promote lifelong benefits in other professional and civic organizations.

### **C. TECHNOLOGY KNOWLEDGE**

1. Demonstrate proficiency and skills associated with the use of technologies that are common to a specific occupation.
2. Identify proper netiquette when using e-mail, social media, and other technologies for communication purposes.
3. Identify potential abuse and unethical uses of laptops, tablets, computers, and/or networks.
4. Explain the consequences of social, illegal, and unethical uses of technology (e.g., piracy; illegal downloading; licensing infringement; inappropriate uses of software, hardware, and mobile devices in the work environment).
5. Discuss legal issues and the terms of use related to copyright laws, fair use laws, and ethics pertaining to downloading of images, photographs, documents, video, sounds, music, trademarks, and other elements for personal use.
6. Describe ethical and legal practices of safeguarding the confidentiality of business-related information.
7. Describe possible threats to a laptop, tablet, computer, and/or network and methods of avoiding attacks.

### **D. PERSONAL QUALITIES AND EMPLOYABILITY SKILLS**

1. Demonstrate punctuality.
2. Demonstrate self-representation.
3. Demonstrate work ethic.
4. Demonstrate respect.
5. Demonstrate time management.
6. Demonstrate integrity.
7. Demonstrate leadership.
8. Demonstrate teamwork and collaboration.
9. Demonstrate conflict resolution.
10. Demonstrate perseverance.
11. Demonstrate commitment.
12. Demonstrate a healthy view of competition.
13. Demonstrate a global perspective.
14. Demonstrate health and fitness.
15. Demonstrate self-direction.
16. Demonstrate lifelong learning.

### **E. PROFESSIONAL KNOWLEDGE**

1. Demonstrate effective speaking and listening skills.
2. Demonstrate effective reading and writing skills.
3. Demonstrate mathematical reasoning.

4. Demonstrate job-specific mathematics skills.
5. Demonstrate critical-thinking and problem-solving skills.
6. Demonstrate creativity and resourcefulness.
7. Demonstrate an understanding of business ethics.
8. Demonstrate confidentiality.
9. Demonstrate an understanding of workplace structures, organizations, systems, and climates.
10. Demonstrate diversity awareness.
11. Demonstrate job acquisition and advancement skills.
12. Demonstrate task management skills.
13. Demonstrate customer-service skills.

## **F. NETWORKING INDUSTRY-SPECIFIC CONTENT**

### **1.0 Advanced Network Architecture**

- 1.1 Explain the functions and applications of various network devices.
  - Router
  - Switch
  - Multilayer switch
  - Firewall
  - HIDS
  - IDS/IPS
  - Access point (wireless/wired)
  - Content filter
  - Load balancer
  - Hub
  - Analog modem
  - Packet shaper
  - VPN concentrator
- 1.2 Compare and contrast the use of networking services and applications.
  - VPN
    - o Site to site/host to site/host to host
    - o Protocols
      - IPsec
      - GRE
      - SSL VPN
      - PTP/PPTP
  - TACACS/RADIUS
  - RAS
  - Web services
  - Unified voice services
  - Network controllers

1.3 Install and configure the following networking services/applications.

- DHCP
  - o Static vs dynamic IP addressing
  - o Reservations
  - o Scopes
  - o Leases
  - o Options (DNS servers, suffixes)
  - o IP helper/DHCP relay
- DNS
  - o DNS servers
  - o DNS records (A, MX, AAAA, CNAME, PTR)
  - o Dynamic DNS
- Proxy/reverse proxy
- NAT
  - o PAT
  - o SNAT
  - o DNAT
- Port forwarding

1.4 Explain the characteristics and benefits of various WAN technologies.

- Fiber
  - o SONET
  - o DWDM
  - o CWDM
- Frame relay
- Satellite
- Broadband cable
- DSL/ADSL
- ISDN
- ATM
- PPP/Multilink PPP
- MPLS
- GSM/CDMA
  - o LTE/4G
  - o HSPA+
  - o 3G
  - o Edge
- Dialup
- WiMAX
- Metro-Ethernet
- Leased lines
  - o T-1
  - o T-3
  - o E-1
  - o E-3
  - o OC3

- o OC12
  - Circuit switch vs packet switch
- 1.5 Install and properly terminate various cable types and connectors using appropriate tools.
  - Copper connectors
    - o RJ-11
    - o RJ-45
    - o RJ-48C
    - o DB-9/RS-232
    - o DB-25
    - o UTP coupler
    - o BNC coupler
    - o BNC
    - o F-connector
    - o 110 block
    - o 66 block
  - Copper cables
    - o Shielded vs unshielded
    - o CAT3, CAT5, CAT5e, CAT6, CAT6a
    - o PVC vs plenum
    - o RG-59
    - o RG-6
    - o Straight-through vs crossover vs rollover
  - Fiber connectors
    - o ST
    - o SC
    - o LC
    - o MTRJ
    - o FC
    - o Fiber coupler
  - Fiber cables
    - o Single mode
    - o Multimode
    - o APC vs UPC
  - Media converters
    - o Single mode fiber to Ethernet
    - o Multimode fiber to Ethernet
    - o Fiber to coaxial
    - o Single mode to multimode fiber
  - Tools
    - o Cable crimpers
    - o Punch down tool
    - o Wire strippers
    - o Snips
    - o OTDR
    - o Cable certifier

1.6 Differentiate between common network topologies.

- Mesh
  - o Partial
  - o Full
- Bus
- Ring
- Star
- Hybrid
- Point-to-point
- Point-to-multipoint
- Client-server
- Peer-to-peer

1.7 Differentiate between network infrastructure implementations.

- WAN
- MAN
- LAN
- WLAN
  - o Hotspot
- PAN
  - o Bluetooth
  - o IR
  - o NFC
- SCADA/ICS
  - o ICS server
  - o DCS/closed network
  - o Remote terminal unit
  - o Programmable logic controller
- Medianets
  - o VTC
    - ISDN
    - IP/SIP

1.8 Implement and configure the appropriate addressing schema given a scenario.

- IPv6
  - o Auto-configuration
    - EUI 64
  - o DHCP6
  - o Link local
  - o Address structure
  - o Address compression
  - o Tunneling 6to4, 4to6
    - Teredo, miredo
- IPv4
  - o Address structure
  - o Subnetting

- o APIPA
- o Classful A, B, C, D
- o Classless
- Private vs public
- NAT/PAT
- MAC addressing
- Multicast
- Unicast
- Broadcast
- Broadcast domains vs collision domains

1.9 Explain the basics of routing concepts and protocols.

- Loopback interface
- Routing loops
- Routing tables
- Static vs dynamic routes
- Default route
- Distance vector routing protocols
  - o RIP v2
- Hybrid routing protocols
  - o BGP
- Link state routing protocols
  - o OSPF
  - o IS-IS
- Interior vs exterior gateway routing protocols
- Autonomous system numbers
- Route redistribution
- High availability
  - o VRRP
  - o Virtual IP
  - o HSRP
- Route aggregation
- Routing metrics
  - o Hop counts
  - o MTU, bandwidth
  - o Costs
  - o Latency
  - o Administrative distance
  - o SPB

1.10 Identify the basic elements of unified communication technologies.

- VoIP
- Video
- Real time services
  - o Presence
  - o Multicast vs unicast

- QoS
  - o DSCP
  - o COS
- Devices
  - o UC servers
  - o UC devices
  - o UC gateways

1.11 Compare and contrast technologies that support cloud and virtualization.

- Virtualization
  - o Virtual switches
  - o Virtual routers
  - o Virtual firewall
  - o Virtual vs physical NICs
  - o Software defined networking
- Storage area network
  - o iSCSI
  - o Jumbo frame
  - o Fibre Channel
  - o Network attached storage
- Cloud concepts
  - o Public IaaS, SaaS, PaaS
  - o Private IaaS, SaaS, PaaS
  - o Hybrid IaaS, SaaS, PaaS
  - o Community IaaS, SaaS, PaaS

1.12 Given a set of requirements, implement a basic network.

- List of requirements
- Device types/requirements
- Environment limitations
- Equipment limitations
- Compatibility requirements
- Wired/wireless considerations
- Security considerations

## 2.0 Advanced Network Operations

2.1 Use appropriate monitoring tools given a scenario.

- Packet/network analyzer
- Interface monitoring tools
- Port scanner
- Top talkers/listeners
- SNMP management software
  - o Trap
  - o Get
  - o Walk

- o MIBS
- Alerts
  - o Email
  - o SMS
- Packet flow monitoring
- SYSLOG
- SIEM
- Environmental monitoring tools
  - o Temperature
  - o Humidity
- Power monitoring tools
- Wireless survey tools
- Wireless analyzers

2.2 Analyze metrics and reports from monitoring and tracking performance tools given a scenario.

- Baseline
- Bottleneck
- Log management
- Graphing
- Utilization
  - o Bandwidth
  - o Storage
  - o Network device CPU
  - o Network device memory
  - o Wireless channel utilization
- Link status
- Interface monitoring
  - o Errors
  - o Utilization
  - o Discards
  - o Packet drops
  - o Interface resets
  - o Speed and duplex

2.3 Use appropriate resources to support configuration management given a scenario.

- Archives/backups
- Baselines
- On-boarding and off-boarding of mobile devices
- NAC
- Documentation
  - o Network diagrams (logical/physical)
  - o Asset management
  - o IP address utilization
  - o Vendor documentation
  - o Internal operating procedures/policies/standards

2.4 Explain the importance of implementing network segmentation.

- SCADA systems/Industrial control systems
- Legacy systems
- Separate private/public networks
- Honeypot/honeynet
- Testing lab
- Load balancing
- Performance optimization
- Security
- Compliance

2.5 Install and apply patches and updates given a scenario.

- OS updates
- Firmware updates
- Driver updates
- Feature changes/updates
- Major vs minor updates
- Vulnerability patches
- Upgrading vs downgrading
  - o Configuration backup

2.6 Configure a switch using proper features given a scenario.

- VLAN
  - o Native VLAN/Default VLAN
  - o VTP
- Spanning tree (802.1d)/rapid spanning tree (802.1w)
  - o Flooding
  - o Forwarding/blocking
  - o Filtering
- Interface configuration
  - o Trunking/802.1q
  - o Tag vs untag VLANs
  - o Port bonding (LACP)
  - o Port mirroring (local vs remote)
  - o Speed and duplexing
  - o IP address assignment
  - o VLAN assignment
- Default gateway
- PoE and PoE+ (802.3af, 802.3at)
- Switch management
  - o User/passwords
  - o AAA configuration
  - o Console
  - o Virtual terminals
  - o In-band/Out-of-band management
- Managed vs unmanaged

2.7 Install and configure wireless LAN infrastructure and implement the appropriate technologies in support of wireless capable devices.

Small office/home office wireless router

Wireless access points

o Device density

o Roaming

o Wireless controllers

VLAN pooling

LWAPP

Wireless bridge

Site surveys

o Heat maps

Frequencies

o 2.4 Ghz

o 5.0 Ghz

Channels

Goodput

Connection types

o 802.11a-ht

o 802.11g-ht

Antenna placement

Antenna types

o Omnidirectional

o Unidirectional

MIMO/MUMIMO

Signal strength

o Coverage

o Differences between device antennas

SSID broadcast

Topologies

o Adhoc

o Mesh

o Infrastructure

Mobile devices

o Cell phones

o Laptops

o Tablets

o Gaming devices

o Media devices

**3.0 Advanced Network Security**

3.1 Compare and contrast risk related concepts.

Disaster recovery

Business continuity

Battery backups/UPS

- First responders
- Data breach
- End user awareness and training
- Single point of failure
  - o Critical nodes
  - o Critical assets
  - o Redundancy
- Adherence to standards and policies
- Vulnerability scanning
- Penetration testing

### 3.2 Compare and contrast common network vulnerabilities and threats.

- Attacks/threats
  - o Denial of service
    - Distributed DoS
      - Botnet
      - Traffic spike
      - Coordinated attack
    - Reflective/amplified
      - DNS
      - NTP
      - Smurfing
    - Friendly/unintentional DoS
    - Physical attack
      - Permanent DoS
  - o ARP cache poisoning
  - o Packet/protocol abuse
  - o Spoofing
  - o Wireless
    - Evil twin
    - Rogue AP
    - War driving
    - War chalking
    - Bluejacking
    - Bluesnarfing
    - WPA/WEP/WPS attacks
  - o Brute force
  - o Session hijacking
  - o Social engineering
  - o Man-in-the-middle
  - o VLAN hopping
  - o Compromised system
  - o Effect of malware on the network
  - o Insider threat/malicious employee
  - o Zero day attacks

- Vulnerabilities
  - o Unnecessary running services
  - o Open ports
  - o Unpatched/legacy systems
  - o Unencrypted channels
  - o Clear text credentials
  - o Unsecure protocols
    - TELNET
    - HTTP
    - SLIP
    - FTP
    - TFTP
    - SNMPv1 and SNMPv2
  - o TEMPEST/RF emanation

### 3.3 Implement network hardening techniques given a scenario.

- Anti-malware software
  - o Host-based
  - o Cloud/server-based
  - o Network-based
- Switch port security
  - o DHCP snooping
  - o ARP inspection
  - o MAC address filtering
  - o VLAN assignments
    - Network segmentation
- Security policies
- Disable unneeded network services
- Use secure protocols
  - o SSH
  - o SNMPv3
  - o TLS/SSL
  - o SFTP
  - o HTTPS
  - o IPsec
- Access lists
  - o Web/content filtering
  - o Port filtering
  - o IP filtering
  - o Implicit deny
- Wireless security
  - o WEP
  - o WPA/WPA2
    - Enterprise
    - Personal
  - o TKIP/AES

- o 802.1x
- o TLS/TTLS
- o MAC filtering
- User authentication
  - o CHAP/MSCHAP
  - o PAP
  - o EAP
  - o Kerberos
  - o Multifactor authentication
  - o Two-factor authentication
  - o Single sign-on
- Hashes
  - o MD5
  - o SHA

### 3.4 Compare and contrast physical security controls.

- Mantraps
- Network closets
- Video monitoring
  - o IP cameras/CCTVs
- Door access controls
- Proximity readers/key fob
- Biometrics
- Keypad/cipher locks
- Security guard

### 3.5 Install and configure a basic firewall given a scenario.

- Types of firewalls
  - o Host-based
  - o Network-based
  - o Software vs hardware
  - o Application aware/context aware
  - o Small office/home office firewall
  - o Stateful vs stateless inspection
  - o UTM
- Settings/techniques
  - o ACL
  - o Virtual wire vs routed
  - o DMZ
  - o Implicit deny
  - o Block/allow
    - Outbound traffic
    - Inbound traffic
  - o Firewall placement
    - Internal/external

3.6 Explain the purpose of various network access control models.

- 802.1x
- Posture assessment
- Guest network
- Persistent vs non-persistent agents
- Quarantine network
- Edge vs access control

3.7 Summarize basic forensic concepts.

- First responder
- Secure the area
  - o Escalate when necessary
- Document the scene
- eDiscovery
- Evidence/data collection
- Chain of custody
- Data transport
- Forensics report
- Legal hold

#### **4.0 Advanced Troubleshooting**

4.1 Implement the following network troubleshooting methodology given a scenario.

- Identify the problem.
  - o Gather information.
  - o Duplicate the problem, if possible.
  - o Question users.
  - o Identify symptoms.
  - o Determine if anything has changed.
  - o Approach multiple problems individually.
- Establish a theory of probable cause.
  - o Question the obvious.
  - o Consider multiple approaches.
    - Top-to-bottom/bottom-to-top OSI model
    - Divide and conquer
- Test the theory to determine cause.
  - o Once theory is confirmed, determine next steps to resolve problem.
  - o If theory is not confirmed, re-establish new theory or escalate.
- Establish a plan of action to resolve the problem and identify potential effects.
- Implement the solution or escalate as necessary.
- Verify full system functionality and if applicable implement preventative measures.
- Document findings, actions, and outcomes.

4.2 Given a scenario, analyze and interpret the output of troubleshooting tools.

- Command line tools
  - o ipconfig

- o netstat
- o ifconfig
- o ping/ping6/ping -6
- o tracert/tracert -6/traceroute6/traceroute -6
- o nbtstat
- o nslookup
- o arp
- o mac address lookup table
- o pathping
- Line testers
- Certifiers
- Multimeter
- Cable tester
- Light meter
- Toner probe
- Speed test sites
- Looking glass sites
- WiFi analyzer
- Protocol analyzer

4.3 Given a scenario, troubleshoot and resolve common wireless issues.

- Signal loss
- Interference
- Overlapping channels
  - o Mismatched channels
- Signal-to-noise ratio
- Device saturation
- Bandwidth saturation
- Untested updates
- Wrong SSID
- Power levels
- Open networks
- Rogue access point
- Wrong antenna type
- Incompatibilities
- Wrong encryption
- Bounce
- MIMO
- AP placement
- AP configurations
  - o LWAPP
  - o Thin vs thick
- Environmental factors
  - o Concrete walls
  - o Window film
  - o Metal studs

- Wireless standard related issues
  - o Throughput
  - o Frequency
  - o Distance
  - o Channels
  
- 4.4 Given a scenario, troubleshoot and resolve common copper cable issues.
  - Shorts
  - Opens
  - Incorrect termination (mismatched standards)
    - o Straight-through
    - o Crossover
  - Cross-talk
    - o Near end
    - o Far end
  - EMI/RFI
  - Distance limitations
  - Attenuation/Db loss
  - Bad connector
  - Bad wiring
  - Split pairs
  - Tx/Rx reverse
  - Cable placement
  - Bad SFP/GBIC - cable or transceiver
  
- 4.5 Given a scenario, troubleshoot and resolve common fiber cable issues.
  - Attenuation/Db loss
  - SFP/GBIC - cable mismatch
  - Bad SFP/GBIC - cable or transceiver
  - Wavelength mismatch
  - Fiber type mismatch
  - Dirty connectors
  - Connector mismatch
  - Bend radius limitations
  - Distance limitations
  
- 4.6 Given a scenario, troubleshoot and resolve common network issues.
  - Incorrect IP configuration/default gateway
  - Broadcast storms/switching loop
  - Duplicate IP
  - Speed and duplex mismatch
  - End-to-end connectivity
  - Incorrect VLAN assignment
  - Hardware failure
  - Misconfigured DHCP
  - Misconfigured DNS

- Incorrect interface/interface misconfiguration
- Cable placement
- Interface errors
- Simultaneous wired/wireless connections
- Discovering neighboring devices/nodes
- Power failure/power anomalies
- MTU/MTU black hole
- Missing IP routes
- NIC teaming misconfiguration
  - o Active-active vs active-passive
  - o Multicast vs broadcast

4.7 Given a scenario, troubleshoot and resolve common security issues.

- Misconfigured firewall
- Misconfigured ACLs/applications
- Malware
- Denial of service
- Open/closed ports
- ICMP related issues
  - o Ping of death
  - o Unreachable default gateway
- Unpatched firmware/OSs
- Malicious users
  - o Trusted
  - o Untrusted users
  - o Packet sniffing
- Authentication issues
  - o TACACS/RADIUS misconfigurations
  - o Default passwords/settings
- Improper access/backdoor access
- ARP issues
- Banner grabbing/OUI
- Domain/local group configurations
- Jamming

4.8 Given a scenario, troubleshoot and resolve common WAN issues.

- Loss of internet connectivity
- Interface errors
- Split horizon
- DNS issues
- Interference
- Router configurations
- Customer premise equipment
  - o Smart jack/NIU
  - o Demarc
  - o Loopback

- o CSU/DSU
- o Copper line drivers/repeaters
- Company security policy
  - o Throttling
  - o Blocking
  - o Fair access policy/utilization limits
- Satellite issues
  - o Latency

## 5.0 Industry Standards, Advanced Practices, and Advanced Network Theory

5.1 Analyze a scenario and determine the corresponding OSI layer.

- Layer 1 – Physical
- Layer 2 – Data link
- Layer 3 – Network
- Layer 4 – Transport
- Layer 5 – Session
- Layer 6 – Presentation
- Layer 7 – Application

5.2 Explain the basics of network theory and concepts.

- Encapsulation/de-encapsulation
- Modulation techniques
  - o Multiplexing
  - o De-multiplexing
  - o Analog and digital techniques
  - o TDM
- Numbering systems
  - o Binary
  - o Hexadecimal
  - o Octal
- Broadband/base band
- Bit rates vs baud rate
- Sampling size
- CDMA/CD and CSMA/CA
- Carrier detect/sense
- Wavelength
- TCP/IP suite
  - o ICMP
  - o UDP
  - o TCP
- Collision

5.3 Given a scenario, deploy the appropriate wireless standard.

- 802.11a
- 802.11b

- 802.11g
  - 802.11n
  - 802.11ac
- 5.4 Deploy the appropriate wired connectivity standard given a scenario.
- Ethernet standards
    - 10BaseT
    - 100BaseT
    - 1000BaseT
    - 1000BaseTX
    - 10GBaseT
    - 100BaseFX
    - 10Base2
    - 10GBaseSR
    - 10GBaseER
    - 10GBaseSW
    - IEEE 1905.1-2013
      - Ethernet over HDMI
      - Ethernet over power line
  - Wiring standards
    - EIA/TIA 568A/568B
  - Broadband standards
    - DOCSIS
- 5.5 Implement the appropriate policies or procedures given a scenario.
- Security policies
    - Consent to monitoring
  - Network policies
  - Acceptable use policy
  - Standard business documents
    - SLA
    - MOU
    - MSA
    - SOW
- 5.6 Summarize safety practices.
- Electrical safety
    - Grounding
  - ESD
    - Static
  - Installation safety
    - Lifting equipment
    - Rack installation
    - Placement
    - Tool safety
  - MSDS

- Emergency procedures
  - o Building layout
  - o Fire escape plan
  - o Safety/emergency exits
  - o Fail open/fail close
  - o Emergency alert system
- Fire suppression systems
- HVAC

5.7 Install and configure equipment in the appropriate location using best practices given a scenario.

- Intermediate distribution frame
- Main distribution frame
- Cable management
  - o Patch panels
- Power management
  - o Power converters
  - o Circuits
  - o UPS
  - o Inverters
  - o Power redundancy
- Device placement
- Air flow
- Cable trays
- Rack systems
  - o Server rail racks
  - o Two-post racks
  - o Four-post racks
  - o Free-standing racks
- Labeling
  - o Port labeling
  - o System labeling
  - o Circuit labeling
  - o Naming conventions
  - o Patch panel labeling
- Rack monitoring
- Rack security

5.8 Explain the basics of change management procedures.

- Documenting reason for a change
- Change request
  - o Configuration procedures
  - o Rollback process
  - o Potential impact
  - o Notification
- Approval process

- Maintenance window
  - o Authorized downtime
- Notification of change
- Documentation
  - o Network configurations
  - o Additions to network
  - o Physical location changes

5.9 Compare and contrast the following ports and protocols.

- 80 HTTP
- 443 HTTPS
- 137-139 NetBIOS
- 110 POP
- 143 IMAP
- 25 SMTP
- 5060/5061 SIP
- 2427/2727 MGCP
- 5004/5005 RTP
- 1720 H.323
- TCP
  - o Connection-oriented
- UDP
  - o Connectionless

5.10 Configure and apply the appropriate ports and protocols given a scenario.

- 20,21 FTP
- 161 SNMP
- 22 SSH
- 23 Telnet
- 53 DNS
- 67,68 DHCP
- 69 TFTP
- 445 SMB
- 3389 RDP