Hálózatok II. javítóvizsga témakörök – 13.A

Modul 1: Egyterületű OSPFv2-alapfogalmak

1.1. Az OSPF funkciói és jellemzői

1.2. OSPF-csomagok

1.3. Az OSPF működése

Modul 2: Egyterületű OSPFv2 konfigurálása

2.1. OSPF router ID

2.2. Pont-pont OSPF-hálózatok

2.3. OSPF többes hozzáférésű hálózatokban

2.4. Egyterületű OSPFv2 módosítása

2.5. Alapértelmezett útvonal terjesztése

2.6. Egyterületű OSPFv2 ellenőrzése

Modul 3: Hálózatbiztonsági fogalmak

3.1. A kiberbiztonság jelenlegi helyzete
Kiberfenyegetés, Kiberháború, Kiberbiztonsági incidens

3.2. Támadók
Hackerek, Cybercriminals (kiberbűnözők), Internetezési profilok

3.3. Támadóeszközök
Penetrációs tesztelő eszközök, Malware (kártevők) típusok, Social engineering eszközök

3.4. Kártevők
Vírusok, Trójaiak, Ransomware (zsarolóprogramok)

3.5. Gyakori hálózati támadások
DDoS támadások, MITM (Man-In-The-Middle) támadások, Phishing

3.6. IP sebezhetőségek és fenyegetések
IP spoofing, Packet sniffing, IP hijacking

3.7. TCP és UDP sérülékenységek
TCP SYN Flood, UDP Flood, TCP Session Hijacking

3.8. IP szolgáltatások
NAT (Network Address Translation), DHCP (Dynamic Host Configuration Protocol), DNS (Domain Name System)

3.9. Bevált hálózatbiztonsági gyakorlatok
Biztonsági házirendek, Hálózati monitorozás, Incident Response (incident kezelése)

3.10. Kriptográfia
Szimmetrikus és aszimmetrikus titkosítás, Hash funkciók, Digitális aláírások

Modul 4: ACL-alapfogalmak

4.1. Az ACL célja
Hozzáférés-vezérlés lista (ACL), Szűrési politikák, Forrás- és célállomás szűrés

4.2. Helyettesítő maszkok az ACL-ekben
Helyettesítő maszk (Wildcard Mask), CIDR (Classless Inter-Domain Routing), Bit-maszkok

4.3. Útmutató ACL létrehozásához
ACL konfigurációs lépések, ACL szabályok és prioritás, Hozzáférési listák típusai

4.4. Az IPv4-es ACL-ek típusai
Standard ACL, Kiterjesztett ACL, Különleges ACL (pl. név alapú ACL)

4.5. Gyakorlás és ellenőrzés
ACL hibakeresés, Szabályok érvényesítése

Modul 5: Az IPv4-es ACL beállítása

5.1. Normál IPv4-es ACL beállítása
Normál ACL, IP-forrás cím szűrés, ACL konfigurálási parancsok

5.2. IPv4-es ACL módosítása
ACL frissítési parancsok, Szabályok módosítása és eltávolítása, ACL hatékonyságának megőrzése

5.3. VTY-vonalak védelme normál IPv4 ACL-lel
VTY-vonalak (Virtual Terminal Lines), Hozzáférés-szabályozás VTY-vonalakon keresztül, ACL alkalmazás VTY-vonalak védelmére

5.4. Kiterjesztett IPv4-es ACL-ek beállítása
Kiterjesztett ACL, IP-forrás és cél szűrés, Protokoll szűrés és portszámok

Modul 6: IPv4-címfordítás

6.1. A NAT jellemzői
NAT (Network Address Translation), Belépési és kilépési IP-címek, IP-címek átkonvertálása

6.2. A NAT típusai
Statikus NAT, Dinamikus NAT, PAT (Port Address Translation), NAT64

6.3. A NAT előnyei és hátrányai
NAT előnyök (pl. IP-címek megtakarítása, biztonság növelése), NAT hátrányok (pl. teljesítmény csökkenés, problémák a peer-to-peer alkalmazásokkal)

6.4. Statikus NAT
Statikus NAT konfigurálás, IP-címek állandó átkonvertálása

6.5. Dinamikus NAT
Dinamikus NAT konfigurálás, IP-címek dinamikus átkonvertálása

6.6. PAT
Port Address Translation (PAT), NAT overload, Portok használata az IP-címek átkonvertálására

6.7. NAT64
NAT64 konfigurálás, IPv6 és IPv4 közötti átkonvertálás, NAT64 működési elv

Modul 7: WAN Alapismeretek

7.1. Mire jó a WAN?
WAN (Wide Area Network) célja és előnyei, WAN alkalmazások, például távoli irodák összekapcsolása

7.2. A WAN működése
WAN működési elvei, például adatcsomagok továbbítása, WAN komponensek: routerek, switch-ek, stb.

7.3. Hagyományos WAN-kapcsolat

Hagyományos WAN-technológiák (pl. MPLS, Frame Relay, ISDN), Beállítás és konfigurációs lépések

7.4. Korszerű WAN-kapcsolat
Korszerű WAN-technológiák (pl. SD-WAN, MPLS), Korszerű WAN-kapcsolatok előnyei és konfigurálási lehetőségek

7.5. Internet alapú kapcsolat
Internet alapú WAN-kapcsolatok (pl. VPN, Direct Internet Access), Internet alapú kapcsolat előnyei és hátrányai

Modul 8: A VPN és az IPsec Alapfogalmai

8.1. VPN-technológiák
VPN (Virtual Private Network) célja és előnyei, VPN-alapú titkosítás és biztonsági rétegek, VPN-kapcsolatok létrehozásának folyamata

8.2. VPN-típusok
VPN-típusok: Site-to-Site, Remote Access, Client-to-Site, MPLS VPN, Minden típus működési elve és alkalmazási területe

8.3. IPsec
IPsec (Internet Protocol Security) célja és funkciói, IPsec komponensei: AH (Authentication Header), ESP (Encapsulating Security Payload), IPsec működése és konfigurálásának alapjai

Modul 9: A QoS Alapfogalmai

9.1. A hálózati átvitel minősége
QoS (Quality of Service) fogalma, Az átvitel minősége és hatása a hálózati teljesítményre, QoS mérési paraméterek: sávszélesség, késleltetés, jitter, csomagvesztés

9.2. Forgalmi jellemzők
Forgalmi jellemzők: sávszélesség, késleltetés, jitter, csomagvesztés, Forgalmi profilok és típusok

9.3. Várakoztatási algoritmusok
Várakoztatási algoritmusok szerepe és típusai: FIFO (First In, First Out), Priority Queuing, Weighted Fair Queuing (WFQ), Class-Based Weighted Fair Queuing (CBWFQ), Algoritmusok működési elvei és hatásuk a QoS-ra

9.4. QoS-modellek

QoS modellek: IntServ (Integrated Services), DiffServ (Differentiated Services), Modell típusok, jellemzőik és alkalmazási területeik

9.5. A QoS megvalósításának technikái
QoS megvalósítási technikák: Traffic Shaping, Traffic Policing, Congestion Management, QoS mechanizmusok és eszközök

Modul 10: Hálózatfelügyelet

10.1. Eszközfelderítés CDP-vel
CDP (Cisco Discovery Protocol): működés, előnyök, és alapvető parancsok, CDP-táblák és azok elemzése

10.2. Eszközfelderítés LLDP-vel
LLDP (Link Layer Discovery Protocol): működés, előnyök, és alapvető parancsok, LLDP táblák és azok elemzése

10.3. NTP
NTP (Network Time Protocol): működés, szerepe és konfigurációs lehetőségek, NTP időszinkronizálás és időforrások beállítása

10.4. SNMP
SNMP (Simple Network Management Protocol): verziók, működés és alapvető parancsok, SNMP táblák és MIB (Management Information Base) struktúra

10.5. Syslog
Syslog: működés, konfigurálás és üzenetformátumok, Syslog szintjei és jelentések kezelése

10.6. Fájlkezelés routeren és switch-en
Fájlkezelési alapok routereken és switch-eken: fájlok másolása, törlése, áthelyezése, Konfigurációs és rendszerfájlok kezelése

10.7. IOS-képfájl kezelés
IOS-képfájlok: típusok, frissítési eljárások, és kezelési technikák, IOS-képfájlok telepítése és frissítése

Modul 11: Hálózattervezés

11.1. Hierarchikus hálózat
Hierarchikus hálózati architektúra: három szintű felépítés (mag, elosztó, végpont). Előnyök: könnyebb skálázás, kezelhetőség és hibakeresés. Tervezési elvek: sávszélesség, redundancia, forgalomirányítás

11.2. Skálázható hálózatok
Skálázhatóság: hálózati eszközök és topológiák bővíthetősége. Tervezési szempontok: terheléselosztás, redundancia, késleltetés minimalizálás

11.3. Switch hardver
Switch típusok: unmanaged, smart managed, managed. Hardver jellemzők: portok száma, sávszélesség, throughput, stackelési lehetőségek

11.4. Router hardver
Router típusok: core, edge, branch. Hardver jellemzők: processzor teljesítmény, memória, portok típusa és száma

Modul 12: Hálózati hibaelhárítás

12.1. Hálózati dokumentáció
Dokumentáció típusok: topológiai térképek, konfigurációs fájlok, eszközjegyzékek. Dokumentáció célja: hibakeresés támogatása, hálózat kezelhetősége, változáskövetés

12.2. Hibaelhárítási folyamat
Hibaelhárítási lépések: probléma azonosítása, diagnosztika, megoldási javaslatok, tesztelés. Hibaelhárítási metodológia: strukturált megközelítés, szisztematikus problémamegoldás

12.3. Hibaelhárítási eszközök
Eszközök típusai: ping, traceroute, ipconfig/ifconfig, netstat, Wireshark. Eszközök használata: hálózati forgalom elemzése, kapcsolat tesztelése, konfigurációs problémák azonosítása

12.4. Hálózati hibák tünetei és okai
Hálózati hibák típusai: csomagvesztés, késleltetés, hálózati szeparáció. Tünetek és okok: alacsony sávszélesség, megszakadások, konfigurációs hibák

12.5. Az IP-kapcsolat hibaelhárítása
IP-kapcsolat hibái: IP címkonfliktusok, DNS hibák, hálózati forgalom problémák. Hibaelhárítási lépések: IP konfiguráció ellenőrzése, kapcsolat tesztelése, hibás beállítások kijavítása

12.6. Gyakorlás és ellenőrzés
Hibaelhárítási szcenáriók: valós és szimulált hálózati problémák kezelése. Ellenőrzési technikák: megoldások hatékonyságának tesztelése, hibaelhárítási eredmények kiértékelése

Modul 13: Hálózatvirtualizáció

13.1. Felhőalapú szolgáltatások
Felhőszolgáltatások típusai: IaaS (Infrastructure as a Service), PaaS (Platform as a Service), SaaS (Software as a Service). Felhőszolgáltatások előnyei: skálázhatóság, költséghatékonyság, rugalmasság

13.2. Virtualizáció
Virtualizáció típusai: szervervirtualizáció, asztali virtualizáció, alkalmazásvirtualizáció. Virtualizációs technológiák: VMware, Hyper-V, KVM, Xen

13.3. Virtuális hálózati infrastruktúra
Virtuális hálózatok: VLAN, VXLAN, VRF. Virtuális switch-ek és router-ek: OSPF és BGP virtuális környezetben

13.4. Szoftveralapú hálózatok
Szoftveralapú hálózat (SDN): elkülönített vezérlő- és adatlapok. SDN előnyei: dinamikus skálázhatóság, központosított menedzsment

13.5. Kontrollerek
Hálózati kontrollerek szerepe: központosított irányítás és menedzsment. Kontroller típusok: SDN kontrollerek, WLAN kontrollerek

Modul 14: Hálózatautomatizálás

14.1. Az automatizálás áttekintése
Automatizálás szerepe: hatékonyság növelése, hibák csökkentése, gyorsabb konfigurációs változtatások. Automatizálási eszközök: Ansible, Puppet, Chef

14.2. Adatformátumok
Elterjedt adatformátumok: JSON, XML, YAML. Adatformátumok szerepe: adatstruktúrák egységesítése, adatátviteli hatékonyság

14.3. API-k
API (Application Programming Interface): felületek az alkalmazások közötti kommunikációhoz. API típusok: RESTful API, SOAP API

14.4. REST
REST (Representational State Transfer): architekturális stílus az API-k számára. REST alapelvek: stateless, cacheable, uniform interface

14.5. Konfigurációkezelő eszközök
Konfigurációkezelés: eszközök a hálózati konfigurációk automatizálására. Népszerű eszközök: Ansible, Puppet, Chef, SaltStack

14.6. IBN és Cisco DNA Center

IBN (Intent-Based Networking): hálózati automatikus irányítás a szándékok alapján. Cisco DNA Center: Cisco által biztosított IBN platform