Ôn tập NT113 - Thiết kế mạng

Chương 1

- OSI model: 7 tầng
  - Segment: A single network bounded by a switch or router and based on a particular Layer 1 and Layer 2 protocol such as Fast Ethernet.
  - LAN: A set of switched segments based on a particular Layer 2 protocol such as Fast Ethernet and an interswitch trunking protocol such as the IEEE 802.1Q standard.
  - Building network: Multiple LANs within a building, usually connected to a building backbone network.
  - Campus network: Multiple buildings within a local geographical area (within a few miles), usually connected to a campus-backbone network.
- SDLC:
  - Plan: Network requirements are identified in this phase. This phase also includes an analysis of areas where the network will be installed and an identification of users who will require network services.
  - Design: In this phase, the network designers accomplish the bulk of the logical and physical design, according to requirements gathered during the plan phase.
  - Implement: After the design has been approved, implementation begins. The network is built according to the design specifications. Implementation also serves to verify the design.
  - Operate: Operation is the final test of the effectiveness of the design. The network is monitored during this phase for performance problems and any faults to provide input into the optimize phase of the network life cycle.
  - Optimize: The optimize phase may lead to a network redesign if too many problems arise because of design errors or as network performance degrades over time as actual use and capabilities diverge. Redesign can also be required when requirements change significantly
  - Retire: When the network, or a part of the network, is out-of-date, it might be taken out of production. Although Retire is not incorporated into the name of the life cycle(PDIOO), it is nonetheless an important phase. The retire phase wraps around to the plan phase. The PDIOO life cycle repeats as network requirements evolve.

Chương 2

- Tính sẵn sàng: `Availability = MTBF / (MTBF + MTTR)`

- Giải thích ký hiệu:
  - MTBF: mean time between failure/thời gian không lỗi
  - MTTR: mean time to repair/thời gian sửa lỗi
- Đánh giá hiệu năng:
  - Capacity(bandwith): khả năng truyền dữ liệu, tính bằng bps.
  - Utilization(khả năng sử dụng): phần trăm **capacity** được đang sử dụng.
  - Optimum ultilization(khả năng sử dụng tối đa): trung bình lớn nhất của **utilization**.
  - Throughput(thông lượng): lượng data truyền đi không lỗi trong khoảng thời gian.
  - Offered load: tổng data của các node trong mạng.
  - Accuracy: độ chính xác, liên quan tới các traffic.
  - Efficiency: độ hiệu quả

    ...
- Bốn nguồn gây trễ gói tin:
  $d*{nodal}* = *d*{proc} + d*{queue}* + *d*{trans} + d_{prop} $
  - d_{proc}: xử lí tại nút
  - d_{queue}: xếp hàng
  - d_{trans}: truyền,
    $d_{trans} = \text{chiều dài gói tin(bits)} \ / \ \text{băng thông liên kết(bps)}$
  - d_{prop}: lan truyền,
    $d_{prop} = \text{độ dài đường liên kết vật lí(m)} / \text{tốc độ lan truyền(m/s)}$
  - Queuing delay and bandwidth utilization:
    `queue depth = utilization/(1-utilization)`
    Ex: A packet switch has **five** users, each offering packets at a rate of **10 bps**. The average length of the packets is **1024 bits**. The packet switch needs to transmit this data over a **56-kbps** WAN circuit.
    - Load $= 5 \times 10 \times 1024 = 51,200 (bps)$.
    - Utilization $= \frac{51,200}{56,000}= 91.4 % $
    - Avg packets in queue $= \frac{0.914}{1-0.914} = 10.63 (packets)$

Chương 3

- Data link layer map includes:
  - An indication of the data link layer technology for WANs and LANs (Frame Relay, Point-to-Point Protocol [PPP], VPN, 100-Mbps or 1000-Mbps Ethernet, and so on)
  - The name of the service provider for WANs
  - WAN circuit IDs
  - The location and high-level configuration information for LAN switches (for example, the location of the desired root bridge if the Spanning Tree Protocol [STP] is used)

    - The location and reach of any VLANs and VLAN Trunking Protocol (VTP) configurations
    - The location and high-level configuration of trunks between LAN switches
    - The location and high-level configuration of any Layer 2 firewalls
- Naming network element:
    - Airport code styles: `San Francisco = SFO, Oakland = OAK,...`
    - Standard naming systems: `DNS, for IP networks, or NetBIOS Windows Internet Naming Service (WINS) on Windows networks`
- Wireless installation:
    - Reflection/Phản xạ: Reflection causes the signal to bounce back on itself. The signal can interfere with itself in the air and affect the receiver's ability to discriminate between the signal and noise in the environment. Reflection is caused by metal surfaces such as steel girders, scaffolding, shelving units, steel pillars, and metal doors. Implementing a Wireless LAN (WLAN) across a parking lot can be tricky because of metal cars that come and go.
    - Absorption/Hấp thụ: Some of the electromagnetic energy of the signal can be absorbed by the material in objects through which it passes, resulting in a reduced signal level. Water has significant absorption properties, and objects such as trees or thick wooden structures can have a high water content. Implementing a WLAN in a coffee shop can be tricky if there are large canisters of liquid coffee. Coffee-shop WLAN users have also noticed that people coming and going can affect the signal level. (On StarTrek, a non-human character once called a human "an ugly giant bag of mostly water"!)
    - Refraction/Khúc xạ: When an RF signal passes from a medium with one density into a medium with another density, the signal can be bent, much like light passing through a prism. The signal changes direction and may interfere with the non-refracted signal. It can take a different path and encounter other, unexpected obstructions, and arrive at recipients damaged or later than expected. As an example, a water tank not only introduces absorption, but the difference in density between the atmosphere and the water can bend the RF signal.
    - Diffraction/Nhiễu xạ: Diffraction, which is similar to refraction, results when a region through which the RF signal can pass easily is adjacent to a region in which reflective obstructions exist. Like refraction, the RF signal is bent around the edge of the diffractive region and can then interfere with that part of the RF signal that is not bent.
- Network healthcheck:
    - Performance: peak load
    - Availability: MTBF, MTTR
    - Network utilization: time

- Bandwidth utilization: **absolute usage** specifies how much bandwidth is used by the protocol in comparison to the total capacity of the segment (for example, in comparison to 100 Mbps on Fast Ethernet)
- Accuracy: bit error rate test(BERT), CRC
- Switch ethernet networks: CSMA/CD
- Efficiency: maximum transmission unit(MTU)
- Delay and response time: round-trip time (RTT)
- Status routers, switches, firewalls: CISCO commands
    - `show buffers`
    - `show cdp neighbors detail`
    - `show environment`
    - `show interfaces`
    - `show ip cache flow`
    - `show memory`
    - `show processes`
    - `show running-config`
    - `show startup-config`
    - `show version`

Chương 4

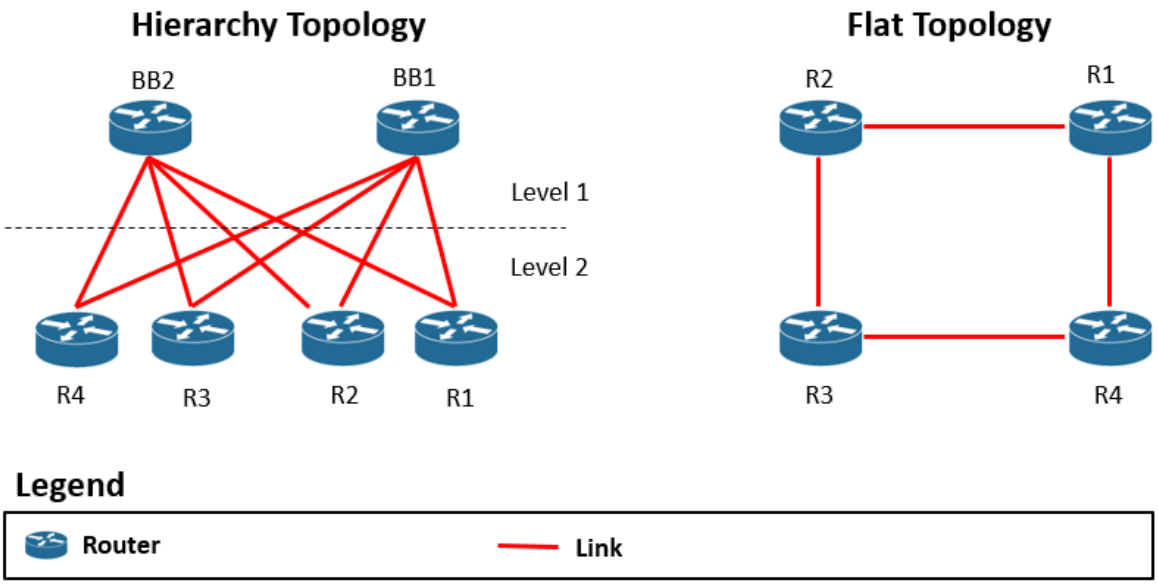
- Traffic flow for network app:
    - Terminal/Host: asysmmetric. The terminal sends a few characters and the host sends many characters.
    - Client/Server: most widely used.
        - Clients send queries and requests to a server. The server responds with data or permission for the client to send data.
        - The flow is usually **bidirectional** and **asymmetric**.
        - Requests from the client are typically small frames, except when writing data to the server, in which case they are larger.
        - Responses from the server range from **64 bytes to 1500 bytes or more**, depending on the maximum frame size allowed for the data link layer in use.
        - Include: Server Message Block (SMB), Network File System (NFS), Apple Filing Protocol (AFP), and NetWare Core Protocol (NCP)
    - Thin Client:
        - A special case of Client/Server, simple.
        - With thin client technology (also known as server-based computing), user applications originate on a central server. In some cases, the application runs on

the central server, and in other cases, the software is installed on the server and is downloaded into the client machine for execution.
        - Advantage: Lower support costs.
        - Disadvantage: the amount of data flowing from the server to the client can be substantial(lớn)
    - Peer-to-Peer:
        - **bidirectional and symmetric**
        - Each host acts as both a client and server.
        - Use: downloading
    - Server/Server:
        - Servers talk to other servers to implement directory services, to cache heavily used data, to mirror data for load balancing and redundancy, to back up data, and to broadcast service availability
        - Bidrectional
    - Distribute computing:
        - Require multiple computing nodes working together to complete a job.
- Broadcast/Multicast:
    - A broadcast frame is a frame that goes to all network stations on a LAN. At the data link layer, the destination address of a broadcast frame is `FF:FF:FF:FF:FF:FF` (all 1s in binary).
    - A multicast frame is a frame that goes to a subset of stations. For example, a frame destined to `01:00:0C:CC:CC:CC` goes to Cisco routers and switches that are running the Cisco Discovery Protocol (CDP) on a LAN.
- Network efficency:
    - Frame size:
        - Using a frame size that is the maximum supported for the medium in use has a positive impact on network performance for bulk applications.
        - In an IP environment, you should avoid increasing the MTU to larger than the maximum supported for the media traversed by the frames, to avoid fragmentation and reassembly of frames.
        - Modern operating systems support MTU discovery, dynamic change.
    - Windowing and flow control:
        - FTP: TCP port 20(data) and TCP port 21(control)
        - Telnet: TCP port 23
        - SMTP: TCP port 25
        - HTTP: TCP port 80
        - SNMP: UDP port 161 and 162
        - DNS: UDP port 53

    - TFTP: UDP port 69
    - DHCP: UDP port 67(server)/68(client)
    - RCP: UDP port 111
- ATM QoS specification:
    - Constant bit rate(CBR)
    - Realtime variable bit rate(rt-VBR)
    - Non-Realtime variable bit rate(nrt-VBR)
    - Unspecified bit rate(UBR)
    - Available bit rate(ABR)
    - Guaranteed frame rate(GFR)

Chương 5

- A typical hierachical topology:
    - `Core layer`: high-end router and switches, optimized for availability and performance.
    - `Distribution layer`: routers and switches, implement policies. In SME, core layer and distribution layer can be combined
- Flat WAN topology:
    - Each site has a WAN router that connects to two other adjacent sites via point-to-point links
    - Low cost and reasonably good availability.



- Flat LAN topology:
    - The PCs and servers implemented a media-access control process, such as token passing or carrier sense multiple access with collision detection (CSMA/CD) to

control access to the shared bandwidth.
    - ...
- Mesh Versus Hierarchical-Mesh Topologies
    - A full-mesh network provides complete redundancy and offers good performance because there is just a single-link delay between any two sites.
    - A partial-mesh network has fewer connections.
    - `number of links in a full-mesh topology = (N * (N - 1)) / 2, N is the number of routers or switches.`
- Classic Three-Layer Hierarchical Model
    - The core layer provides optimal transport between sites.
    - The distribution layer connects network services to the access layer and implements policies regarding security, traffic loading, and routing.
    - In a WAN design, the access layer consists of the routers at the edge of the campus networks. In a campus network, the access layer provides switches or hubs for end user access.
    - Core layer: ACL, Firewalls, IDS(intrusion detection systems)...
    - Distribution layer: VLAN
    - Access layer: routers, switches, bridges shared-media hubs, and wireless access points
- Cisco SAFE architechture:
    - Core: high-speed infrastructure that provides reliable and scalable Layer 2 and Layer 3 transport.
    - Data center: :
        - The data center hosts servers, applications, and storage devices for use by internal users.
        - The data center also connects the network infrastructure that these devices require, including routers, switches, load balancers, content delivery devices, and application acceleration devices.
    - Campus: The campus network provides network access to end users and devices located in a single geographical location.
    - Management:
        - The management network provides monitoring, analysis, authentication, and logging services.
        - Support: RADIUS, Kerberos, Network Time Protocol (NTP), Simple Network Management Protocol (SNMP), and syslog traffic
    - WAN edge: The WAN edge is the portion of the network that aggregates WAN links that connect geographically distant branch offices to a central site or regional hub.

    - Internet edge: The Internet edge is the infrastructure that provides connectivity to the Internet and that acts as a gateway for the enterprise to the rest of the world.
    - Branches: Branches provide connectivity to users and devices at remote locations.
    - Extranet: An extranet allows selected business partners, customers, and suppliers to access a portion of the network via secure protocols.
    - Partner site: Partner sites are networks owned by business partners, customers, and suppliers.
    - E-commerce: The e-commerce module hosts applications, servers, and data used in the selling and buying of products.
    - Teleworker: The teleworker module is the home office of a full-time or part-time employee.
    - Cisco SensorBase: : Cisco SensorBase consists of threat collection servers that receive daily updates from globally deployed sensors regarding threats.
- Rapid Spanning Tree Protocol(RSTP)
    - Bridge port states:
        - `Discarding`: port không học từ địa chỉ MAC hay chuyển tiếp user's frame
        - `Learning`: port học từ địa chỉ MAC để thêm vào bảng địa chỉ MAC nhưng không chuyển tiếp user's frame
        - `Forwarding`: trái ngược `Discarding`
    - Bridge port roles:
        - `Root`: Assigned to the one port on a nonroot bridge that provides the lowest-cost path to the root bridge.
        - `Designated`: Assigned to the one port attached to a LAN that provides the lowest-cost path from that LAN to the root bridge.
        - `Alternate`: Assigned to a port that offers an alternative path in the direction of the root bridge to that provided by the bridge’s root port.
        - `Backup`: Assigned to a port on a designated bridge that acts as a backup for the path provided by a designated port in the direction of the leaves of the spanning tree.
        - `Disabled`: Assigned to a port that is not operational or is excluded from the active topology by network management.
- Hot Standby Router Protocol(HSRP)
    - HSRP works by creating a virtual router, also called a phantom router.
    - The virtual router has its own IP and MAC addresses.
    - Each workstation is configured to use the virtual router as its default gateway.
    - HSRP routers on a LAN communicate among themselves to designate an active and standby router.
    - HSRP also works for proxy ARP.

- Virtual Private Network(VPN)
  - Virtual private networks (VPN) use advanced encryption and tunneling to permit organizations to establish secure, end-to-end, private network connections over a third-party network.
  - Point-to-point connectivity across the third-party network is typically provided by a tunneling protocol. Tunneling is a technique for encapsulating packets of one protocol inside another protocol.
  - **Layer 2** tunneling methods encapsulate at the **data link** layer of the OSI model.
  - **Layer 3** tunneling encapsulates at the **network layer**.
  - Site-to-Site VPN:
    - Most common topologies: Hub-and-spoke, Mesh, Hierarchical network.
  - Remote-access VPN:

Chương 6

- 5 Regional Internet Registries(RIRs)
  - American Registry for Internet Numbers (ARIN)
  - RIPE Network Coordination Centre (RIPE NCC)
  - Asia-Pacific Network Information Centre (APNIC)
  - Latin American and Caribbean Internet Addresses Registry (LACNIC)
  - African Network Information Centre (AfriNIC)
- Private networks:
  - `10.0.0.0 – 10.255.255.255`
  - `172.16.0.0 – 172.31.255.255`
  - `192.168.0.0 – 192.168.255.255`
- Dynamic Host Configuration Protocol(DHCP)
  - DHCP is based on BOOTP, which hosts can interoperate with DHCP hosts
  - DHCP uses a client/server model.
  - DHCP supports three methods for IP address allocation:
    - `Automatic allocation`: A **DHCP server** assigns a **permanent** IP address to a client.
    - `Dynamic allocation`: A **DHCP server** assigns an IP address to a client for a **limited period of time**.
    - `Manual allocation`: A **network administrator** assigns a **permanent** IP address to a client, and DHCP is used simply to convey the assigned address to the client.
  - DHCP Relay Agents:

        - With Cisco routers, you can use the `ip helper-address` command on each router interface where clients reside to cause the router to become a DHCP relay agent.
- Network Address Translation(NAT)
    - Converting addresses from an inside network to addresses that are appropriate for an outside network, and vice versa.
    - NAT is useful when hosts that need access to Internet services have private addresses.
- Classless Routing Versus Classful Routing
    - Class A - C:
        - `Class A`: First bit = 0, Prefix = 8 bits
        - `Class B`: First 2 bits = 10, Prefix = 16 bits
        - `Class C`: First 3 bits = 110, Prefix = 24 bits
    - Route Summarization example(*slide 18 chapter 6*)
        - The branch-office has 4 subnets:
            - `172.16.0.0`
            - `172.17.0.0`
            - `172.18.0.0`
            - `172.19.0.0`
        - The branch-office router can summarize its local network numbers and report that it can reach `172.16.0.0/14`.
        - By advertising this single route, the router is saying, "Route packets to me if the destination has the first 14 bits set to 172.16"
        - The router is reporting a route to all networks where the first 14 bits are equal to `10101100000100` in binary
        - To understand the summarization in this example, you should convert the number 172 to binary, which results in the binary number `10101100`. Convert number 16 - 19 to binary (*slide 19 chapter 6*)
        - Notice that the leftmost 6 bits for the numbers 16 through 19 are identical. This is what makes route summarization with a prefix length of 14 possible in this example.
        - First 8 bits for the networks are identical (all the networks have 172 for the first octet), and the next 6 bits are also identical.
        - TIPS:
            - Mạng lớp nào
            - Cần bao nhiêu mạng con -> mượn bao nhiêu bit
            - Trừ số bit mượn -> CIDR block
- Hierarchy in IPv6 address

- IPv6 increases the IP address size from 32 bits to 128 bits.
- Format: `x:x:x:x:x:x:x:x`
- Must be at least one numeral in every field (except when suppressing multiple fields of 0s)
- You can substitute double colons (::) at the start, middle, or end of an address to indicate consecutive 16-bit fields of 0s.
- Example:
  - This Ipv6: `2031:0000:130F:0000:0000:09C0:876A:130B`
  - Can be: `2031:0:130F::9C0:876A:130B`
  - Can not be: `2031::130F::9C0:876A:130B`
- Global unicast address:
  - `Global routing prefix: n bits`
  - `Subnet ID: m bits`
  - `Interface ID: 128-n-m bits`

Một số cấu hình cơ bản

- VPN-GRE:
  - Configure default route to ISP router:
    - `ip route 0.0.0.0 0.0.0.0 <serial-port-ip>`
  - Configure the GRE tunnel on tunnel router:
    - `interface tunnel <tunnel-interface-name>`
    - `ip address <tunnel-ip> <tunnel-subnetmask>`
    - `tunnel source <tunnel-ip-source>`. **không dùng TUNNEL NAME hoặc TUNNEL IP ADDRESS cho source**
    - `tunnel destination <tunnel-ip-destination>`
  - Enable Routing over the GRE Tunnel on tunnel router:
    - `router ospf <ospf-id>`
    - `network <tunnel-ip> <tunnel-subnetmask> area <area-id>`
- HSRP:
  - Configure HSRP on active router:
    - `interface <hrsp-interface>`
    - `standby version 2`
    - `standby <standby-group-id> ip <hsrp-ip>`. **hsrp-ip thông thường là địa chỉ cuối của mạng(không phải địa chỉ broadcast)**
    - `standby <standby-group-id> priority <priority-num>`. **priority-num mặc định là 100, chọn 1 số lớn hơn cho active router**
    - `standby <standby-group-id> preempt`. **lệnh này chỉ có trên active router**

- Configure HRSP on standby router: tương tự, bỏ 2 câu lệnh cuối.