CompTIA

Network +
N10-007

Reference Pack

Green Acres Technology, LLC CompTIA N10-007 Network + Reference Pack

Written by Aaron Galipeau

http://www.greenacres.tech

First Edition: May 2020

Trademark Acknowledgements

Warning and Disclaimer

This book is designed to provide information about the CompTIA N10-007 Network + certification exam. This pack may include content, typographical, and/or other errors. Therefore, this book should serve only as a general guide and not as the ultimate source of subject information. The author shall have no liability or responsibility to any person or entity regarding any loss or damage incurred, or alleged to have incurred, directly or indirectly, by the information contained in this book.

Table of Contents

1.0 Networking Concepts

1.1 – Explain the purposes and uses of ports and protocols

Ports and Protocols

Protocols are sets of clearly defined rules, regs, standards, and procedures that enable hardware and software developers to make devices and apps function properly at a specific layer.

Protocol	Protocol Name	Port	Description
SSH	Secure Shell	22	Encrypted console login
DNS	Domain Name System	53	Converts domain names to IP addresses
SMTP	Simple Mail Transfer Protocol	25	Transfer email between mail servers
SFTP	Secure File Transfer Protocol	22	Secure file transfer
FTP	File Transfer Protocol	20, 21	Sends and receives files between systems
TFTP	Trivial File Transfer Protocol	69	Primarily designed to read or write files by using a remote server
TELNET	Telecommunication Network	23	Remote console login to network devices
DHCP	Dynamic Host Configuration Protocol	67, 68	Automated IP addressing and configuration
HTTP	Hypertext Transfer Protocol	80	Web server communication
HTTPS	Hypertext Transfer Protocol Secure	443	Web server communication, encrypted
SNMP	Simple Network Management Protocol	161	Gather statistics and manage network devices
RDP	Remote Desktop Protocol	3389	Graphical display of remote device
NTP	Network Time Protocol	123	Synchronize clocks on the Network
SIP	Session Initiation Protocol	5060, 5061	Voice over IP signaling protocol
SMB	Server Message Block	445	Windows file transfers and printer sharing
POP	Post Office Protocol	110	Receive mail into a mail client
IMAP	Interactive Mail Access Protocol	143	A newer mail client protocol
LDAP	Lightweight Directory Access Protocol	389	Communicate with network directories
LDAPS	SSL/TSL Version Lightweight Directory Access Protocol	636	Communicate with network directories, over SSL

H.323	ITU Telecommunication H.32x protocol series	1720	Voice over IP signaling (VoIP)

Protocol types

Protocol	Name	Description
ICMP	Internet Control Messaging Protocol	https://tools.ietf.org/html/rfc792
UDP	User Datagram Protocol	Connectionless network communication
TCP	Transmission Control Protocol	Connection-oriented network communication
IP	Internet Protocol	Host-to-Host datagram service

Connection-oriented vs. connectionless

Connectionless - Communication sent between two network endpoints without any prior arrangement

- Rules represent the connection
- Stateless connections
- This is the case with most Internet transmissions
- Examples
  - IP/UDP/ICMP/IPX
- Receiver does not acknowledge receipt of packet
- Sending device assumes packet arrived successfully
- Enable faster communication between devices

Connection-Oriented

An established connection must be made in order for communication to happen. TCP is a good example because, if working, the rules governing TCP ensure that "that" connection between the systems is reliable and connected.

- Reliable transport method
- Receiving device sends an acknowledgement upon successfully receiving packet

1.2 – Explain devices, applications, protocols and services at their appropriate OSI layers

Layer 1 – Physical

The physical movement of data between devices is the physical layer. The physical layer also includes the cabling and hardware.

What's important?

- Understanding the basics of how it works
- What media is being used?
- What are the physical requirements?
- What can also work or is compatible?

Layer 2 – Data Link

The second layer uses MAC addresses (media access control).

- 48-bit address written in hex code
- Split up into two parts: EUI ~~OUI~~/ Device ID
    - Extended ~~Organizational~~ Unique Identifier – no other manufacturer may use these – first 6 digits
    - Device ID - Last 6 digits

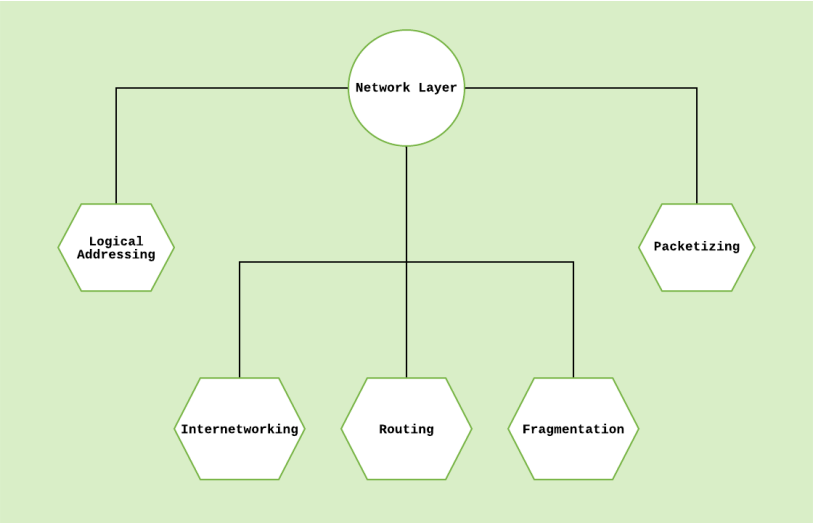
NO TWO NICS ever share the same MAC address. (However, you can run into duplicate MACs, see section 5.5)

Layer 3 – Network

This layer is responsible for packet addressing and converting addresses logical to physical. Routing is performed exclusively at the network layer.

Layer three uses IP addresses. There are two kinds: IPv4 and IPv6.

IPv4 – 32-bit address / IPv6 – 128-bit address



The network layer takes services from the data link layer and performs functions in order to move up the ladder to the transport layer.

Functions:

- Subnet Control
- Subnet Usage Accounting
- Address mapping
    - Translate logical addresses into physical addresses
- Internetworking
    - Provide internetworking between networks
- Logical Addressing
    - Combine large number of networks

    - Define addressing scheme to uniquely identify each device on internetwork
- Packetizing
    - Creates packets upon receiving data from upper layers
    - Packets are created by way of encapsulation
- Fragmentation
    - Divide larger packets into smaller units and identify each one in order to reassemble them into a larger data chunk

Layer 4 – Transport

This layer manages end-to-end message delivery

- Source to destination

Resides at the core of the OSI model

Transport layer takes services from the network layer →Transport layer then provides services to the application layers (upper) [Session layer]

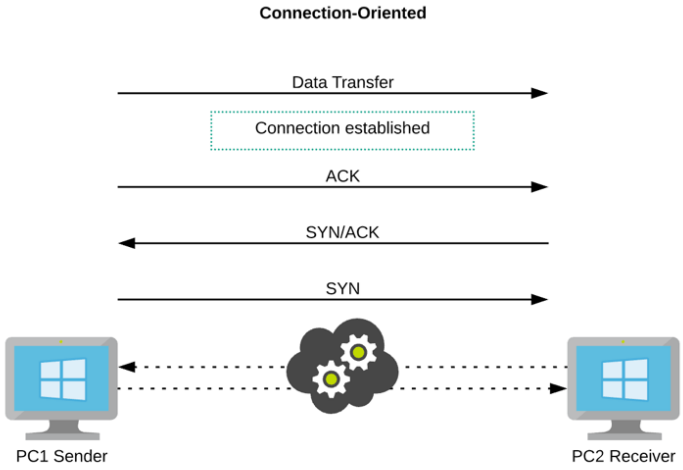
Functions:

- Segmentation of message
    - Accepts message from session layer and passes it to network layer
        - Splits message into packets
- Message acknowledgement and traffic control
- Session multiplexing

    - Uses one logical link
    - Tracks which messages belong to which sessions
- Service point addressing
- Flow control
    - Prevent source device from sending data packets at a faster rate than the destination can handle
- Error control

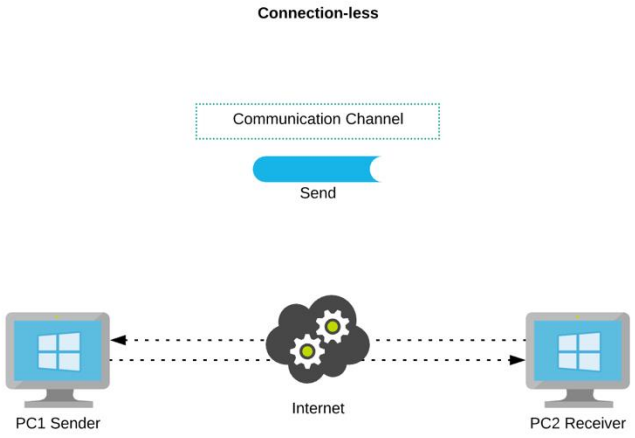
Connection-oriented transmission

- Reliable transport method
- Receiving device sends an acknowledgement upon successfully receiving packet



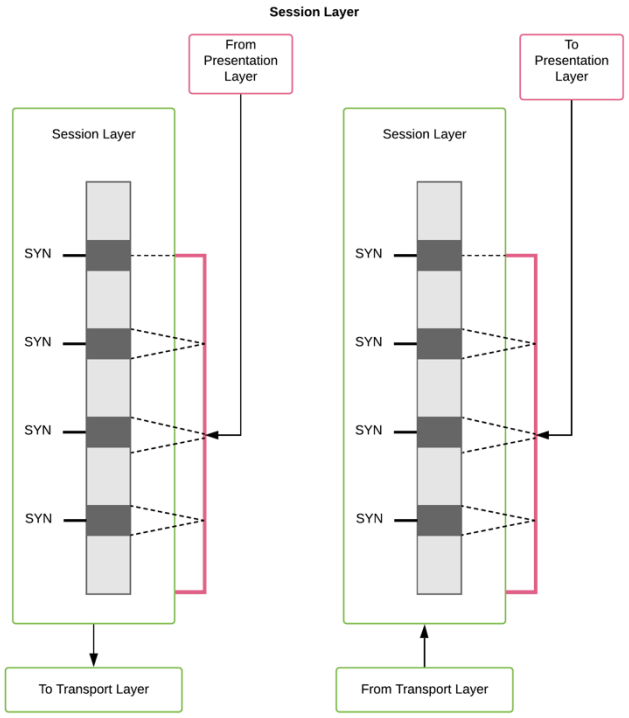
Connectionless transmission

- Receiver does not acknowledge receipt of packet
- Sending device assumes packet arrived successfully
- Enable faster communication between devices



Layer 5 – Session

This layer represents the beginning, maintenance, and ending of a communication. The session layer regulates the flow of data between devices.



Session protocol defines the parameters for the connections.

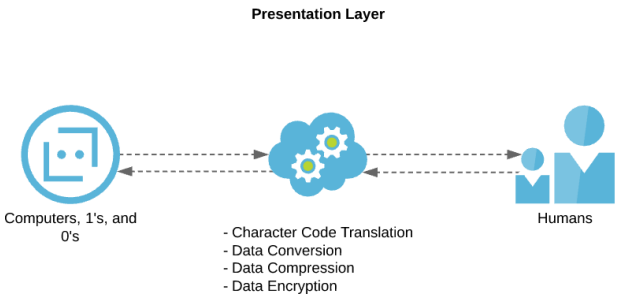
- Manages the transfer of data
    - Who can transfer? How long?

Functions:

- Session establishment, maintenance, termination
    - Enables two different machines to establish a session
- Session support
    - Security, Name recognition, Login
- Dialog control
    - Determines which device communicates first and how much data will be sent
    - Types of dialog control:
        - Simplex – One-way street
        - Half duplex – Two-way street / I go then you go
        - Full duplex – Two-way street / We both go at the same time
- Dialog separation
    - Adds checkpoints or markers within a message
- Protocols
    - NetBIOS, Named pipes, RPC

Layer 6 – Presentation

The “translation” layer



Presents data in a uniform format

- Masks any difference in data between two different systems

Formats data that will be presented to the application layer

Translates data into a common format known to the application layer at the receiving station

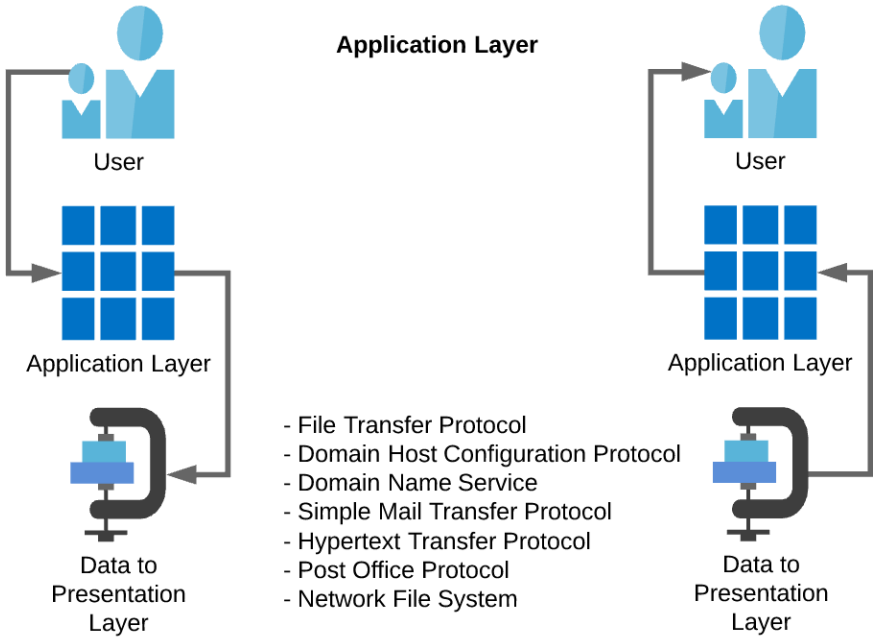
Functions:

- Character code translation
    - ASCII - American Standard Code for Information Interchange
    - EBCDIC – Extended Binary Coded Decimal Interchange Code
- Data conversion
    - Bit order
    - CR-CR/LF – Carriage Return and Carriage Return Line feed
        - When you hit enter and the carriage is moved back to starting position
        - Line feed: Essentially the same thing for Linux/Unix Systems
    - Integer-floating point
- Data compression
    - Reduce number of bits transmitted on the network
- Data encryption
    - Encrypt data for security – NOTE: Encryption generally adds way more data than is required in order to secure the information
        - Passwords

Layer 7 – Application

This layer serves as the window for users and application processes accessing network services

- Interface between program and protocol stack



Provides network services: FTP | DHCP | DNS | SMTP | HTTP | POP3 | NFS

Functions: Allows users to interact with applications

- Application accepts user input and passes data down to lower layers
- Allows for easier application compatibility and implementation
- Applications do not have to be rewritten for different types of network environments

FTAM applications – File Transfer, Access, and Management

- Multiple types of FTAM applications can be used to access and modify files remotely

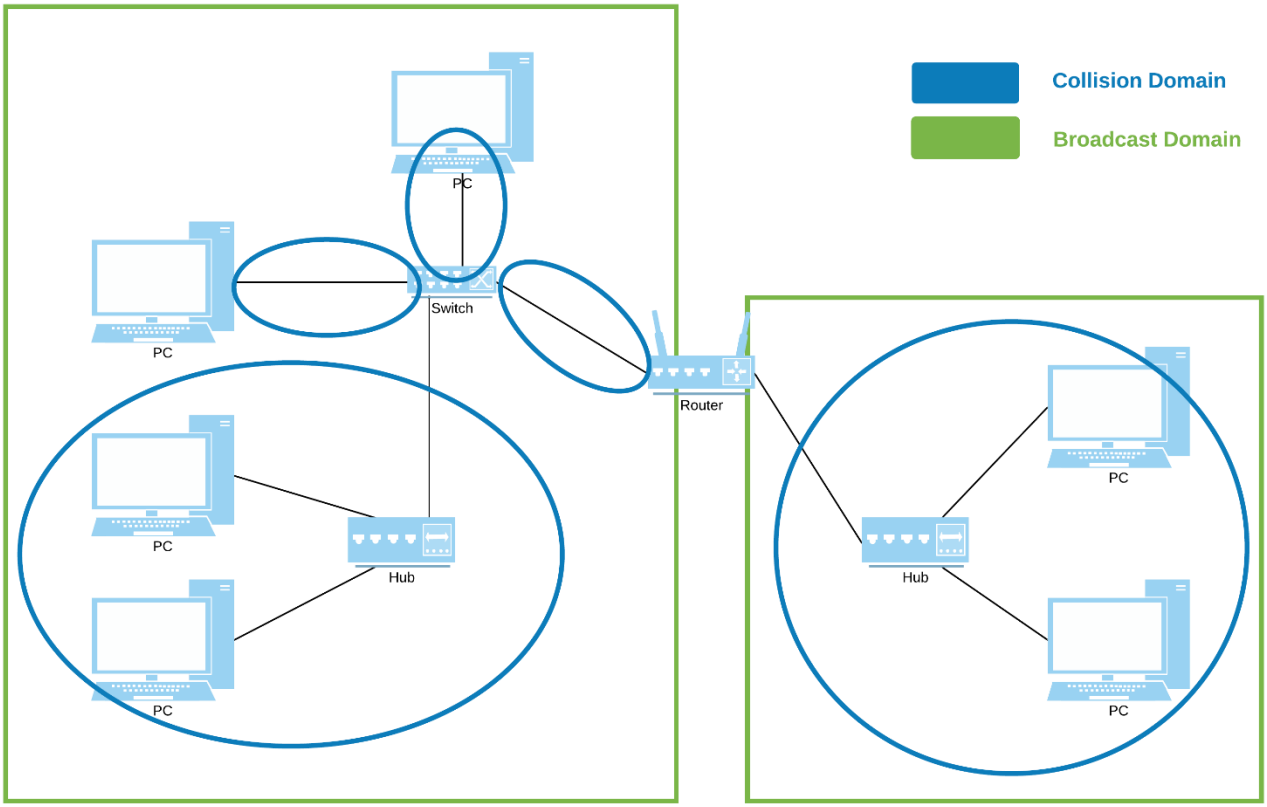
Author Note: As a developer, I don't have to worry about developing something for the user on a specific networking environment. It's taken care of if I'm doing everything within the standard protocols. **Compatibility is not really a concern.**

1.3 – Explain the concepts and characteristics of routing and switching

Properties of network traffic

Broadcast domains

A logical division of a computer network, where all nodes can connect, by broadcast, at the data link layer. It can be within the same LAN segment or it can be bridged to other



LAN segments.

According to Mike Meyer's, it is a network of computers that will hear each other's broadcasts. It is the same as collision domain.

CSMA/CD

Carrier Sense Multiple Access / Collision Detection – In Ethernet networks, this is used to determine if the line is being used. If the line is used, the node will wait, then try again. If not, the node will send the data frame.

CSMA/CA

Carrier Sense Multiple Access / Collision Avoidance – Unlike CSMA/CD which deals with actual collisions, this protocol is used to prevent collisions before they happen.

Collision domains

A segment of a network connected by shared unit where simultaneous data transmissions collide with each other.

Protocol data units

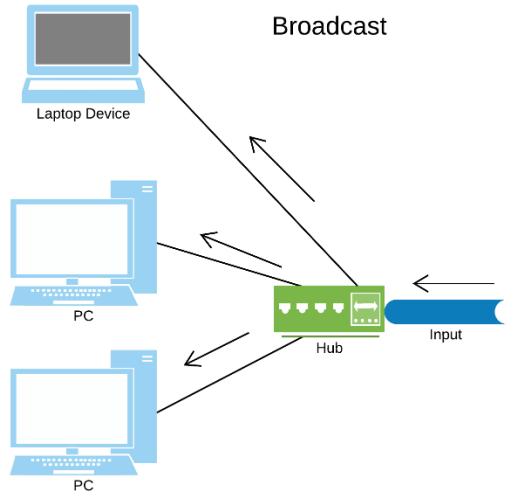
A PDU is a single unit of information transmitted among peer entities of a computer network. It is made up of protocol specific control information and user data.

MTU

A maximum transmission unit is the largest packet or frame size, specified in octets that can be sent in a single packet- or frame-based network.

Broadcast

A broadcast is a method of transferring data to all users at the same time.

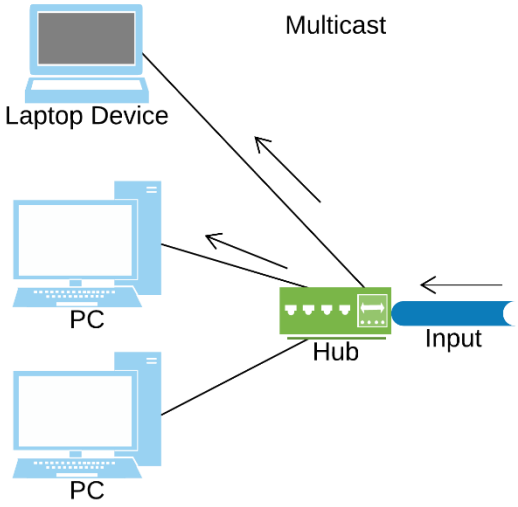


Multicast

A multicast is group communication where data transmission is addressed to a group of computers simultaneously.

Unicast

A unicast is a transmission of a data package or an audiovisual signal to a single recipient. It represents a transmission from one sender and one receiver.



Segmentation and interface properties

VLANs

Virtual Local Area Networks are any broadcast domain that is partitioned and isolated in a computer network at layer 2 of the OSI model. It represents a subnetwork which can group together collections of devices on separate physical LANs.

Trunking (802.1q)

Referred to as Dot1q, Trunking is a networking standard that supports virtual LANs on an Ethernet network. It adds a 32-bit field between the source MAC address and the EtherType fields of the original frame.