31270 Networking Essentials Focus, Pre-Quiz, and Sample Exam Answers

CONTENTS

FOCUS QUESTIONS

CHAPTER 1: EXPLORE THE NETWORK

Server: Computers with software that enable them to provide information, like *email* or *web pages*, to other end devices on the network
Client: Computers with software installed that enable them to request and display the information obtained from the server
Peer-to-Peer: Many computers functioning as the servers and clients on the network
Devices: Physical elements, or hardware, of the network. E.g. PC, switch, router, wireless access point.
Services: Common network applications. E.g. Email hosting services and web hosting services.
Media/Medium: Provides a channel over which a message travels from source to destination
Physical topology diagrams: Identifies the physical location of intermediary devices and cable installation
Logical topology diagrams: Identifies devices, ports, and addressing scheme
LAN (Local Area Network): A network infrastructure that provides access to users and end devices in a small geographical area, which is typically an enterprise, home, or small business network owned and managed by an individual or IT department
WAN (Wide Area Network): A network infrastructure that provides access to other networks over a wide geographical area, which is typically owned and managed by a telecommunications service provider
MAN (Metropolitan Area Network): A network infrastructure that spans a physical area larger than a LAN but smaller than a WAN (e.g., a city). Mans are typically operated by a single entity such as a large organisation.
SAN (Storage Area Network): A network infrastructure designed to support file servers and provide data storage, retrieval and replication.
WLAN (Wireless LAN): Similar to a LAN but wirelessly interconnects users and end points in a small geographical area.
Internet: A worldwide collection of interconnected networks
Intranet: A private connection of LANs and WANs that belong to an organisation – only accessible by the organisation's members/employees
Extranet: Provides secure and safe access to individuals who work for a different organisation, but require access to the organisation's data. E.g., suppliers, customers, and collaborators
Fault Tolerance: a fault tolerant network is one that limits the impact of a failure, so that the fewest number of devices are affected. It is built in a way that allows quick recovery when such a failure occurs.
Scalability: A scalable network can expand quickly to support new users and applications without impacting the performance of the service being delivered to existing users.
Quality of Service (QoS): Managed by the router to ensure that priorities are matched with the type of communication and its importance to the organisation
Security: Securing a network infrastructure includes the physical securing of devices that provide network connectivity, and preventing unauthorized access to the management software that resides on them

Circuit-Switched: A network traditionally used for voice communications. It establishes a dedicated circuit between the source and destination before the user may communicate. If the call is unexpectedly terminated, the users must initiate a new connection.
Packet-Switched: Packet switching splits traffic into packets that are routed over a shared network. A single message, such as an email or a video stream, is broken into multiple message blocks, called packets. Each packet has the necessary addressing information of the source and destination of the message. The routers within the network switch the packets based on the condition of the network at that moment. This means that all the packets in a single message could take very different paths to the destination.
Video Communication: Video is being used for communications, collaboration, and entertainment.
Cloud Computing: Cloud computing allows us to store personal files, even backup our entire hard disk drive on servers over the Internet.

1. What is meant by the Client/Server model of Networking?

In the client-server model, the device requesting the information is called a client and the device responding to the request is called a server.

- **What is a client?** Computers with software installed that enable them to request and display the information obtained from the server
- **What is a server?** Computers with software that enable them to provide information, like *email* or *web pages*, to other end devices on the network
- **Can a client also be a server?** Yes, a peer-to-peer network.
- **Can a server be a client?** Yes, a peer-to-peer network.

2. What is meant by Peer-to-Peer networking? How do peers connect to each other?

- In the peer-to-peer (P2P) networking model, the data is accessed from a peer device without the use of a dedicated server.The P2P network model involves two parts: P2P networks and P2P applications. Both parts have similar features, but in practice work quite differently.
- In a P2P network, two or more computers are connected via a network and can share resources (such as printers and files) without having a dedicated server.

3. Explain the following:

- **LANs**: A network infrastructure that provides access to users and end devices in a small geographical area, which is typically an enterprise, home, or small business network owned and managed by an individual or IT department
- **WANs**: A network infrastructure that provides access to other networks over a wide geographical area, which is typically owned and managed by a telecommunications service provider

How and when are each used?

Lans are used for:

- enterprises, homes, small business networks owned and managed by individual/IT department.
- Interconnect end devices in a limited area. E.g., home, school, office building

WANs are:

- owned and managed by a telecommunications service provider.
- Connect between cities, states, provinces, countries, or continents

4. **Who uses the following Internet connections? How and why are they used?**

- **Leased lines**: reserved circuits within the service provider's network that connect geographically separated offices for private voice and/or data networking. Used by businesses because it offers higher bandwidth.
- **Metro Ethernet**: Ethernet WANs extend LAN access technology into the WAN.
- **DSL** (Digital subscriber line): home users, remote workers, and small office
- **Satellite**: provides a connection when a wired solution is not available. Used by businesses.

5. Some of the new networking trends include:

- **Bring Your Own Device (BYOD)**: BYOD is about end users having the freedom to use personal tools to access information and communicate across a business or campus network.
- **Online collaboration**: the act of working with another or others on a joint project
- **Use of Video**: Video is being used for communications, collaboration, and entertainment. Video calls can be made to and from anywhere with an Internet connection.
- **Cloud computing**: Cloud computing allows us to store personal files, even backup our entire hard disk drive on servers over the Internet.

How are these trends changing the way the Internet is used?

- BYOD gives students flexibility and more learning opportunities
- No longer limited to specific devices that were only tools for work – any device, with any ownership, used anywhere
- For businesses, Cloud computing extends IT's capabilities without requiring investment in new infrastructure, training new personnel, or licensing new software. These services are available on demand and delivered economically to any device anywhere in the world without compromising security or function.
- 'Smart home technology' is technology that is integrated into every-day appliances allowing them to interconnect with other devices, making them more 'smart' or automated.

6. Online Collaboration is now commonplace. Online collaborative includes the use of:

- Communications
- Use of Applications
- Messaging
- Online Collaboration
- Facebook, Twitter, Tumblr etc etc

How can online collaboration be used positively? Are there any negative aspects to online collaboration?

- For organisations across geographic and cultural boundaries
- Gives employees, students, teachers, customers, and partners a way to instantly connect, interact, and achieve their objectives
- Allows businesses to remain competitive
- Education: students need to collaborate to assist in learning, developing team skills, and work on team-based projects

7. What connections are used to access the Internet?

a. Leased lines: Leased lines are actually reserved circuits within the service provider's network that connect geographically separated offices for private voice and/or data networking. The circuits are typically rented at a monthly or yearly rate. They can be expensive.

b. Ethernet – (both cable and fibre):

- Cable - Typically offered by cable television service providers, the Internet data signal is carried on the same cable that delivers cable television. It provides a high bandwidth, always on, connection to the Internet.
- Fibre - Many homes and small offices are more commonly being connected directly with fiber optic cables. This enables an ISP to provide higher bandwidth speeds and support more services such as Internet, phone, and TV.

c. DSL: Business DSL is available in various formats. A popular choice is Symmetric Digital Subscriber Lines (SDSL) which is similar to the consumer version of DSL, but provides uploads and downloads at the same speeds.

8. What are the important features that are required in all networks? Why are these important?

a. Fault tolerance – We want to always stay connected: a fault tolerant network is one that limits the impact of a failure, so that the fewest number of devices are affected. It is built in a way that allows quick recovery when such a failure occurs.

b. Scalability – As we get more devices and hosts it still needs to work: A scalable network can expand quickly to support new users and applications without impacting the performance of the service being delivered to existing users.

c. QoS – Jitter and the breaking up of signals, poor connections: Managed by the router to ensure that priorities are matched with the type of communication and its importance to the organisation

d. Security –

- Security should be implemented in multiple layers, using more than one security solution. If one security component fails to identify and protect the network, others still stand.
- Securing a network infrastructure includes the physical securing of devices that provide network connectivity, and preventing unauthorized access to the management software that resides on them

CHAPTER 2: CONFIGURE A NETWORK OPERATING SYSTEM

1. **Telnet and SSH are two methods of accessing switches and routers. What is the difference between these two methods? Which is the preferred method of connection? Why is this the preferred method?**
    - Telnet:
        - Insecure method of remotely establishing a CLI session through a virtual interface, over a network
        - Does not provide securely encrypted connection
        - User authentication, passwords, and commands are sent over the network in plaintext
    - SSH:
        - Recommended for remote management
        - Provides a secure connection
        - Provides encrypted password authentication and transport of session data

- Keeps user ID, password, and the details of the management session private

2. **Why would ping be used by a network administrator?** To test end-to-end connectivity to another device on the network or a website on the Internet.
3. **How can the '?' be used at the command line when connected to a router or switch?** Entering a question mark '?' at the CLI accesses context-sensitive help to quickly find which commands are available in each command mode.
4. **What are 'Hot Keys' and why should they be used?** 'Hot Keys' make configuring, monitoring, and troubleshooting easier. E.g., tab completes a partial command name entry, Ctrl-Shift-6 is an all-purpose break sequence used to abort DNS lookups, traceroutes, and pings.
5. **What information can be obtained by issuing the 'show version' command? Why is this information important?** The show version command displays information about the version of the Cisco IOS software currently running on the router, the version of the bootstrap program, and information about the hardware configuration, including the amount of system memory.

CHAPTER 3: NETWORK PROTOCOLS & COMMUNICATIONS

COMMUNICATIONS

- **Why are rules necessary?** Rules allow messages to be successfully delivered or processed by the destination host.
- **Who uses rules?** The sender (source), receiver (destination) and a channel (the media that provides the pathway over which the message travels from source to destination).
- **How are rules standardised?** A group of inter-related protocols necessary to perform a communication function is called a protocol suite. Protocol suites are implemented by hosts and networking devices in software, hardware or both.

PROTOCOL SUITES

- **What occurs at each layer of the TCP/IP stack? Example: web server transmitting data to a client.**
    - **Application:** Adds a header to the front of the HTML data, which includes information such as the HTTP version. The layer delivers the data to the transport layer.
    - **Transport:** The transport layer manages individual conversations and adds IP information to the front of the TCP information. IP assigns the appropriate source and destination IP addresses. This information is known as an IP packet.
    - **Internet**: Adds information to both ends of the IP packet, known as a data link frame.
    - **Network Access Layers:** Responsible for delivering the IP packet over the physical medium
- **Who determines the protocols used?** Communications protocols have to be agreed upon by the parties involved. A protocol suite may be specified by a standards organization or developed by a vendor.
- **What are 'Open Standards'?** These protocols are freely available to the public, and any vendor is able to implement these protocols on their hardware or in their software.

What would occur if standards and protocols were not universally adopted? The use of standards in developing and implementing protocols ensures that products from different manufacturers can interoperate successfully. If a protocol is not rigidly observed by a particular