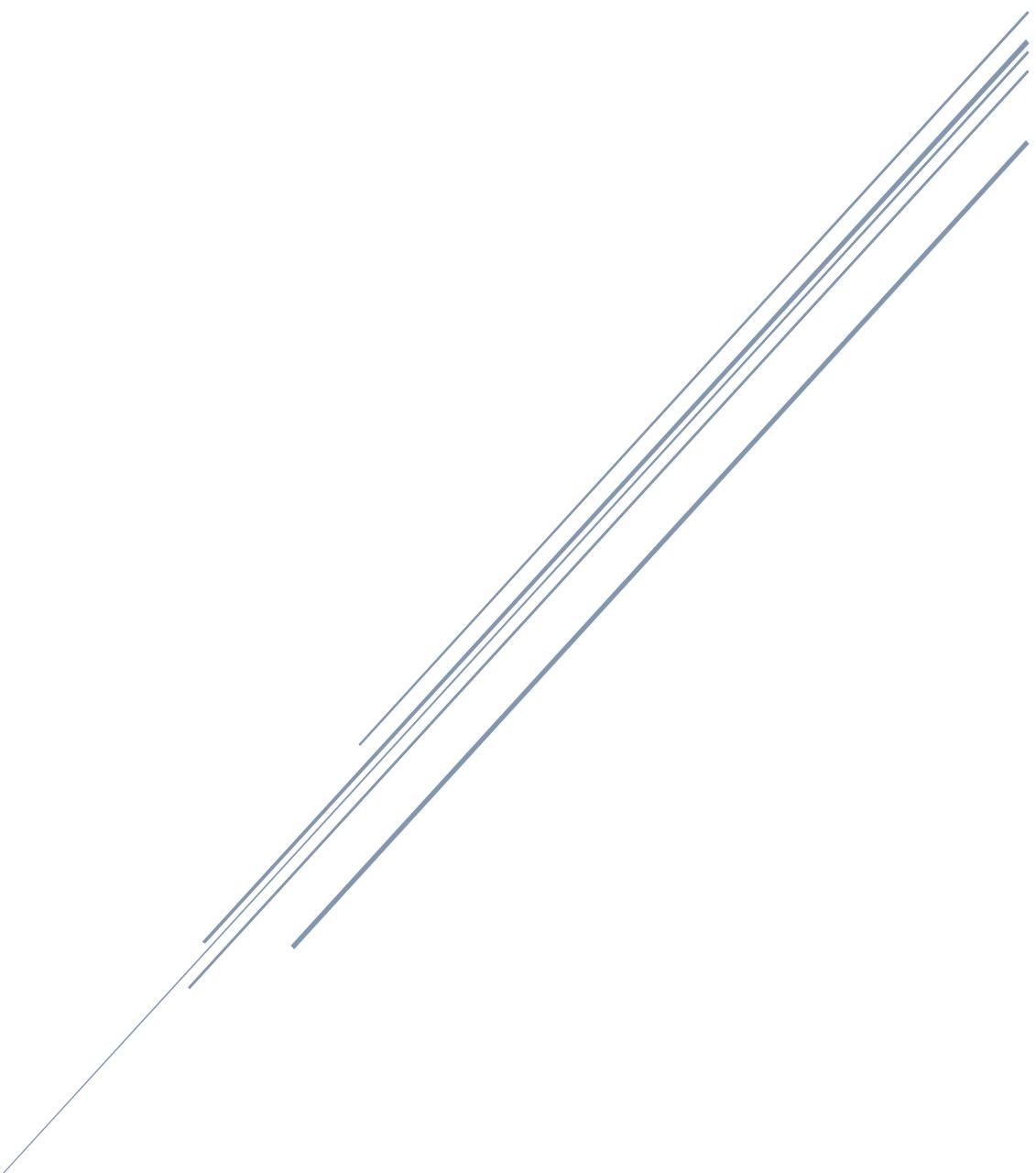


FELHŐSZOLGÁLTATÁSI TECHNOLÓGIÁK ÉS IT BIZTONSÁG SPECIALIZÁCIÓ/HÁLÓZATOK SÁV

(Záróvizsga témakörök)



Óbudai Egyetem
2022/23 tanév

Tartalom

1. Kommunikációs rendszerek alapfunkciói és kialakítási lehetőségeik	17
Protokoll, a protokollfunkciók interfész fogalomra épülő bemutatása	17
Protokollfunkciók.....	17
Kommunikációs rendszerek hierarchikusan rétegezett megvalósításának lényege, előnyei	17
A rétegmodell előnyei:	18
Az átviteli egység (PDU) fogalma, felépítése, az átviteli folyamat leírása.....	18
Felépítése:.....	18
Szomszéd- (kiszolgáló-, kiszolgált-) és társ- (egyenrangú) rétegek közötti kommunikáció	19
Adatbeágyazás, az adatbeágyazás lépései, adatfolyam-vezérlés.....	19
Adatfolyam vezérlés - Flow control.....	19
Az összeköttetés alapú és az összeköttetés-mentes hálózati szolgáltatás, a köztük levő fontosabb különbségek.....	20
Összeköttetés alapú hálózati szolgáltatás	20
Összeköttetés mentes hálózati szolgáltatás	21
2. Hálózati rendszerek ISO OSI modell szerinti kialakítása	23
Miért használjuk a kommunikáció rétegezett modelljét	23
OSI modell rétegei, átviteli egységei, adatbeágyazás lépései, adatfolyam-vezérlés	23
A TCP/IP és az OSI modellek kapcsolata (különbségek, azonosságok).....	26
Hasonlóságok	26
Különbségek.....	26
3. Hálózati rendszerek TCP-IP modell szerinti kialakítása.....	27
Miért használja a hálózati ipar a TCP/IP modellt.....	27
A TCP/IP hálózati modell rétegei és ezek feladatai	27
Az alkalmazási réteg	27
A szállítási réteg	27
Az internetréteg	28
A hálózatelérési réteg	28
Összeköttetés alapú és összeköttetés nélküli szolgáltatások, különbségek, mintapéldák	28
Összeköttetés alapú szolgáltatások.....	28
Összeköttetés nélküli szolgáltatások	28
Hibafeltárási és hibajavítási technikák, ezek megvalósítása a TCP/IP modellben	29
A TCP/IP és az OSI modellek kapcsolata (különbségek, azonosságok).....	30
Hasonlóságok	30
Különbségek.....	30

4. Átviteli közeg	31
Az átviteli közeg rendeltetése, tipikus közegek, jellemzőik, előnyök, korlátok	31
Jelek és zajok, a jeltozulás okai a réz alapú és az optikai átvivő közegben.....	32
Csillapítás és csillapítás torzítás	32
Késleltetés torzítás.....	32
Zaj.....	32
Termikus zaj.....	33
Áthallás.....	33
Impulzus	33
Az osztott használatú átviteli közeg hozzáférési problémái, megoldások	33
A determinisztikus és a nemdeterminisztikus közeghozzáférés indokai, jellemzői és alkalmazása	34
Nemdeterminisztikus.....	34
Determinisztikus.....	34
5. Adatkapcsolat	35
A 2. réteg szolgáltatása, fajtái, mit és hogyan javít az 1. réteg szolgáltatásain.....	35
L2 – Adatkapcsolati réteg	35
A 2. réteg feladatai általánosan és példákon keresztül is a különböző megvalósításokban.	35
A hálózati rétegnek nyújtott szolgáltatások	35
Az adatátviteli szolgáltatás fajtái.....	35
Az adatkapcsolati réteg feladatai.....	36
Adatkapcsolati réteg jellemzői	36
Keretezés	37
Átviteli módok.....	37
Az átviteli hibák felismerési és javítási mechanizmusai, példák	37
Hibajavító kódok	38
6. Az Ethernet rendszer alapjellemzői.....	39
Helyi hálózatok – Local Area Network.....	39
Helyi hálózatok történelmi fejlődése.....	39
Helyi hálózatok jellemzői.....	39
Topológiák	39
Az Ethernet ma használt átviteli közegeire, csatlakozóira es 1. rétegbeli eszközeire vonatkozó követelmények és szabványok	40
LAN szabványok.....	40
IEEE LAN szabványok	40
Gyors Ethernet – Fast Ethernet	41

Gigabit Ethernet	41
Maximális kábelhosszok	41
10 Gbps Ethernet jellemzői	42
Az Ethernet és az OSI modell, az Ethernet PDU felépítése és mezői.....	42
Az Ethernet kapcsolás	43
Az Ethernet hálózatok szegmentálása	43
2. rétegbeli LAN Kapcsoló.....	45
Kerettovábbítási módszerek	46
Az Ethernet kerethossz minimális értéke, a megkötés indoka	46
Közeghuzzáférés-vezérlés, az ütközések felismerése a különféle Ethernet változatoknál ..	46
Véletlen vezérlésű módszerek	46
Multiple-Access with Collision Detection (CSMA/CD).....	47
Ütközéstípusok, ezek kialakulásának okai és következményei	47
7. Hálózati réteg	48
Az Ethernet LAN korlátai	48
Összekapcsolt LAN – WAN hálózatok.....	48
Hálózati protokoll.....	48
A hálózati réteg szolgáltatása és feladatai, példákkal	49
Hálózati szolgáltatás (Network Service)	49
A hálózati réteg feladatai.....	49
A hálózati réteg – összeköttetés alapú vagy összeköttetés mentes?.....	49
Címzés (Addressing)	50
Forgalomirányítás (Routing)	50
Az útválasztás lehetőségei.....	50
Maximális csomagmáret	51
Forgalomszabályozás és torlódásvezérlés (Flow and congestion control).....	51
Hibajelzés (Error reporting)	51
A szolgáltatás minősége (Quality of Service: QoS).....	51
Hálózati forgalom.....	52
8. Hálózati rendszerek címzési megoldásai.....	52
Az OSI rendszer rétegeiben hol és miért van szükség címekre, mi a jellemző ezekre	52
Miért van szükség logikai és fizikai címekre mi indokolja ezeket a megnevezéseket.....	52
A 2. rétegbeli címzés alapvető rendeltetése, elvárások, megvalósítás, működés.....	52
A 3. rétegbeli címek alapvető rendeltetése, elvárások, megvalósítás, működés	52
A 4. rétegbeli címek alapvető rendeltetése, elvárások, megvalósítás, működés	52

A 2. és a 3. rétegbeli címek közötti kapcsolat, a kapcsolat szükségessége, megvalósítása	52
9. Az IPv4 címtér kezelése	53
Az IP protokoll jellemzői	53
Kapcsolat nélküli kommunikáció jellemzői	53
Megbízhatatlan	53
Médiafüggetlenség	53
IPv4 csomag fejrésze	54
Az IP csomag formátuma – mezők	54
A hálózati protokoll-adategység keretbe foglalása – beágyazás	55
Az IPv4 protokoll	55
IPv4 címek	55
Alhálózati maszk	55
Egyedi, üzenetszórásos és csoportos címzés	55
Az osztály alapú IPv4 címzés, cím-osztályok, az osztály nélküli címzés	56
Privát és nyilvános címek	56
Speciális címek	56
10. Az IPv6 címtér kezelése	57
Miért van szükség nagyobb címtartományra?	57
IPv6 célok	57
Új IPv6 funkciók	57
Nagyobb címtartomány	58
Az IPv6 fejléc	58
Egyszerűbb és hatékonyabb protokoll fejléc	58
Az IPv4 és IPv6 fejlécek összehasonlítása	59
Az IPv6 fejléc mezők	60
A FLOW LABEL szerkezete	60
IPv6 kiegészítő fejlécek (Extension Headers)	61
IPv6 cím reprezentáció	62
Az IPv6 címek méretének csökkentése	62
Hálózati prefix	62
Összes bit 0 – cím	62
IPv6 címzés típusok	62
UNICAST címek fajtái:	63
UNICAST	64
Multicast	64

Anycast.....	64
IPv6 Global Unicast (és Anycast) címek	65
Dinamikus IPv6 címzés – Állomás ID meghatározása	66
IPv6 multicasting.....	67
DHCPv6 protokoll bemutatása.....	68
ICMPv6 protokoll bemutatása	69
Az Internet Control Message Protocol (ICMP).....	69
Az Internet Control Message Protocol (ICMP) jellemzői.....	69
Hibajelzés vagy hibajavítás	69
Az ICMP üzenetkézbesítés – beágyazás	70
ICMPv6 általános információk	70
Neighbor Discovery Protocol.....	70
11. VLSM és CIDR	72
A VLSM fogalma, rendeltetése, kialakításának okai, miért szükséges a VLSM.....	72
Az alhálózatokra bontás lehetősége és technikája VLSM alkalmazása esetén, mintapélda	72
A címösszevonás fogalma, előnyei, szupernet fogalma, megvalósítási technikája konkrét példán bemutatva.....	72
Irányító protokollok és a VLSM kapcsolata	72
Nemfolytonos IPv4 hálózatok problémái és kezelése.....	72
12. DHCP és DHCPv6 szolgáltatás.....	73
A SLAAC bemutatása	73
Stateless Address Autoconfiguration (SLAAC)	74
Állapot nélküli automatikus címkiosztás	74
SLAAC működés	75
DHCPv6 működése	76
13-14. Szállítási réteg	77
A szállítási szolgáltatások	77
A szállítási réteg feladatai	77
Összeköttetés létesítése, fenntartása és lebontása	77
Kapcsolat kiépítése – Hárromutas kézfogás	78
1. nyugtázás	78
2. újraküldés	78
3. sorszámozás.....	78
Kapcsolat lebontása	79
Megbízhatóság – Hibakezelés	79

Forgalomszabályozás	79
Adatfolyam vezérlés - Csúszó ablakok (Sliding Windows).....	79
3 csomag elküldése csúszó ablakos protokoll használatával.....	80
User Datagram Protocol – UDP	80
Az UDP üzenet formátuma	82
UDP multiplexálás/demultiplexálás	82
Transmission Control Protocol – TCP	83
A megbízható adatfolyam szolgáltatás jellemzői.....	83
A TCP feladatai.....	83
Portok, kapcsolatok és végpontok.....	84
TCP üzenettípusok	84
TCP szegmensformátum	84
A TCP szegmens mezőinek jelentése.....	85
Címzés: Portok és socket-ek	85
A portok és socketek szerepe	85
Portok	85
Socketek	86
15. WAN szolgáltatások.....	87
WAN	87
WANs in the OSI Model.....	87
Layer 1 Protocols	87
Layer 2 Protocols	87
Fogalmak	87
Demarkációs pont.....	88
DTE és DCE.....	88
Private and Public WANs	89
WAN beágyazási protokollok	89
WAN topológiák	89
Vonalkapcsolt technológiák	90
Csomagkapcsolt technológiák	90
A széles körben használt WAN szolgáltatástípusok és protokollok	90
ISDN.....	90
FRAME RELAY.....	90
ATM.....	90
Ethernet WAN.....	91

MPLS	91
HDLC - High-level Data Link Control	91
PPP – Point to Point Protocol (16. téTEL)	92
A PPP a következő interfészeket támogatja:	92
A PPP két alprotokollal rendelkezik:	92
Kapcsolatvezérlő protokoll (LCP)	93
Hálózatvezérlő protokoll (NCP).....	93
PPP összeköttetés kiépítése	93
PPP hitelesítés	94
PAP hitelesítés.....	94
CHAP hitelesítés	94
PPP konfiguráció	95
17-18-19. Forgalomirányítás	95
A forgalomirányítás feladatai és fogalmai	95
Autonóm körzet.....	95
Irányítótábla szerepe a forgalomirányításban.....	96
Statikus forgalomirányítás indokai.....	96
Dinamikus forgalomirányítás	96
Irányított és Irányító protokollok	96
Irányító protokoll.....	97
Kapcsolatállapot alapú protokollok.....	98
Távolságvektor alapú irányítóprotokollok	98
Az IP Routing Information Protocol (RIP) jellemzői	98
Az útvonalak kiértékelése	99
Útvonalfrissítések.....	99
Irányítási hurkok	99
A RIP korlátai.....	100
20. OSPF alapú forgalomirányítás	101
Kapcsolatállapot alapú irányító protokollok (Linkstate routing protocols)	101
Routing protokoll jellemzők.....	101
Link-state routing protocols	101
A kapcsolat-állapot forgalomirányító folyamat (Link-state routing process).....	102
A Link-state protokollok előnyei	102
Hierarchikus hálózattervezés – Multiple areas.....	102
A Link-state protokollok erőforrás igénye	102

Open Shortest Path First (OSPF) forgalomirányító protokoll.....	103
OSPF történelem	103
Az OSPF jellemzői.....	103
Az OSPF üzenet beágyazás	103
OSPF Network Types.....	104
Az OSPF Hello protokoll	104
Electing a DR and BDR	104
OSPF működése	105
Router ID meghatározása	105
OSPF költség.....	106
The OSPF Priority	106
Adminisztratív távolság – Administrative distance.....	106
21. Ethernet kapcsolók alkalmazása.....	107
Az Ethernet kapcsolás jellemzői	107
Kapcsolás	107
Mikroszegmentáció	107
A kapcsolók fajtái.....	108
Szimmetrikus, aszimmetrikus kapcsolók	108
Duplex – fél-duplex átvitel.....	108
Torlódások elkerülése, pufferek használata	109
A kerettovábbítás módjai	109
Tárol-továbbít (Store and forward)	109
Gyors továbbítás (Cut through).....	109
Töredékkentes továbbítás (Fragment free).....	109
A továbbítás megkezdésének legkorábbi ideje	109
A kapcsolótábla felépítése.....	110
Az Ethernet kapcsolók konfigurálása.....	110
22. Redundáns kapcsoló-topológiák	111
Redundancy at OSI Layers 1 and 2	111
MAC Database Instability	111
Issues with Layer 1 Redundancy: Broadcast Storms	111
Issues with Layer 1 Redundancy: Duplicate Unicast Frames	111
Issues with Layer 1 Redundancy: Duplicate Unicast Frames	111
Feszítőfa protokoll – STP működése	112
Miért kell elosztott működés?	112

Az elosztott működés lényege.....	112
Fa szerkezet kialakításának elsődleges paraméterei.....	112
BPDU	113
BPDU prioritás vektor.....	113
Hogyan használja a prioritás vektorokat?	114
Az STP kiválasztási folyamata.....	114
23-24. Virtuális LAN hálózatok (VLAN-ok), Trönkprotokoll	114
Virtuális LAN.....	114
A VLAN-ok létrehozásának okai	114
A VLAN-ok jellemzői.....	114
A VLAN-ok közötti kommunikáció	115
Portok VLAN-okhoz rendelése	115
VLAN típusok funkció alapján	115
VLAN tartományok.....	115
Több kapcsolóra kiterjesztett VLAN-ok: Trunk (trönk)	116
Keret címkézése	116
VLAN-ok közötti forgalomirányítás	117
VLAN Trunking Protocol (VTP)	117
VTP Modes	117
VTP operations.....	118
Jellemzők.....	118
VTP Message Types.....	119
VTP Authentication.....	119
DTP (Dynamic Trunking Protocol).....	120
25. LAN redundancia és link összefogás	120
LAN redundancy	120
Default Gateway Limitations	120
Static Default Gateway.....	120
Router Redundancy	120
First-Hop Redundancy Protocols	120
Hot Standby Router Protocol (HSRP).....	121
HSRP Failover.....	121
HSRP Operation	121
HSRP States	121
HSRP State Transition	122

HSRP Active Router and Spanning Tree Topology.....	122
HSRP Versions.....	122
EtherChannel Technology.....	123
EtherChannel Management Protocols	123
26. Külső átjáró protokoll.....	124
Autonomous Systems (AS)	124
AS Numbers	124
Miért van rá szükség?.....	124
Connection Redundancy	124
Using BGP in an Enterprise Network	125
EBGP szomszédság követelményei	125
IBGP szomszédság követelményei	125
BGP jellemzők	125
BGP működés – üzenetek	126
BGP Tables	126
BGP Üzenet típusok	126
Open Message	126
Update Message	127
Notification Message.....	127
Keepalive Message Type	127
Útvonal attribútumok	128
BGP útválasztás folyamata.....	128
BGP States.....	128
27. Szolgáltatásminőség	129
Előzmény.....	129
Probléma.....	129
A szolgáltatásminőség biztosításának szempontjai.....	130
Queueing – Várakozási sorok	130
Torlódási pontok	130
A csomagkésleltetés különböző okai	130
QoS nélkül.....	131
QoS eszközök.....	131
Queueing algorithm – várakozási sor kezelő algoritmusok	131
FIFO	131
Fair Queueing (WFQ)	132

Weighted Fair Queuing (WFQ).....	132
Priority Queuing (PQ)	132
Class-Based Weighted Fair Queuing (CBWFQ)	132
Low Latency Queuing (LLQ)	132
Lyukas és Vezérjeles Vödör - Leaky and Token Buckets.....	133
Classification and Marking	133
L2 marking	133
L3 marking	133
Congestion Avoidance	134
RED – Random Early detection	134
WRED – Weighted Random Early Detection.....	134
Forgalomformálás (Shaping) és rendfenntartás (policing).....	134
QoS models	135
Best-Effort.....	135
IntServ - Integrated Services (Integrált szolgáltatások)	135
DiffServ – Differentiated Services (Megkülönböztetett szolgáltatások)	137
28. Hálózatfelügyelet	138
29. A hálózati eszközök egyedi védelme	145
Hálózatbiztonság „definiálása”	145
Tudásmegosztás	145
Biztonsági alapelvek	145
Védekezési technikák	145
Határvédelem (perimeter defence)	145
Mélységi védelem (defence in dept)	145
A biztonság (védelem) megteremtése	147
A támadás fajtái.....	147
Aktív.....	147
Passzív.....	147
A forgalomirányítók operációsrendszere	148
A forgalomirányító védelmének három területe	148
1. Fizikai védelem	148
2. Operációs rendszer védelme.....	148
3. Router hardening	149
A megelőzés érdekében.....	149
Adminisztratív hozzáférés védelme	149

A forgalomirányító jelszavai	149
Helyi adatbázis használata.....	149
Jelszavak titkosítása	150
Többszöri próbálkozások korlátozása	150
Telnet tiltása, SSH v2 engedélyezése.....	150
Banner üzenetek beállítása	150
Jogosultságok kezelése.....	150
Privilege Levels.....	150
Role-based CLI access – szerep-alapú CLI hozzáférés.....	151
30. Hálózatok centralizált védelme	152
Hogyan csináltuk eddig?	152
Hogyan lehetne jobban?	152
AAA komponensek	152
Authentication	153
AAA Authorization	153
AAA Accounting.....	154
AAA előnyei	154
Szerver alapú hitelesítés	155
TACACS+ Authentication	156
RADIUS Authentication	156
Jogosultság-kezelés	157
Könyvelés/számlázás	157
31. Tűzfalak.....	157
Defining Firewalls.....	157
Firewalls characteristics	157
Firewalls do not provide.....	157
Firewall Type Descriptions	158
1st generation – packet filtering firewall.....	158
2nd generation - Stateful Firewalls	159
Application level firewall.....	160
Proxy firewalls	160
Deep Packet Inspection Firewalls	160
Next generation firewalls	161
Firewall architectures	161
Dual-homed	161

Single-homed – screened host.....	161
Single-homed – screened subnet	162
Multi-homed.....	163
Demilitarized Zone – DMZ.....	163
Forgalomirányítón megvalósítható tűzfalak – CBAC.....	163
1. Access Control List	163
2. CBAC - context-based access control.....	163
Forgalomirányítón megvalósítható tűzfalak – ZPF (33. téTEL)	165
Benefits of ZPF	165
Zone-based policy firewall.....	165
Basic ZPF Zone Topology	165
3 Actions of ZPF	166
ZPF, ZBF Szabályok	166
The Self Zone	166
ZPF konfigurálás	167
32. Állapot mentes tűzfalak.....	168
Az ACL elve.....	168
ACL működése.....	168
Az ACL típusai.....	168
Kiterjesztett ACL	168
Wildcard maszk használata	168
Konfigurálási szabály	169
ACL elhelyezése a hálózatban	169
IPv6 ACL	169
IPv6 ACL konfigurálás	169
34. Behatolás elleni védelem.....	170
Lehetséges Megoldások	170
A biztonsági célok és a megvalósítás lépései	170
Behatolás érzékelő (IDS) és megelőző (IPS) rendszerek	171
Behatolás Detektálás	171
Behatolás Megelőzés.....	172
IDS és IPS közötti hasonlóságok	172
IDS és IPS közötti különbségek	172
Host-based IPS	173
Hálózati IPS szenzorok (network-based IPS)	173

Port Mirroring	174
Cisco SPAN (Switched Port Analyzer).....	174
Signatures (szignatúrák, minták).....	174
Minták	174
Atomi minták.....	175
Összetett Minták (állapotteljes).....	175
Signature micro-engine, SME	175
A behatolás érzékelők fajtái	175
Pattern-matching detection (minták illesztésén alapuló érzékelés).....	176
Anomaly detection (rendellenes viselkedés érzékelése)	176
Policy-based	176
Honey pot – „mézes bődön”.....	177
Riasztások fajtái	177
Észlelés után.....	177
Riasztás menedzselése.....	177
Logolás	177
Aktivitás megszakítása/letiltás	178
Reset TCP kapcsolat.....	178
Figyelembe kell venni	178
35. Publikus hálózatokon haladó információ védelme.....	179
A széles körben alkalmazott kriptográfiai eljárások rendszerezése és feladatai	179
Hitelesítési és integritásvédelmi megoldások elve, megvalósítása, alaptípusai, alkalmazása	179
Hitelesítés és integritás védelem	179
Authenticity (hmac-sha-256).....	179
Integrity (SHA-256)	180
A kulcskezelés lényege, problémái, elterjed megoldásai, működése és beállítása	180
DH (Diffie-Hellman),.....	181
Szimmetrikus és aszimmetrikus titkosítási megoldások jellemzői, beállítás.....	181
Szimmetrikus algoritmusok.....	181
Aszimmetrikus algoritmusok	181
Nyilvános és titkos kulcsok.....	181
SEAL (Software-Optimized Encryption Algorithm)	182
RC {2,4,5,6}	182
Digitális aláírás, nyilvános kulcsú infrastruktúra (PKI), tanúsítvány alapú működés	182

Digitális aláírás.....	182
Tanúsító hatóságok.....	182
A digitális aláírásnak két formája van.....	183
A PKI.....	183
PKI (Public Key Infrastructure)	183
36. Virtuális magánhálózat (VPN) – L3.....	184
Virtual Private Networks.....	184
VPN Benefits.....	184
Site-to-Site and Remote Access VPNs.....	184
Enterprise and Service Provider VPNs	184
Remote-Access VPNs	185
SSL VPNs	185
Site-to-Site IPsec VPNs	185
GRE over IPsec	186
IPsec	187
IPsec Technologies.....	187
IPsec Protocol Encapsulation	187
Confidentiality.....	187
Integrity	188
Authentication	188
Secure Key Exchange with Diffie – Hellman	188
IPsec működése	188
37. Helyi hálózatok védelme.....	189
Instructions for the attacks	189
CAM Table Attacks	189
Megoldás	189
Attack the root	189
Megoldás	190
Megoldások részletezése	190
DTP és VTP támadások	190
Megoldások	190
Vlan Hopping támadás	191
Megoldás	191
DHCP Starvation.....	191
Megoldás	191

DHCP Spoofing.....	191
Megoldás	191
ARP attack.....	192
Megoldás	192
Forgalomirányítás támadás	192
Megoldás	192
Összegzés	192
First line of defence (restrict access).....	192
Second line of defence (protocol security).....	192
38. Dedikált tűzfalak, új generációs tűzfalak	193
Általános jellemzők.....	193
Az ASA képességei	193
Tűzfal működési módok.....	193
Biztonsági szintek	194
Alapértelmezett beállítások	194
RAS beállítás.....	194
NTP beállítása	194
DHCP beállítása	194
Objects and Object Groups	194
Network Object	195
Service Object	195
Object Group és beállítása.....	195
ACL.....	195
ACL-ek – hasonlóságok	195
ACL-ek – különbségek.....	195
Az ASA-n elérhető ACL-ek.....	195
Címfordítás.....	196
AAA	196
Modular Policy Framework	196

1. KOMMUNIKÁCIÓS RENDSZEREK ALAPFUNKCIÓI ÉS KIALAKÍTÁSI LEHETŐSÉGEIK

Protokoll, a protokollfunkciók interfész fogalomra épülő bemutatása

Protokoll: A kommunikáció írott és íratlan szabályainak összessége.

Protokollkészlet: Egy rendszer rétegeihez tartozó protokollok összesége.

Hálózati architektúra: A rétegek és protokollok halmaza.

Minden rétegnek van egy vagy több protokollja, melynek segítségével az egyik gép n-edik rétege párbeszédét folytat a másik gép n-edik rétegével → társ (peer) rétegek kommunikációja

Protokollfunkciók

- Megbízhatóság – nyugtázás
- Hibajelzés
- Hibajavítás
- Útválasztás
- Címzés és névkezelés
- Különbözőségek elrejtése
- Forgalomszabályozás
- Torlódáskezelés
- Valósidejű továbbítás – QoS (Quality of Service)
- Biztonság – titkosság, hitelesítés, sérzetlenség

Kommunikációs rendszerek hierarchikusan rétegezett megvalósításának lényege, előnyei

A komplex rendszerek tervezése esetén bevett szokás azok kisebb részekre darabolása. Ekkor két megközelítési módot tartunk számon:

- Moduláris
- Réteges

A hálózat tervezése során a komplexitás csökkentése érdekében a szétdarabolás mellett döntöttek, a darabokat rétegekké alakítva egy hierarchikus felépítést hoztak létre. Ilyen réteges rendszer az OSI -és a TCP/IP modellek. A rétegek száma, elnevezése, tartalma és feladata más és más a különböző hálózatokban. A rétegmodellben az egyes rétegek szolgáltatásokat nyújtanak az alatta, illetve a fölötte levő rétegeknek, miközben elrejti előlük a szolgáltatások tényleges megvalósításának részleteit. A verem alsóbb rétegei az adatok hálózaton kereszttüli mozgásával és a felső rétegek számára nyújtott szolgáltatásokkal foglalkoznak, amelyek a küldött üzenet tartalmára összpontosítanak.

A rétegmodell előnyei:

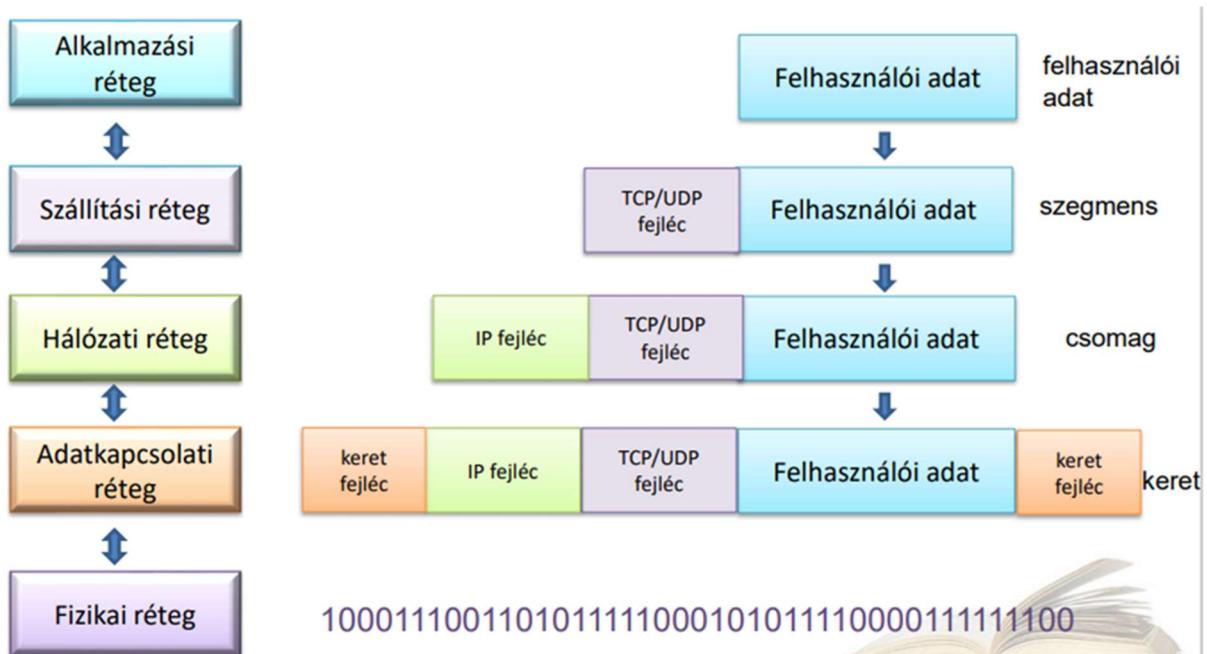
- Segít a protokolltervezésnél, mert egy adott rétegen működő protokoll esetén egyértelműen specifikált, hogy mit kell tennie és, hogy milyenek az alsóbb illetve a felsőbb rétegek felé használható interfészei.
- Elősegíti a versenyt, mivel a különböző gyártótól származó termékek képesek együtt működni.
- Véd attól, hogy az egyik réteg technológiájának vagy adottságainak változásai hatással legyenek az alatta vagy a felette levő másik rétegre.
- Általános nyelvet biztosít a hálózat működésének és képességeinek leírásához.

Az átviteli egység (PDU) fogalma, felépítése, az átviteli folyamat leírása

Ahogy az alkalmazás adatai haladnak lefelé a protokollveremben, a különböző protokollok minden szinten további adatokkal egészítik ki. Ezt általánosan beágyazási folyamatnak hívjuk. Az egyes rétegekhez használt adathalmazt protokoll adategységnek nevezzük (**Protocol Data Unit, PDU**). Az adatbeágyazás során minden újabb réteg becsomagolja a felsőbb rétegből származó PDU-t az alkalmazott protokollnak megfelelő módon. A folyamat minden egyes szakaszában a PDU egy másik nevet kap, jelezve ezáltal az új funkcióját is. A PDU-kat a TCP/IP protokolcsalád szerint nevezzük meg.

Felépítése:

- Adat: Általános kifejezés az alkalmazási rétegen használt PDU-ra.
- Szegmens: Szállítási rétegbeli PDU.
- Csomag: Internet rétegbeli PDU.
- Keret: Hálózatelérési rétegbeli PDU.
- Bitek: Az átviteli közegen történő fizikai adattovábbításhoz használt PDU.



Szomszéd- (kiszolgáló-, kiszolgált-) és társ- (egyenrangú) rétegek közötti kommunikáció

Az alacsonyabb szintű rétegek protokolljait a gépek a közvetlen szomszédjukkal való kommunikációhoz használják, nem pedig a tényleges küldő és a fogadó kommunikál velük, hiszen ezeket több útválasztó is elválaszthatja egymástól. Egy adott rétegen található társprotokollok működése csak a rétegre tartozik. Egy konkrét feladat elvégzéséhez (tehát szolgáltatás nyújtásához) a réteg olyan protokollt használ, amilyet csak akar. Tetszése szerint válthat egyikről a másikra anélkül, hogy a felette levő rétegek szoftvereinek működését befolyásolná.

Adatbeágyazás, az adatbeágyazás lépései, adatfolyam-vezérlés

Az adatok beágyazása az a folyamat, ahol az adatot a továbbítása előtt további protokollfejlécettel lájtják el. A legtöbb adatkommunikációs folyamatban az eredeti adatot több különböző protokoll szerint ágyazzák vagy csomagolják be a tényleges továbbítás előtt.

Amikor üzeneteket küldenek egy hálózaton, a beágyazás folyamata fentről lefelé működik. Az egyes rétegekben a felső réteg információi a beágyazott protokoll adatainak tekinthetők. Például a TCP szegmens adatnak tekinthető az IP-csomagban.

A folyamatot az alkalmazási rétegbeli HTTP protokoll kezdi a HTML formátumú adatok továbbításával a szállítási réteg felé. Ott az alkalmazás adatai TCP szegmensekre lesznek széttörölve. Mindegyik TCP szegmens kap egy címkét, az úgynevezett fejlécet, amely többek között beazonosítja azt az alkalmazást, amelynek az üzenetet a célállomáson majd fel kell dolgozni. A fejléc az eredeti információ visszaállítását segítő információkat is tartalmaz.

A szállítási réteg beágyazza a weboldal HTML-adatrészeit egy szegmensbe, és elküldi azt az internet réteg számára, ahol az IP protokoll működik. Itt a teljes TCP szegmens beágyazásra kerül egy IP csomagba, amely egy újabb címke, az IP-fejléc hozzáadását jelenti. Az IP-fejléc tartalmazza a forrás- és célállomás IP-címét, valamint a csomag feldolgozását szabályozó folyamatok meghatározását.

Ezután az IP csomagot a hálózatelérési réteg kapja meg, ahol egy keretfejléc és egy utótag közé ágyazzák be a csomagot. minden keret fejléce tartalmazza a forrás és a cél fizikai címét. Az eszközök a fizikai cím egyedileg azonosítja a helyi hálózaton. Az utótag hibaellenőrzési információkat tartalmaz. Végül a szerver hálózati kártyája (NIC) az átviteli közegen történő továbbításhoz a biteket megfelelően kódolja.

Adatfolyam vezérlés - Flow control

Ha a vevő számítógép nem képes olyan ütemben feldolgozni a kereteket, mint amilyen ütemben érkeznek, akkor a vevőállomás pufferei megtelhetnek. Gondoskodni kell valamilyen vezérlő mechanizmusról, amellyel a keret küldés leállítható, majd újra indítható. Ez a mechanizmus az adatfolyam vezérlés.

Az összeköttetés alapú és az összeköttetés-mentes hálózati szolgáltatás, a köztük levő fontosabb különbségek

Összeköttetés alapú hálózati szolgáltatás

Az összeköttetés alapú, másnéven virtuálisáramkör-alapú hálózatnak szükséges az átvitel előtt egy kapcsolatot felépíteni a küldő és a címzett között, majd ezután lehet küldeni a kívánt információkat. Az adatblokk elküldése előtt a küldő hálózati rétegének fel kell építeni egy kapcsolatot a címzettel. Ez a fizikai összeköttetés mindenkor fennmarad, amíg a teljes blokk küldését be nem fejezték. Ezután a vonalat bontva az felszabadul a többi kapcsolat számára. Amikor a vonal foglalt, minden két végpont küldhet adatot a másik számára, tehát a kapcsolat kétirányú is lehet (nyugtázás). A forgalomszabályozásnak biztosítania kell, hogy az adó csak olyan sebességgel küldhesse az információt, amilyen gyorsan a vevő ezt érzékelni képes, vagyis ne léphessen fel torlódás. Mindezekből láthatjuk, hogy szükség van összeköttetésre, de ez az esetek többségében csak az átvitel idejére áll fenn. Ilyen pl a TCP protokol

Az összeköttetésalapú hálózati szolgáltatás olyan kommunikációs szolgáltatás típusa, amely az adatátvitel előtt logikai kapcsolatot hoz létre két végpont között. Biztosítja az adat megbízható és rendezett kézbesítését a küldő és a fogadó között azáltal, hogy létrehoz egy kapcsolatot vagy munkamenetet.

Az összeköttetésalapú hálózati szolgáltatásban a kommunikáció egy meghatározott lépéssorozatot követ:

1. Kapcsolatfelépítés:
 - Az indító eszköz elküldi a kapcsolatfelépítési kérést a fogadó eszköznek.
 - A fogadó eszköz elismeri a kérelmet és kapcsolatot létesít, erőforrásokat kiosztva a kommunikációs munkamenethez.
2. Adatátvitel:
 - Miután a kapcsolat felépült, az adat átvitele megtörténhet az eszközök között.
 - A küldő lebontja az adatot kisebb egységekre, ún. csomagokra vagy szegmentekre, és elküldi azokat a fogadónak.
 - A fogadó visszaigazolja az egyes csomagok fogadását, biztosítva, hogy az adat ne vesszen el vagy sérüljön meg a továbbítás során.
3. Kapcsolat lezárása:
 - Az adatátvitel befejezése után az eszközök kapcsolatleállítási folyamatot hajtanak végre a munkamenet megszüntetésére.
 - Az indító eszköz elküldi a kapcsolatleállítási kérelmet.
 - A fogadó eszköz elismeri a kérelmet és feloldja a kiosztott erőforrásokat, lezárva ezzel a kapcsolatot.

Az összeköttetésalapú hálózati szolgáltatások példái:

1. Transmission Control Protocol (TCP):
 - A TCP széles körben használt összeköttetésalapú protokoll a TCP/IP protokollrendszerben.
 - Megbízható, rendezett és hibamentes adatátvitelt biztosít az alkalmazások között.
 - A TCP háromlépcsős kézfogással hoz létre kapcsolatot, és a sorrendszámok, visszaigazolások és újraküldési mechanizmusok révén biztosítja az adatintegritást.
 - Garantálja, hogy az adat ugyanabban a sorrendben érkezik meg, mint ahogy elküldték.
2. X.25:
 - Az X.25 egy összeköttetésalapú protokollrendszer, amelyet régebbi nyilvános csomókapcsolt hálózatokban használnak.
 - Megbízható és rendezett adatátvitelt kínál a hálózaton keresztül.
 - Az X.25 virtuális áramköröket használ a végpontok közötti logikai kapcsolatok létrehozásához.
 - Áramvezérlést, hibajavítást és torlódásvezérlést biztosít.

Az összeköttetésalapú hálózati szolgáltatások általában olyan helyzetekben használatosak, ahol az adat megbízható és rendezett kézbesítése kritikus fontosságú, például fájlátvitel, e-mail továbbítás, böngészés és más alkalmazások esetén, amelyek hibamentes kommunikációt igényelnek. Ezek a szolgáltatások biztosítják, hogy az adat pontosan és a megfelelő sorrendben érkezzen meg, így magas szintű adatintegritást és megbízhatóságot nyújtanak.

Összeköttetés mentes hálózati szolgáltatás

Az összeköttetés mentes, vagyis datagram alapú kommunikáció lényege, hogy az adatküldést megelőzően a végpontok között nem épül ki kapcsolat. Ez hasonló ahhoz, mint amikor egy levelet küldünk anélkül, hogy arról a címzettet előre értesítenénk. Mivel az IP összeköttetésmentes, így a csomagtovábbítás előtt nincs szükség a végpontok közötti kapcsolat kiépítéséhez fontos vezérlési információk cseréjére sem. Szintén nincs szükség a PDU-fejlécében olyan további információkra, amelyek a felépített kapcsolat kezelését segítenék. Mindezek nagy mértékben csökkentik az IP által okozott többletterhelését. Mivel nem épül fel kapcsolat a végpontok között, így a küldőnek nincs információja a megcímzett eszköz létezéséről vagy működéséről, illetve arról sem, hogy a csomagja megérkezik-e vagy hogy a címzett fel tudja-e azt dolgozni.

A kapcsolat nélküli hálózati szolgáltatás egy olyan kommunikációs szolgáltatás, amely nem igényel előzetes kapcsolat létrehozását a küldő és a fogadó között. Az adatátvitel a kapcsolat nélküli szolgáltatás esetén azonnal megkezdődik anélkül, hogy előzetesen kialakítanának egy hálózati munkamenetet.

A kapcsolat nélküli hálózati szolgáltatásnál a kommunikáció az alábbi módon zajlik:

1. Adatcsomag elküldése:
 - Az adatküldő eszköz az adatot felosztja kisebb egységekre, amelyeket csomagoknak vagy üzeneteknek nevezünk.
 - Az adatküldő azonnal elküldi ezeket a csomagokat a hálózatra a fogadó eszközhöz.
2. Csomagok független kézbesítése:
 - A csomagokat függetlenül kezeli a hálózat, és nem szükséges előzetes kapcsolat a küldő és a fogadó között.
 - A csomagok külön-külön továbbítódnak a hálózaton a legmegfelelőbb útvonalakon.
3. Csomagok fogadása és feldolgozása:
 - A fogadó eszköz a kapcsolat nélküli hálózati szolgáltatásnál fogadja a csomagokat.
 - A csomagokat külön-külön dolgozza fel a fogadó eszköz, és visszaállítja az eredeti adatot.

A kapcsolat nélküli hálózati szolgáltatásnál nincs szükség előzetes kapcsolat létrehozására, és az adatátvitel azonnal megtörténik a csomagok küldésekor. Az adatokat függetlenül kezeli a hálózat, és minden csomagot külön-külön továbbít a célhelyre. Ez a fajta szolgáltatás gyorsabb és egyszerűbb kommunikációt tesz lehetővé, de nem garantálja az adatok megbízható és rendezett kézbesítését, mivel a csomagok külön-külön továbbítódnak és feldolgozódnak. Ezért a kapcsolat nélküli hálózati szolgáltatások gyakran alkalmazásokban használatosak, ahol a kis méretű adatok gyors és hatékony továbbítása a cél.

2. HÁLÓZATI RENDSZEREK ISO OSI MODELL SZERINTI KIALAKÍTÁSA

Miért használjuk a kommunikáció rétegezett modelljét

- Komplex rendszerek tervezése részekre bontással:
- Réteges, Moduláris
- Réteges modellt használták bevált és azóta is így működik.
- Segít a protokolltervezésnél, mert egy adott rétegben működő protokoll esetén egyértelműen specifikált, hogy mit kell tennie és, hogy milyenek az alsóbb illetve a felsőbb rétegek felé használható interfészei.
- Elősegíti a versenyt, mivel a különböző gyártótól származó termékek képesek együtt működni.
- Véd attól, hogy az egyik réteg technológiájának vagy adottságainak változásai hatással legyenek az alatta vagy a felette levő másik rétegre.
- Általános nyelvet biztosít a hálózat működésének és képességeinek leírásához.

OSI modell rétegei, átviteli egységei, adatbeágyazás lépései, adatfolyam-vezérlés

Az ISO OSI modell az adatkommunikációs rendszerek strukturált leírására szolgáló referenciamodell. Az OSI (Open Systems Interconnection) modell hét rétegből áll, amelyek különböző funkcionális feladatokat látnak el az adatkommunikáció során. Az alábbiakban ismertetem a rétegeket és a rétegek közötti adatátvitel egységeit (PDU-kat) a magyar nyelven.

1. Fizikai réteg:

- A fizikai réteg a legalsó réteg és az adatok fizikai továbbításával foglalkozik.
- Ez a réteg a biteket az adatátviteli közegre alakítja át, például elektromos jelek formájában.
- PDU: Bit (bit)
- A bitek továbbításáért felelős a kommunikációs csatornán
- Feszültség szintek, bithossz, egyszerre egyirányú vagy kétirányú átvitel
- Felépíti és lebontja a kapcsolatot
- Leírja a csatlakozók típusát, a vezetékek funkcióját, stb.
- Mechanikai és elektromos interfész biztosít, amelyek az átviteli közeggel is kapcsolatos

2. Adatkapcsolati réteg:

- Az adatkapcsolati réteg az adatátvitel megbízhatóságáért és az adatfolyam vezérléséért felelős.
- Ez a réteg az adatot kisebb egységekre, ún. keretekre bontja, hozzáadva keretek közötti ellenőrző összegeket.
- PDU: Keret (frame)
- A hálózati réteg számára hibamentesnek tűnő vonalat mutat
- A küldő az adatokat adatkeretekké tördeli, sorrendhelyesen továbbítja, végül a vevő nyugta keretét feldolgozza
- Felismeri az adatkeretek határait, hibás keret esetén újra továbbítja
- Sérült, elveszett, kettözött keretek miatt bekövetkező problémák megoldása

- Forgalom szabályozási mechanizmust biztosít (flow control) (gyors adó - lassú vevő probléma megoldása)

3. Hálózati réteg:

- A hálózati réteg az útválasztást és az adatok címzését végzi.
- Ez a réteg határozza meg a legmegfelelőbb útvonalat az adatok továbbításához a hálózaton keresztül.
- PDU: Csomag (packet)
- A kommunikációs alrendszer működését vezérli
- A csomagok útvonalának meghatározása a forrástól a célig
- Az útvonal lehet:
 - behuzalozott
 - a kapcsolat felépülésekor jön létre
 - minden csomagra külön-külön lesz meghatározva
- Torlódások elkerülése
- Forgalom szerinti számlázás

Ha a csomagok több, heterogén hálózaton mennek keresztül, eltérő lehet a hálózatok címzési módszere, maximális csomagmérete, protokolljai, ennek a rétegnak a feladata ezeket a különbségeket elrejteni.

4. Szállítási réteg:

- A szállítási réteg az end-to-end adatátvitelért és az adatok feldarabolásáért és összeszereléséért felelős.
- Ez a réteg biztosítja az adatok megbízható, rendezett és hibajavított kézbesítését.
- PDU: Szegmens (segment)
- Adatokat fogad a viszony rétegtől, kisebb darabokra tördeli (ha kell), majd továbbadja a hálózati rétegnek, és biztosítja, hogy minden darab hibátlanul megérkezzék a másik oldalra
- Elfedi a hardver technikában bekövetkező változásokat
- A szállítási réteg - a viszony réteg kérésére - létrehozza a hálózati összeköttetést
- Valódi End to End réteg, közvetlenül a partner számítógép szállítási rétegével társalog
- Az alatta lévő rétegek még közbenső eszközöknek küldenek üzenetet
- A szállítási réteg az összeköttetés létrehozásán kívül valamilyen névadási mechanizmussal is rendelkezik. Az egyik gépen futó folyamat megnevezi azt a folyamatot a másik gépen, amellyel társalogni kíván (folyamat-folyamat összekapcsolás)
- Információ áramlási mechanizmussal is rendelkezik

5. Viszony réteg:

- A szolgáltatási réteg a kommunikációs partnerek közötti munkameneteket kezeli és ellenőrzi.
- Ez a réteg biztosítja a megbízható kommunikációt az alkalmazások között.
- PDU: Üzenet (message)
- Lehetővé teszi, hogy különböző gépek felhasználói viszonyt létesítsenek egymással
- A szállítási réteghez hasonlóan közönséges adatátvitelt tesz lehetővé kiegészítve néhány szolgáltatással pl. távoli bejelentkezés vagy állomány továbbítás
- Párbeszéd szervezése: egyszerre egy vagy kétirányú összeköttetés
- Ha csak egyirányú, nyomon követi, hogy melyik fél következik

6. Megjelenítményi réteg:

- A megjelenítményi réteg adatainak kódolásáért, titkosításáért és dekódolásáért felelős.
- Ez a réteg gondoskodik az adatok formátumának konverziójáról és a különböző rendszerek közötti kompatibilitásról.
- PDU: Adat (data)
- Az átvendő adat szintaktikájával és szemantikájával is foglalkozik
- A karaktereket, numerikus értékeket szabványos módon ábrázolja, és elvégzi az oda - vissza konvertálást
- Adattömörítés, hitelesítés, titkosítás

7. Alkalmazási réteg:

- Az alkalmazási réteg az alkalmazások közvetlen kapcsolatát szolgálja ki.
- Ez a réteg biztosítja az alkalmazások közötti kommunikációt és az alkalmazás-specifikus protokollok működését.
- PDU: Adat (data)
-
- Az alkalmazások számára biztosít elosztott hálózati szolgáltatásokhoz megfelelő interfész:

 - Hálózati virtuális terminál kezelése
 - Állomány továbbítás
 - Elektronikus posta
 - Távoli munka bevitel
 - Katalógus kikeresés

Ezek a rétegek és az adatátvitel egységei (PDU-k) lehetővé teszik az adatkommunikáció szervezett és standardizált működését az OSI modell szerint. minden réteg specifikus funkciókat lát el a kommunikáció során, és egymással szorosan összehangolva biztosítják az adatok megbízható, hatékony és hibamentes átvitelét a hálózaton keresztül.

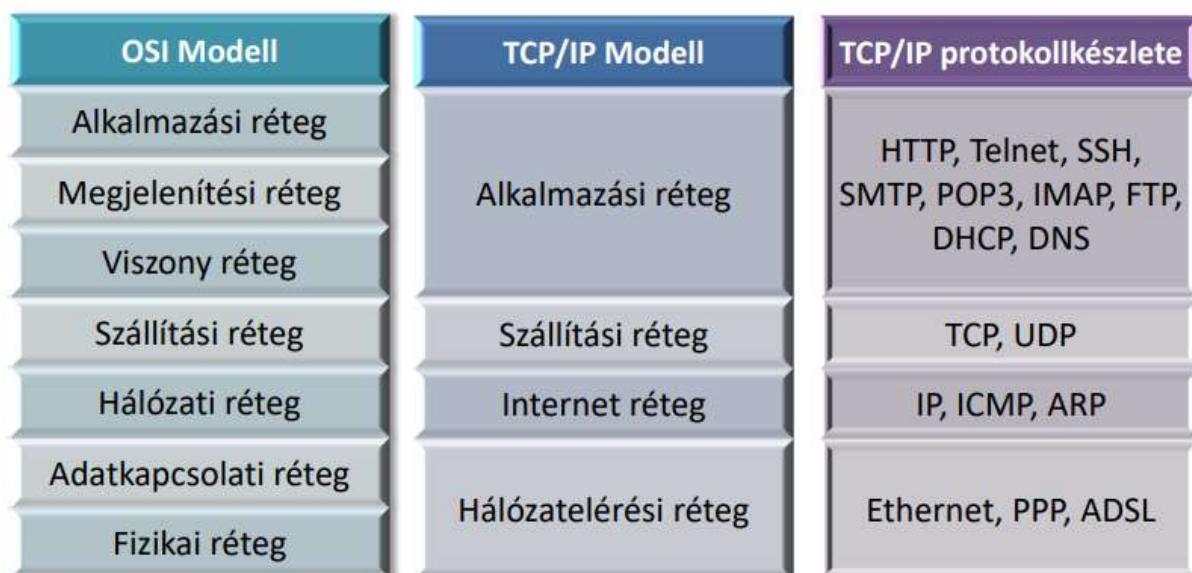
A TCP/IP és az OSI modellek kapcsolata (különbségek, azonosságok)

Hasonlóságok

1. Mindkettő rétegmodell, hierarchikusan egymásra épülő rétegekkel, melyeknek protokolljai egymástól függetlenek
2. A rétegek feladatai is hasonlóak, egymásnak megfeleltethetők

Különbségek

1. Az OSI modell három fő fogalom köré összpontosul:
 1. Szolgáltatások
 2. Interfészek
 3. Protokollok
2. Előbb volt a modell, a szolgáltatások és a protokollok csak később a rétegnek megfelelően
3. A TCP/IP esetén fordítva történt, a protokoll készlet volt előbb, ehhez igazították a rétegeket
4. A rétegek száma különbözik, az OSI
5. Az OSI a 3. rétegen támogatja az összeköttetés alapú és az összeköttetés mentes kommunikációt, de a 4. rétegen csak az összeköttetés alapút.
6. A TCP/IP a hálózatban csak az összeköttetés mentes, míg a szállítási rétegen minden két kommunikációt támogatja



3. HÁLÓZATI RENDSZEREK TCP-IP MODELL SZERINTI KIALAKÍTÁSA

Miért használja a hálózati ipar a TCP/IP modellt

A hálózatközi kommunikáció első rétegmodellje az 1970-es évek elején került kidolgozásra, melyet Internet modellnek nevezünk. Meghatározta a működés azon négy kategóriáját mely nélkülözhetetlen a sikeres kommunikációhoz. A TCP/IP protokollok szerkezete ennek a modellnek a struktúráját követi. Ezért általában az Internet modellt úgy nevezzük, hogy TCP/IP modell.

A TCP/IP hálózati modell rétegei és ezek feladatai

Az alkalmazási réteg

A szállítási réteg fölött az alkalmazási réteg található. Ez tartalmazza az összes magasabb szintű protokollet. Eredetileg csak a virtuális terminál (TELNET), a fájltranszfer (FTP) és az elektronikus levelezés (SMTP) protokolljait tartalmazta, amelyeket a 3. táblázatban is láthattunk. A virtuális terminál lehetővé teszi, hogy bejelentkezzünk egy távoli gépre, és azon dolgozzunk. A fájltranszfer protokoll segítségével hatékonyan tudunk adatokat átvinni egy gépről a másikra. Az évek során számos más protokollal bővítették az alkalmazási réteget. Ilyen például a Domain Name Service (DNS), amely a hosztok nevét képezi le a hálózati címükre; a HTTP, amely a World Wide Web oldalak letöltését segíti.

A szállítási réteg

A TCP/IP-modellben az internetréteg fölötti réteget általában szállítási rétegnak nevezik. Feladata az, hogy lehetővé tegye a forrás- és a célállomásokban található társentitások közötti párbeszédet.

Az egyik szállítási protokoll az átvitelvezérlő protokoll (Transmission Control Protocol, TCP), amely egy megbízható összeköttetés alapú protokoll. Feladata az, hogy hibamentes bájtos átvitelt biztosítson bármely két gép között az interneten. A beérkező bájtos adatfolyamot diszkrét méretű üzenetekre osztja, majd azokat egyesével továbbítja az internetrétegnek. A célállomás TCP-folyamata összegyűjti a beérkezett üzeneteket, és egyetlen kimeneti adatfolyamként továbbítja őket. A TCP forgalomszabályozást is végez annak érdekében, hogy egy gyors forrásállomás csak annyi üzenetet küldjön egy lassabb célállomásnak, amennyit az fogadni képes.

A másik átviteli protokoll ebben a rétegen a felhasználói datagram protokoll (User Datagram Protocol, UDP) amely egy nem megbízható, összeköttetés nélküli protokoll. Jelentősége akkor van, amikor nem szükséges sem az üzenetek TCP-féle sorbarendezése, sem a forgalomszabályozás. Elsősorban olyan egylövetű, kliens-szerver típusú kérdés-válasz alkalmazásokban terjedt el, ahol a gyors válasz sokkal fontosabb, mint a pontos. Ilyen például a beszéd- vagy videó átvitel.

Az internetréteg

Mindezen az elvárások olyan csomagkapcsolt hálózathoz vezettek, amely egy összeköttetés nélküli internetwork rétegen alapulnak. Ez a réteg az internetréteg, amely az egész architektúrát összefogja. Ennek a rétegnak az a feladata, hogy egy hoszt bármilyen hálózatba csomagokat tudjon küldeni, illetve a csomagokat a célállomástól függetlenül (lehetőleg egy másik hálózatba) képes legyen továbbítani. Az sem gond, ha a csomagok nem az elküldés sorrendjében érkeznek meg, ugyanis, ha erre szükség van, akkor a magasabb rétegek visszarendezik őket a megfelelő sorrendbe. Azt viszont ne felejtsük el, hogy az „internet” szó most általános értelemben használjuk annak ellenére, hogy ez a réteg az internetben is jelen van. Az internetréteg meghatároz egy hivatalos csomagformátumot, illetve egy protokolلت, amelyet internetprotokollnak (Internet Protocol, IP) hívnak. A csomagok kézbesítése során azok útvonalának meghatározása, valamint a torlódás elkerülése itt most a legfontosabb feladat. Ezért hasonlít funkciója egy másik modell hálózati rétegére.

A hálózatelérési réteg

Az internetréteg alatt egy nagy Żr tátong. A TCP/IP hivatkozási modell ugyanis nem mondja meg, hogy mi legyen itt, csak annyi megkötést tesz, hogy a hosztnak egy olyan hálózathoz kell csatlakozni, amely az IP-csomagok továbbítására alkalmas protokollal rendelkezik. Ez a protokoll hosztonként, illetve hálózatonként más és más lehet.

Összeköttetés alapú és összeköttetés nélküli szolgáltatások, különbségek, mintapéldák

Az összeköttetés alapú és összeköttetés nélküli szolgáltatások a hálózatok kommunikációs módját írják le. Itt van néhány alapvető különbség közöttük:

Összeköttetés alapú szolgáltatások

- Az adatátvitel előtt előzetes kapcsolat létrehozása szükséges a kommunikáló felek között.
- A kapcsolat felépítése során ellenőrzik az útvonalat, a forrás és cél közötti rendelkezésre álló erőforrásokat, és paramétereket állapítanak meg a kommunikációhoz.
- Az adatokat sorrendben és hibamentesen továbbítják a kapcsolat fenntartása alatt.
- Példák ilyen szolgáltatásokra: TCP (Transmission Control Protocol) a TCP/IP modellben, telefonhívások, video konferenciák.

Összeköttetés nélküli szolgáltatások

- Az adatátvitel előtt nincs szükség előzetes kapcsolat felépítésére a kommunikáló felek között.
- Az adatokat azonnal továbbítják a hálózaton, anélkül, hogy előzetesen ellenőriznék az útvonalat vagy a rendelkezésre álló erőforrásokat.
- Az adatokat független csomagok formájában küldik, és a címzés alapján továbbítják őket a hálózaton.
- A csomagokat nem feltétlenül érkeznek meg az eredeti sorrendben vagy hibamentesen.

- Példák ilyen szolgáltatásokra: UDP (User Datagram Protocol) a TCP/IP modellben, DNS (Domain Name System) lekérdezések, streaming média.

Az összeköttetés alapú szolgáltatások megbízhatóbbak, mivel a kapcsolat felépítése és fenntartása során ellenőrzik az adatok továbbítását. Az összeköttetés nélküli szolgáltatások gyorsabbak és egyszerűbbek, mivel nincs szükség előzetes kapcsolat felépítésére, de nem garantálják a megbízható adatátvitelt.

Fontos megjegyezni, hogy minden típusú szolgáltatás hasznos és alkalmazható különböző helyzetekben, attól függően, hogy milyen követelményeket támasztunk a kommunikációval szemben.

Hibafeltárási és hibajavítási technikák, ezek megvalósítása a TCP/IP modellben

A hibafeltárási és hibajavítási technikák a hálózatokban használatosak a megbízható adatátvitel biztosítására. A TCP/IP modellben több ilyen technika is alkalmazható. Itt vannak a legfontosabbak:

1. Hibafeltárás:
 - Címzéhiányzás: Az IP protokoll a címzéhiányzás (addressing) segítségével azonosítja az adatok forrását és célját. Ha a címzési információk hibásak vagy hiányosak, a hálózat képes észlelni és hibaüzenetet küldeni.
 - Csomagellenőrzés: Az IP protokoll ellenőrzőösszegeket (checksum) használ az adatok integritásának ellenőrzésére. Az ellenőrzőösszeg hibás értéke esetén a hálózat észleli a hibát és eldobja vagy újraküldi a csomagot.
2. Hibajavítás:
 - Visszajelzés alapú hibajavítás: Az összeköttetés alapú szolgáltatások, például a TCP, visszajelzéseket használnak a hibajavításhoz. Amikor a fogadó felet hibás vagy hiányzó adatok érkeznek, visszajelzést küld a forrásnak, hogy újraküldje az adatokat.
 - Csomagösszerakás: A fogadó oldalon a TCP/IP modell összerakja a fogadott adatokat a csomagokból a helyes sorrendben. Ha hiányzó vagy hibás csomagok érkeznek, a fogadó visszajelzést küld a forrásnak a hiányzó adatok újraküldéséhez.

Ezeket a hibafeltárási és hibajavítási technikákat a TCP/IP protokollrétegek implementálják:

- Az IP réteg ellenőri az IP címeket és az ellenőrzőösszegeket a hibafeltárás szempontjából.
- Az UDP (User Datagram Protocol) a hibafeltárási funkciók hiányában összeköttetés nélküli szolgáltatást nyújt, és nem végez hibajavítást.
- A TCP (Transmission Control Protocol) összeköttetés alapú szolgáltatást nyújt, amely hibafeltárási és hibajavítási mechanizmusokat használ, például visszajelzéseket, szekvenszámokat és időzítéseket a megbízható adatátvitel biztosításához.

Fontos megjegyezni, hogy a hibafeltárási és hibajavítási technikák beépülnek az egyes protokollok és rétegek működésébe a TCP/IP modellben annak érdekében, hogy a hálózati kommunikáció megbízható és hibamentes legyen.

A TCP/IP és az OSI modellek kapcsolata (különbségek, azonosságok)

Hasonlóságok

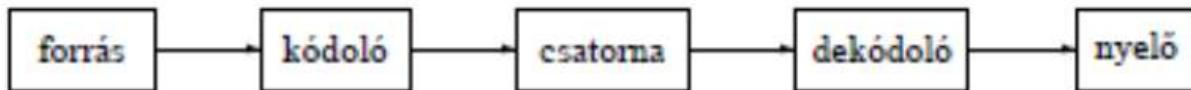
1. Mindkettő rétegmodell, hierarchikusan egymásra épülő rétegekkel, melyeknek protokolljai egymástól függetlenek
2. A rétegek feladatai is hasonlóak, egymásnak megfeleltethetők

Különbségek

1. Az OSI modell három fő fogalom köré összpontosul:
 1. Szolgáltatások
 2. Interfészek
 3. Protokollok
2. Előbb volt a modell, a szolgáltatások és a protokollok csak később a rétegnék megfelelően
3. A TCP/IP esetén fordítva történt, a protokoll készlet volt előbb, ehhez igazították a rétegeket
4. A rétegek száma különbözik, az OSI
5. Az OSI a 3. rétegben támogatja az összeköttetés alapú és az összeköttetés mentes kommunikációt, de a 4. rétegben csak az összeköttetés alapút.
6. A TCP/IP a hálózatban csak az összeköttetés mentes, míg a szállítási rétegen mindenkét kommunikációt támogatja

4. ÁTVITELI KÖZEG

Az átviteli közeg rendeltetése, tipikus közegek, jellemzőik, előnyök, korlátok



- Az átviteli közeg egy fizikai útvonal az átviteli rendszer adója és vevője között.
- Lehet irányított (vezetékes) és irányíthatlan (vezeték nélküli).
- A közegek lehetnek vezetők és nem vezetők, de a kommunikáció minden esetben elektromágneses hullámokkal történik.
 - Vezető közegek a csavart érpáras rézvezetékek, a koaxiális kábelek és az optikai szálak.
 - Nem vezető közegek pedig az atmoszféra és az űr.

A modern hálózatok általában három különböző közeget használnak az eszközök összekapcsolására, illetve az adatok továbbítására:

- rézkábelek,
- üveg vagy műanyag szálak (optikai kábelek),
- vezeték nélküli átvitel.

A jel továbbításához szükséges kódolás minden átviteli közegen különböző.

A fémvezetékeken az adatokat speciális mintáknak megfelelő elektromos impulzusokkal kódolják.

Ide tartozik például az STP kábel, ScTP kábel, UTP kábel, koax kábel.

Optikai átvitelnél az infravörös vagy a látható fény tartományában használt fény impulzusok adják a jeleket.

- Előnyei: – Kevésbé érzékeny a külső zajokra, nincs interferencia – Nincs áthallás – Magasabb sávszélesség – Nagyobb távolság – Nem kell földelni – Kevésbé érzékeny a környezeti hatásokra – Biztonságos (nehezen lehallgatható).
- Hárányai: – Drága – Képzett szakemberek – Időigényes kiépítés

A vezeték nélküli adatátvitelnél pedig az elektromágneses hullámok segítségével biztosítják a különböző biteket. Vezetéknélküli technológiák a Wi-Fi, Bluetooth, WiMAX.

Az egyes adatátviteli közegek egyedi sajátosságokkal és előnyökkel rendelkeznek. Nem minden hálózati közeg rendelkezik ugyanolyan tulajdonságokkal, illetve nem mindenkor alkalmass ugyanarra a célra. Az átviteli közeg megválasztásának szempontjai:

- a távolság, amelyen keresztül a közeg képes a jelet továbbítani,
- a környezet, ahol az átviteli közeget ki kell építeni,
- az adatok mennyisége, valamint az a sebesség, amellyel azokat továbbítani kell,
- a közeg anyag- és telepítési költsége.

Jelek és zajok, a jeltorzulás okai a réz alapú és az optikai átvivő közegben

Többféle jel létezik, ilyenek például az analóg - digitális, periodikus (akár szinuszos) - aperiodikus jel. Zajról beszélünk, amikor az adó és a vevő között olyan összetevők adódnak hozzá a jelhez, amelyek eredetileg elküldött jelben nem voltak benne. Jelterjedés akadályozói lehetnek a réz alapú és az optikai átvivő közegben:

- Csillapítás
- Forrasztás minősége
- Patch panelek, csatlakozók
- Szűrők, erősítők
- Hurkok, hajlások a kábelben
- Szennyeződés a csatlakozókon

Csillapítás és csillapítás torzítás

- A jel erőssége a távolság növekedésével csökken
- Az átviteli közeg függvénye
- A vett jel erősségének legalább akkorának kell lennie, hogy:
 - Érzékelni lehessen
 - Elegendően nagynak kell lennie ahhoz, hogy a vétel hiba nélkül megvalósuljon (sokkal nagyobb legyen a zajnál)
- A jel erősségének növelésére erősítőket/ismétlőket használnak
- A csillapítás a frekvencia függvényében változik (általában minél nagyobb a frekvencia, annál nagyobb)

Késleltetés torzítás

- Csak irányított közegen fordul elő
- A terjedési sebesség a frekvenciától függően változik
- Ennek következtében a különböző frekvenciájú összetevők eltérő időpillanatokban érkeznek meg
- Elsősorban digitális adatok esetén kritikus
- Egy adott bithez tartozó összetevők más bit idejében érkeznek meg
- Szimbólumközi áthalláshoz vezet

Zaj

Az adó és a vevő között olyan összetevők adódnak hozzá a jelhez, amelyek eredetileg elküldött jelben nem voltak benne

Fajtái:

- Termikus zaj
- Áthallás
- Impulzus

Termikus zaj

- Az elektronok termikus mozgásának a következménye
- Egyenletes eloszlású
- Fehér zaj

Áthallás

- Az egyik vonalon elküldött jel megjelenik a másik vonalon (valamilyen csatolás következtében)

Impulzus

- Szabálytalan impulzusok vagy tüskék (pl. villám)
pl. külső elektromágneses interferencia
- Rövid idejű
- Nagy amplitúdójú
- Analóg jelek esetén kevésbé zavaró tényező
- Digitális adatok esetén komoly hibaforrás

Egy zavaró impulzus több bitet is tönkretehet

Az osztott használatú átviteli közeg hozzáférési problémái, megoldások

Osztott használatú átviteli közeg: minden állomás közvetlenül ugyanahhoz a kábelhez csatlakozik, amely bármelyik két állomás közötti adatátvitelre használnak (többszörös hozzáférés). Az átvinni kívánt adatot az állomás keretbe foglalja a célállomás és a saját címével együtt, majd ráadja a kábelre. A keretet minden állomás érzékelni, de csak az dolgozza fel, amelyik a saját címét találja a keret elején. A feladó állomás címéből tudja a célállomás, hogy kitől származik az üzenet, és kinek kell válaszolnia.

Ha két állomás egyszerre bocsát keretet a kábelre, a villamos jelek összeadódnak, és az üzenetek hibásak lesznek (ütközés). Az ütközések valószínűsége csökkenhető azzal, hogy az állomások a keret elküldése előtt elektronikusan figyelik a csatornát (csatornafigyelő), hogy folyik-e átvitel rajta, és csak akkor küldenek keretet, ha a csatorna tétlen.

Ütközés mégis bekövetkezhet a kábelek késleltetése miatt. Az állomások az átvitel közben is figyelik a kábelben lévő jelet, és ha az eltér a továbbított jeltől, úgy tekinti, hogy ütközés következett be (ütközésérzékelés). Hogy minden állomás tudomást szerezzen az ütközésről, az érintett állomások egy rövid ideig véletlen bit-mintát (jam sequence) továbbítanak. Az ütközésben érintett állomások ezután egy rövid, véletlen idejű várakozás után próbálják újra továbbítani a keretet.

A determinisztikus és a nemdeterminisztikus közeghozzáférés indokai, jellemzői és alkalmazása

Nemdeterminisztikus

Nem determinisztikus versengéses módszer használatakor a hálózati eszköz bármikor hozzáférhet a közeghez, amikor küldeni szeretne. Az ilyen módszerek a teljes káosz elkerülése érdekében a vivőérzékeléses többszörös hozzáférés (Carrier Sense Multiple Access, CSMA) nevű technikát használják annak megállapítására, hogy a közegen van-e jeltovábbítás.

Egy másik csomóponttól származó vivőjel érzékelése esetén megállapítható, hogy a közegen éppen adatátvitel zajlik. Ha a készülék ilyenkor próbál meg adni, a közeg foglaltságát fogja tapasztalni. Ekkor várakozni kényszerül, majd egy rövid idő múlva újra próbálkozhat. Ha nem észleli a vivőjelet, akkor továbbíthatja az adatokat. Az Ethernet és a vezeték nélküli hálózatok versengéses közeg-hozzáférési módszert használnak.

Determinisztikus

A determinisztikus hozzáférési mód használatakor a hálózati eszközök felváltva, egymás után férnek hozzá a közeghez. Ha valamelyik végberendezés nem kívánja használni a közeget, a lehetőség továbbadódik a következő eszköznek. A folyamatot vezérjel használatával lehet megkönnyíteni. A végberendezés a megszerzett vezérjel birtokában keretet helyezhet el a közegen. Más eszköz csak azután teheti ezt meg, miután a keret megérkezik a célohoz, amely feldolgozza azt, majd felszabadítja a vezérjelet. Annak ellenére, hogy ez a hozzáférés jól tervezhető és kiszámítható teljesítménnyel rendelkezik, a determinisztikus módszereket kevésbé hatékonynak is ítélni lehet, mivel az eszközöknek várniuk kell, mielőtt használni tudják a közeget.

5. ADATKAPCSOLAT

A 2. réteg szolgáltatása, fajtái, mit és hogyan javít az 1. réteg szolgáltatásain

L2 – Adatkapcsolati réteg

- Fizikai címzés (MAC címek)
- A hálózati réteg számára hibamentesnek tűnő vonalat mutat.
- A küldő az adatokat adatkeretekké tördeli, sorrendhelyesen továbbítja, végül a vevő nyugta keretét feldolgozza (keretezés)
- Hibakezelés (detektálás, javítás).
 - Felismeri az adatkeretek határait, hibás keret esetén újra továbbítja
 - Sérült, elveszett, kettőzött keretek miatt bekövetkező problémák megoldása
- Forgalom szabályozási és torlódáskezelési mechanizmust biztosít (flow control) (gyors adó - lassú vevő probléma megoldása)
- Közeghözáférés vezérlése (többszörös hozzáférésű csatorna esetén)

A 2. réteg feladatai általánosan és példákon keresztül is a különböző megvalósításokban

A hálózati rétegnek nyújtott szolgáltatások

- Elsődlegesen az adatok átvitelét biztosítja az adó gép hálózati rétegétől a vevőgép hálózati rétegéig
- Átviteli hibák kezelése
- Az adatforgalom szabályozása

Az adatátviteli szolgáltatás fajtái

- Nyugtáztlan összeköttetés nélküli
 - Nem épít ki kapcsolatot, az adatokat egymástól függetlenül küldi (pl. Ethernet), akkor jó, ha a hibaarány alacsony
- Nyugtáztott, összeköttetés nélküli
 - Nincs felépített kapcsolat, de nyugtázza a kereteket (pl. Wi-Fi)
- Nyugtáztott, összeköttetés-alapú
 - Felépít majd lebont egy kapcsolatot, Pl. Műholdas összeköttetés

Az adatkapcsolati réteg feladatai

- A hálózati réteg számára hibamentesnek tűnő vonalat mutat
- A küldő az adatokat adatkeretekké tördeli, sorrendhelyesen továbbítja, végül a vevő nyugta keretét feldolgozza - keretezés
- Felismeri az adatkeretek határait, hibás keret esetén újra továbbítja
- Azonosítani kell az adott adatkapcsolathoz csatlakozó eszközöket – fizikai címzés
- Sérült, elveszett, kettőzött keretek miatt bekövetkező problémák megoldása
- Forgalom szabályozási mechanizmust biztosít (flow control) (gyors adó - lassú vevő probléma megoldása)
- Keretképzés
- Fizikai címzés
- Hibakezelés
 - Detektálás
 - Javítás
- Forgalomszabályozás és torlódáskezelés
- Közeghözáférés vezérlése (többszörös hozzáféréső csatorna esetén)

Adatkapcsolati réteg jellemzői

- Az adatkapcsolati réteg feladata adatok átvitele valamilyen soros adatkapcsolaton
- Az átviteli vonal lehet:
 - vezetékes pont-pont fizikai áramkör (csavart érpár, koaxiális kábel, optikai szál)
 - vezeték nélküli kapcsolat (mikrohullám, stb.)
 - fizikai vagy logikai kapcsolat valamilyen kapcsolt hálózaton keresztül
- Az átviteli mód lehet:
 - aszinkron
 - szinkron
- Az átvitelt vezérlő protokoll lehet:
 - karakter-orientált
 - bit-orientált
- A magasabb hálózati rétegek számára nyújtott szolgáltatás lehet:
 - megbízhatatlan (best-try), összeköttetés-mentes (kapcsolat nélküli)
 - megbízható (reliable), összeköttetés-alapú (kapcsolat-orientált)

Keretezés

A fizikai réteg szolgáltatásait veszi igénybe, ami bitsorozatot továbbít → KERETEKET kell készíteni

- Bájtszámlálás
 - Megadja a keretben levő bájtok számát, ebből tudja a vevő a keret végét
 - Probléma: „könnyű elveszíteni a fonalat”
- Kezdő- és végkarakterek használata bájtbeszúrással
 - Keretkezdet megjelölése → FLAG (pl.: HDLC)
- Kezdő- és végjelek használata bitbeszúrással (pl.: PPP)
- Kódolási eljárással – pl.: 4B5B

Átviteli módok

- A szinkronizáció alapvetően kétféleképpen valósítható meg attól függően, hogy az adó és a vevő órajele független (aszinkron) vagy szinkronizált (szinkron)
 - Aszinkron átvitel
 - A byte-ok, karakterek tetszőleges időközönként követik egymást, az adó és a vevő órajelét a byte-ok kezdetén kell szinkronizálni
 - Szinkron átvitel
 - Az egész keretet egy összefüggő bit-folyamként továbbítják, az adó és a vevő órajelét a keret átvitele alatt szinkronban kell tartani

Az átviteli hibák felismerési és javítási mechanizmusai, példák

- Ha a vevő hibát észlel, szükség van valamilyen mechanizmusra, amellyel a remélhetően hibamentes információt megkapja.
- Ez háromféleképpen érhető el:
 - Hibajavítással: Az átvitt keret olyan redundáns információt tartalmaz, amelyből a hiba jelenléte és helye észlelhető. A hibás bitek invertálásával a hiba javítható.
 - Visszacsatolásos hiba kezeléssel: Az keret olyan redundáns információt tartalmaz (ellenőrző összeg, ciklikus redundancia kód), amelyből a hiba jelenléte észlelhető. Ezután a vevő a hibás keret újra átvitelével juthat a remélhetően hibamentes információhoz.
 - A hiba vezérlés a keret nyugtázásán alapul. Hibás keretet nem nyugtáznak, vagy negatív nyugtát küldenek. A küldő a nyugta hiányából, vagy a negatív nyugtából értesül, hogy a keret nem érkezett meg.
- A hálózatok világában a visszacsatolásos módszer dominál.

Hibajavító kódok

- Hamming kódok
- Bináris konvolúciós kódok
- Reed-Solomon kódok
- Alacsony sűrűségű paritásellenőrző kódok
- Hibajelző kódok
- Paritásbit képzése
- Ellenőrző összeg képzése
- Ciklikus redundancia ellenőrzés

6. AZ ETHERNET RENDSZER ALAPJELLEMZŐI

Helyi hálózatok – Local Area Network

- Egymással adatkommunikációs kapcsolatban lévő számítógépek együttese – peer-to-peer kapcsolatban
- Kiterjedésük viszonylag kicsi (néhány km²), egy-egy intézményre, telephelyre terjednek ki (manapság már az otthonokban is minden napos)
- Állandó hozzáférést biztosítanak a hálózati szolgáltatásokhoz illetve lehetővé teszik nyomtatónak és egyéb erőforrások megosztását
- Egy LAN megtervezését, kiépítését, menedzselését maga az intézmény végzi → egy adminisztrációs terület alá tartozik
- A LAN-ok átviteli sebessége viszonylag nagy lehet (10 mbps – 10 gbps)
- Az adatátvitel biztonsága a rövid távolságok és a technológiából eredően magas

Helyi hálózatok történelmi fejlődése

- Kezdetben osztott közegű – hub-ok alkalmazásával
- Később bridge segítségével szegmentált
- Napjainkban Full-duplex módú, kapcsolókkal mikroszegmentált illetve osztott közegű Wi-fi

Helyi hálózatok jellemzői

A helyi hálózatokat három fő jellemzője különbözteti meg a többi hálózattól:

- Kiterjedésük – korlátos (intézményen, telephelyen belül)
- átviteli módjuk – nagy átviteli sebességgel rendelkező, általában Ethernet vagy Wi-fi technológián alapul
- Topológiájuk – kiterjesztett csillag

Topológiák

- Busz (sín)
- Sínhálózat
Sínhálózatokban ütközés előfordul, mivel az állomások jeleit a sín eljuttatja minden állomáshoz, ill. a hubok a beérkező jeleket minden portjukon továbbítják
- Csillag
 - Kapcsolt hálózat
 - Irányított hálózat
- Gyűrű

Az Ethernet ma használt átviteli közegeire, csatlakozóira es 1. rétegbeli eszközeire vonatkozó követelmények és szabványok

LAN szabványok

- A legelterjedtebbet használt LAN-okat az IEEE szabványosította, amelyeket az ISO is elfogadott
- A LAN szabványok az IEEE 802, illetve az ISO 8802 sorozatba tartoznak
- Az egyes LAN típusok az alkalmazott topológiában, a közeghozzáférés módjában (MAC) és az alkalmazások jellegében különböznek
- Típusok:
 - CSMA/CD bus (IEEE 802.3)
 - Fast Ethernet (IEEE 802.3u)
 - Gbit Ethernet (IEEE 802.3z, IEEE 802.3ab)
 - 10Gbit Ethernet (IEEE 802.3ae)
 - Token bus (IEEE 802.4)
 - Token ring (IEEE 802.5)
 - FDDI (ISO 9314)

IEEE LAN szabványok

OSI referencia modell	Adatkapcsolati réteg	LLC alréteg	IEEE 802.2				IEEE 802 szabványok
		MAC alréteg	IEEE 8002.3 CSMA/CD Ethernet	IEEE 802.4 Vezérlés busz	IEEE 802.5 Vezérlés gyűrű Token Ring	FDDI	
	Fizikai réteg						

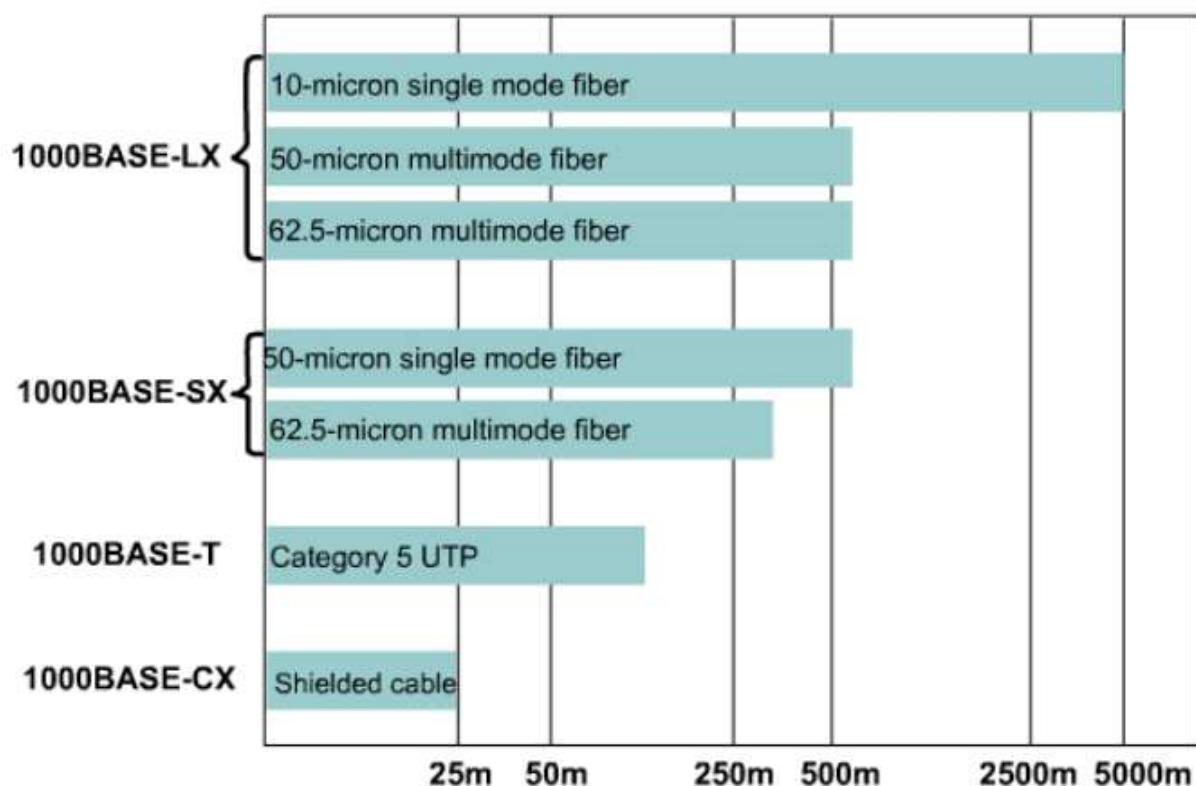
Gyors Ethernet – Fast Ethernet

- Fajtái:
 - 100Base-TX
 - 100Base-FX
- max. 100 szegmenshossz
- szinkron
- fél-duplex/duplex
- 2 kódolási lépés
 - 1. 4B/5B
 - 2. átviteli közegre jellemző vonali kódolás

Gigabit Ethernet

- Fajtái:
 - 1000Base-T (IEEE 802.3z)
 - 1000Base-LX, 1000Base-SX (IEEE 802.3ab)
- 1998
- 1Gbps átviteli sebesség
- szinkron

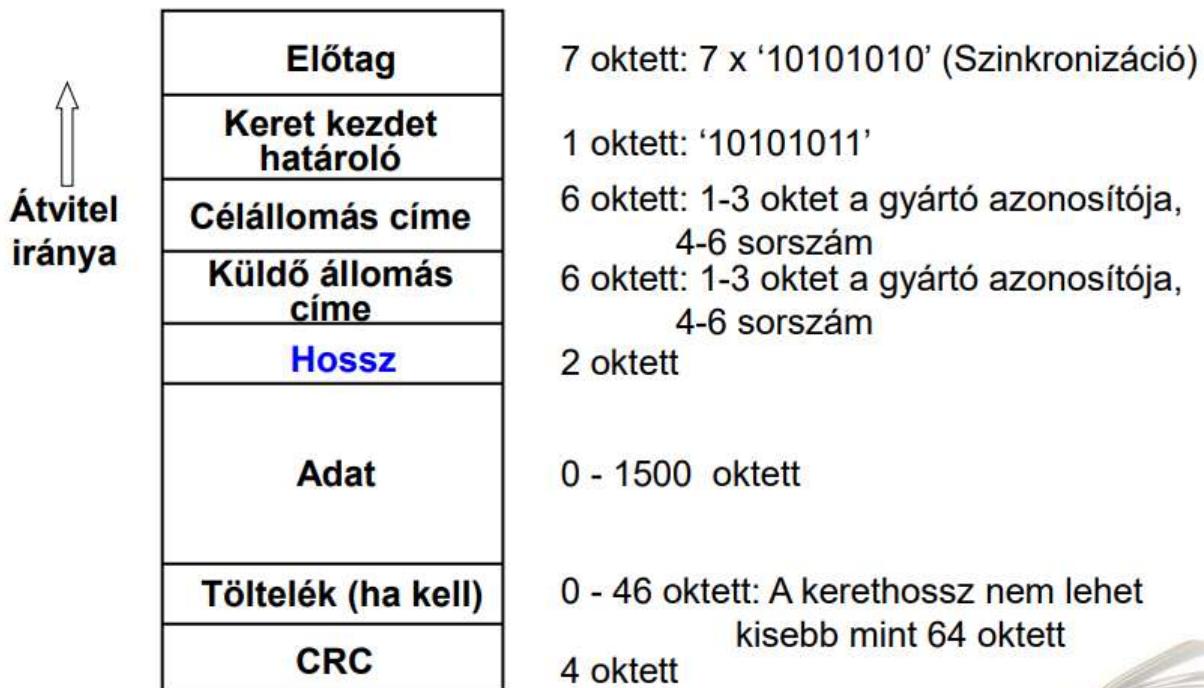
Maximális kábelhosszok



10 Gbps Ethernet jellemzői

- Az IEEE 802.3ae szabvány írja a 10 Gbps sebességű, optikai szálak feletti, duplex Ethernet működését
- A 10 Gigabit Ethernet (10 GbE) már nemcsak a LAN-okban, de a MAN-okban és a WAN-okban is fontos szerephez jut
- Keretformátuma és egyéb második rétegbeli jellemzői a korábbi szabványokkal kompatibilisek
- A 10 gigabites változatok újrakeretezés és protokoll átalakítás nélkül is képesek egymással és a korábbi technológiákkal együttműködni
- Mivel az optikai szálakon csak duplex átvitel folyik, a CSMA/CD alkalmazása szükségtelen
- Rugalmas, hatékony, megbízható, viszonylag alacsony költségű, végponttól végpontig terjedő kapcsolatokat biztosító Ethernet hálózatok építése lehetséges
- A TCP/IP a LAN-okon, MAN-okon és WAN-okon egyetlen második rétegbeli szállítási megoldással használható

Az Ethernet és az OSI modell, az Ethernet PDU felépítése és mezői



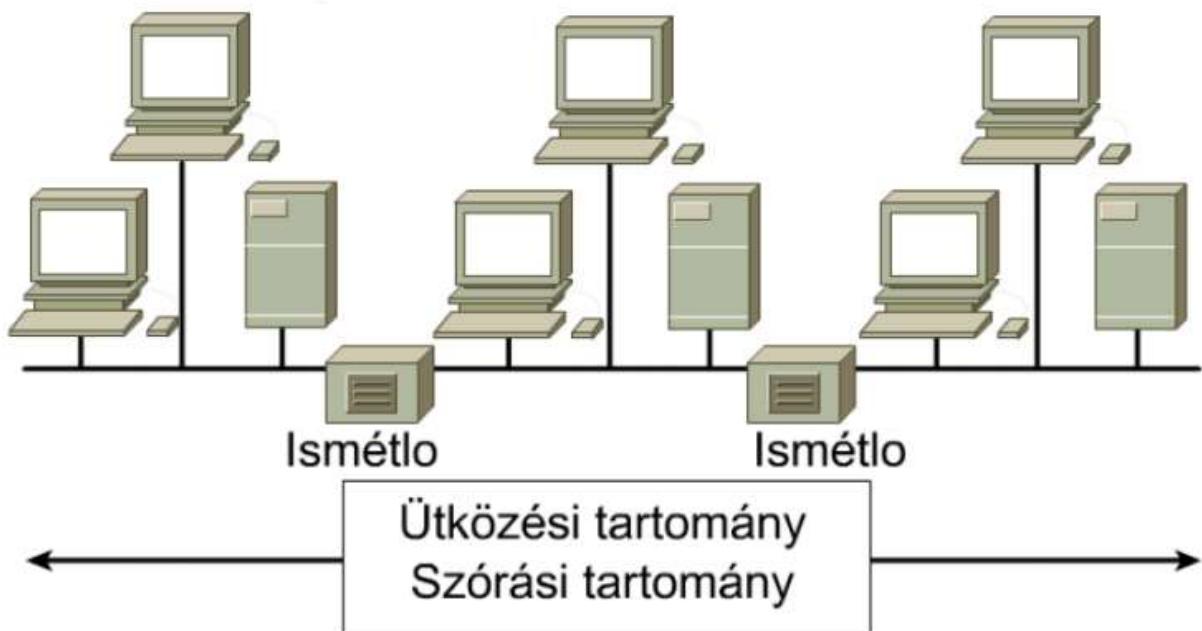
Átvitel iránya	Előtag	
	Keret kezdet határoló	7 oktet: 7 x '10101010' (Szinkronizáció)
	Célállomás címe	1 oktet: '10101011'
	Küldő állomás címe	6 oktet: 1-3 oktet a gyártó azonosítója, 4-6 sorszám
	Hossz	6 oktet: 1-3 oktet a gyártó azonosítója, 4-6 sorszám
	Adat	2 oktet
	Töltelék (ha kell)	0 - 1500 oktet
	CRC	0 - 46 oktet: A kerethossz nem lehet kisebb mint 64 oktet 4 oktet

Az Ethernet kapcsolás

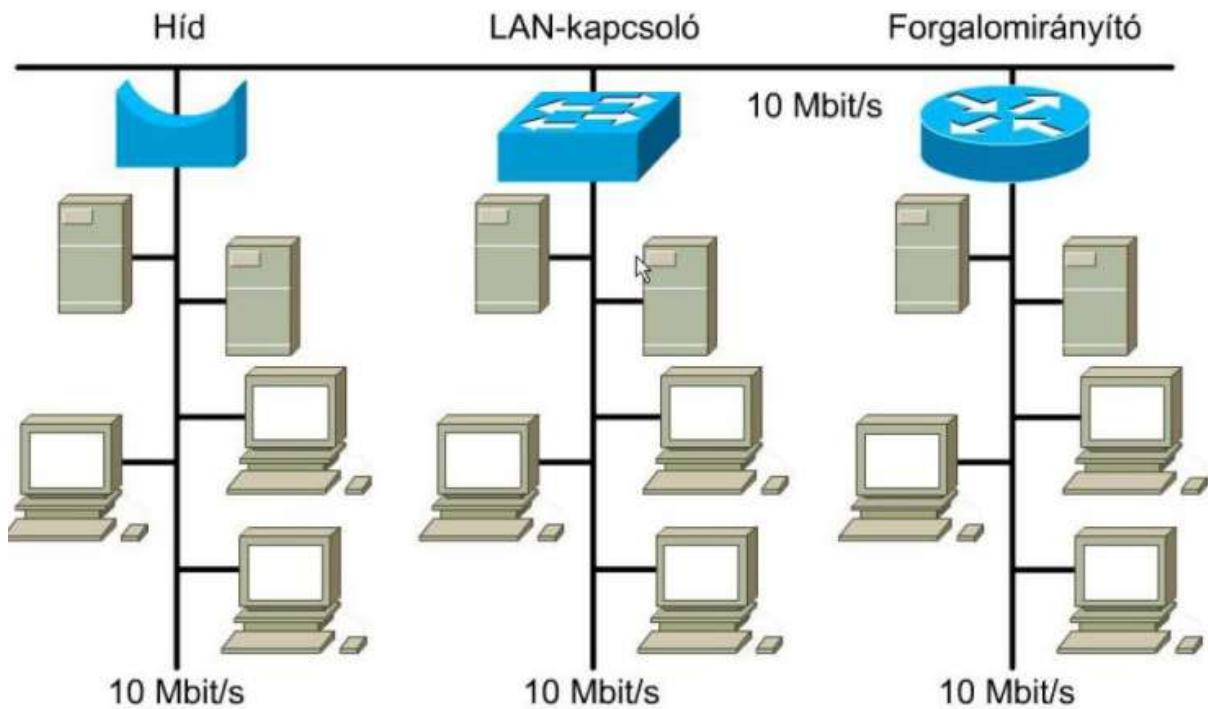
- A mai LAN-ok leggyakrabban használt eszközei
- Különböző sebességű és port-számú eszközök léteznek
- Felváltották az ismétlőket, Hub-okat és hidakat
- A portokra érkező keretet szelektíven csak arra a portjára továbbítja, amelyre a címzett számítógép vagy az azt tartalmazó hálózat csatlakozik
- Egyidejűleg képes a különböző eszköz-párok közötti kerettovábbításra
- A szórásos (broadcast) üzeneteket valamennyi portjára kiküldi
- Duplex átvitel is lehetséges
- A kapcsoló táblázatot tart fenn az egyes portjaira kapcsolt hálózati eszközök címeiről (MAC címtáblázat)
- A porton bejövő kereteket puffereiben tárolja, a célállomás címét megkeresi a táblázatában, és ha megtalálja, a keretet megfelelő portra továbbítja
- Ha nem találja meg, a keretet valamennyi portjára eljuttatja (elárasztás)
- A táblázatot ‘tanulással’ építi fel, vagyis a bejövő keretek forrás címéből tanulja meg, hogy melyik állomás melyik portján található
- A kapcsolóban torlódás léphet fel, ha valamelyik bemeneti puffer megtelik

Az Ethernet hálózatok szegmentálása

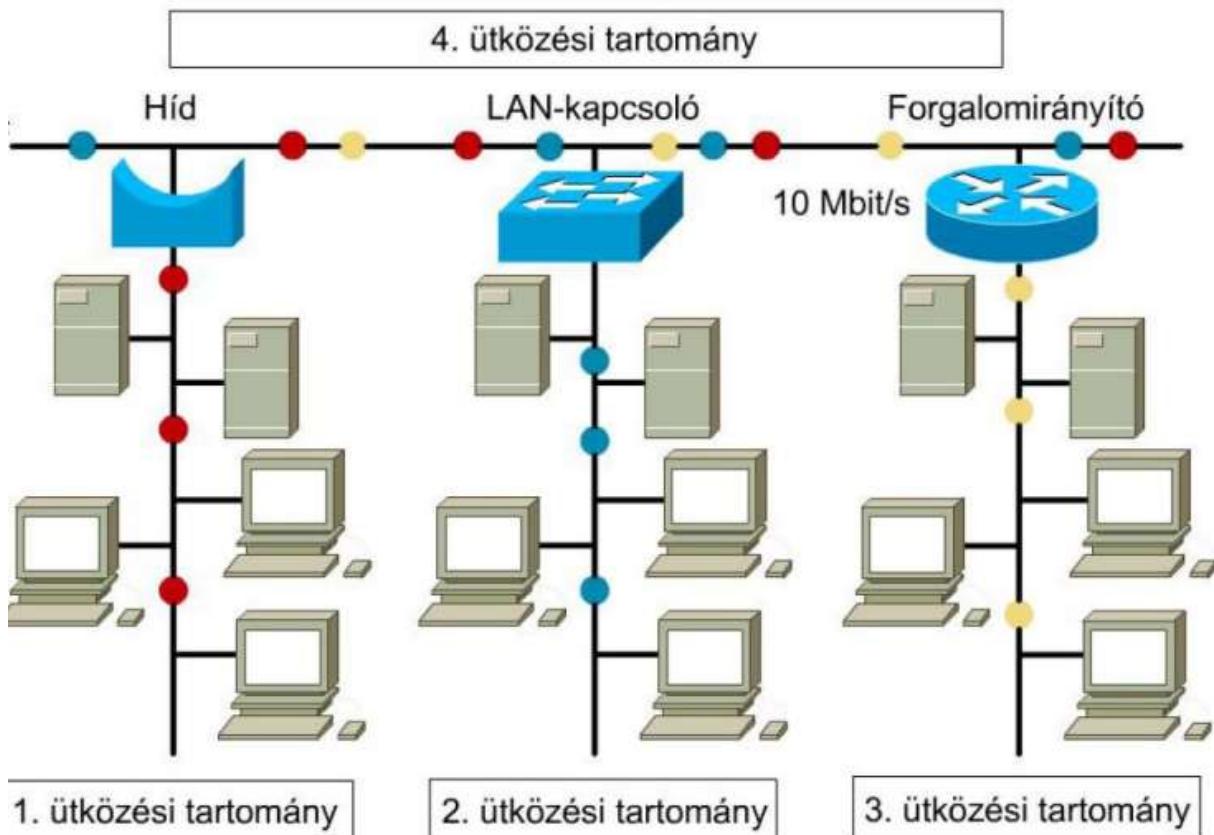
- Az ismétlők/HUB-ok az ütközési tartományt és a szórási tartományt is kiterjesztik
- A szórásos üzenet (cél-Ethernet cím: FF.FF.FF) a hálózati infrastruktúra, az operációs rendszerek és néhány alkalmazás legális üzenettípusa



- A szegmentálás elszigeteli az egyes szegmensek hálózati forgalmát
- Nagyobb felhasználói sávszélesség
- Csökken az ütközések száma



- Mindhárom eszköztípus önálló ütközési tartományt alkot
- A szórásos üzeneteket a híd és a kapcsoló továbbítja, a forgalomirányító nem



2. rétegbeli LAN Kapcsoló

- Ethernet kapcsolók a 2. OSI rétegben működő berendezések
- Több (sok) porttal rendelkeznek, amelyekhez munkaállomások, szerverek, hubok, forgalomirányítók, más kapcsolók csatlakoztathatók
- A kapcsolók rendelkeznek: processzorral, memóriával, speciális áramkörökkel, operációs rendszerrel
- A portjaira kapcsolt eszközök között nagy sebességgel, kis késleltetéssel végez kapcsolást
- A kapcsolást a keretben foglalt célállomás MAC-címe alapján végzi
- A keretbe beágyazott protokollt (alapfunkciója szerint) nem vizsgálja
- Port –MAC-cím táblázato(ka)t tart fenn, amelynek alapján a beérkező kereteket a kimenő porthoz rendeli
- Ezt a táblázatot tanulással építi fel. A beérkező keretek forrás MAC-címéből tanulja meg, hogy az egyes MAC című készülékek a kapcsoló melyik portjára vannak csatlakoztatva
- Egy-egy porthoz több eszköz is csatlakozhat, Hub vagy másik kapcsoló segítségével
- A kapcsolók, ellentétben a Hub-akkal, duplex működésre képesek
- A kapcsolók dedikált sávszélességet biztosítanak az egyes portjai közötti forgalom számára
- A kapcsolók portjai ún. mikro szegmenseket alkotnak. Ideális esetben a szegmens egyetlen (a portra csatolt) készülékből áll, így ütközés nem fordulhat elő
- A keretátvitel idejére két port között egy ún. virtuális áramkör jön létre, amelyen a keret áthalad. Ez a virtuális áramkör teljes (a portra) jellemző sávszélességet biztosít a kommunikáló gépek számára
- A kapcsoló portjai egyetlen szórási tartományt (broadcast domain) alkotnak. A szórásos üzeneteket és a többes küldés (multicast) üzeneteket a kapcsoló a bejövő port kivételével minden portjára kiküldi
- Nem ismert célport esetén a keretet minden kimenetén továbbítja (elárasztás)

Ethernet kapcsoló

- A legtöbb Ethernet hálózaton hosztokat kapcsol egy központi hálózati eszközhöz
- A MAC címtől függően kapcsolási és szűrési feladatot lát el
- MAC cím táblát tart fenn és ez alapján továbbít
- Forgalomirányító szükséges a különböző alhálózatok közötti forgalom továbbításához

Kerettovábbítási módszerek

- Store-and-forward (tárol és továbbít)
megvárja míg az egész keret megérkezik, kiszámítja a CRC-t és ha helyes, akkor a megfelelő portra továbbítja a keretet
- Cut-through switching
mielőtt az egész keret megérkezne, már továbbítja is
 - Fast-forward – amint a célcímet kiolvassa, márto vissza a keretet, legkisebb késleltetés
 - Fragment free – 64 byte-ot vár

Az Ethernet kerethossz minimális értéke, a megkötés indoka

A hosszmező (length field) az adatmezőben található adatbájtok számát adja meg. A minimum 0, a maximum 1500 bajt: Bár egy 0 hosszúságú adatmező érvényes, de problémákat okozhat. Amikor egy adó-vevő ütközést érzékel, csonkolja az aktuális keretet, ami azt jelenti; hogy kóbor bitek, keretdarabkák minden jelen lehetnek a kábelen. Az érvényes keretek és a szemét megkülönböztetése érdekében a 802.3 szabvány szerint egy érvényes keretnek legalább 64 bajt hosszúnak kell lennie, a célcímtől az ellenőrzőösszeget is beleértve. Ha tehát egy keret adatrésze 46 bajtnál rövidebb, akkor kitöltő mezőt kell használni a minimális kerethossz eléréséhez. A minimális kerethosszúság alkalmazásának másik oka az, hogy egy rövid keret küldését egy állomás még azelőtt befejezhetné, mielőtt a keret első bitje elérné a kábel legtávolabbi végét, ahol is az egy másik kerettel ütközhet

Közeghosszaférés-vezérlés, az ütközések felismerése a különféle Ethernet változatoknál

Véletlen vezérlésű módszerek

- Aloha - csatornafigyelés nélkül többszörös hozzáférés (ha ütközés van véletlen ideig vár)
- CSMA csatornafigyelés többszörös hozzáférés
 - 1-perzisztens (adás esetén vár az adás végéig)
 - Nem perzisztens (adás esetén vár véletlen ideig; és ütközés esetén leadja a teljes keretet + vár véletlen ideig)
 - P-perzisztens
- CSMA/CD – ütközésfigyeléssel (ütközés esetén abbaagyja az adást és vár véletlen ideig)
 - Klasszikus Ethernet

Multiple-Access with Collision Detection (CSMA/CD)

- minden állomás közvetlenül ugyanahoz a kábelhez csatlakozik, amely bármelyik két állomás közötti adatátvitelre használnak (többszörös hozzáférés)
- az átvinni kívánt adatot az állomás keretbe foglalja a célállomás és a saját címével együtt, majd ráadja a kábelre
- A keretet minden állomás érzékeli, de csak az dolgozza fel, amelyik a saját címét találja a keret elején
- A feladó állomás címéből tudja a célállomás, hogy kitől származik az üzenet, és kinek kell válaszolnia
- Ha két állomás egyszerre bocsát keretet a kábelre, a villamos jelek összeadódnak, és az üzenetek hibásak lesznek (ütközés)
- Az ütközések valószínűsége csökkenhető azzal, hogy az állomások a keret elküldése előtt elektronikusan figyelik a csatornát (csatornafigyelő), hogy folyik-e átvitel rajta, és csak akkor küldenek keretet, ha a csatorna tétlen
- Ütközés mégis bekövetkezhet a kábelek késleltetése miatt
- Az állomások az átvitel közben is figyelik a kábelen lévő jelet, és ha az eltér a továbbított jeltől, úgy tekinti, hogy ütközés következett be (ütközésérzékelés)
- Hogy minden állomás tudomást szerezzen az ütközésről, az érintett állomások egy rövid ideig véletlen bit-mintát (jam sequence) továbbítanak
- Az ütközésben érintett állomások ezután egy rövid, véletlen idejű várakozás után próbálják újra továbbítani a keretet

Ütközéstípusok, ezek kialakulásának okai és következményei

- **Helyi ütközés** koaxiális kábelben (10BASE2 és 10BASE5) úgy keletkezhet, hogy a jel addig utazik a kábelben, amíg egy másik állomás jelével nem találkozik. A hullámformák ekkor átlapolódnak, egy részük kioltja, más részük felerősíti, megduplázza egymást. A jelek duplázódásával a feszültségszint a maximálisan megengedett fölé emelkedik. A feszültségtúllépést a helyi kábelszegmens minden állomása ütközésként érzékelí
- **Távoli ütközésre** következtethetünk, ha a minimális hosszt el nem érő keretet kapunk, aminek ellenőrző összege érvénytelen, ám helyi ütközésre utaló feszültségtúllépést vagy egyidejű RX/TX használatot nem tapasztaltunk. Az ilyen ütközések általában valamilyen ismétlő túloldalán történnek. Az ismétlő ilyenkor a feszültségtúllépést nem továbbítja
- Ha egy állomás az adatok első 64 oktettjét már elküldte, akkor normál, szabályos ütközésre már nincs esély. Az első 64 oktett elküldése után fellépő ütközéseket **kései ütközéseknek** nevezzük

7. HÁLÓZATI RÉTEG

Az Ethernet LAN korlátai

- Az ismétlőkkel összekapcsolt hálózati szegmensek egyetlen ütközési tartományt alkotnak. A gépek osztoznak a sávszélességen
- Az ismétlőkkel (HUB), kapcsolókkal (Switch), hidakkal (Bridge) felépített LAN-ok egyetlen szórási tartományt alkotnak, azaz a szórásos és a többes címzésű keretek a hálózat összes gépére eljutnak
- Az egyedi címzéshez elegendő a MAC cím
- Ha a hálózat nem homogén (Ethernet, FDDI, Token Ring, stb.), az összekapcsolás az adatkapcsolati rétegben nehézkes, lehetetlen vagy nem hatékony
- A hálózat mérete (kiterjedése, gépek száma) nem növelhető minden határon túl a szórásos üzenetek nagy száma és a nagy méretű kapcsolótáblák miatt → nem skálázható
- A MAC címek nem hierarchikusak, ezért a gépek számával arányosan nőnek a kapcsolótáblák is
- **A hálózati protokoll és a hálózati címzés jelenti a megoldást**

Összekapcsolt LAN – WAN hálózatok

- A WAN-ok címzése más mint a LAN-oké
- A különböző WAN technológiák eltérő címzéssel rendelkeznek
- Az Interneten különböző LAN és WAN technológiákat kell összekapcsolnunk
 - Olyan címzésre van szükség, amely a teljes összekapcsolt hálózaton (Interneten) egyedi azonosítást biztosít az egyes hálózatok számára, és a hálózatokon belül minden egyes gép számára
- A továbbítást végző eszközök (forgalomirányítók) címtáblázatot tartanak fent az adatok célba juttatására. Ezek méretét a lehető legkisebbre kell szorítani
 - Ennek érdekében hierarchikus címzésre van szükség, amely külön azonosítja a hálózatokat és ezen belül külön azonosítja az állomásokat
- A fizikai hálózaton továbbra is az adatkapcsolati címek (MAC) címek alapján lehet elérni az állomásokat
- A hálózati címek és az adatkapcsolati címek összerendelését meg kell oldani
- A hálózati címzést és az adattovábbítást a hálózati réteg protokolljai és eszközei írják le, ill. végezik el

Hálózati protokoll

- A hálózati protokoll adatalegysége a protokoll-készletnek megfelelő felépítéssel rendelkezik. Fej-résziből és adat-résziből áll.
- A fej-rész tartalmazza a forrásállomás és a céllállomás címét is
- A hálózati réteg protokoll adatalegysége minden adatkapcsolati protokoll adatalegységének adat-részébe beágyazva halad a hálózaton
- Többféle protokoll készlet létezik (pl. TCP/IP, OSI, DECNET, IPX)

A hálózati réteg szolgáltatása és feladatai, példákkal

Hálózati szolgáltatás (Network Service)

- Csomagok eljuttatása forrásból célba, miközben több csomópontron kell keresztül haladniuk
- A szolgáltatásnak függetlennek kell lennie az alhálózat technikájától
- A szállítási réteg elől el kell takarni a jelenlévő alhálózatok számát, típusát és topológiáját
- A szállítási réteg számára hozzáférhető hálózati címeknek egységes címzési rendszert kell alkotniuk (LAN-okon és WAN-okon egyaránt)

A hálózati réteg feladatai

- Hálózati szolgáltatás (Network Service)
- Címzés (Addressing)
- Forgalomirányítás vagy útválasztás (Routing)
- A szolgáltatás minősége (Quality of Service: QoS)
- Maximális csomagméréret
- Forgalomszabályozás és torlódás vezérlés (Flow and congestion control)
- Hibajelzés (Error reporting)

A hálózati réteg – összeköttetés alapú vagy összeköttetés mentes?

- Összeköttetés mentes – datagram-alapú hálózat – pl.: IP
- Összeköttetés alapú – virtuális áramkör-alapú – pl.: MPLS

Kérdés	DG alhálózatokban	VÁ alhálózatokban
Áramkör-felépítés	Nem szükséges	Megkövetelt
Címzés	Minden csomag tartalmazza a teljes forrás- és célcímet	Minden csomag egy rövid VÁ számot tartalmaz
Állapotinformáció	Az alhálózat nem tartalmaz állapotinformációkat	Minden VÁ táblázat helyet követel az alhálózatban
Forgalomirányítás	Minden csomagot függetlenül irányítanak	Az útvonalat akkor választják ki, amikor a VÁ felépül; minden csomag ezt az útvonalat követi
A forgalomirányítók meghibásodásainak hatása	Semmi, eltekintve az összeomlás során elveszett csomagoktól	Minden VÁ megszakad, amely a csödöt mondott forgalomirányítón keresztülhaladt
Szolgálatminőség	Bonyolult	Könnyű, ha elég erőforrást lehet előre lefoglalni minden VÁ számára
Torlódásvédelem	Bonyolult	Könnyű, ha elég erőforrást lehet előre lefoglalni minden VÁ számára

5.4. ábra. A datagram és a virtuális áramkör alapú alhálózatok összehasonlítása

Címzés (Addressing)

- A hálózati rétegben használt címek a teljes hálózaton azonosítania kell a számítógépet
- A MAC címek nem használhatók a teljes hálózat címzésére
- A hálózati címet és a fizikai címet együttesen alkalmazzák
- A közeghosszaféréshez a fizikai címet (pl. Ethernet cím), a teljes hálózati címzésre a hálózati (logikai) címet (pl. IP cím) használják
- A forgalomirányítónak (router) minden interfészének rendelkeznie kell MAC címmel

Forgalomirányítás (Routing)

- Ha az együttműködő gépek ugyanazon a hálózaton vannak, elegendő lenne a MAC címek használata
- Ellenkező esetben a hálózati cím azonosítja a partner számítógépet egy másik hálózaton
- A hálózati csomagok irányításáról (routing) gondoskodni kell
- A hálózati cím önmagában nem elegendő a csomag irányítására
- A továbbítandó csomagot a célállomás hálózati címével együtt el kell küldeni az ugyanazon a hálózaton lévő forgalomirányító MAC címére
- A forgalomirányítónak pedig vagy a célállomás MAC címére, vagy egy másik forgalomirányító MAC címére kell továbbítania a kézbesítendő csomagot
- Az alábbi példában az 1. hálózat 1. gépe küld csomagot a 4. hálózat 2. gépének

Az útválasztás lehetőségei

- Legrövidebb útvonal alapján történő útválasztás
- Elárasztás
- Távolságvektor-alapú útválasztás
- Kapcsolatállapot-alapú útválasztás
- Hierarchikus útválasztás
- Adatszóró útválasztás
- Többesküldéses útválasztás
- Bárkinek küldéses útválasztás (anycast routing)
- Útválasztás mozgó hosztokhoz
- Útválasztás ad hoc hálózatokban

Maximális csomagméret

- A maximális csomagmáretet az egyes hálózat típusokban különböző
- A maximális csomagmáretet az alábbi tényezők befolyásolják
 - hibaarány
 - átviteli késleltetés
 - puffer méret igény
 - többletterhelés (overhead = a hasznos adatot kísérő egyéb információ mennyisége: címek, CRC, stb.)
- A szállítási réteg szükség szerint tördeli (fragmentálja) az átvienő adatokat a hálózati réteg számára továbbításra
- A hálózati réteg a különböző alhálózatokon történő továbbítás során tovább tördeli, majd a vétel helyén újra összeállítja a csomagokat

Forgalomszabályozás és torlódásvezérlés (Flow and congestion control)

- Flow control mechanizmus szabályozza a különböző sebességű és terheltségű végállomások közötti adatforgalmat
- A congestion control az adatok hálózaton belüli torlódásának feloldását jelenti

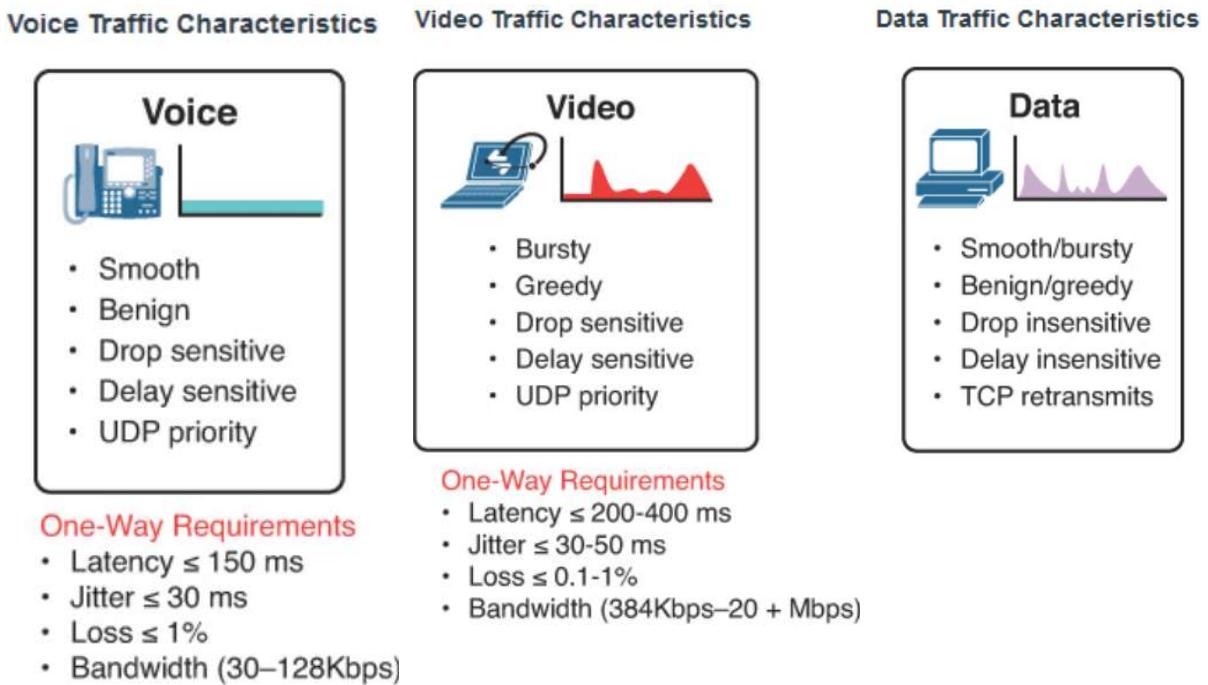
Hibajelzés (Error reporting)

- A hibák jelzésének módja hálózatonként eltérő
- Több összekapcsolt és eltérő típusú hálózat esetén a megfelelő hibajelzésről gondoskodni kell

A szolgáltatás minősége (Quality of Service: QoS)

- QoS: Paraméterek összessége, amelyek leírják a szolgáltatás teljesítményét egy adott forgalmi osztályra, jóságát, amelyet a hálózatot használó elvár a szolgáltatótól
- Ezek:
 - átviteli sebesség (sávszélesség)
 - Csomagkésleltetés - delay
 - A csomagkésleltetés ingadozása – jitter
 - a továbbítás költsége
 - az átviteli hiba valószínűsége, megbízhatósága – csomagvesztés
 - a relatív prioritás
- Ehhez két modellt is definiáltak, amelyeken keresztül megvalósítható egy minőségi, forgalmi osztálytól és prioritástól függő szolgáltatás:
 - Integrated services
 - Differentiated Services

Hálózati forgalom



8. HÁLÓZATI RENDSZEREK CÍMZÉSI MEGOLDÁSAI

Az OSI rendszer rétegeiben hol és miért van szükség címekre, mi a jellemző ezekre

Miért van szükség logikai és fizikai címekre mi indokolja ezeket a megnevezéseket

A 2. rétegbeli címzés alapvető rendeltetése, elvárások, megvalósítás, működés

A 3. rétegbeli címek alapvető rendeltetése, elvárások, megvalósítás, működés

A 4. rétegbeli címek alapvető rendeltetése, elvárások, megvalósítás, működés

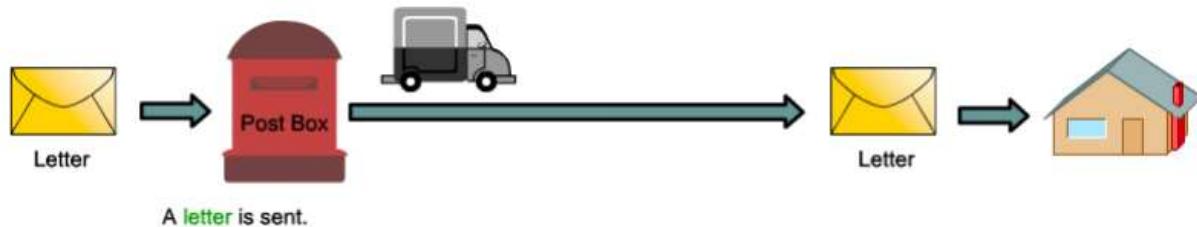
A 2. és a 3. rétegbeli címek közötti kapcsolat, a kapcsolat szükségessége, megvalósítása

9. AZ IPV4 CÍMTÉR KEZELÉSE

Az IP protokoll jellemzői

- **Kapcsolat nélküli/Összeköttetés-mentes** – nem épít ki kapcsolatot az adatcsomagok küldése előtt, a csomagok egymástól függetlenül lesznek továbbítva, ezért akár különböző útvonalon is haladhatnak
- **Megbízhatatlan** - a csomagok elveszhetnek, kettőződhetnek, készhetnek, helytelen sorrendben érkezhetnek
 - nincs mód a hiba kijavításra, ezt a feladatot a magasabb rétegekben lévő protokollok oldhatják meg: TCP, alkalmazás
- **Legjobb szándékú (best effort)** – A hálózat a legjobb tudása szerint kézbesíti a csomagokat a forrástól a célig, azonban a kézbesítés nem szavatolt
- **Médiafüggetlen** – Az átviteli közegektől függetlenül továbbítja az adatot

Kapcsolat nélküli kommunikáció jellemzői



- A küldőnek nincs tudomása:
 - a fogadó fél jelenlétééről
 - a csomag megérkezéséről
 - Arról, hogy a fogadó el tudja-e olvasni a csomagot
- A küldő fél nem tudja mikor érkezett a csomag

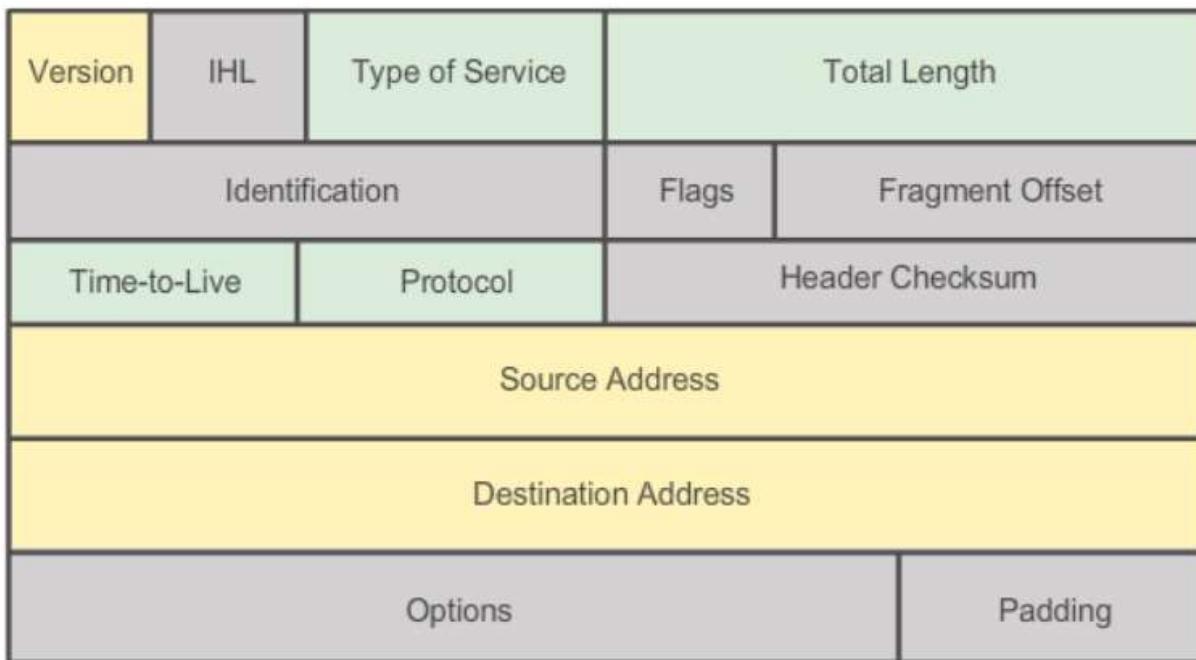
Megbízhatatlan

Az IP egy megbízhatatlan protokoll abban az értelemben, hogy a forgalomirányító a csomag továbbítása után nem biztosítja és nem is foglalkozik a csomag kézhezvételével (ezt a felsőbb rétegbeli protokollok fogják garantálni)

Médiafüggetlenség

Az IP csomag különböző átviteli közegeken és technológiákon haladhat keresztül (Ethernet, PPP, Frame Relay)

IPv4 csomag fejrésze



Az IP csomag formátuma – mezők

VERS = 4	- az IP verziója (minden IP szoftver ellenőrzi)
HLEN	<ul style="list-style-type: none"> - a fejléc (header) hossza 32 bit-es egységekben - az IP opciók miatt a fejléc változó hosszúságú lehet - az opciók nélküli fejléc 20 byte-os
SERVICE TYPE	- a szolgáltatás minőségének magadására használják (QoS)
TOTAL LENGTH	<ul style="list-style-type: none"> - a teljes csomag hossza byte-okban - a maximális hossz: 65,535 byte
IDENTIFICATION	<ul style="list-style-type: none"> - IP csomag tördelésekor használt mezők
FLAGS	
FRAGMENT OFFSET	
TIME TO LIVE	- a csomag élettartama
PROTOCOL	- a DATA mező protokoll típusa (pl. TCP)
HEADER CHECKSUM	- fejléc ellenőrző összeg
SOURCE IP ADDR.	- a forrás IP-címe
DEST. IP ADDR.	- a cél IP-címe

A hálózati protokoll-adategység keretbe foglalása – beágyazás

- Az IP csomagok a fizikai hálózaton keretbe ágyazva továbbíthatók
- A keret típusa a hálózat típusától függ: Ethernet, HDLC, PPP, Frame Relay, stb.
- Az IP csomag hossza max. 65,535 bájt, a fizikai keret hossza jóval rövidebb. Célszerű az IP csomagot olyan hosszúra választani, hogy az elférjen egy fizikai keretben
- Ha ez nem lehetséges, az IP tovább tördeli a csomagokat

Az IPv4 protokoll

IPv4 címek

- Az IP-cím egy logikai hálózati cím, ami azonosítja az állomást minden eszköznek, amelyet hálózatban használnak rendelkeznie kell IP címmel
 - pl. munkaállomások, kiszolgálók, hálózati nyomtatók és IP-telefonok
- 32 bites bináris szám, 4x8 bitenként csoportosítva → 4 oktet
- 8 bitenként ponttal elválasztva decimálisan ábrázoljuk → pontozott decimális forma
- Egy oktet decimális értéke 0-255 között mozoghat
- A forgalomirányítók IP-t használnak a továbbításra
- A csomagnak tartalmaznia kell a forrás és a célhálózat IP címét

Alhálózati maszk

- Az IP címhez hasonló 32 bites bináris szám, amit pontozott decimális formában ábrázolunk
- Az IP címtől abban különbözik, hogy bináris formában 0 után nem állhat 1
- Az alhálózati maszk jelöli ki, hogy az IP cím melyik része a hálózatcím és melyik az állomáscím

Egyedi, üzenetszórásos és csoportos címzés

Az állomások az IPv4 címeket használhatják

- egy-az-egyhez (egyedi) – unicast
- egy-a-többhöz (csoportos címzés) – multicast
- egy mindenkihez (üzenetszórásos) – broadcast – típusú

kommunikációra.

Egyedi címzés

Egy egyedi célcímmel ellátott csomag egy megadott állomásnak szól

A leggyakoribb típusú kommunikáció egy IP hálózaton

Limited Broadcast

Egy csomag küldése egy állomástól a hálózat minden állomásának Az IP cím minden bitje 1

Figyelem: A forgalomirányítók nem továbbítják a limited broadcast-ot

Directed broadcast

A csomag olyan cél IP címet tartalmaz, aminél csupa 1-es áll az állomásazonosítónál.

Ez azt jelenti, hogy a helyi hálózat összes állomása (szórási tartomány) megkapja és megvizsgálja a csomagot.

A hálózat üzenetszórási IP címének van egy megfelelő MAC szórási címe is az Ethernet keretben. Az Ethernet hálózatokon a MAC szórási cím 48 darab egyes, hexadecimálisan megjelenítve FF-FF-FF-FF-FF-FF.

Csoportos címzés

A csoportos címek lehetővé teszik a forrásesköz számára, hogy eszközök egy olyan csoportjának küldjön csomagot, amelyek többes címzésű csoporthoz tartoznak, csoportos IP címe van

A csoportos címek tartománya 224.0.0.0-tól 239.255.255.255-ig terjed

Például: távoli játékokat, távoktatás és videokonferencia

csoportos MAC cím: egy speciális érték, ami hexadecimális 01-00-5E-vel kezdődik. A vége pedig a csoportos IP cím alsó 23 bitjének átalakításával áll elő (01-00-5E-0F64-C5)

Az osztály alapú IPv4 címzés, cím-osztályok, az osztály nélküli címzés

Privát és nyilvános címek

- Azok az állomások amelyek nem akarnak az Interneten kommunikálni használhatnak privát címeket:
 - 10.0.0.0 to 10.255.255.255 (10.0.0.0/8)
 - 172.16.0.0 to 172.31.255.255 (172.16.0.0/12)
 - 192.168.0.0 to 192.168.255.255 (192.168.0.0/16)
- Az interneten használható – a forgalomirányítók által továbbított – címeket nyilvános címeknek nevezzük

Speciális címek

- Hálózati és Broadcast címek – minden hálózatban az első és az utolsó cím nem kiosztható
- Loopback cím – 127.0.0.1 speciális cím az állomás saját magának megcímzésére (127.0.0.0 - 127.255.255.255 foglaltak)
- Link-Local cím – 169.254.0.0 - 169.254.255.255 (169.254.0.0/16) automatikus konfiguráció
- TEST-NET cím – 192.0.2.0 - 192.0.2.255 (192.0.2.0/24) oktatási cérla fenntartott
- Experimental addresses – 240.0.0.0 - 255.255.255.254 foglaltak

10. AZ IPV6 CÍMTÉR KEZELÉSE

Miért van szükség nagyobb címtartományra?

- Az internetet használók számának növekedése
- Mobile felhasználók
- Mobile telefonálás
- Közlekedés (autók)
- Fogyasztói készülékek

IPv6 célok

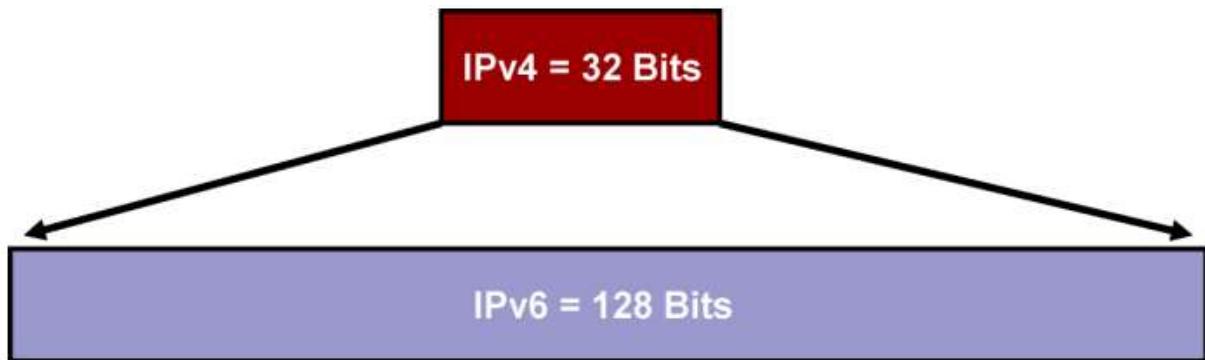
- Támogatni a több milliárd hosztot
- Csökkenteni az irányító táblák méretét → gyorsabb továbbítás
- Egyszerűsíteni a protokollt → gyorsabb feldolgozás
- Nagyobb biztonság → IPSec
- Differenciált szolgáltatás a különböző típusú forgalmak esetén → QoS

Új IPv6 funkciók

- Cím hozzárendelés szolgáltatás
 - DHCP használata, és állapot nélküli autó-konfiguráció (Stateless autoconfiguration)
- Mobilitás támogatása eleve beépített
 - IPv6 állomások mozgathatók a hálózatok között, megtarthatják IPv6 címüket anélkül, hogy elvesztenék a kapcsolatukat az alkalmazásokkal
- Cím-összevonás megkönnyítése
 - A nagy IPv6 címtartomány megkönnyíti az IP-cím blokkok összevonását az interneten, amely hatékonyabbá teszi a forgalomirányítást
- NAT/PAT használata szükségtelen
 - A nagy IPv6 címtartomány szükségtelenné teszi a NAT/PAT használatát: ezzel elkerüli bizonyos protokollok és alkalmazások működési problémáit, és hatékonyabb lesz a forgalomirányítás
- Nincs broadcast
 - Az IPv6 nem használ 3. rétegű szórást, helyette többes-címzést (multicast) használ
- Az IPv4-ről IPv6-ra való áttérést segítő eszközök
 - Több módszer és eszköz segíti az áttérést, amely a két protokoll együttelését is magában foglalja

Nagyobb címtartomány

- IPv4
 - 32 bit vagy 4 byte hosszú cím
 - 4,200,000,000 lehetséges csomópont
- IPv6
 - 128 bit vagy 16 byte: 4-szer annyi bit mint az IPv4-ben
 - $3.4 * 10^{38}$ lehetséges csomópont
($340,282,366,920,938,463,374,607,432,768,211,456$)
 - $5 * 10^{28}$ cím személyenként (50,000,000,000,000,000,000,000,000)



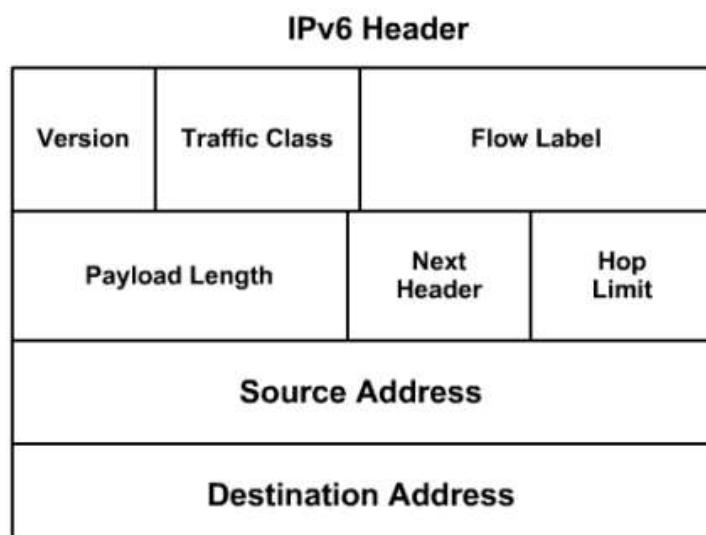
A nagyobb címtartomány megkönnyíti a cím összevonását

- Prefix-ek összevonása (aggregation) és ezek hirdetése a globális hálózaton
- Hatékonyabb és jobban méretezhető forgalomirányítás

Az IPv6 fejléc

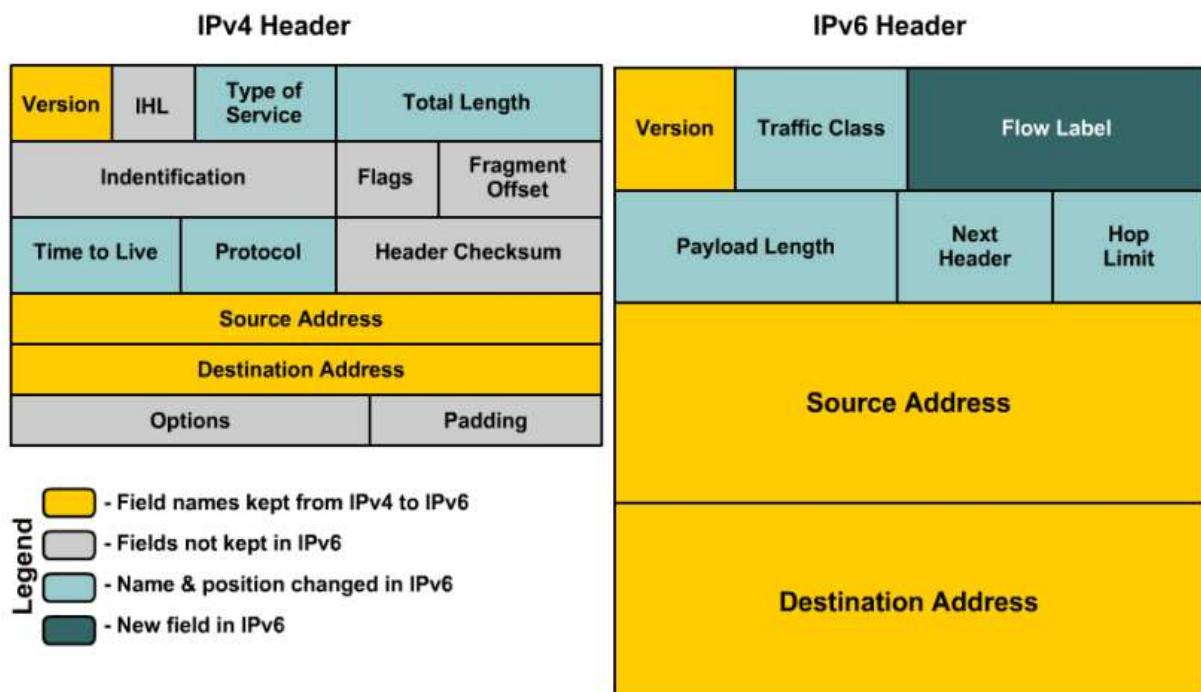
Egyszerűbb és hatékonyabb protokoll fejléc

- 64-bitre illesztett, és kevesebb mezőt tartalmazó fejléc
- Hardveres feldolgozást segítő kialakítás
- A hatékonyabb forgalomirányítást segítő kialakítás
- Gyorsabb csomagtovábbítás lehetősége és jobb méretezhetőség



- Az IPv6 forgalomirányítók (router) nem végeznek csomag tördelést
- Egy felderítési folyamat határozza meg az optimális maximum transmission unitot (MTU) egy adott kapcsolatra
- A forrás IPv6 eszköz a felső protokoll réteg által javasolt csomag mérettel indít. Ha „ICMP packet too big” üzenet érkezik, csökkenti a méretet. Ezt addig folytatja, amíg át nem jut a csomag
- A forgalomirányítók 5 percentként megismétlik a felderítési folyamatot, hogy a leghatékonyabb csomagméréset alkalmazzák minden kapcsolatra
- A forgalomirányítók nyilvántartást vezetnek a helyes csomagmérőről a cél IPcím alapján (cache)
- Elhagyták az IPv4 fejléc ellenőrző összeget, mivel az adatkapcsolati réteg megbízható
- A korábban opcionális felsőbb rétegbeli ellenőrző összeg használata kötelező lett (pl. UDP)

Az IPv4 és IPv6 fejlécek összehasonlítása

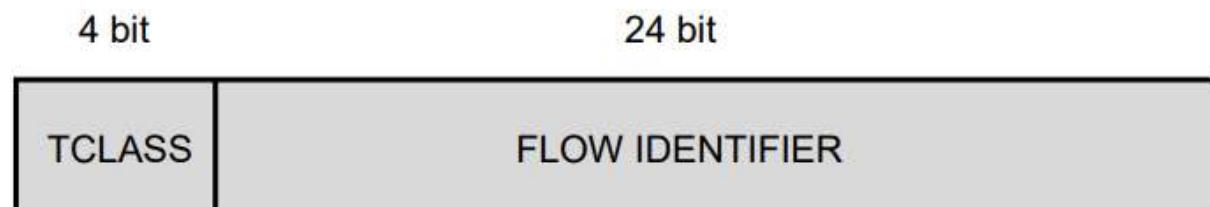


Az IPv6 fejléc mezők

- Version:
4-bit-es mező. Szerepe ugyanaz mint az IPv4-ben. Értéke:6
- Traffic Class:
8-bit-es mező. Szerepe hasonló az IPv4 TOS mezőjéhez. A csomag forgalmi osztályát jelöli, amelyet a Differentiated Services (DiffServ) hasznosít (QoS)
- Flow Label:
20-bitess mező. Egy adatfolyamot jelöl. Többrétegű kapcsolás alkalmazásakor megnöveli a csomagtovábbítás teljesítményét
- Payload Length:
A hasznos adattartalom hossza bájtban
- Next Header:
Meghatározza az IPv6 fejlécet követő fejléc típusát. Pl. TCP, UDP, vagy kiegészítő fejléc (extension header)
- Hop Limit:
Ugrások (Hop) maximális száma. (Az IPv4 TTL megfelelője)
- Source Address / Forrás cím: 128 bit
- Destination Address / Cél cím: 128 bit
- Extension Headers
 - Kiegészítő fejlécek
 - A fejlécek száma nincs meghatározva
 - Egyfajta láncot alkotnak
 - minden fejléc tartalmaz egy NEXT HEADER mezőt, amely a következő fejléc - az utolsóban a protokoll - típusát határozza meg
 - A forgalomirányítók és a célállomás a fejléceket sorban (szekvenciálisan) dolgozzák fel

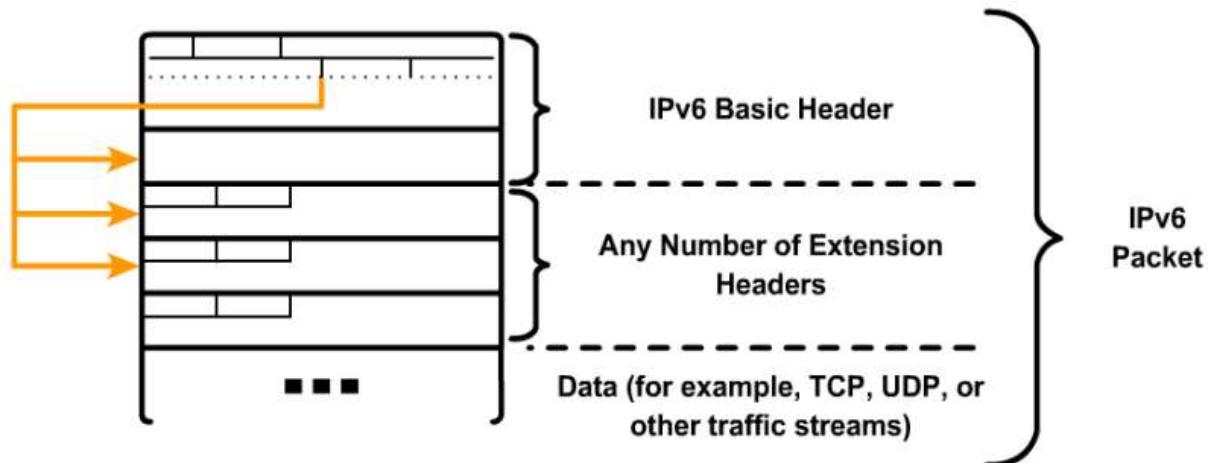
A FLOW LABEL szerkezete

- TCLASS: a csomag forgalmi osztálya
 - 0 - 7 = folyamhoz tartozó csomag időérzékenysége
 - 8 - 15 = nem-folyamhoz tartozó csomag
- FLOW IDENTIFIER: a folyam létesítésekor lefoglalt azonosító
- Az IPv6 csomag bázis fejléce 40 byte



IPv6 kiegészítő fejlécek (Extension Headers)

- IPv6 header
A korábban bemutatott fix méretű, minden csomagban jelenlévő fejléc
- Hop-by-hop options header (érték: 0)
Resource Reservation Protocol [RSVP] és Multicast Listener Discovery version 1 [MLDv1] célra használják
Minden forgalomirányító feldolgozza



- Destination options header (when the routing header is used) (érték: 60)
Ez a mező követheti a hop-by-hop options headert. Ekkor a végállomás és a forgalomirányítók is feldolgozzák. Követheti az ESP headert. Ekkor csak a végállomás dolgozza fel. Használata pl. mobile IP
- Routing header (érték: 43)
Forrás alapú forgalomirányításra és mobil IPv6-ra használják
- Fragment header
Akkor használják, ha a forrás eszköznek tördeleznie kell a csomagot, mert az nagyobb mint önmaga és a célcélállomás közötti MTU
A fejlécet az összes tördelt csomag tartalmazza
- Authentication header and Encapsulating Security Payload header (érték: 50)
Az IPsec adatait tartalmazza. Authentication header (érték = 51), ESP header (érték = 50)
- Upper-layer header (érték: TCP=6, UDP=17)
Általában a csomag szállítási protokolljára utal

IPv6 cím reprezentáció

- 128-bit IPv6 megjelenítésekor/leírásakor nyolc 16-bites szegmensre bontjuk
- minden szegmensét hexadecimálisan ábrázoljuk: 0x0000 - 0xFFFF, és kettősponttal választjuk el őket
- Példa: 3ffe:1944:0100:000a:0000:00bc:2500:0d0b

Az IPv6 címek méretének csökkentése

- Vezető nullák elhagyása
- 0000...0000 = ::
Egy vagy több folytonos, 0 értékű 16 bites lánc helyettesítése dupla kettőspontokkal (0000...0000 = ::)
- Bármelyik 16-bites szegmens vezető nullát nem kell kiírni
- Ha bármelyik 16-bites szegmens 4-nél kevesebb hexadecimális számjegyet tartalmaz, a hiányzó számjegyek nullák

Hálózati prefix

- Prefix – az IP cím hálózati részét adja meg
- Az IPv4-ben a prefix – a cím hálózati része – leírható ponttal elválasztott decimális számokkal (dotted decimal) és bit darabszámmal (bit count) is 255.255.255.0 vagy /24
- Az IPv6 prefix csak a bit darabszámmal azonosítható
- Az IPv6-ban a bit darabszám (/nn) azt jelzi, hogy a cím első hány bitje azonosítja a cím hálózati részét (prefix)
- CIDR vagy prefix jelölés: 3ffe:1944:100:a::/64

Összes bit 0 – cím

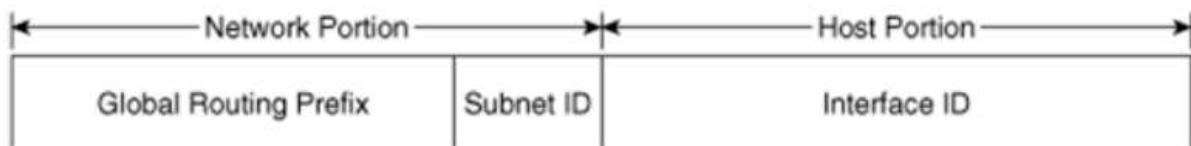
- Egy csupa 0 bitet tartalmazó IPv6 cím dupla kettősponttal leírható ::
- Két esetben használható ilyen cím:
 - Alapértelmezett cím (default address): ::/0
 - Nem meghatározott cím (Unspecified address)
 - Valós IPv6 cím hiányát jelzi
 - Az alapértelmezett címtől a prefix hosszában tér el ::/128
 - Neighbor Discovery Protocol eljárásban használható

IPv6 címzés típusok

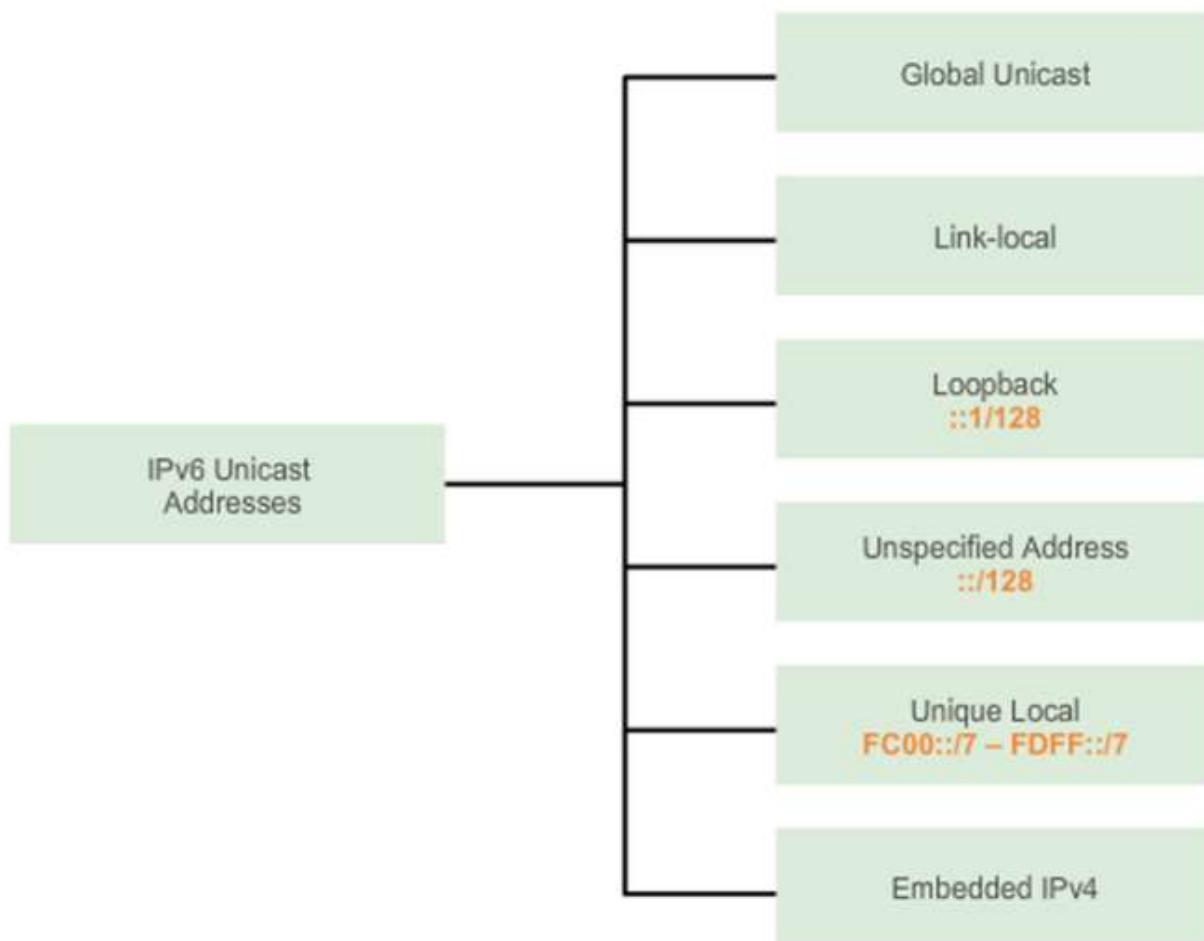
1. Unicast
 - Global Unicast (2000::/3)
 - Link Local Unicast (FE80::/10)
 - Unique Local Unicast (FEC0)
2. Multicast (FF00::/8)
3. Anycast

- Az IPv6-ban nincs broadcast címzés
- Helyette az „all nodes” multicast címzést használják
- Egy interfész bármelyik típusból több címmel is rendelkezhet
- Loopback cím: ::1/128

Az IPv6 unicast cím általános szerkeze



UNICAST címek fajtái:



UNICAST

Link-local unicast cím: Hatóköre egyetlen kapcsolatra terjed ki, a forgalomirányítók nem továbbítják

- FE80::/10 tartomány jelöli,
- az első 10 bit 1111 1110 10xx xxxx
- 1111 1110 1000 0000 (FE80) - 1111 1110 1011 1111 (FEBF)

Global unicast cím: Globálisan egyedi az interneten, ezért a forgalomirányítók gond nélkül továbbítják

- A nyilvános IPv4 címek megfelelője
- Statikusan vagy dinamikusan konfigurálható

Minden interfésznek rendelkeznie kell legalább egy link-local unicast címmel

Unique local cím: Hatóköre egyetlen alhálózatra terjed ki, a privát IPv4 címekhez hasonló

- A forgalomirányítók nem továbbítják
- Az FC00::/7 - FDFF::/7 címtartomány jelöli

Loopback cím: ::1/128

Unspecified cím: „Csupa 0” cím, ::/128 vagy egyszerűen ::

- Nem rendelhető interfészhez, forráscímként használt, ha a forrásnak nincs állandó IPv6 címe vagy nem releváns

Multicast

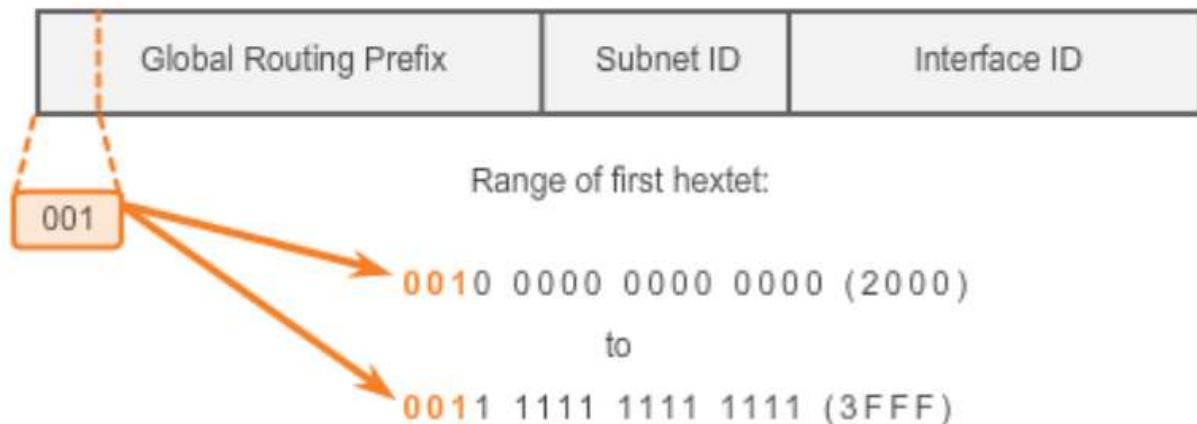
- Az IPv6 nem használ broadcast-ot
- Az IPv4-ben a broadcast gyakran ún. „broadcast vihart” okozott
- A broadcast-ot az IPv6-ban multicast címzéssel helyettesítik
- Csak funkcionálisan specifikus multicast csoportoknak küldenek üzenetet, amely hatékonyabbá teszi a hálózatot
- Az IPv6 multicast címtartománya nagyobb az IPv4-esénél
- Multicast prefix: FF00::/8

Anycast

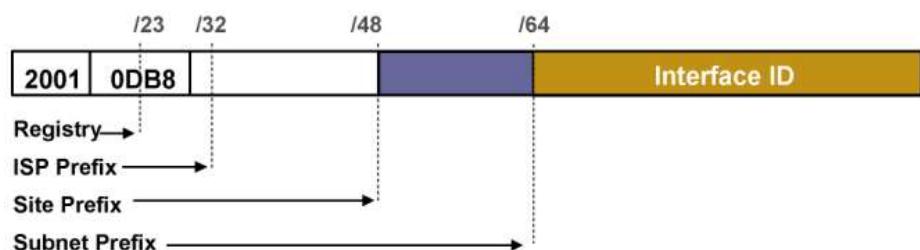
- Több eszközt vagy interfészt azonosít
- Több anycast node ugyanazt a szolgáltatást nyújtja
- Használata: terhelés megszűtés, tartalom szolgáltatás
- Egy anycast címre küldött csomag a forgalomirányító tábla szerinti legközelebbi interfészre lesz továbbítva
- Az anycast címeket a global unicast címtartományból allokálják, ezért szintaktikusan nem is különböztethetők meg tőlük

IPv6 Global Unicast (és Anycast) címek

- A global unicast és az anycast ugyanazt a formátumot használja
- Globális routing prefixet használ, amely lehetővé teszi a címösszevonást (aggregation)
- Egy interfész több címmel is rendelkezhet (unicast, anycast, multicast)
- minden interfésznek legalább egy link-local és egy loopback (::1/128) interfésszel kell rendelkeznie
- minden interfész több unique és global címmel is rendelkezhet
- Az anycast cím egy global unicast címtartományból származó cím, amelyet több interfészhez (akár különböző eszközön) is hozzárendelnek
- Példa az anycast cím használatára:
 - Egy LAN több forgalomirányítóhoz is csatlakozik
 - A forgalomirányítók ugyanazt az IPv6 anycast címet kapják
 - A távoli eszközök csak egyetlen anycast címet kell azonosítniuk
 - A közbenső eszközök a legrövidebb (legkisebb költségű) útvonalat fogják választani az alhálózat elérésére



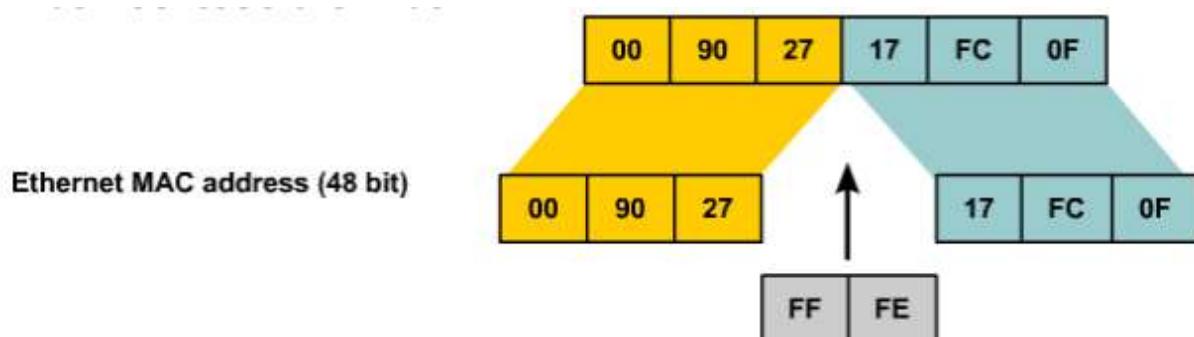
- Az IPv6 global unicast címek megfelelnek az IPv4 global unicast címeknek
- A global unicast cím egy IPv6 cím a global unicast prefix által meghatározott hálózatból
- A global unicast cím struktúrája lehetővé teszi a routing prefixek összevonását, amely a forgalomirányító táblák méretének csökkenésével jár
- A címösszevonás vállalati és szolgáltatói szintre is kiterjedhet
- A global unicast és anycast címeket egy global prefix, egy alhálózat azonosító és egy interfész azonosító írja le (lásd az árat)
- Egy global unicast cím általában egy 48-bites global routing prefix-ből és egy 16-bites subnet ID-ből áll
- A 16-bites subnet ID segítségével a szervezetek kialakíthatják a saját hálózati hierarchiájukat



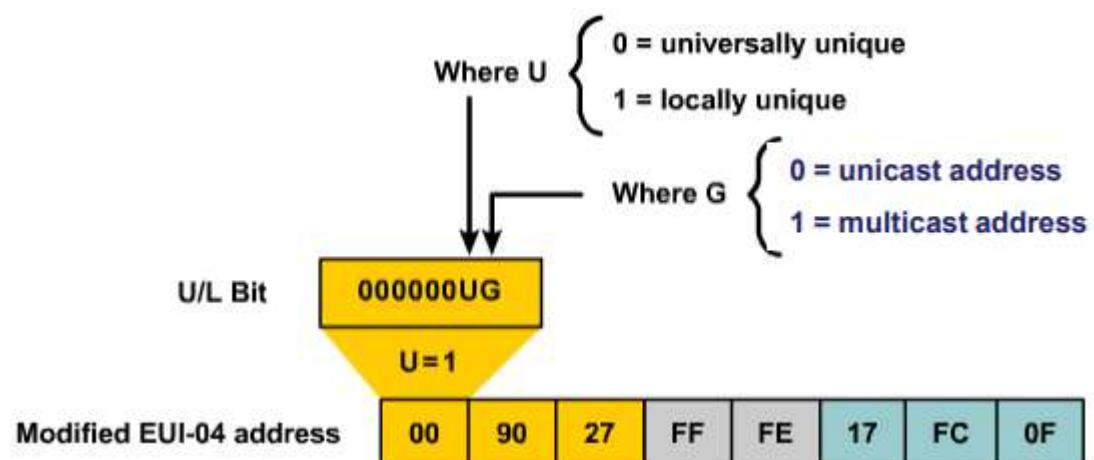
Dinamikus IPv6 címzés – Állomás ID meghatározása

- Alhálózat (subnet) prefix: az a hálózat, amelyre az interfész csatlakozik
- Az alhálózat prefix mindig 64-bit hosszúságú
- A helyi cím (local ID): az állomás interfészét azonosítja az alhálózaton
- A helyi cím mindig 64-bit hosszúságú
- Stateless auto configuration használata esetén az interfész cím dinamikusan jön létre az interfész MAC címéből
- Ethernet interfész esetén a helyi cím az EUI-48 MAC (Extended Universal Identifier - EUI) címből lesz kialakítva
- A 48-bites MAC címet kiterjeszti 64 bitesre úgy, hogy a MAC cím közepére az "FFFE" értéket illeszti be
- A cím egyediségét úgy biztosítja, hogy a universal/local (U/L) bit értékét a címben '0'-ra állítja (global scope), vagyis az Ethernet cím első 3 bájtja (Organizational Unique Identifier [OUI] mező) az interneten adminisztrálva van
- Ha az OUI mező nem egyedi (pl. kézi beállítású), az U/L bitet '1'-re kell állítani (local scope)

„FFFE” beillesztése a címbe

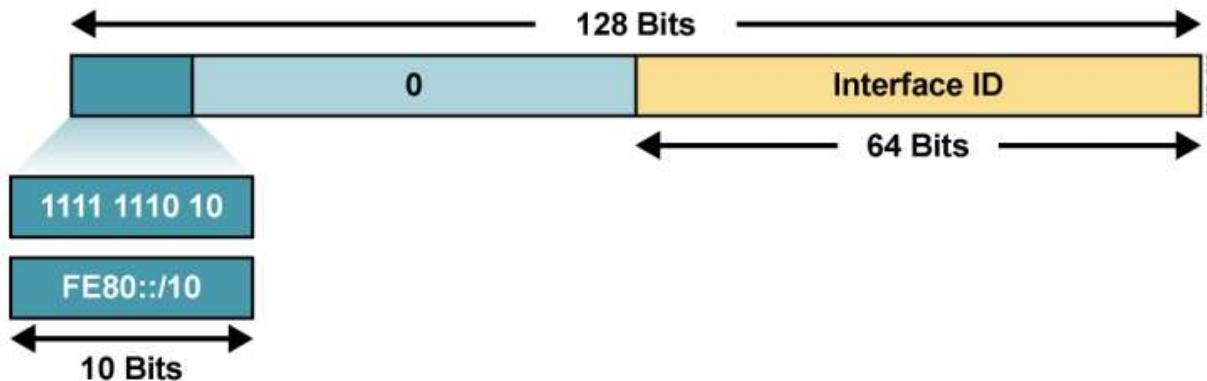


A cím egyediségének biztosítása (U-bit beállítása)



- **Link-local address**

- Két IPv6 eszköz közötti kommunikációban kötelezően használt cím (hasonlít az ARP-hez, de a Layer 3-ban)
- Az IPv6 engedélyezésekor a forgalomirányító rendeli az eszközökhöz
- A következő ugrás (next hop) meghatározásakor a routing protokollok is ezt a címet használják
- Hatókörre az adott kapcsolatra terjed ki
- A hálózati cím többi 54 bitje lehet 0 vagy kézzel beállított bármilyen érték
- Az interfész címet az eszközök a stateless auto configuration módszerrel határozzák meg



- Ha az eszköz az interfész azonosítóját az Ethernet MAC címből képezi, a MAC címét „universally unique”-nak tekinti
- A link-local címet automatikus cím konfiguráláshoz (global unique), szomszéd felfedezéshez (neighbor discovery) és forgalomirányító felfedezéshez (router discovery) használják
- A link-local cím segítségével az eszközök globális cím nélkül kommunikálhatnak egymással
- Ha egy eszköz a link-local címével kommunikál, meg kell adni a kimenő interfészt is, mivel minden interfész az FE80::/10 hálózathoz csatlakozik

IPv6 multicasting

- A multicast-et gyakran használják az IPv6-os hálózatokban, mivel a broadcast helyett is multicast-et használnak
- A multicast cím az interfészek egy csoporthoz azonosítják
- A multicast címre küldött keretek egyidejűleg eljutnak a multicast csoport összes résztvevőjéhez
- Egy interfész tetszőleges számú multicast csoporthoz tartozhat
- A multicast egy sor IPv6 funkció működéséhez szükséges
- Az IPv6 multicast címet a FF00::/8 prefix írja le
- A prefix második octetje a multicast cím élettartamát (flag) és a hatókörét (scope) írja le
- Flag paraméter
 - 0: állandó vagy well-known multicast cím
 - 1: ideiglenes multicast cím

	Meaning	Scope
FF02::1	All nodes 	Link-local
FF02::2	All routers 	Link-local
FF02::9	All RIP routers 	Link-local
FF02::1:FFXX:XXXX	Solicited-node 	Link-local
FF05::101	All NTP servers 	Site-local

Prefix	Név	Jelentés	IPv4 megfelelő
::1/128	loopback	loop	127.0.0.1/8
fe80::/10	link-local	local addresses	does not exist
fec0::/10	site-local	cancelled	10.0.0.0/8, 172.16.0.0/12, 192.168.0.0/16
fc00::/7	unique-local	unique private addresses	
ff00::/8	multicast	group calls	224.0.0.0/4
does not exist	broadcast	broadcast	255.255.255.255
2000::/3	global	global addresses	global ipv4 addresses

DHCPv6 protokoll bemutatása

12. téTELben részletezve

ICMPv6 protokoll bemutatása

Az Internet Control Message Protocol (ICMP)

Habár maga az IP nem megbízható protokoll, a TCP/IP protokollcsalád tartalmaz olyan üzeneteket, amelyek bizonyos hibák előfordulása esetén küldhetők. Ezek az üzenetek az ICMP protokoll szolgáltatásaival küldhetők el. A cél nem az, hogy megbízhatóvá tegye az IP protokollt, inkább az IP csomagok feldolgozása során felmerült jelenségekről küldhet visszajelzést. Az ICMP üzenetek nem szükségesek, bizonyos hálózatokon belül biztonsági okokból sokszor nem is engedélyezettek

Az Internet Control Message Protocol (ICMP) jellemzői

- A csomag útja során forgalomirányítók sorozatán halad, míg eléri célállomást
- Ha egy forgalomirányító nem képes továbbítani a csomagot, vagy valamilyen rendellenességet tapasztal (pl. torlódás) értesítenie kell a csomagot feladó számítógépet, hogy orvosolja a problémát
- Az állomások és forgalomirányítók az ICMP protokoll segítségével küldhetnek hiba- és vezérlő információt
- Néhány lehetséges hiba, ami miatt hibajelzésről gondoskodni kell:
 - Vonalak, hardver eszközök meghibásodása
 - Az IP nem tudja eljuttatni a csomagot a célba, mert a célállomás átmenetileg vagy véglegesen ki van kapcsolva, vagy nincs csatlakoztatva a hálózatra
 - A Time-to-Live számláló értéke eléri a 0-át
 - A forgalomirányítókon torlódnak a csomagok
- A hibák jelzését a TCP/IP protokoll család ICMP protokollja segítségével oldják meg
- Az ICMP üzenetek az IP üzenetek adatrészében utaznak
- Az ICMP üzenet célja nem az alkalmazói program vagy felhasználó, hanem a célállomás ICMP modulja
- Az ICMP modul dönti el, hogy mit kezd az üzenettel, melyik szoftver modult értesíti
- Összefoglalva:
 - **Az ICMP lehetővé teszi, hogy állomások vagy forgalomirányítók hiba- vagy vezérlőüzenetet küldjenek más állomásoknak vagy forgalomirányítóknak**
 - **Az ICMP minden két gép IP szoftvere között biztosít kommunikációt**

Hibajelzés vagy hibajavítás

- Az ICMP technikailag egy hibajelző mechanizmus
- Amikor egy üzenet (IP csomag) hibát okoz, az ICMP jelzi a hibát a csomag eredeti feladójának
- A feladó állomásnak kell a hibát összekapcsolnia a megfelelő alkalmazással, vagy megtenni a szükséges intézkedést a hiba kiküszöbölésére
- A hibák egy része az üzenet eredeti feladójától származik, más része nem
- Az ICMP mégis minden hibát az üzenet eredeti feladóját értesíti, a közbenső forgalomirányítókat nem képes értesíteni
- Tegyük fel, hogy az üzenet az R1, R2, ..., Rk forgalomirányítókon halad keresztül

- Ha Rk hibás irányítási információk alapján RE -nek továbbítja a csomagot, RE nem tudja az ICMP-vel értesíteni az Rk forgalomirányítót, hanem csak a csomag eredeti feladóját
- Ennek oka az IP üzenet struktúrájában rejlik
- Az IP fejrészé csak a feladó és a célállomás IP címét tartalmazza
- A forgalomirányítók nem rendelkeznek azon eszközök címével, amelyeken a csomag áthaladt

Az ICMP üzenetkézbesítés – beágyazás

- Az ICMP üzenet egy IP csomagban utazik az interneten
- Ugyanúgy halad forgalomirányítókon keresztül, mint a normális adatot szállító IP csomag
- Az ICMP üzenet továbbítása is lehet sikertelen, azonban egy ICMP üzenetet szállító IP csomag elakadásáról újabb ICMP üzenet nem generálódik

ICMPv6 általános információk

Az ICMPv6 célja megegyezik az IPv4 ICMP céljával, de változtatások szükségesek (pl. „Neighbor Discovery”).

IPv6 fejrész „Next header” érték: 58 (IPv4: 1)

Hibaüzenetek (kód érték 0-127):

- Destination unreachable
- Packet too big
- Time exceeded
- Parameter problem

Információs üzenetek (kód érték 128-255):

- Echo request
- Echo reply
- Neighbour discovery

Neighbor Discovery Protocol

The Neighbor Discovery Protocol (NDP, ND) is a protocol in the Internet protocol suite used with Internet Protocol Version 6 (IPv6). It operates at the Link Layer of the Internet model (RFC 1122), and is responsible for gathering various information required for internet communication, including the configuration of local connections and the domain name servers and gateways used to communicate with more distant systems.

[Router Solicitation](#) (Type 133)

Hosts inquire with Router Solicitation messages to locate routers on an attached link.[3] Routers which forward packets not addressed to them generate Router Advertisements immediately upon receipt of this message rather than at their next scheduled time

Router Advertisement (Type 134)

Routers advertise their presence together with various link and Internet parameters either periodically, or in response to a Router Solicitation message

Neighbor Solicitation (Type 135)

Neighbor solicitations are used by nodes to determine the link layer address of a neighbor, or to verify that a neighbor is still reachable via a cached link layer address.

Neighbor Advertisement (Type 136)

Neighbor advertisements are used by nodes to respond to a Neighbor Solicitation message.

Redirect (Type 137)

Routers may inform hosts of a better first hop router for a destination

- Prefix discovery: hosts can discover address prefixes that are on-link for attached links.
- Parameter discovery: hosts can find link parameters (e.g., MTU).
- Address autoconfiguration: optional stateless configuration of addresses of network interfaces (Stateless address autoconfiguration (SLAAC) and IPv6 address (Stateless address autoconfiguration)).
- Address resolution: mapping between IP addresses and link-layer addresses
- Next-hop determination: hosts can find next-hop routers for a destination
- Neighbor unreachability detection (NUD): determine that a neighbor is no longer reachable on the link
- Duplicate address detection (DAD): nodes can check whether an address is already in use
- Packet redirection to provide a better next-hop route for certain destinations. Router discovery: hosts can locate routers residing on attached links

11. VLSM ÉS CIDR

A VLSM fogalma, rendeltetése, kialakításának okai, miért szükséges a VLSM

Az alhálózatokra bontás lehetősége és technikája VLSM alkalmazása esetén, mintapélda

A címösszevonás fogalma, előnyei, szupernet fogalma, megvalósítási technikája konkrét példán bemutatva

Irányító protokollok és a VLSM kapcsolata

Nemfolytonos IPv4 hálózatok problémái és kezelése

Ezt a fejezetet nem találtam meg moodle-ben.

VLSM: változó hosszúságú alhálózati maszkok:

- célja a kisebb alhálózatok létrehozása (/12, /30, stb.)
- subnetting

CIDR: osztályok nélküli címzés:

- Az A,B,C,D,E osztályok elhagyása.
- célja a routing táblák méreteinek csökkentése.
- VLSM alapú
- supernetting

12. DHCP ÉS DHCPV6 SZOLGÁLTATÁS

Az IPv4-hez hasonlóan az IPv6 globális egyedi címek beállítása történhet manuálisan és dinamikusan egyaránt

Az IPv6 globális egyedi címek dinamikus kiosztására viszont két módszer is létezik:

- SLAAC
- Állapottartó DHCPv6

A SLAAC bemutatása

A SLAAC egy olyan módszer, amellyel egy DHCPv6-szerver szolgáltatásai nélkül szerezhetnek az eszközök IPv6 globális egyedi címet. A SLAAC működése az ICMPv6 protokollen alapul. Az ICMPv6 az ICMPv4-hez hasonló, de annál sokkal robusztusabb protokoll, amely további funkcionalitást kínál. A SLAAC az ICMPv6 protokoll forgalomirányító-keresés és forgalomirányító-hirdetés üzeneteinek segítségével kínál címzési és egyéb konfigurációs adatokat, amelyeket normál esetben egy DHCP-szerver biztosítana.

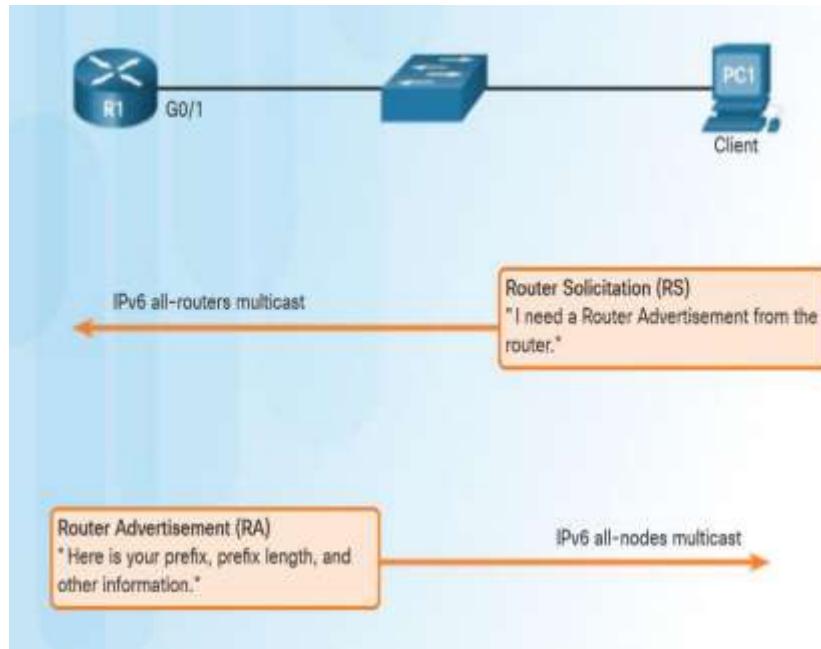
- **Forgalomirányító-keresés (Router Solicitation, RS) üzenet** - Ha egy kliens úgy van beállítva, hogy a címzési adatokat automatikusan a SLAAC-tól kapja, akkor egy RS-üzenetet küld a forgalomirányítónak. Az RS-üzenetet az IPv6 összes forgalomirányítót magába foglaló (all-routers nevű) FF02::2 csoporthoz köthető címre küldik el
- **Forgalomirányító-hirdetés (Router Advertisement, RA) üzenet** Az RA-üzeneteket a forgalomirányítók küldik, hogy címzési információt biztosítsanak azon klienseknek, amelyeket az IPv6-címük automatikus megszerzésére állítottak be. Az RA-üzenet tartalmazza a helyi szegmens előtagját és az előtag hosszát. A kliens ezen információk segítségével hozza létre a saját IPv6 globális egyedi címét. A forgalomirányító rendszeres időközönként, vagy egy RS-üzenetre válaszolva küld ki RA-üzeneteket. Alapértelmezés szerint a Cisco forgalomirányítók 200 másodpercenként küldenek RA-üzenetet. Az RA-üzeneteket minden IPv6 összes állomást tartalmazó (all-nodes nevű) FF02::1 csoporthoz köthető címre küldik.

Stateless Address Autoconfiguration (SLAAC)

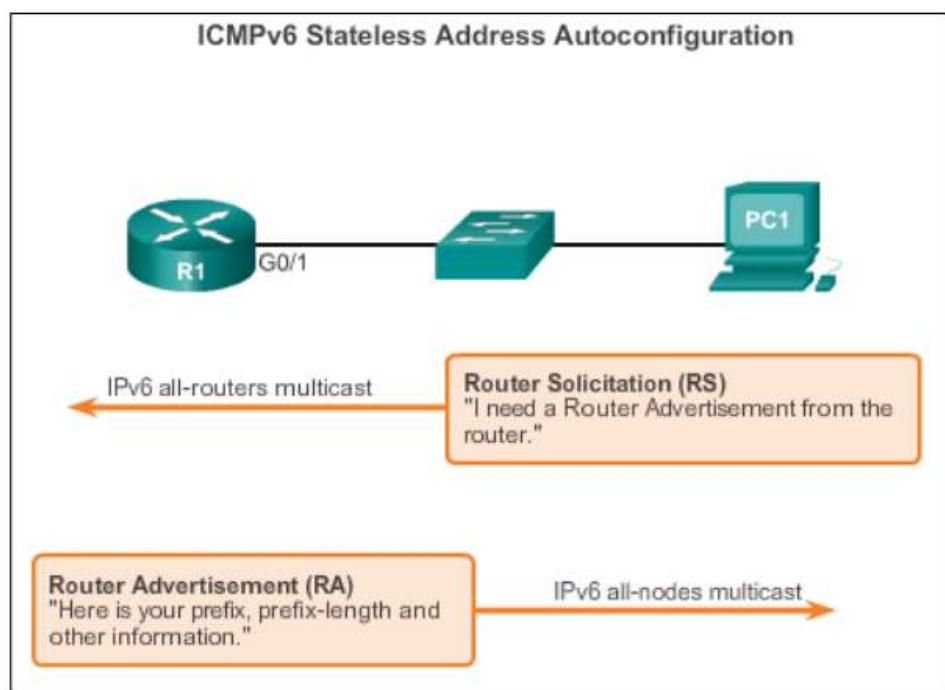
Two methods to dynamically assign IPv6 global unicast addresses:

- Stateless Address Autoconfiguration (SLAAC)
- Dynamic Host Configuration Protocol for IPv6 (Stateful DHCPv6)

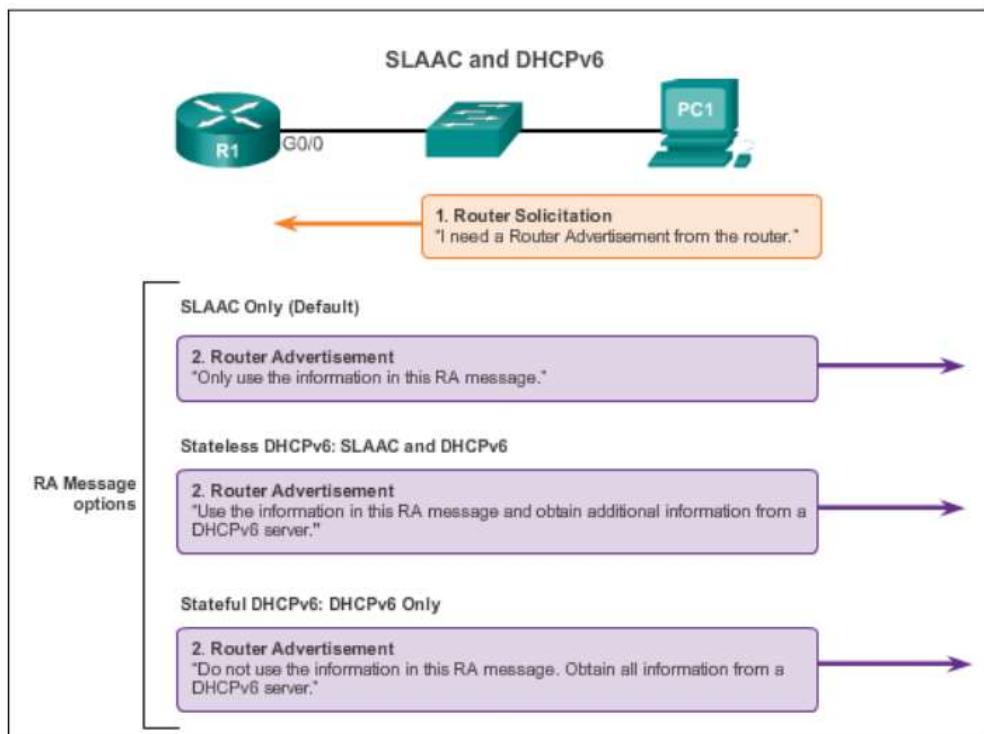
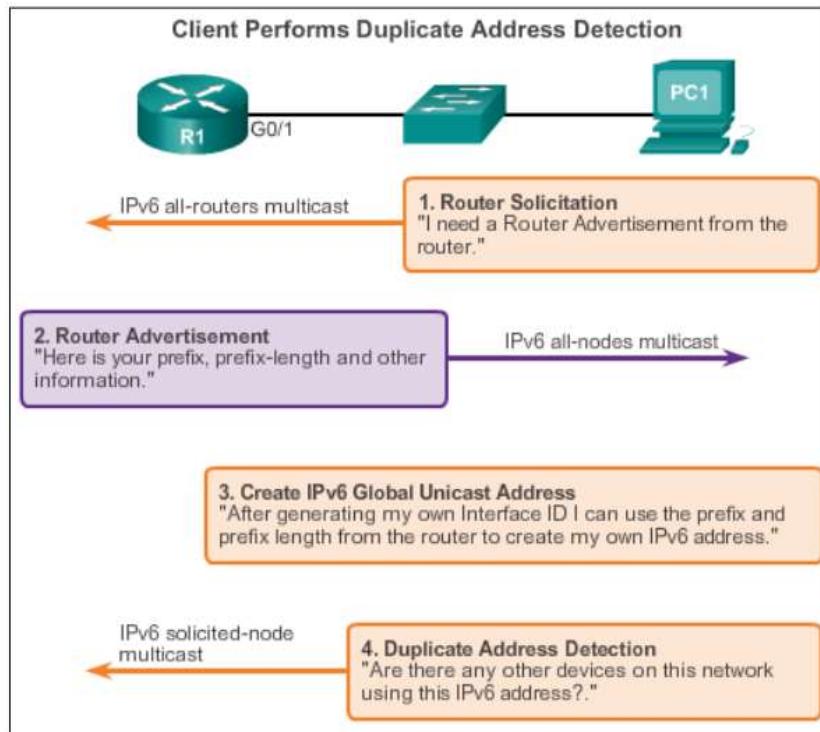
SLAAC uses ICMPv6 Router Solicitation and Router Advertisement messages to provide addressing and other configuration information.



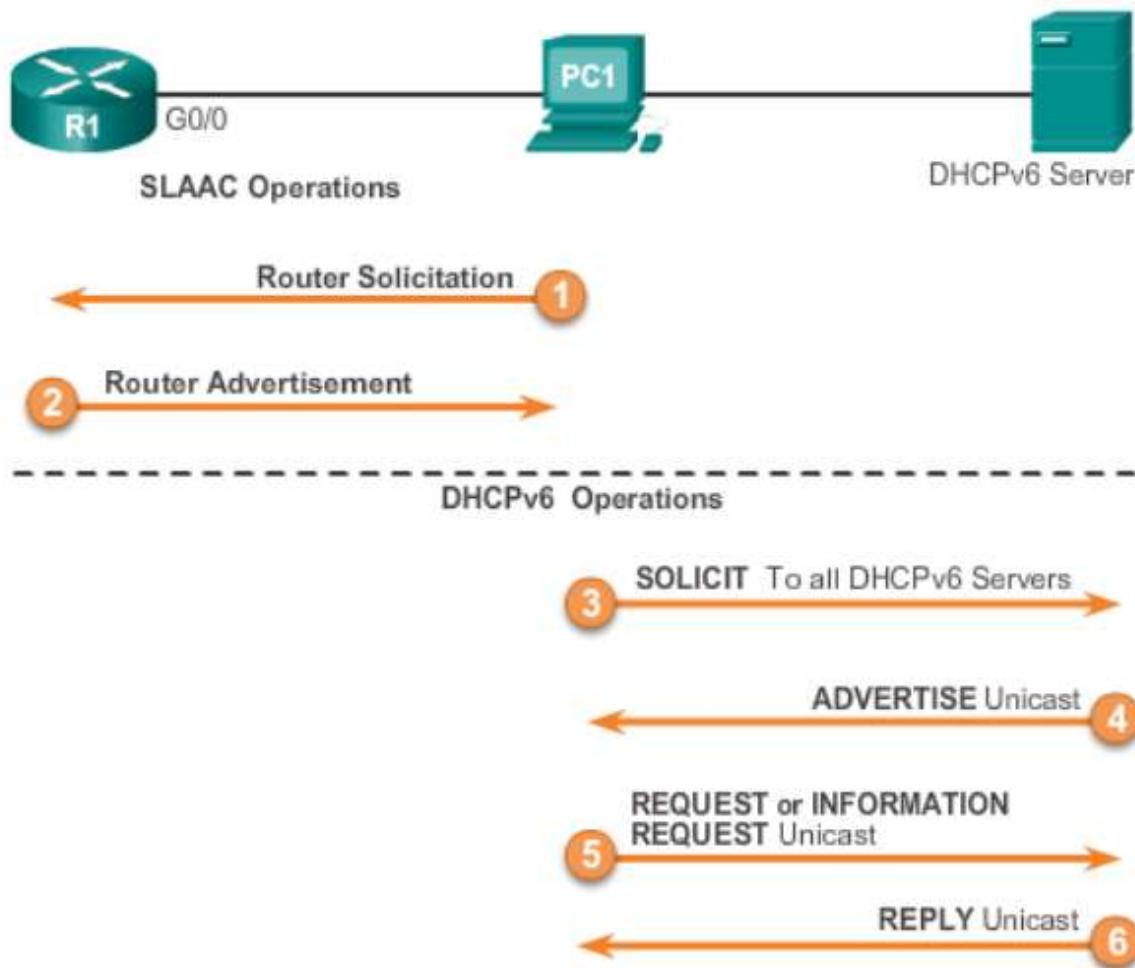
Állapot nélküli automatikus címkiosztás



SLAAC működés



DHCPv6 működése



13-14. SZÁLLÍTÁSI RÉTEG

A szállítási szolgáltatások

- Az OSI protokoll készletben a szállítási réteg a hálózati réteg felett helyezkedik el
- Ez a protokoll a hierarchia központja: az alhálózattól független adatszállítást biztosít a két állomás egy-egy folyamata között → Végponttól végpontig terjedő szolgáltatás
- A szállítási réteg szolgáltatásai a felette levő rétegek:
 - Összeköttetés mentes - Összeköttetés alapú (felépítés, adatszállítás, lebontás)
 - Megbízható – megbízhatatlan átvitel

Szállítási réteg	Összeköttetés alapú: TCP Összeköttetés mentes: UDP
Hálózati réteg	Összeköttetés alapú: MPLS – (2.5 réteg) Összeköttetés mentes: IP
Adatkapcsolati réteg	Összeköttetés alapú: ATM, Frame Relay Összeköttetés mentes: Ethernet
Fizikai réteg	

A szállítási réteg feladatai

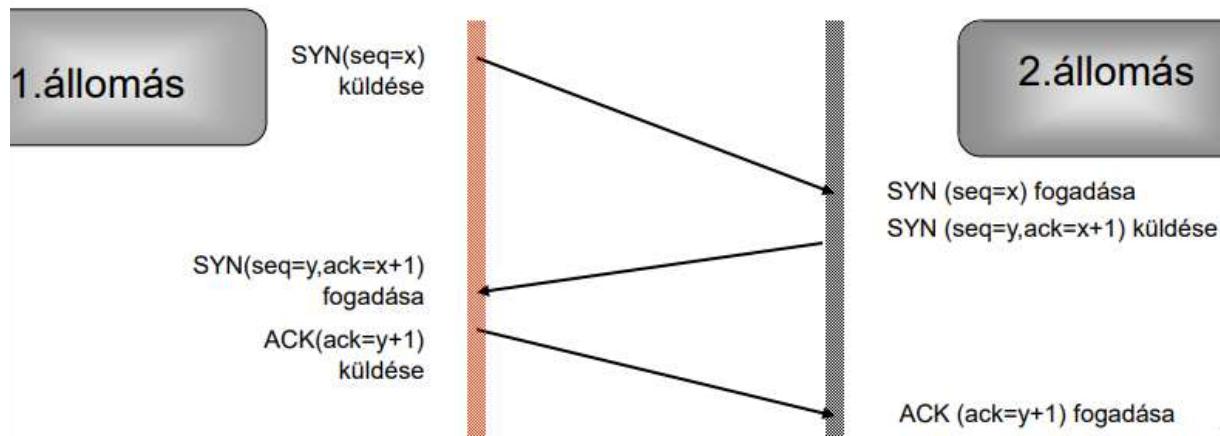
- Címzés – portok (alkalmazásokat címzi!)
 - Összeköttetés létesítése, fenntartása és lebontása
 - Hibakezelés
 - Forgalomszabályozás és torlódáskezelés
 - Multiplexelés (nyalábolás) a különböző alkalmazási folyamatok között
- A szállítási rétegen belül az a hardver/szoftver elem, amely a munkát végzi a szállítási entitás
- A szállítási szolgáltatást a szállítási entitások között a szállítási protokoll valósítja meg.

Összeköttetés létesítése, fenntartása és lebontása

Probléma: nem megbízható hálózati szolgáltatások (kettőzött csomagok, késleltetés)

- Egyedi összeköttetés-azonosító
- Csomagok élettartamának korlátozása
 - Korlátozott hálózat tervezése
 - Ugrásszámláló
 - Időbényeg használata
- Hárrom utas kézfogás
- Lebontás: szimmetrikus és aszimmetrikus
 - Probléma: adatvesztés

Kapcsolat kiépítése – Háromutas kézfogás



- A TCP, ellentétben az UDP-vel kapcsolat orientált, tehát minden két végpontnak egyet kell értenie a részvételben
- Az alkalmazás az egyik végpontron végrehajt egy ún. passzív megnyitást, jelezve, hogy hajlandó bejövő kapcsolatot fogadni
- Ekkor egy TCP port szám lesz hozzárendelve ehhez a végponthoz
- Az alkalmazás a másik végpontron pedig kéri az operációs rendszert, hogy végezzen aktív megnyitást a kapcsolat létrehozására
- A két TCP szoftver felépíti a kapcsolatot, majd kezdődhet az alkalmazások adatcseréje

1. nyugtázs

- Hogyan tud a protokoll szoftver megbízható szállítási szolgáltatást nyújtani megbízhatatlan csomagátviteli szolgáltatással (IP)?
- A megoldás:
 - Pozitív nyugtázs ismételt átvitellel (positive acknowledgement with retransmission, PAR)
 - A vételi oldalon lévő protokoll szoftver nyugtát (acknowledgement=ACK) küld a feladónak, ha adat érkezik
 - A küldő minden átküldött üzenetet nyilvántart, és vár a nyugtára
 - Várományi nyugta : a nyugta az üzenet következő byte-jára mutat

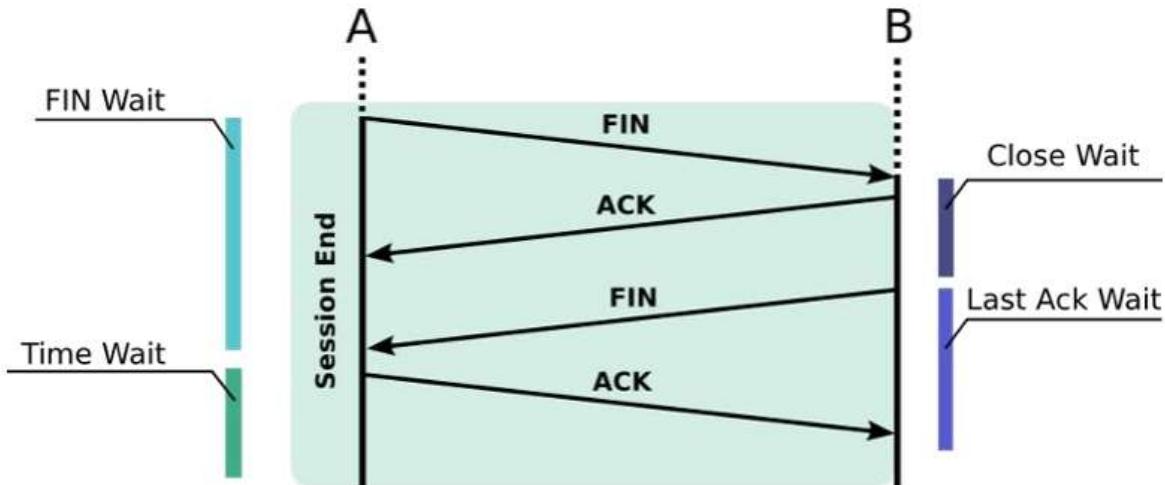
2. újraküldés

- Újraküldés, ha nyugta nem érkezik/csomag elvész

3. sorszámozás

- Ha az átviteli rendszernek nagy a késleltetése, az üzenetek kettőződhettek (adat és a nyugtája egyaránt)
- A protokoll szoftver minden üzenetet egy sorszámmal lát el, és a vevőnek emlékeznie kell, hogy mely sorszámú üzenetek érkeztek meg
- A nyugtában a protokoll szoftver visszaküldi a sorszámot a küldőnek, így az a nyugtákat és az elküldött üzeneteket egymáshoz tudja rendelni

Kapcsolat lebontása



Megbízhatóság – Hibakezelés

- Hibajelzőkód (ellenőrzőösszeg vagy CRC)
- Nyugtázás
- Sorszámozás
- Kint lévő szegmensek számának korlátozása

Forgalomszabályozás

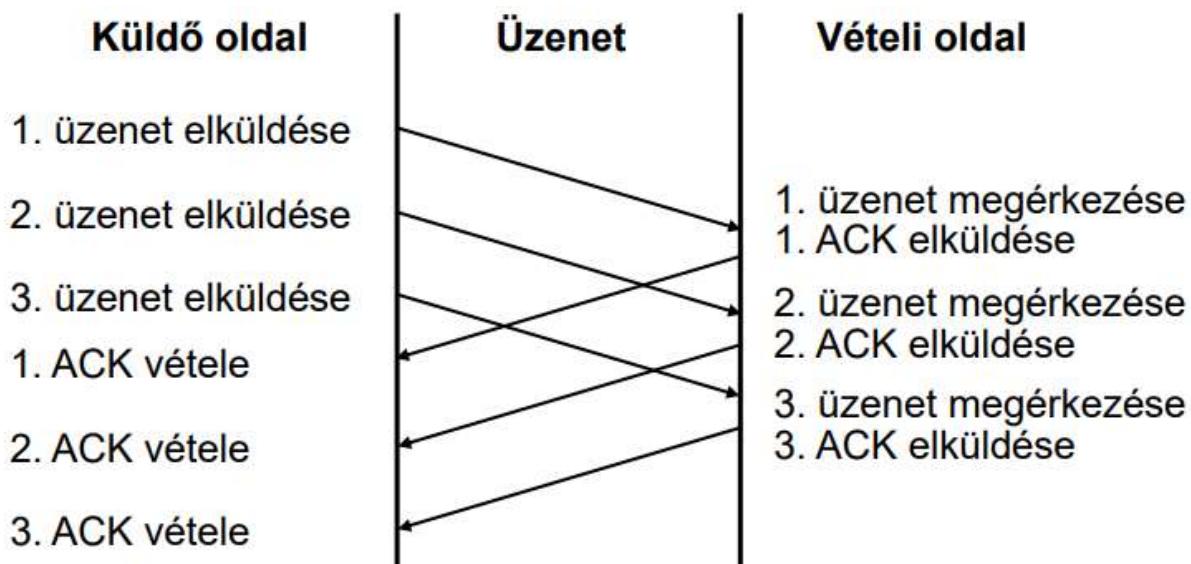
- Torlódáskezelés
 - torlódás jelzés
- A küldési sebesség szabályozása
 - Csúszóablak (Sliding Window)

Adatfolyam vezérlés - Csúszó ablakok (Sliding Windows)

- A protokoll működése nem lenne hatékony, ha minden átküldött üzenet után megvárna a nyugtát, mielőtt a következő üzenetet küldené
- Ekkor egyszerre csak egy irányba haladnának az üzenetek
- A csúszó ablakos technikával több üzenet is elküldhető, mielőtt a korábban elküldött üzenetek nyugtája megérkezne
- A protokoll szoftver az átküldendő üzenetek sorozatára egy kis méretű ablakot fektet, és az ablak összes üzenetét elküldi
- Ha az ablak bal szélénő üzenetére pozitív nyugta érkezik, az ablak egygyel jobbra csúszik
- Az ablakban lehetnek elküldetlen üzenetek, és elküldött, de nem nyugtázott üzenetek
- Az ablak méretének helyes megválasztása nagyban befolyásolja a protokoll hatékonyságát
- A csúszó ablakos protokoll minden üzenetre külön időzítőt működtet
- A protokoll szoftver a vételi oldalon hasonló ablakkal rendelkezik, amelyben összeállítja a bejövő adatokat, és tárolja, hogy melyeket nyugtázta

- A full duplex kommunikáció miatt valójában minden két oldalon két-két ablak van a független kétféle irányú kommunikációra
- A TCP-ben alkalmazott csúszó ablak technikával a flow control (végállomások közötti adatfolyam vezérlés) is megoldható
- Az állomások az ablak méretét tudják változtatni
- A fogadott nyugták tartalmaznak az ablakra vonatkozó információt (window advertisement), amely lényegében a másik fél szabad puffer méretét tartalmazza
- A küldő fél ennek alapján változtatja a saját ablakának méretét
- Ha a fogadó pufferei kezdenek megtelni, kisebb ablakot jelölő közleményt küld a feladónak
- A küldő a nyugták hiányából következtet a csomagvesztésre, így az ablakméretet csökkenti

3 csomag elküldése csúszó ablakos protokoll használatával

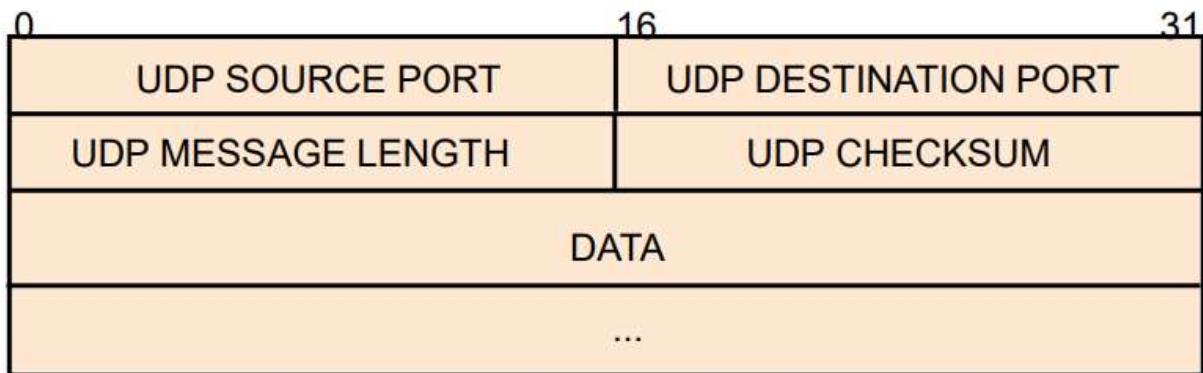


User Datagram Protocol – UDP

- Összeköttetés mentes protokoll
- Az egymástól függetlenül feladott üzeneteket továbbítja a két kommunikáló folyamat között
- A szintén összeköttetés nélküli, megbízhatatlan IP hálózati protokoll szolgáltatásait veszi igénybe. (A csomagok elveszhetnek, kettőződhetnek, és a feladás sorrendjétől eltérő sorrendben is érkezhetnek a különböző útvonalak miatt)
- Nem javítja fel a hálózati szolgáltatást
- Olyan alkalmazásoknál használják, amelyek kevésbé érzékenyek az adatvesztéssel szemben (pl. kép átvitel), vagy az üzenetek mindenkorral egy csomagból állnak
- Ha bizonyos időn belül nincs válasz, az adatgrammot újra el kell küldeni
- Előnye a hatékonysága: kis többlet terhelés (overhead), kevés adminisztráció
- A kommunikáló folyamatok azonosítása (címzése) azonos a TCP protokolléval
- Ha megbízható átvitelre van szükség, az alkalmazások a TCP-t használják

- RFC 768
- Az IP protokoll csak két gép közötti adattovábbítást biztosít
- Az UDP szállítási protokoll biztosítja, hogy egy gépen egyidejűleg futó több alkalmazói program egymástól függetlenül küldhessen és fogadhasson csomagokat
- Összeköttetésmentes szolgáltatást nyújt
- A csomag legvégső célpontját a portokkal lehet azonosítani
- A port-ok elérése általában szinkronizált, ami azt jelenti, hogy ha egy folyamat adatot kér egy portról, a futása felfügesztődik mindaddig, amíg az adat be nem érkezik. Ekkor az operációs rendszer a pufferben tárolt adatot átadja a folyamatnak, majd újra engedélyezi a futását
- A protokoll szoftver az adatokat átmenetileg egy, a porthoz rendelt sorban tárolja, amíg a folyamat feldolgozza
- A folyamatok közötti kommunikációhoz a folyamatoknak ismerniük kell a cél gép IP címét és a protokoll port számát, és minden üzenetnek tartalmaznia kell a cél és a forrás protokoll port számot
- Az UDP csomag fejlécében lévő cél és forrás port szám biztosítja, hogy a csomag a megfelelő folyamathoz kerüljön feldolgozásra, és hogy a válaszüzenet is a megfelelő helyre érkezzen
- Az UDP az IP protokollt használja az üzenet továbbítására
- Az IP szolgáltatását nem javítja fel, ugyanolyan megbízhatatlan, összeköttetés nélküli protokoll, mint az IP
- Az üzeneteket nem nyugtázza
- A megbízhatatlanságból eredő problémák megoldása az alkalmazói programok feladata

Az UDP üzenet formátuma



UDP multiplexálás/demultiplexálás

- A protokoll hierarchiában egy-egy réteg objektuma és a következő réteg több objektuma között multiplexálni ill. demultiplexálni kell
- Például az UDP szoftver üzeneteket fogad számos alkalmazástól és átadja az IP-nek továbbításra, és megfordítva, az IP-től kapott csomagokat továbbítja a megfelelő alkalmazásnak
- Ha az alkalmazás egy bizonyos protokoll port-on küld egy üzenetet, a port szám bekerül az UDP üzenet SOURCE PORT mezőjébe
- Bejövő üzenet esetén az UDP az IP-től kapott üzenetet az UDP DESTINATION PORT száma alapján demultiplexálja a megfelelő alkalmazásnak
- A port-ot leginkább egy sornak tekinthetjük
- Ebben tároljuk a bejövő üzeneteket feldolgozás előtt
- Az UDP megvizsgálja a bejövő üzenetek port számát, hogy az megfelel-e egy létező port-nak
- Ha nem, ICMP port unreachable hibaüzenetet generál, és eldobja az üzenetet, egyébként a megfelelő alkalmazásnak továbbítja

Transmission Control Protocol – TCP

- Összeköttetés alapú protokoll
 - Az alacsony szintű hálózati szolgáltatást (IP) feljavítja
 - Az alkalmazásokat egy szabványos primitív halmazzal lehet megírni:
 - Logikai kapcsolatot kell létesíteni két alkalmazás között
 - A két folyamat duplex (egyidejűleg kétirányú) kommunikációt folytat
 - Le kell bontani a kapcsolatot
 - Le kell bontani a kapcsolatot:
 - hibamentes
 - nincs adatvesztés és adatkettőzés
 - az adatok sorrendhelyesek
 - ha az összeköttetés lebomlik, újra létesíti a másik szállítási réteggel
 - A TCP az üzenetet:
 - szegmensekre darabolja
 - a vételi oldalon újra összeállítja
 - az elveszett adatot újra küldi
 - az adatokat helyes sorrendbe rakja
-
- RFC 793
 - Megbízható, összeköttetés alapú szállítási rétegbeli adatfolyam átviteli protokoll
 - Azon alkalmazások számára, amelyek nagy adatmennyiségeket forgalmaznak a hálózaton, nem megfelelő az IP és az UDP által biztosított megbízhatatlan szállítási szolgáltatás
 - Nem praktikus minden egyes alkalmazásba külön-külön beépíteni a hibavizsgálatot és annak korrekcióját
 - Ezért szükség van egy megbízható adatfolyam átviteli protokollra

A megbízható adatfolyam szolgáltatás jellemzői

- Adatfolyam orientált (Stream oriented)
- Virtuális áramköri kapcsolat (Virtual Circuit Connection)
- Pufferelt átvitel (Buffered Transfer)
- Strukturálatlan adatfolyam (Unstructured Stream)
- Egyszerre kétirányú kapcsolat (Full Duplex Connection)

A TCP feladatai

1. Kapcsolatok felépítése, fenntartása, lebontás
2. Az alkalmazások azonosítása/címzése (portcímek)
3. Nyugtázás, sorszámozás
4. Forgalomszabályozás (Sliding Window)

Portok, kapcsolatok és végpontok

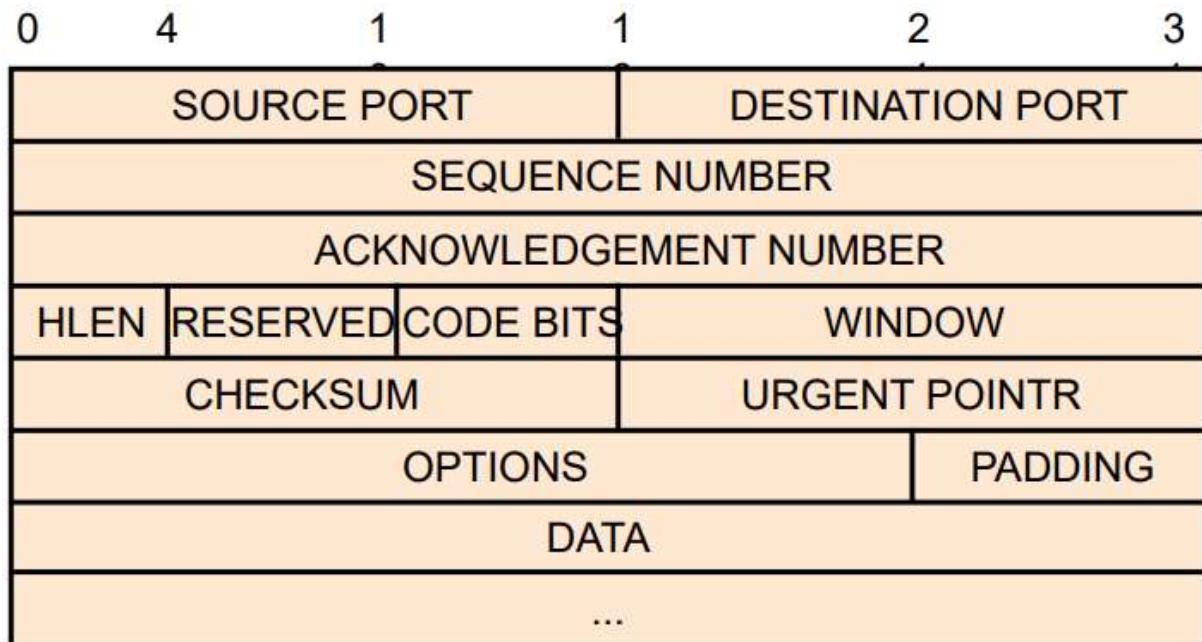
- A TCP lehetővé teszi, hogy több alkalmazás egyidejűleg kommunikáljon, és az üzenetet a megfelelő alkalmazáshoz továbbítja
- Az UDP-hez hasonlóan a TCP is a protokoll port számokat használja, az üzenet végső címzettjének azonosításához
- A TCP port azonban önmagában nem azonosítja a cél objektumot
- A TCP a kapcsolat (connection) fogalmát használja fel az azonosításhoz
- Két végpont azonosítja a kapcsolatot. Pl.: (192.190.173.37, 25) és (192.190.173.55, 1071)
- Elegendő, ha a kapcsolatot azonosító 4 szám közül 1 különbözik

TCP üzenettípusok

Minden TCP forgalom az alábbi szerkezetű szegmensben lesz továbbítva:

- kapcsolat felépítése
- adatok átvitеле
- nyugta küldése
- ablak méret hirdetmény
- kapcsolat lezárása

TCP szegmensformátum



A TCP szegmens mezőinek jelentése

SOURCE PORT	Feladó TCP port száma
DESTINATION PORT	Címzett TCP port száma
SEQUENCE NUMBER	A küldött adatok pozíciója a byte folyamban
ACKNOWLEDGEMENT NUMBER	Annak byte-nak a sorszáma az adatfolyamban, amelyet a feladó legközelebb meg akar kapni. Ez az ellenkező irányú folyamra vonatkozik!
HLEN	A szegmens hossza 32 bit-es egységekben
CODE BITS	Az üzenet tartalmára utal
WINDOW	Mekkora puffer áll rendelkezésére, mennyi adatot képes fogadni

Címzés: Portok és socket-ek

A portok és socketek szerepe

- A portok és socket-ek a kommunikáló felek folyamatainak azonosításában játszanak szerepet
- A hálózaton továbbított adatszegmenseket össze kell kapcsolni a számítógépen futó folyamatokkal. Problémák:
 - Az alkalmazói folyamatokat az operációs rendszerek egy-egy folyamataazonosítóval (process ID) azonosítják. Ezek különbözhettek a folyamat minden indításakor
 - A folyamatazonosítók nem szabványosak, operációs rendszerenként különbözhettek
 - A szerver folyamatok egyszerre több ügyfél folyamattal is tarthatnak kapcsolatot, ezért egyszerű folyamatazonosítók használata nem lenne egyértelmű
- A portok és socketek a folyamatok és a hálózaton továbbított adategységek (adatszegmensek) egységes és egyértelmű egymáshoz rendelését segítik és függetlenítik az adott operációs rendszer folyamatazonosítójától

Portok

- A folyamatok egy vagy több 16 bites port azonosítóval azonosítják magukat TCP/IP protokollkészletben: 1 – 65535
- A port azonosító jelzi, hogy a bejövő üzeneteket melyik folyamatnak kell továbbítani
- A portok típusai:
 - Jól ismert portok (well-known ports):
 - Standard szolgáltatásokhoz tartoznak: 1-1023
 - Pl. Telnet port = 23
 - A legtöbb szolgáltatás egyetlen portot használ
 - Az Ftp szerver 2 portot használ: 20 and 21

- A jól ismert portokat az Internet Assigned Number Authority (IANA) felügyeli
 - Többségüket a rendszerfolyamatok vagy privilegizált felhasználók programjai használják
 - A jól ismert portok használata lehetővé teszi, hogy az ügyfél programok konfigurálás nélkül is megtalálják a szolgáltatást
- A portok típusai:
 - Ideiglenesen használt portok (ephemeral):
 - Az ügyfeleknek nincs szükségek jól ismert portokra
 - Az ügyfél port azonosítókat az ügyfelek az operációs rendszertől kapják
 - Az ügyfél portok 1024 – 65535 közötti értékek
 - Az operációs rendszer úgy választja, hogy a <szállítási protokoll, IP cím, port azonosító> hármas egyedi legyen
 - Az ideiglenesen használt portokat az IANA nem felügyeli, szabadon használható a felhasználói programokban
 - Az UDP, a TCP és az ISO TP-4 a fenti port sémát használja

Socketek

- A socket interfész egy API (application programming interface), amely hozzáférést biztosít a kommunikációs protokollhoz
- Először a 4.2 BSD UNIX-ban vezették be, majd továbbfejlesztették a 4.3 és a 4.4 BSD-ben
- Terminológia:
 - Socket: speciális file handle, amely lehetővé teszi hálózati szolgáltatás kérését az operációs rendszertől
 - Socket cím: számhármas:
Pl. a TCP/IP-ben: <tcp, 193.44.234.3 12345>
 - Beszélgetés (conversation): kommunikációs kapcsolat két folyamat között
 - Asszociáció: számötös, amely teljesen azonosítja a két kommunikáló folyamatot:
<protokoll, helyi cím, helyi folyamat, távoli cím, távoli folyamat>
Pl. a TCP/IP-ben: <tcp, 193.44.234.3, 1500, 193.44.234.5, 21>
 - Fél asszociáció: egyenként azonosítja a kapcsolat végpontjait:
<protokoll, helyi cím, helyi folyamat>
vagy
<protokoll, távoli cím, távoli folyamat>
 - A fél asszociációt socket-nek vagy szállítási címnak is nevezik. Ez a kommunikáció megnevezhető, címezhető végpontja
- Két folyamat TCP socket-eken keresztül kommunikál
- A socket modell duplex byte csatornákat biztosít a két folyamat számára
- Az alkalmazásnak nem kell foglalkoznia a csatorna menedzselésével, ezt elvégzi a TCP
- A szerver folyamatok gyakran egyetlen porton keresztül egyidejűleg több kapcsolatot is kiszolgálnak
- A port koncepciót az UDP és a TCP hasonlóan használja

15. WAN SZOLGÁLTATÁSOK

WAN

- Nagy földrajzi távolságokat ölel át
- LAN hálózatok összekapcsolására használják
- Internetszolgáltatók birtokában van
- A szervezetek fizetnek a szolgáltatásért

WANs in the OSI Model

Most WAN standards focus on the physical layer and the data link layer.

Layer 1 Protocols

- Synchronous Digital Hierarchy (SDH)
- Synchronous Optical Networking (SONET)
- Dense Wavelength Division Multiplexing (DWDM)

Layer 2 Protocols

- Broadband (i.e., DSL and Cable)
- Wireless
- Ethernet WAN (Metro Ethernet)
- Multiprotocol Label Switching (MPLS)
- Point-to-Point Protocol (PPP) (less used)
- High-Level Data Link Control (HDLC) (less used)
- Frame Relay (legacy)
- Asynchronous Transfer Mode (ATM) (legacy)

Fogalmak

Customer Premises Equipment (CPE) – owned by the business or leased from the service provider

Data Communications Equipment (DCE) – provides an interface to connect subscribers to a communication link on the WAN cloud

Data Terminal Equipment (DTE) – connects to the local loop through the DCE

Demarcation Point – separates customer equipment from service provider equipment and is the place where the responsibility for the connection changes from the user to the service provider

Local Loop – cable that connects the CPE to the CO of the service provider (last mile)

Central Office (CO) – local service provider facility or building that connects the CPE to the provider network

Toll network – all the cabling and equipment inside the WAN provider network

Dialup modem – legacy WAN technology that converts digital signals into voice frequencies to be transmitted over the analog lines of the public telephone network

Access server – legacy WAN technology that coordinates dial-in and dial-out user communications.

Broadband modem – used with high-speed DSL or cable Internet service

CSU/DSU – used to convert digital, leased-line signals into frames that the LAN can interpret and vice versa

WAN switch – multiport internetworking device used in service provider networks

Router – provides internetworking and WAN access interface ports to connect to the service provider network

Core router/Multilayer switch – resides within the backbone of the WAN, supports multiple interfaces, and forwards IP packets at full line speed

Demarkációs pont

A Csatorna szolgáltatási egység (CSU) olyan eszköz, amely a terminált köti össze digitális vonallal.

Az Adat szolgáltatási egység (DSU) olyan eszköz, amely védelmi és diagnosztikai funkciókat hajt végre a telekommunikációs vonalakon. Jellemzően a két eszközt egyetlen egységeként (CSU/DSU) szerelik.

A CSU/DSU egységet nagyon nagy teljesítményű, drága modemként kell elközelni. Ilyen eszköz kell a T-1 vagy a T-3 összeköttetés minden két végére, és az egységeknek ugyanattól a gyártótól kell származniuk.

DTE és DCE

DTE – Commonly CPE, generally a router, could also be a terminal, computer, printer, or fax machine if they connect directly to the service provider network.

DCE – Commonly a modem or CSU/DSU, it is a device used to convert the user data from the DTE into a form acceptable to the WAN service provider transmission link. The signal is received at the remote DCE, which decodes the signal back into a sequence of bits; the remote DCE then signals this sequence to the remote DTE.

Private and Public WANs

A private WAN is a connection that is dedicated to a single customer.

Private WANs provide the following:

- Guaranteed service level
- Consistent bandwidth
- Security

A public WAN connection is typically provided by an ISP or telecommunications service provider using the internet. In this case, the service levels and bandwidth may vary, and the shared connections do not guarantee security.

WAN beágyazási protokollok

- Bérelt vonal: HDLC, PPP, SLIP
- Vonal-kapcsolt: HDLC, PPP, SLIP
- Csomag-kapcsolt: X.25, Frame Relay, ATM

WAN topológiák

- Point-to-Point
 - Employs a point-to-point circuit between two endpoints.
 - Involves a Layer 2 transport service through the service provider network.
 - The point-to-point connection is transparent to the customer network.
- Hub-and-Spoke
 - Enables a single interface on the hub router to be shared by all spoke circuits
 - Spoke routers can be interconnected through the hub router using virtual circuits and routed subinterfaces
 - Spoke routers can only communicate with each other through the hub router
- Full Mesh
 - Fully Mesh
 - Uses multiple virtual circuits to connect all sites
 - The most fault-tolerant topology
 - Parsally Meshed
 - Connects many but not all sites
- Dual-Homed
 - Offers enhanced network redundancy, load balancing, distributed computing and processing, and the ability to implement backup service provider connections.
 - More expensive to implement than single-homed topologies. This is because they require additional networking hardware, such as additional routers and switches
 - More difficult to implement because they require additional, and more complex, configurations

Vonalkapcsolt technológiák

A kapcsolat felépül a kommunikáció előtt, egy dedikált kapcsolat alakul ki a forrás és a cél között

Példák:

- telefonhálózat
- Integrated Services Digital Network (ISDN)

Csomagkapcsolt technológiák

Az adat kisebb egységekben – csomagokban – egymástól függetlenül jut el a célohoz egy osztottan használt hálózaton keresztül

Példák:

- FRAME RELAY
- ATM
- MPLS
- Ethernet WAN

A széles körben használt WAN szolgáltatástípusok és protokollok

ISDN

Vonalkapcsolt technológia

Az ISDN (Integrated Services Digital Network – Integrált szolgáltatású digitális hálózat) alapjait az AT&T amerikai távközlési cég fektette le, 1976 - ban. Az ún. CCIS (Common Channel Interoffice Signaling – közös csatornás központi jelzésmód) megoldás legnagyobb előnye az analóg vonallal szemben, hogy képes több csatornán adatot továbbítani. A hang és az adatcsatornát elkülönítették. Ez nemcsak szolgáltatásaiban hozott újat (egyszerre lehetett telefonálni és internetezni), hanem sebességen is többet nyújtott adatátvitelnél.

Egy speciális, külön csatorna biztosítja az állandó kapcsolatot az ügyfél és a szolgáltató között. Az ügyfelnél el kell helyezni egy végponti berendezést (NT – Network Terminal), melyre ugyanaz a réz érpár csatlakozik, amely az analóg vonalat biztosította

FRAME RELAY

Csomagkapcsolt technológia

Kétirányú, állandó virtuális áramköröket (Permanent Virtual Circuit, PVC) használ a kapcsolatokhoz.

A PVC-keket adatkapcsolati azonosítóval (DLCI) látja el.

ATM

Cellakapcsolt technológia, 56 byte-os csomagokban, „cellákban” továbbítja az adatokat, multiplexelést használ

Ethernet WAN

Service providers now offer Ethernet WAN service using fiber-optic cabling.

The Ethernet WAN service can go by many names, including the following:

- Metropolitan Ethernet (Metro E)
- Ethernet over MPLS (EoMPLS)
- Virtual Private LAN Service (VPLS)

There are several benefits to an Ethernet WAN:

- Reduced expenses and administration
- Easy integration with existing networks
- Enhanced business productivity

MPLS

Multiprotocol Label Switching (MPLS) is a high-performance service provider WAN routing technology to interconnect clients without regard to access method or payload.

- MPLS supports a variety of client access methods (e.g., Ethernet, DSL, Cable, Frame Relay).
- MPLS can encapsulate all types of protocols including IPv4 and IPv6 traffic
- An MPLS router can be a customer edge (CE) router, a provider edge (PE) router, or an internal provider (P) router.
- MPLS routers are label switched routers (LSRs). They attach labels to packets that are then used by other MPLS routers to forward traffic
- MPLS also provides services for QoS support, traffic engineering, redundancy, and VPNs

HDLC - High-level Data Link Control

- A HDLC és a PPP a két leggyakoribb soros vonali 2. rétegbeli beágyazási típus – WAN kapcsolati protokollok
- A HDLC (High-level Data Link Control) szabványos, bit-orientált adatkapcsolati rétegbeli beágyazási típus
- A HDLC szinkron soros átvitelt használ, mely hibamentes kommunikációt biztosít két pont között
- A HDLC protokoll definiál egy 2. rétegbeli keretszervezési (frame) struktúrát, amely nyugtázás és ablakozási rendszer használatával áramlásvezérlésre és hibakezelésre ad lehetőséget
- minden keret ugyanolyan formátumú, akár adatkeretről, akár vezérlőkeretről legyen szó
- A szabványos HDLC keretformátum nem tartalmaz olyan adatmezőt, amely azonosítaná a keret által hordozott protokoll típusát
- A szabványos HDLC emiatt nem képes többfajta protokoll átvitelére ugyanazon az összeköttetésen keresztül.

Jelző	Cím	Vezérlés	Információ	Keret-ellenőrző összeg	Jelző
8 bit	8 bit	8 vagy 16 bit	Változó hossz, 0 vagy több bit, 8 többszöröse	16 vagy 32 bit	8 bit

- Flag: keret kezdő mező: 0111110.
- Vezérlés:
 - I-frame: felsőbb rétegbeli protokollok adatait szállítja
 - S-frame: vezérlő üzeneteket szállít – Request and suspend transmission, report on status, and acknowledge receipt of I-frame
 - U-frame: számoszatlan vezérlő üzenetek

PPP – Point to Point Protocol (16. téTEL)

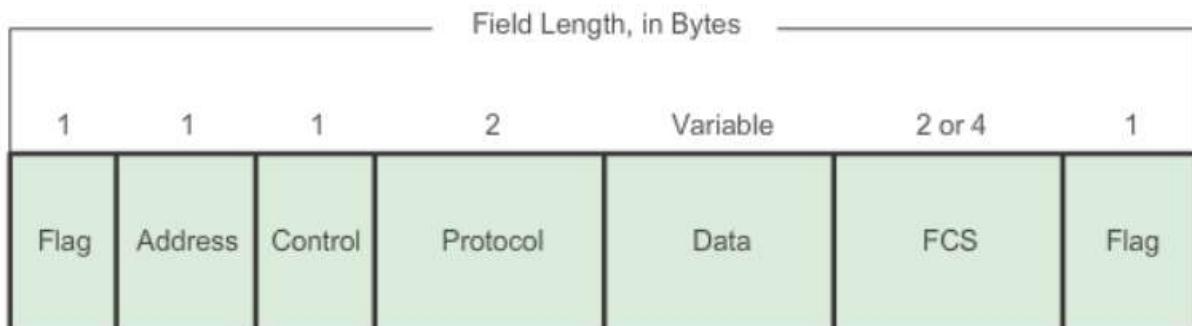
- A HDLC-hez hasonlóan a Pont-Pont Protokoll (PPP) is soros összeköttetések számára készült adatkapcsolat rétegbeli beágyazási típus
- Réteges felépítést használ, mely segítségével képes multi-protokoll adatcsomagok beágyazására és átvitelére pont-pont kapcsolatokon keresztül
- Mivel a PPP protokoll szabványokon alapul, lehetővé teszi a kommunikációt a különböző gyártótól származó készülékek között.

A PPP a következő interfészeket támogatja:

- aszinkron soros
- szinkron soros
- HSSI (High-Speed Serial Interface)
- ISDN

A PPP két alprotokollal rendelkezik:

- Kapcsolatvezérlő protokoll (Link Control Protocol, LCP) – a pont-pont kapcsolatok felépítéséért, fenntartásáért és lebontásáért felelős
- Hálózatvezérlő protokoll (Network Control Protocol, NCP) – együttműködést biztosít a különböző hálózat rétegbeli protokollokkal



Kapcsolatvezérlő protokoll (LCP)

- A PPP az LCP-t használja pont-pont összeköttetések kialakítására, fenntartására, tesztelésére és befejezésére
- Az LCP észleli és konfigurálja a WAN-kapcsolat vezérlőbeállításait.
- Beállítási lehetőségek, amiket az LCP kezel:
 - hitelesítés (authentication)
 - tömörítés
 - hibafelismerés
 - minőség-ellenőrzés
 - több kapcsolat (multilink)
 - PPP visszahívás

Hálózatvezérlő protokoll (NCP)

- A PPP az NCP-t használja a különböző hálózat rétegbeli protokollok beágyazására, így azok képesek ugyanazon kommunikációs kapcsolaton keresztül működni
- A PPP kapcsolatokon használt hálózati protokolloknak saját hálózatvezérlő protokollra van szüksége
- Az internetprotokoll (IP) például, az IP vezérlőprotokollt (IPCP), az IPX pedig az IPX vezérlőprotokollt (IPXCP) használja
- Az NCP-k a beágyazott hálózati rétegbeli protokollok azonosítására jelzőkódokat tartalmazó adatmezőket használnak

PPP összeköttetés kiépítése

A PPP-kapcsolatok létrehozásának folyamata három fázisra bontható:

- ezek az összeköttetés létrehozása, kapcsolat konfigurálás

LCP must first open the connection and negotiate configuration options; it completes when the receiving router sends a configuration-acknowledgment frame back to the router initiating the connection

- minőség-ellenőrzés

LCP tests the link to determine whether the link quality is sufficient to bring up network layer protocols.

- a hálózati rétegbeli protokoll használatának fázisa

After the LCP has finished the link quality determination phase, the appropriate NCP can separately configure the network layer protocols, and bring them up and take them down at any time

PPP hitelesítés

- PPP összeköttetések hitelesítésének beállítása elhagyható
- Ha be van állítva, a hitelesítési folyamat közvetlenül a kapcsolat létrehozása után, de még a hálózati rétegbeli protokollok konfigurációs fázisa előtt lezajlik
- A PPP összeköttetések két lehetséges hitelesítési típusa a jelszó hitelesítő protokoll (Password Authentication Protocol, PAP), illetve a kihívásos kézfogás hitelesítési protokoll (Challenge Handshake Authentication Protocol, CHAP).

PAP hitelesítés

- A PAP egyszerű eljárást biztosít a távoli állomás azonosításához.
- Kétfázisú (kétutas, két üzenetből álló) kézfogást használ a felhasználói név és a jelszó elküldéséhez.
- A hívott eszköz megvizsgálja a kezdeményező eszköz felhasználói nevét, majd meggyőződik arról, hogy a fogadott jelszó megegyezik-e az adatbázisában találhatóval
- Ha a két jelszó megegyezik, a hitelesítés sikeres

CHAP hitelesítés

- A másik PPP hitelesítési módszer a kihívásos kézfogás hitelesítési protokoll (CHAP).
- A kihívásos kézfogás hitelesítési protokoll
- A CHAP sokkal biztonságosabb hitelesítési folyamat, mint a PAP. A CHAP nem küldi el a jelszót az összeköttetésen keresztül.
- A CHAP alapú hitelesítés az összeköttetés felépítésekor történik meg először, majd annak lebontásáig újra és újra megismétlődik
- Itt a hívott eszköz felel a hitelesítés gyakoriságának szabályozásáért és ütemezéséért, ami elégé valószínűtlenne teszi a jelszólopáson alapuló támadások sikerességét.

A CHAP háromutas kézfogást használ.

1. A PPP-összeköttetés létrehozásának fázisa megtörténik
2. A helyi forgalomirányító kihívó (challenge) üzenetet küld a távoli forgalomirányítónak
3. A távoli forgalomirányító a kapott kihívó üzenet és a megosztott titkos kulcs segítségével, egyirányú hash függvény felhasználásával egy kivonatot hoz létre
4. Ezután a kivonatot visszaküldi a helyi forgalomirányítónak
5. A helyi forgalomirányító összeveti az érkezett választ a saját maga által számított kivonattal, melyet a kihívó üzenet és ugyanazon megosztott titkos jelszó valamint ugyanazon egyirányú hash függvény felhasználásával határoz meg
6. Ha a két számított érték megegyezik, a helyi forgalomirányító nyugtázza a hitelesítést
7. Abban az esetben, ha a két érték nem egyezik meg, a helyi forgalomirányító bontja a kapcsolatot

- A CHAP a kihívó üzenetek értékének megváltoztatásával biztosít védelmet a visszajátszásos támadásokkal szemben
- Mivel a kihívó üzenet értéke egyedi és véletlenszerű, ezért az ebből számított kivonat (hash) értéke is egyedi és véletlenszerű lesz
- Az ismételt kihívások használata csökkenti azt az időtartamot, amíg veszélynek van kitéve a kapcsolat
- A helyi forgalomirányító vagy egy külső hitelesítési kiszolgáló felel a kihívó üzenetek gyakoriságának és ütemezésének szabályozásáért

PPP konfiguráció

A konfigurálni kívánt porton belül:

1. encapsulation ppp
2. compress [predictor|stac]
3. ppp quality [percentage]
4. ppp authentication {chap | chap pap | pap chap | pap}

17-18-19. FORGALOMIRÁNYÍTÁS

A forgalomirányítás feladatai és fogalmai

Autonóm körzet

- Az Internet külön-külön menedzselt internetek összessége
- Ezeket autonóm rendszereknek nevezzük, és saját belső irányító algoritmussal és menedzsment szervezettel rendelkeznek
- Az egyesített Internetet egy mag gerinc hálózatnak tekintjük, amelyhez az autonóm rendszerek csatlakoznak
- Az autonóm rendszereken belül használt forgalomirányítókat interior gatewayeknek, az autonóm rendszereket a mag hálózathoz csatoló forgalomirányítókat pedig exterior gateway-eknek nevezzük
- Az állomások és a forgalomirányítók nem tárolnak a teljes Internetre vonatkozó irányítási információt
- Az irányítási információ tárolása hierarchikus:
 - Az állomások csak annyi irányítási információt tárolnak, amely elegendő ahhoz, hogy az ugyanahhoz a hálózathoz csatolt állomások és interior gateway-ek számára továbbíthassák a csomagokat
 - Az interior gateway-ek csak annyi irányítási információt tárolnak, amely elegendő ahhoz, hogy az ugyanahhoz az autonóm rendszerhez csatlakozó állomások és interior gateway-ek számára továbbíthassák a csomagokat
 - Az exterior gateway-ek csak annyi irányítási információt tárolnak, amely elegendő ahhoz, hogy egy interior gateway vagy egy másik exterior gateway számára továbbíthassák a csomagokat

Irányítótábla szerepe a forgalomirányításban

Az állomások és a forgalomirányítók adatküldése, illetve adattovábbítása az irányítótáblák bejegyzései alapján történik.

Egy bejegyzés (útvonal) jellemzői:

- Típus (közvetlen kapcsolat, helyi hálózati útvonal, helyi alapértelmezett útvonal, távoli útvonal)
- Irány
- Jósága (mértéke, pl. hossza, költsége, késleltetése, terheltsége, sebessége)
- Forrása (honnan származik az információ, mennyire megbízható)

Statikus forgalomirányítás indokai

- Kisméretű hálózatokban jól karbantartható és átlátható
- Zsák hálózatok - stub network - esetén biztonsági és adminisztrációs okokból
- Alapértelmezett útvonalak - single default router – esetén
- Tartalék útvonalak érdekében

Dinamikus forgalomirányítás

Előnyök:

- Az információk automatikus megosztása
- „Legjobb” útvonalak meghatározása és felvétele az irányítótáblába
- A statikus forgalomirányításhoz képest kevesebb adminisztráció szükséges az útvonalak karbantartásához
- Kevesebb konfigurációval nagyobb hálózatokon is működik

Hátrányok:

- Erőforrásigényes (memória, cpu, sávszélesség)
- Bonyolultabb konfiguráció, több beállítási lehetőség (nagyobb szaktudást igényel)

Irányított és Irányító protokollok

Irányított (routed) protokollokat

- Az irányított protokoll a hálózati réteg protokollok valamelyike:
 - IPv4, IPv6, IPX, DECNET, APPLE TALK
- Az irányított protokoll leírja a címzést, a csomag szerkezetét, működési mechanizmust

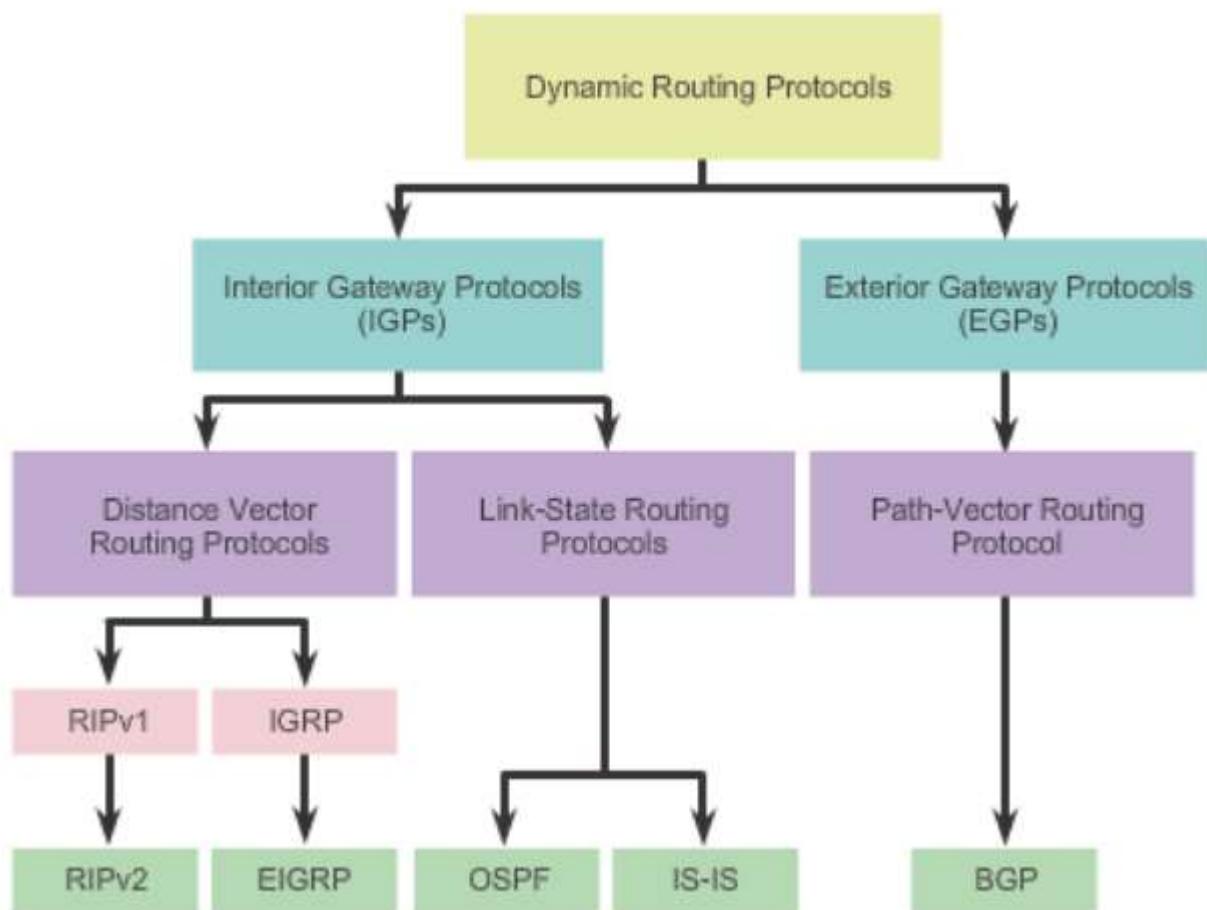
Irányító (routing) protokollokat

- Az irányított protokoll a hálózati réteg protokollok valamelyike:
 - RIP, EIGRP, OSPF, IS-IS
- Feladata:
 - Az irányítótáblák felépítése, karbantartása
 - Kommunikáció a szomszédos forgalomirányítókkal
 - Optimális útvonalak kiválasztása a körzet összes hálózatára

Irányító protokoll

Működési elve szerint lehet:

- Távolságvektor algoritmussal működő protokoll (Distance-Vector Algorithm: DVA): RIP, Novell RIP, IGRP
- Kapcsolatállapot alapú protokoll (Link State protokoll): OSPF, IS-IS



Kapcsolatállapot alapú protokollok

- minden forgalomirányító a teljes hálózat (autonóm körzet) topolóját látja
- tudják, hogy mely forgalomirányítók melyekkel, milyen vonalon kapcsolódnak. minden kapcsolatról rendelkeznek jellemzőkkel
- A topológia és a kapcsolatok jellemzői alapján minden forgalomirányító maga számolja ki a legjobb, hurokmentes útvonalat az összes hálózathoz Ennek alapján építik föl az irányítótáblájukat
- Ha változás van a hálózatban (pl. egy kapcsolat megszakad), csak az állapotváltozásokat terjesztik szét a forgalomirányítók a hálózatban
- Állapotváltozás hiányában a forgalomirányítók csak ritkán terjesztik szét a kapcsolat állapotukat (szomszédjaikhoz való kapcsolódásukat)
- Állapotváltozás esetén minden forgalomirányító újra számolja a hálózat topolóját és irányítótábláját
- Az állapot információk terjesztése kisebb hálózati forgalmat generál, mint a teljes irányítótáblák cseréje
- Változás esetén gyors konvergencia
- Memória- és feldolgozás-igényes algoritmus

Távolságvektor alapú irányítóprotokollok

- Az útvonalak jóságát valamelyen egyszerűen vagy bonyolultabban számított metrika (mérték) írja le
- A metrika számításában résztvevő jellemzők lehetnek: ugrások száma, sávszélesség, késleltetés, terhelés, hibaarány, költség
- A forgalomirányítók csak a szomszédjaikkal tartják a kapcsolatot, útvonal információkat osztanak meg egymással, csak a metrikát és az irányt
- Az elérhető hálózatokat (autonóm körzet) a szomszédok szemszögéből látják, nem ismerik a teljes topológiát

Az IP Routing Information Protocol (RIP) jellemzői

- A távolság-vektor algoritmusra (Distance-Vector Algorithm: DVA) épül
- A legrövidebb útvonalat választja
- A legrégebben használt irányítóprotokoll
- Az IP (routed) protokoll továbbítására használják
- Elosztott irányítóprotokoll
- Az útvonalak jóságát a két forgalomirányító közötti hálózatok számával (hop = ugrás) fejezi ki. A metrika az ugrások számával azonos
- Nem biztos, hogy a legkevesebb ugrás számú útvonal a leghatékonyabb
- A maximális ugrásszám: 16
- Az irányítótáblák cseréje jelentős sávszélességet foglalhat le
- Viszonylag lassú konvergencia az irányítótáblák kialakításában
- Esetlegesen irányítási hurkok alakulhatnak ki

Az útvonalak kiértékelése

- Ha a kapott útvonal ismeretlen, akkor a forgalomirányító beírja az irányítótáblájába
- Ha az útvonalra már található bejegyzés az irányítótáblában egy másik forrástól, akkor az újat csak akkor írja be, ha az jobb ugrásszámmal rendelkezik a réginél.
- Ha az útvonal már a táblában van és ugyanattól a forrástól származik, akkor mindenképpen kicseréli az új bejegyzésre, még akkor is, ha a mérték nem jobb
- A frissen bekapcsolt forgalomirányító ezután egy eseményvezérelt frissítést küld a RIP protokollal konfigurált interfészén a saját irányítótáblája tartalmának elküldésével

Útvonalfrissítések

- Ha a forgalomirányítók a megfelelő verziójú frissítéseket küldik és dolgozzák fel, akkor a RIPv1 és RIPv2 teljesen kompatibilisek egymással
- Alapértelmezésben a RIPv2 csak 2. verziójú frissítéseket küld és fogad
- Ha egy hálózatban minden két verziót kell használni, akkor a hálózati rendszergazda konfigurálhatja úgy a RIPv2-t, hogy 1. és 2. verziójú frissítést egyaránt küldjön és fogadjon
- A RIPv1 alapértelmezésben 1. verziójú frissítéseket küld, de minden kettőt fogadja

Irányítási hurkok

Egy RIP-et használó hálózatban időre van szükség a konvergenciához. A forgalomirányítók helytelen útvonalakat is tárolhatnak az irányítótábláikban mindaddig, amíg az összes forgalomirányító nem frissítette az irányítótábláját, és ugyanazt a képet nem látják a hálózatról. A hibás hálózati információ az irányítási frissítések és más forgalmak végtelen hurokba kerülését okozhatja

- **Visszirányú mérgezés**

A visszirányú mérgezés az útvonal mértékét 16-ra állítja, s így elérhetetlennek nyilvánítja azt. Mivel a RIP a végtelent 16-nak definiálja, ezért minden olyan hálózat mely 15 ugrásnál távolabb van elérhetetlennek minősül. Ha egy hálózat elérhetetlen, akkor a forgalomirányító megváltoztatja arra az útvonalra vonatkozó mértéket 16-ra, hogy minden más forgalomirányító is elérhetetlennek lássa. Ez a tulajdonság akadályozza meg a mérgezett útvonalakon küldött információk terjedését

- **Látóhatármegosztás**

A látóhatármegosztás megakadályozza a hurkok kialakulását. Ha több forgalomirányító is ugyanazt az útvonalat hirdeti egymásnak, akkor irányítási hurok jöhet létre. A látóhatármegosztás megakadályozza, hogy egy forgalomirányító azon az interfészén hirdessen egy útvonalat, amelyiken azt megismerte

- **Visszatartó időzítők**

A visszatartó számlálók stabilizálják az útvonalakat. A visszatartó időzítők ugyanis megakadályozzák egy leállt útvonalra vonatkozó frissítésnek az elfogadását, ha a frissítés a leállást követő meghatározott időintervallumon belül érkezik, és nagyobb mértéket szerepel benne a korábbi értéknél. Ha a visszatartó időzítő lejárta előtt az eredeti útvonal helyreáll, vagy a forgalomirányító olyan útvonal információt kap, mely kisebb mértékkel rendelkezik, akkor a forgalomirányító felveszi az irányítótáblájába, és azonnal használni is kezdi. Az alapértelmezett visszatartási idő 180 másodperc, a rendszeres frissítési idő hatszorosa.

- **Eseményvezérelt frissítések**

Ha egy útvonal kiesik, a RIP nem várja meg a következő frissítési időt, hanem azonnal küld egy rendkívüli frissítést, amit eseményvezérelt frissítésnek nevezünk. A kiesett útvonalat 16-os mértékkel hirdeti, így az utat megmérgezi. Ez a frissítés visszatartási állapotban tartja az útvonalat, mindaddig amíg a RIP egy jobb mértékű alternatív útvonalat nem talál helyette

A RIP korlátai

- Az egyszerű ugrásszám mérték bonyolult hálózatokban nem a legoptimálisabb a legjobb útvonal megtalálásához
- 15 ugrásban maximalizálja a távoli hálózatok elérhetőségét
- Az irányítótáblájáról periodikus frissítéseket küld, mely sávszélességet foglal, még akkor is, ha nem történik változás a hálózatban
- A hosszú konvergencia idő következtében irányítási hurok keletkezhet, mely értékes sávszélességet foglal le

20. OSPF ALAPÚ FORGALOMIRÁNYÍTÁS

Kapcsolatállapot alapú irányító protokollok (Linkstate routing protocols)

Routing protokoll jellemzők

Characteristic	RIPv1	RIPv2	EIGRP	IS-IS	OSPF	BGP
Distance vector	✓	✓	✓			✓
Link-state				✓	✓	
Classless		✓	✓	✓	✓	✓
VLSM support		✓	✓	✓	✓	✓
Automatic route summarization	✓	✓ (can be disabled using no auto-summary)	✓ (can be disabled using no auto-summary)			✓
Manual route summarization		✓	✓	✓	✓	✓
Hierarchical topology required				✓	✓	
Size of network	Small	Small	Large	Large	Large	Very large
Metric	Hops	Hops	Composite metric	Metric	Cost	Path attributes
Convergence time	Slow	Slow	Very fast	Fast	Fast	Slow

Link-state routing protocols

- A Link-state routing protocols vagy shortest path first protocols Edsger Dijkstra shortest path first (SPF) algoritmusára épülnek
- Két megvalósításuk:
 - Open Shortest Path First (OSPF)
 - Intermediate System-to-Intermediate System (IS-IS)
- Bonyolultabbak a távolság vektor protokolloknál (distance vector protocol)
- Az alapvető funkcióik hasonlóak
- Konfigurációjuk nem bonyolultabb

A kapcsolat-állapot forgalomirányító folyamat (Link-state routing process)

1. Mindegyik router feljegyzi a közvetlenül csatolt hálózatainak kapcsolat állapotait
2. Mindegyik router szomszédsági kapcsolatot hoz létre a közvetlenül csatolt hálózaton elérhető routerekkel (Hello üzenetek)
3. Mindegyik router Link-State Packeteket (LSP) készít, amelyek a közvetlen összeköttetéseinek állapotát tartalmazza (Hálózat címe, maszkja, interfész IP címe, link típusa, sávszélesség, szomszéd ID-je, stb.)
4. Mindegyik router elárasztja a szomszédjait az LSP csomagokkal, akik eltárolják ezeket az adatbázisukban. A szomszédok tovább küldik az LSP-et az ő szomszédjainak
5. Mindegyik router teljes térképet készít az adatbázisából a hálózat topolójáról, majd az SPF algoritmus segítségével kiszámítja a legjobb útvonalat az összes célhálózatra

A Link-state protokollok előnyei

- **Topológia térkép készítése**
Ennek segítségével minden router saját maga készíti el a hálózat SPF fáját, majd ennek segítségével a routing tábláját
- **Gyors konvergencia**
Az LSP információkat azonnal tovább küldik a routerek
- **Esemény-vezérelt update**
Egy kezdeti elárasztás után a Link-state routing protokollok csak topológia változás esetén küldenek LSP-ket, amelyek csak az érintett linkekről tartalmaznak információt. Az OSPF csak 30 percenként küld periodikus update-t
- **Hierarchikus tervezés**
A Link-state routing protokollok (OSPF, IS-IS) az area-elvet alkalmazzák, amely:
 - hierarchikus hálózattervezést
 - jobb útvonal összevonást (aggregáció)
 - a routing hibák elszigetelését az areaban tesz lehetővé

Hierarchikus hálózattervezés – Multiple areas

- Csökken a link-state adatbázis mérete
- Csökken a CPU és memória igény
- Csökken az LSP-k száma

A Link-state protokollok erőforrás igénye

- **Memória igény:** Nagyobb memória (Link-State Database és az SPF fa tárolása) szükséglet a Distance Vector Routing protokollokhoz képest
- **Számítási teljesítmény igény:** Nagyobb CPU teljesítmény szükséglet a Link-State protokoll és a teljes topológia térkép építése miatt
- **Sávszélesség igény:** Az LSP-k (link-state packet) továbbítása miatt növekedhet a sávszélesség igény. Ez többnyire csak a routerek indításakor és gyakori topológia vagy link állapot változásakor következik be (instabil hálózat)

Open Shortest Path First (OSPF) forgalomirányító protokoll

OSPF történelem

- 1987: Az Internet Engineering Task Force (IETF) OSPF Working Group kezdte kifejleszteni
- 1989: OSPFv1 specifikáció (RFC 1131). Nem terjesztették
- 1991: OSPFv2 specifikáció (RFC 1247 by John Moy). Az IETF által javasolt IGP (Interior Gateway Protocol)
- 1998: OSPFv2 specifikáció update (RFC 2328 – ez az aktuális RFC)
- 1999: OSPFv3 for IPv6 (RFC 2740)

Az OSPF jellemzői

- RFC 2328 OSPFv2
- Kapcsolat-állapotú forgalomirányító protokoll (Link-State Protocol)
- A RIP felváltására szánták
- Osztály nélküli protokoll (Classless)
- Hierarchikus tervezést tesz lehetővé: area-elv
- Jól méretezhető
- Gyors konvergencia
- Metrika: cost (tetszőleges érték). (Cisco IOS-ek alapértelmezetten a sávszélességet használják költségként)
- 3 adatbázis
 - neighbour table
 - topologie table
 - routing table
- 5 üzenet
 - Hello packet
 - Database Description (DBD) packet
 - Link-State Request (LSR) packet
 - Link-State Update (LSU) packet
 - Link-State Acknowledgment (LSAck) packet
- Dijkstra algoritmus

Az OSPF üzenet beágyazás

- Az OSPF üzenetek IP csomagba ágyazva közlekednek
- Protokoll azonosító: 89
- Cél IP címek (multicast): 224.0.0.5 (All OSPF Routers) vagy 224.0.0.6
- Ethernet keretben a cél MAC címek: 01-00-5E-00-00-05 vagy 01-00- 5E-00-00-06

OSPF Network Types

- **Point-to-point** – Two routers interconnected over a common link. Often the configuration in WAN links
- **Broadcast Multiaccess** – Multiple routers interconnected over an Ethernet network
- **Non-broadcast Multiaccess (NBMA)** – Multiple routers interconnected in a network that does not allow broadcasts, such as Frame Relay
- **Point-to-multipoint** – Multiple routers interconnected in a hub-and-spoke topology over an NBMA network
- **Virtual links** – Special OSPF network used to interconnect distant OSPF areas to the backbone area

Az OSPF Hello protokoll

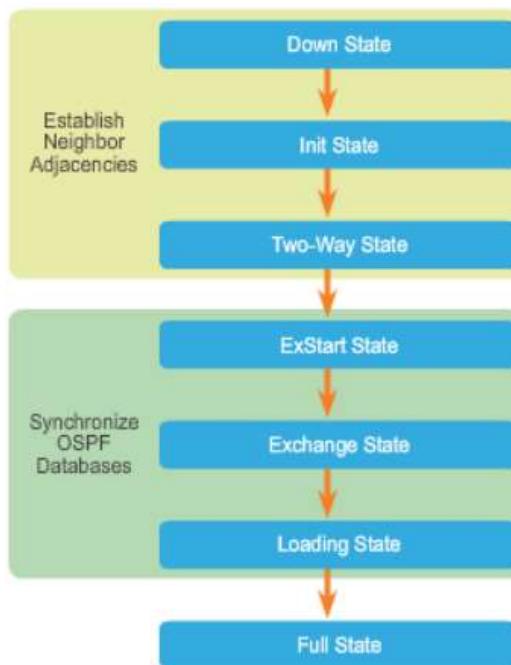
- Neighbor Establishment
- Az LSP üzenetek elárasztása előtt szomszédsági kapcsolatokat kell a routereknek kiépíteniük
- A routerek OSPF Hello üzeneteket küldenek ki minden OSPF-re konfigurált interfészükön
- OSPF Hello válaszok érkezése jelzi, hogy van OSPF router a hálózaton
- Az OSPF szomszédsági kapcsolatot létesít
- OSPF Hello and Dead Intervals
- A szomszédsági kapcsolat kiépítése után megegyeznek a Hello intervallum, a Dead intervallum értékében, és a network típusban:
 - Hello intervallum: milyen gyakran küldenek Hello üzenetet a routerek (pl. 10 mp multiaccess és point-to-point hálózaton)
 - Dead intervallum: mennyi ideig várnak a routerek Hello üzenetre, mielőtt a szomszédot „Leállt” állapotúnak nyilvánítanak (pl. 40 mp multiaccess és point-to-point hálózaton)
- Ha a Dead intervallum lejár, az OSPF link-state (LSP) üzenetet küld szét az állapotváltozásról
- Hello Packets are used to:
 - Discover OSPF neighbors and establish neighbor adjacencies
 - Advertise parameters on which two routers must agree to become neighbors
 - Elect the Designated Router (DR) and Backup Designated Router (BDR) on multi-access networks like Ethernet and Frame Relay
 - OSPF Hello packets are transmitted to multicast address 224.0.0.5 in IPv4 and FF02::5 in IPv6

Electing a DR and BDR

- Az OSPF üzenetek csökkentése érdekében multiaccess hálózatokon a routerek egy-egy Designated Router-t (DR) és Backup Designated Router-t (BDR) választanak
- A DR felelős a többi OSPF router (DROthers) értesítéséről (LSP) változás esetén
- A BDR figyeli a DR működését, és ha nem elérhető, átveszi a feladatát
- Point-to-point hálózaton a routerek nem választanak DR-t és BDR-t

OSPF működése

- Point-to-point hálózaton a routerek nem választanak DR-t és BDR-t
- Down state, Init state, Two-Way state, ExStart state, Exchange state, Loading state, and Full state
- Establishing Adjacencies
- When a neighboring OSPF-enabled router receives a Hello packet with a router ID that is not within its neighbor list, the receiving router attempts to establish an adjacency with the initiating router
- OSPF DR and BDR
- On multiaccess networks, OSPF elects a DR to be the collection and distribution point for LSAs sent and received. A BDR is also elected in case the DR fails
- After the Two-Way state, routers transition to database synchronization states



Router ID meghatározása

- Az OSPF router ID egyedileg azonosítja a routert az OFPF routing tartományban
- A router ID egy IP cím
- Router ID meghatározása Cisco routerekben:
 - Konfigurálás: OSPF router-id parancs
 - Ha a router ID-t nem konfiguráljuk, a router a loopback IP címek közül a legnagyobbat választja
 - Ha nincs loopback interfész, a fizikai interfések IP címei közül a legnagyobbat választja
- A router ID értéke azért fontos, mert értéke befolyásolja a DR/BDR router kiválasztását a multiaccess hálózatokban

OSPF költség

- A Cisco IOS kiszámítja a célhálózat felé vezető útvonal routerei kimenő interfészeinek Cost értékeit, és ezek összege lesz az útvonal költsége
- Az alábbi táblázatban a referencia sávszélesség: 100 Mbps (Fast Ethernet)
- A referencia sávszélesség módosítható gyorsabb hálózatokon az auto-cost reference-bandwidth parancsal

The OSPF Priority

Instead of setting the router ID on all routers, it is better to control the election by setting interface priorities.

To change the priority, use one of the following commands:

- ip ospf priority value (OSPFv2 interface command)
- ipv6 ospf priority value (OSPFv3 interface command)

To begin another OSPF election, use one of the following methods:

- Shutdown the router interfaces and then re-enable them starting with the DR, then the BDR, and then all other routers
- Reset the OSPF process using the clear ip ospf process privileged EXEC mode command on all routers

Adminisztratív távolság – Administrative distance

- A routing protokollok rendelkeznek egy ún. adminisztratív távolság értékkel
- Ennek szerepe az, hogy ha egy router több forgalomirányító protokollt is futtat, és egy célhálózatra két vagy több forgalomirányító protokoll is kínál útvonalat, akkor a router azt az útvonalat választja, amelyet a kisebb adminisztratív távolságú protokoll kínálja
- A protokollok alapértelmezett adminisztratív távolságát a táblázat tartalmazza (OSPF = 110)

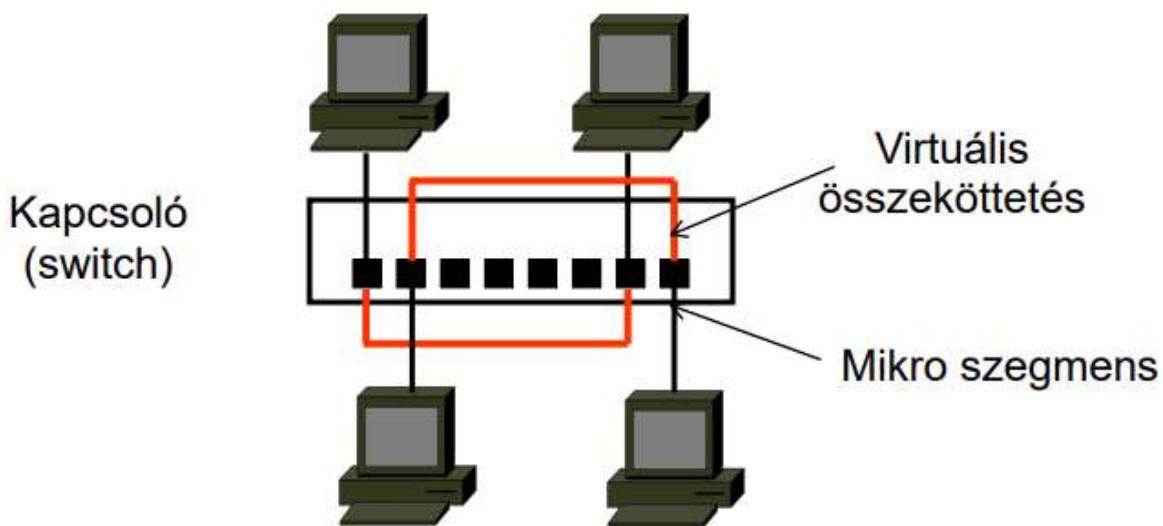
21. ETHERNET KAPCSOLÓK ALKALMAZÁSA

Az Ethernet kapcsolás jellemzői

Ethernet kapcsolók a 2. OSI rétegben működő berendezések. Több (sok) porttal rendelkeznek, amelyekhez munkaállomások, szerverek, hubok, forgalomirányítók, más kapcsolók csatlakoztathatók. A kapcsolók rendelkeznek: processzorral, memóriával, speciális áramkörökkel, operációs rendszerrel. A kapcsolók, ellentétben a Hub-akkal, duplex működésre képesek. A portjaira kapcsolt eszközök között nagy sebességgel, kis késleltetéssel végez kapcsolást, hardveresen.

Kapcsolás

A keretátvitel idejére két port között egy ún. virtuális áramkör jön létre, amelyen a keret áthalad. Ez a virtuális áramkör teljes (a portra) jellemző sávszélességet biztosít a kommunikáló gépek számára. A virtuális áramkörök dedikált sávszélességet biztosítanak a portok között. A kapcsoló biztosítja a port-párok közötti egyidejű kommunikációt. A kacsolást hardver végzi, ezért gyors. Ugyanarra a portra irányuló egyidejű kerettovábbítás esetén felgyülemlő kereteket (torlódás) a kapcsoló pufferben tárolja. Keretvesztés csak a puffer telítődése esetén fordulhat elő.



Mikroszegmentáció

A kapcsolók portjai ún. mikro szegmenseket alkotnak. Ideális esetben a szegmens egyetlen (a porthoz csatlakoztatott) készülékből áll, így ütközés nem fordulhat elő → minden portja egyetlen ütközési tartomány

A kapcsolást a keretben foglalt célállomás MAC-címe alapján végzi, a keretbe beágazott protokollt (alapfunkciója szerint) nem vizsgálja

Port-MAC-cím táblázato(ka)t tart fenn, amelynek alapján a beérkező kereteket a kimenő porthoz rendeli. Egy-egy porthoz több eszköz is csatlakozhat, Hub vagy másik kapcsoló segítségével

A kapcsoló portjai egyetlen szórási tartományt (broadcast domain) alkotnak. A szórásos üzeneteket és a többes küldés (multicast) üzeneteket a kapcsoló a bejövő port kivételével minden portára kiküldi

A kapcsolók fajtái

A munkacsoportos kapcsolók többnyire közös alkalmazást végző felhasználók gépeit kapcsolják össze. Saját szerverrel rendelkeznek

A többrétegű kapcsolók routing funkcióval is rendelkeznek. A router portjai között 3. rétegű irányítást, a kapcsoló portjai között 2. rétegű kapcsolás végeznek. A portok konfigurálhatók egyik vagy másik funkcióra



Munkacsoportos kapcsoló

Workgroup Switch



Többrétegű kapcsoló

Multilayer Switch

Szimmetrikus, aszimmetrikus kapcsolók

- Szimmetrikus kapcsolók azonos sebességű portokkal rendelkeznek
- Aszimmetrikus kapcsolók különböző sebességű portokkal rendelkeznek. A nagyobb sebességű portokat gerinchálózat céljára (kapcsoló-kapcsoló, kapcsoló-forgalomirányító összekötése), szerverek, nagysebességű munkaállomások hálózatra kapcsolása.
Különböző sebességű készülékek összekapcsolása
- Példa: 12 100Mbps és 2 1Gbps sebességű port

Duplex – fél-duplex átvitel

- A portok működési módja egyenként beállítható
- Duplex: egyszerre kétirányú kommunikáció. Ha csak lehet ezt a módot használjuk
- Fél duplex: Felváltva kétirányú kommunikáció. Csak akkor használjuk, ha Hub-ot kapcsolunk a portra, vagy a munkaállomás interféskártyája nem alkalmas duplex átvitelre
- A kapcsoló portok beállíthatók, hogy automatikusan felismerjék a kapcsolódó készülékek beállítását

Torlódások elkerülése, pufferek használata

Torlódás akkor következhet be, ha

- a bejövő port sebessége magasabb mint a kimenőé
 - több porton egy időben bejövő kereteket ugyanazon a kimenő porton kell továbbítani
- A kapcsolók a bejövő kereteket torlódás esetén puffer memóriában tárolják

A kerettovábbítás módjai

A kapcsolók bizonyos késleltetést okoznak a keretek továbbításában.

Ennek összetevői: keret beolvasása, cím kikeresése a kapcsoló táblából, ellenőrző összeg képzése, keret kiküldése a kimenő porton.

Tárol-továbbít (Store and forward)

A keretet teljes egészébe beolvassa, csak a megengedett legrövidebb kerethosszt elérő, hibátlan kereteket továbbítja. Ez a leglassúbb, de a legbiztonságosabb módszer

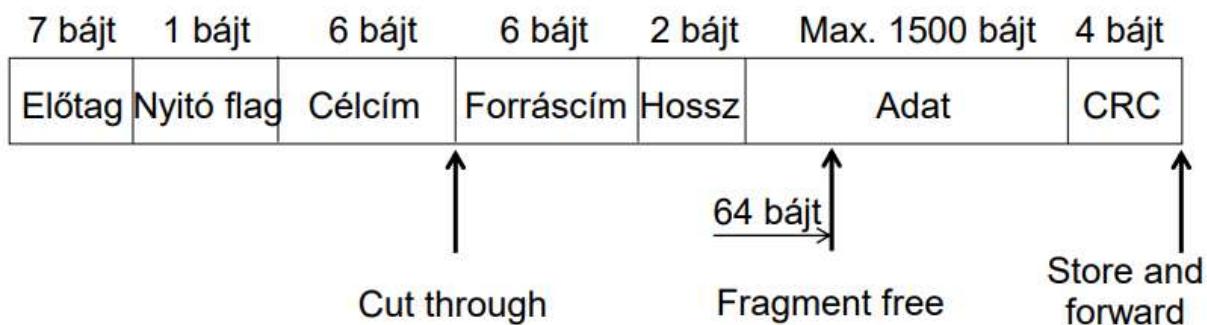
Gyors továbbítás (Cut through)

Nem várja meg a keret teljes beérkezését. Mihelyt beérkezik a célállomás MAC címe, a kimenő portot kikeresi a kapcsolótáblából, majd megkezdi a keret kiküldését a kimenő porton. Túl rövid (runt) és hibás keretek is továbbítva lesznek. Ez a leggyorsabb, de a legkevésbé megbízható továbbítási mód

Töredékmentes továbbítás (Fragment free)

Addig nem továbbítja a keretet, amíg legalább 64 bájt (legrövidebb megengedett keret) be nem érkezik. Hibás CRC-s keretek is továbbítva lesznek

A továbbítás megkezdésének legkorábbi ideje



A kapcsolótábla felépítése

- A kapcsolótábla tartalmazza:
 - MAC cím
 - Port azonosító
 - A bejegyzés kora
- minden portján nyilvántartja a hozzákapcsolódó eszközök MAC címeit.
- A MAC címeket a kapcsoló tanulás útján szerzi be (dinamikus, statikus)
 - A bejövő keretek forrás MAC címéből tanulja meg, hogy a különböző MAC című állomások a kapcsoló melyik portján érhetők el
- Ismeretlen cím esetén a keretet minden portján kiküldi (elárasztás)
- A broadcast és a multicast kereteket minden portján kiküldi
- A bejegyzések újabb hivatkozások elmaradásakor elővülnek (pl. 300 másodperc múlva) és törlődnek a kapcsolótáblából
 - Ennek szerepe az, hogy lehetőleg kis méretűek legyenek a kapcsolótáblák, és hogy a kapcsolók automatikusan kövessék a topológia változásokat
- A MAC címek kézzel is a portokhoz rendelhetők, és maximalizálható az egyes portokhoz rendelhető MAC címek száma is. Ezzel fokozható a biztonság
 - → Portbiztonság (Portsecurity)

Az Ethernet kapcsolók konfigurálása

- A kapcsolók konfigurálható berendezések
- A kapcsolók rendelkeznek speciális portokkal (pl. soros konzol port), amelyen keresztül konfigurálhatók
- LED-ek segítségével lehet követni a kapcsoló és a portok állapotát, aktivitását
- A konfiguráció módjai:
 - Parancssoros (pl. konzol portról HyperTerminal vagy Telnettel, SSH-val)
 - Menü rendszerben karakteres felületen (konzol portról vagy Telnettel)
 - Webes felületen
 - Menedzsment szoftver segítségével (Többnyire az SNMP-t használja)

22. REDUNDÁNS KAPCSOLÓ-TOPOLÓGIÁK

Redundancy at OSI Layers 1 and 2

Multiple cabled paths between switches:

- Provide physical redundancy in a switched network
- Improves the reliability and availability of the network
- Enables users to access network resources, despite path disruption

MAC Database Instability

- Ethernet frames do not have a time to live (TTL) attribute
 - Frames continue to propagate between switches endlessly, or until a link is disrupted and breaks the loop
 - Results in MAC database instability
 - Can occur due to broadcast frames forwarding
- If there is more than one path for the frame to be forwarded out, an endless loop can result
 - When a loop occurs, it is possible for the MAC address table on a switch to constantly change with the updates from the broadcast frames, resulting in MAC database instability.

Issues with Layer 1 Redundancy: Broadcast Storms

- A broadcast storm occurs when there are so many broadcast frames caught in a Layer 2 loop that all available bandwidth is consumed. It is also known as denial of service
- A broadcast storm is inevitable on a looped network
 - As more devices send broadcasts over the network, more traffic is caught within the loop; thus consuming more resources
 - This eventually creates a broadcast storm that causes the network to fail

Issues with Layer 1 Redundancy: Duplicate Unicast Frames

- Unicast frames sent onto a looped network can result in duplicate frames arriving at the destination device
- Most upper layer protocols are not designed to recognize, or cope with, duplicate transmissions
- Layer 2 LAN protocols, such as Ethernet, lack a mechanism to recognize and eliminate endlessly looping frames

Issues with Layer 1 Redundancy: Duplicate Unicast Frames

Feszítőfa protokoll – STP működése

- 1. A hálózat összes kapcsolója közül egy kitüntetett kapcsoló (Root Bridge) kiválasztása
- 2. A root kapcsolón kívül minden kapcsolón, kapcsolónként ki kell választani azt a portot amelyiken át a Root kapcsoló a legjobb útvonalon érhető el (Root port)
- 3. minden hálózati szegmensen szegmensenként ki kell választani azt a portot amelyiken át a szegmens a legjobb útvonalon éri el a Root Bridge-et (Designated Port)

Miért kell elosztott működés?

- Külső szemlélő szempontjából (centralizált irányítással) nem bonyolult az STA algoritmus végrehajtása
 - Kívülről a teljes állapotter jól követhető
 - A teendők egyszerű szabályokkal leírhatók
- A centralizált irányítás azonban
 - Csak korlátolt bővíthetőséget biztosít
 - Csak irreális komplikációval és magas költséggel oldható meg

Az elosztott működés lényege

- A LAN kapcsolók egyike sem ismeri a teljes hálózat topológiáját és állapotterét
- A kapcsolók között olyan belső kommunikációra van szükség amely követni tudja a teljes LAN állapotváltozásait
- A kapcsolók a társaiktól kapott információ alapján önállóan és valós időben döntenek, hogy az eseményekre miként reagáljanak
- Fontos elvárás: a hurokképződést még tranzien állapotban sem szabad megengedni

Fa szerkezet kialakításának elsődleges paraméterei

- Bridge ID
- Path cost



Link Speed	Cost (Revised IEEE Spec)	Cost (Previous IEEE Spec)
10 Gbps	2	1
1 Gbps	4	1
100 Mbps	19	10
10 Mbps	100	100

802.1d BPDU szerkezeti felépítése

Bytes	
2	Always zero
1	Always zero
1	Configuration (0x00) or TCN BPDU (0x80)
1	LSB = Topology change flag (TC), MSB = TC Ack flag (TCA)
8	Who is Root Bridge?
4	How far away is Root Bridge?
8	ID of bridge that sent this BPDU
2	Port-ID of sending bridge (unique: Port1/1=0x8001, 1/2=0x8002, ...)
2	Time since Root generated this BPDU
2	BPDU is discarded if older than this value (default: 20 seconds)
2	Broadcast interval of BPDUs (default: 2 seconds)
2	Time spent in learning and listening states (default: 15 seconds)

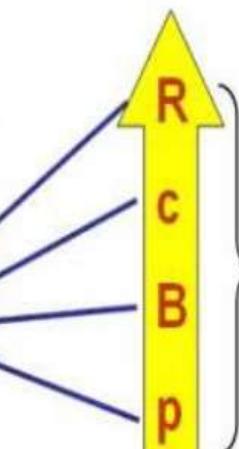
Annotations:

- A TCN-BPDU only consists of these 3 fields !!!
- When first booted, Root-ID == BID
- If value increases, then the originating bridge lost connectivity to Root Bridge
- Predetermined by root bridge
- Affect convergence time
- Misconfigurations cause loops

- BPDUs are sent in 802.3 frames
 - DA = 01-80-C2-00-00-00
 - LLC has DSAP=SSAP = 0x42 ("the answer")
- Configuration BPDUs
 - Originated by Root Bridge periodically (2 sec Hello Time), flow downstream

BPDU prioritás vektor

Bytes	Field
2	Protocol ID
1	Version
1	Message type
1	Flags
8	Root ID
4	Cost of path
8	Bridge ID
2	Port ID
2	Message age
2	Max age
2	Hello time
2	Forward delay



Ezen mezők tartalmát egy 22 bájt hosszúságú egész számként kezeli az STA. Ez az egész szám a **prioritás vektor**. A vektor MSB-je a Root ID MSB-je, LSB je a Port ID LSB-je

Hogyan használja a prioritás vektorokat?

- A kiválasztás során a prioritás vektorokat hasonlítja össze az STA
- minden esetben a kisebb értékű vektor nyer

Az STP kiválasztási folyamata

- **Root Bridge:** az a kapcsoló amely a legjobb prioritás vektorú BPDU-t küldi a többiek felé
 - **Designated Port:** egy szegmens (LAN) azon portja amely a legjobb prioritás vektorú BPDU-t küldi az adott szegmensre
 - **Root Port:** nem root kapcsolók azon portja amely a legjobb prioritás vektorú BPDU-t veszi
 - **Blocked Port:** nem Root, nem Designated (**alternate** vagy **backup**)
- 

23-24. VIRTUÁLIS LAN HÁLÓZATOK (VLAN-OK), TRÖNKPROTOKOLL

Virtuális LAN

A VLAN-ok létrehozásának okai

- A gépeket csoportosíthatjuk szervezeti egység szerint, közös alkalmazások használata szerint
- A szórásokat kordában tarthatjuk. A szórások nem jutnak át másik VLAN-ba
- A hálózat biztonsága növelhető. Adatkapcsolati rétegen a különböző VLAN-okba tartozó gépek nem kommunikálhatnak egymással

A VLAN-ok jellemzői

- Virtuális LAN-okat a kapcsolókban konfigurálás révén hozzuk létre
- A kapcsoló bizonyos portjait az egyik VLAN-hoz, más portjait egy másik VLAN-hoz rendeljük, stb.
- Az egyes VLAN-okhoz rendelt gépek azonos IP hálózathoz (alhálózathoz) tartoznak, azaz IP címük hálózati része azonos
- A VLAN-ok között a kapcsolóban nincs átjárás. Sem az egyedi címmel ellátott (unicast), sem a szórásos, sem az elárasztásos keretek nem jutnak át
- VLAN-ok között csak forgalomirányítóval teremthetünk kapcsolatot, ugyanúgy, mint a valódi LAN-ok között

A VLAN-ok közötti kommunikáció

- Különböző VLAN-ok között forgalomirányítóval teremthető kapcsolat
- A forgalomirányítóban megfelelő védelmi mechanizmusokat lehet alkalmazni, amellyel szabályozzuk a VLAN-ok közötti forgalmat (hozzáférési listák)

Portok VLAN-okhoz rendelése

- Statikus
- Statikus hozzárendelés esetén konfiguráljuk, hogy melyik port, melyik VLAN-ba tartozzon
- Dinamikus
- Dinamikus hozzárendelés esetén egy VLAN felügyeleti szerverben (többnyire egy erre alkalmas kapcsoló) előre rögzítjük, hogy a különböző MAC című készülékek melyik VLAN-ba tartozzanak
- A készülékek tetszőleges portra csatlakoztathatók
- Az első keret küldésekor a kapcsoló a szerverhez fordul, lekéri az adott MAC című eszköz VLAN azonosítóját, ezután a kapcsoló portját a megadott VLAN-ba sorolja
- Ezzel a gépek tetszőleges porthoz csatlakoztathatók, VLAN hozzárendelésük nem változik

VLAN típusok funkció alapján

- Data VLAN
- Default VLAN
- Native VLAN
- Management VLAN

VLAN tartományok

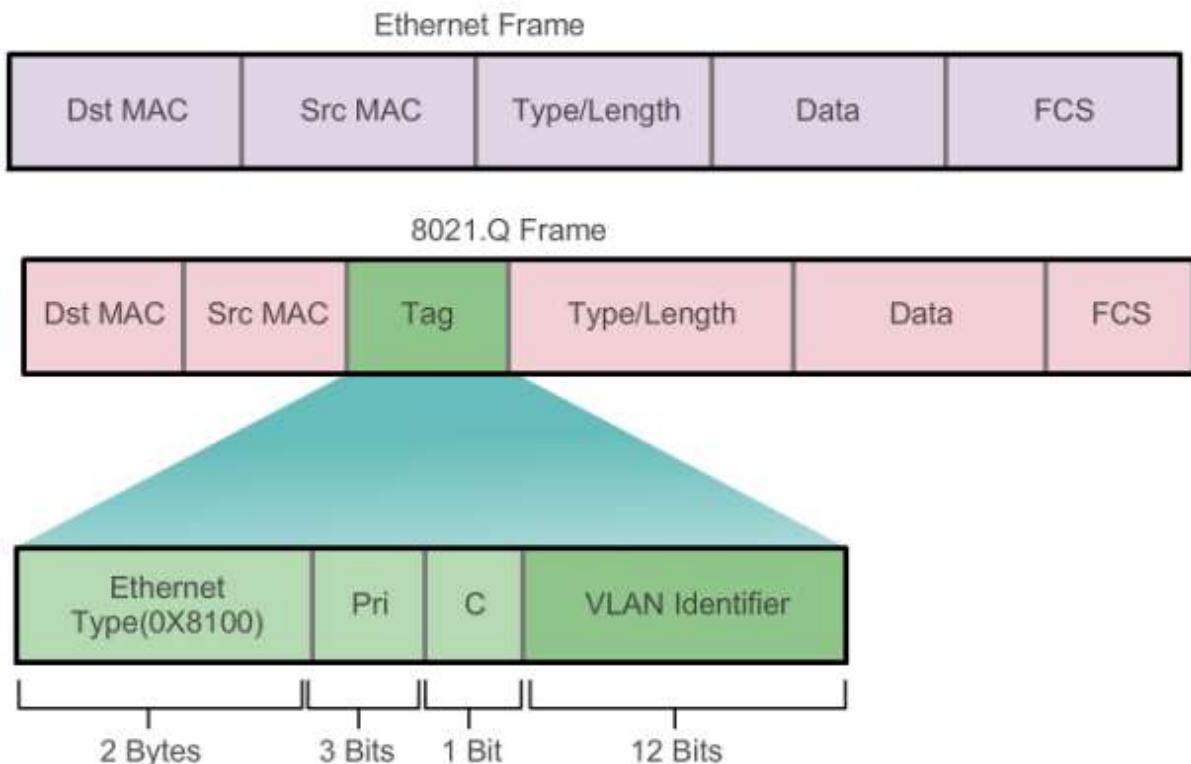
VLANs are split into two categories:

- Normal range VLANs
 - VLAN numbers from 1 to 1,005
 - Configurations stored in the vlan.dat (in the flash memory)
 - VTP can only learn and store normal range VLANs
- Extended Range VLANs
 - VLAN numbers from 1,006 to 4,096
 - Configurations stored in the running configuration (NVRAM)
 - VTP does not learn extended range VLANs

Több kapcsolóra kiterjesztett VLAN-ok: Trunk (trönk)

- A VLAN-ok több kapcsolóra is kiterjedhetnek
- Az ábrán a VLAN 1-be és a VLAN 2-be tartozó gépek minden kapcsolón jelen vannak
- A kapcsolókat trönk portokon keresztül kapcsoljuk össze
- Egyes kapcsolótípusoknak csak kitüntetett portjai (pl. nagyobb sebességű portok), másoknak valamennyi portja konfigurálható trönk portként
- A trönk portok egyik VLAN-ba sem tartoznak, alapesetben az összes VLAN forgalmát továbbítják. Általában konfigurálható, hogy mely VLAN-okat továbbítsák
- A trönk vonalon áthaladó kereteket a kapcsoló címével látja el, amely tartalmazza a keret VLAN azonosítóját is. (A másik kapcsolónak tudnia kell, hogy a keret melyik VLAN-ba tartozik)
- Amíg a keret a gerinchálózaton (trönkön) halad a címke a kereten marad, mi helyt a kapcsoló a keretet egy nem trönk porton küldi ki, eltávolítja a VLAN címét
- A trönk protokoll szabványos: IEEE 802.1Q (dot1q). A különböző gyártók kapcsolói így együttműködhetnek
- Más nem szabványos gyári protokollok is léteznek (pl. Cisco ISL)
- A több kapcsolóra kiterjesztett VLAN-ok előnye, hogy a helytől függetlenül csoporthoz köthető a munkaállomásokat VLAN-okba Ha pl. a VLAN 1 hálózatból egy munkaállomást át kell helyezni egy másik épületbe, a kapcsolónak egy portját a másik épületben a VLAN 1-hez kell rendelni, a munkaállomás megtarthatja az IP címét
- Ha egy állomást másik VLAN-ba kell tennünk, IP címét a másik hálózatból kell adnunk
- A Spanning Tree Protocol-t minden VLAN-ra külön kell alkalmazni

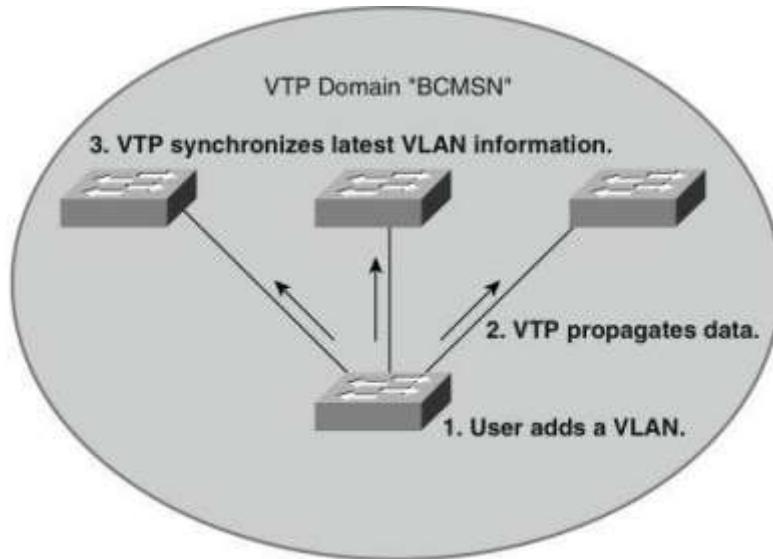
Keret címkézése



VLAN-ok közötti forgalomirányítás

- A VLAN-ok között forgalomirányítóval lehet adatot cserélni
- Használhatnánk minden VLAN-ra külön-külön forgalomirányító-portot. Ez nem gazdaságos sok VLAN esetén
- A forgalomirányító portjait is lehet trónkként konfigurálni.
Alinterfészket kell létrehozni egy fizikai interfészen, és az egyes alinterfészket a VLAN-okhoz rendelni
- Az alinterfészeknek ez esetben saját VLAN-beli IP címet kell adnunk

VLAN Trunking Protocol (VTP)



- VTP is a Cisco-proprietary protocol that automates the propagation of VLAN information between switches via trunk links. This minimizes misconfigurations and configuration inconsistencies.
- VTP does not configure switch ports for VLAN membership
- Three types of VTP messages are sent via Layer 2 multicast on VLAN 1
- VTP domains define sets of interconnected switches sharing the same VTP configuration

VTP Modes

Client

- Cannot create, change, or delete VLANs on command-line interface (CLI)
- Forwards advertisements to other switches
- Synchronizes VLAN configuration with latest information received from other switches in the management domain
- Does not save VLAN configuration in nonvolatile RAM (NVRAM)

Server

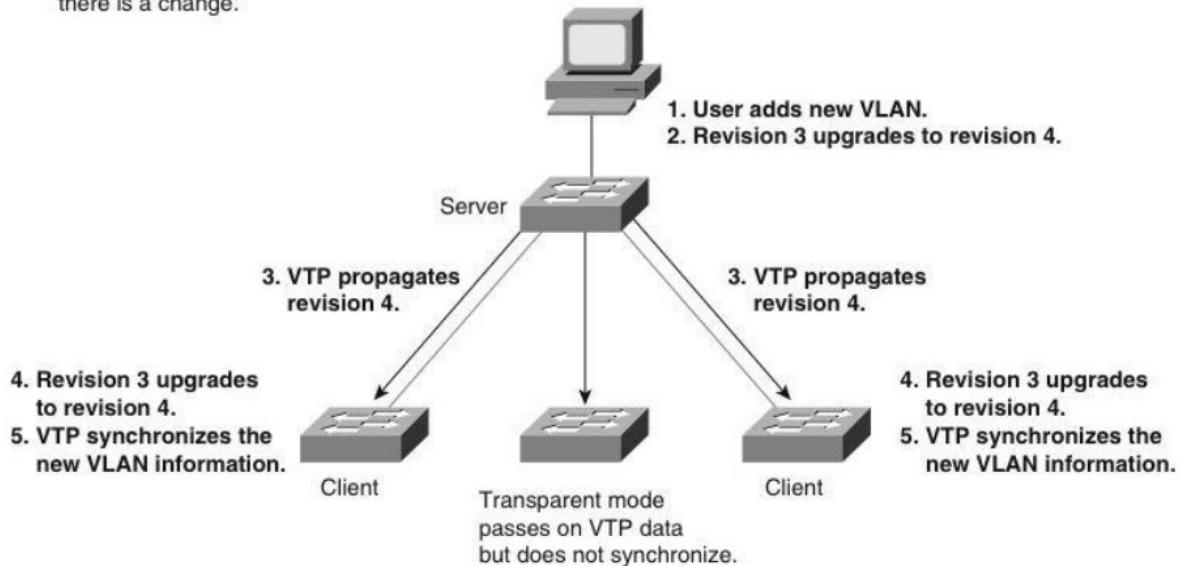
- Can create, modify, and delete VLANs
- Sends and forwards advertisements to other switches
- Synchronizes VLAN configuration with latest information received from other switches in the management domain
- Saves VLAN configuration in NVRAM

Transparent

- Can create, modify, and delete VLANs only on the local switch
- Forwards VTP advertisements received from other switches in the same management domain
- Does not synchronize its VLAN configuration with information received from other switches in the management domain
- Saves VLAN configuration in NVRAM

VTP operations

VTP advertisements are sent as multicast frames.
VTP servers and clients are synchronized to the latest revision number.
VTP advertisements are sent every 5 minutes or when there is a change.



Jellemzők

- Three VTP versions: V1, V2, V3
- Versions are not interoperable (e.g., V2 supports token ring VLANs but V1 does not)
- V1 transparent switches inspect VTP messages for the domain name and version and forward a message only if the version and domain name match
- V2 transparent switches forward VTP messages in transparent mode without checking versions

- Support for extended VLANs (1025 to 4094)
 - Support for the creation and advertising of Private VLANs
 - Improved server authentication
 - Enhancements to a mechanism for protection from the “wrong” database accidentally being inserted into a VTP domain
 - Interaction with VTP versions 1 and 2
 - Configurable on a per-port basis

VTP Message Types

- Summary Advertisements
 - By default, Catalyst switches issue summary advertisements in 5-minute increments. Summary advertisements inform adjacent switches of the current VTP domain name and the configuration revision number.
 - When the switch receives a summary advertisement packet, the switch compares the VTP domain name to its own VTP domain name. If the name is different, the switch ignores the packet. If the name is the same, the switch then compares the configuration revision to its own revision. If its own configuration revision is higher or equal, the packet is ignored. If it is lower, an advertisement request is sent
- Subset Advertisements
 - When you add, delete, or change a VLAN, the VTP server where the changes are made increments the configuration revision and issues a summary advertisement. One or several subset advertisements follow the summary advertisement
 - A subset advertisement contains a list of VLAN information. If there are several VLANs, more than one subset advertisement can be required to advertise all the VLANs
- Advertisement Requests
 - A switch issues a VTP advertisement request in these situations:
 - The switch has been reset
 - The VTP domain name has been changed
 - The switch has received a VTP summary advertisement with a higher configuration revision than its own
 - Upon receipt of an advertisement request, a VTP device sends a summary advertisement
 - One or more subset advertisements follow the summary advertisement

VTP Authentication

VTP domains can be secured by using the VTP password feature. It is important to make sure that all the switches in the VTP domain have the same password and domain name; otherwise, a switch will not become a member of the VTP domain. Cisco switches use MD5 to encode passwords in 16-byte words. These passwords propagate inside VTP summary advertisements. In VTP, passwords are case-sensitive and can be 8 to 64 characters in length. The use of VTP authentication is a recommended practice.

By default, a Catalyst switch does not have a VTP password. The switch does not automatically set the password parameter, unlike other parameters that are set automatically when a VTP advertisement is received.

DTP (Dynamic Trunking Protocol)

By default DTP is enabled and the interfaces of your switches will be in “dynamic auto” or “dynamic desirable” mode. This means that whenever you receive a DTP packet that requests to form a trunk, your interface will be in trunk mode.

There are two ways to disable DTP negotiation:

- Configure the interface for access mode
- Use the switchport nonegotiate command on the interface

25. LAN REDUNDANCIA ÉS LINK ÖSSZEFOGÁS

LAN redundancy

Default Gateway Limitations

If the default gateway cannot be reached, the local device is unable to send packets off the local network segment.

Even if a redundant router exists that could serve as a default gateway for that segment, there is no dynamic method by which these devices can determine the address of a new default gateway.

Static Default Gateway

- Not dynamic.
- Does not provide secondary path.

Router Redundancy

- Multiple routers are configured to work together to present the illusion of a single router to the hosts on the LAN.
- The ability of a network to dynamically recover from the failure of a device acting as a default gateway is known as firsthop redundancy.

First-Hop Redundancy Protocols

- Hot Standby Router Protocol (HSRP)
- HSRP for IPv6
- Virtual Router Redundancy Protocol version 2 (VRRPv2)
- VRRPv3
- Gateway Load Balancing Protocol (GLBP)
- GLBP for IPv6
- ICMP Router Discovery Protocol (IRDP)

Hot Standby Router Protocol (HSRP)

- Cisco-proprietary gateway redundancy protocol.
- Participating routers talk to each other and agree on a virtual router with a virtual IP and a virtual MAC addresses which end systems use as a default gateway

HSRP Failover

- When active router or links between routers fail, the standby router stops seeing hello messages from active router. Standby router then assumes role of forwarding router.
- Because new forwarding router assumes both IP and MAC address of virtual router, end stations see no disruption in service.

HSRP Operation

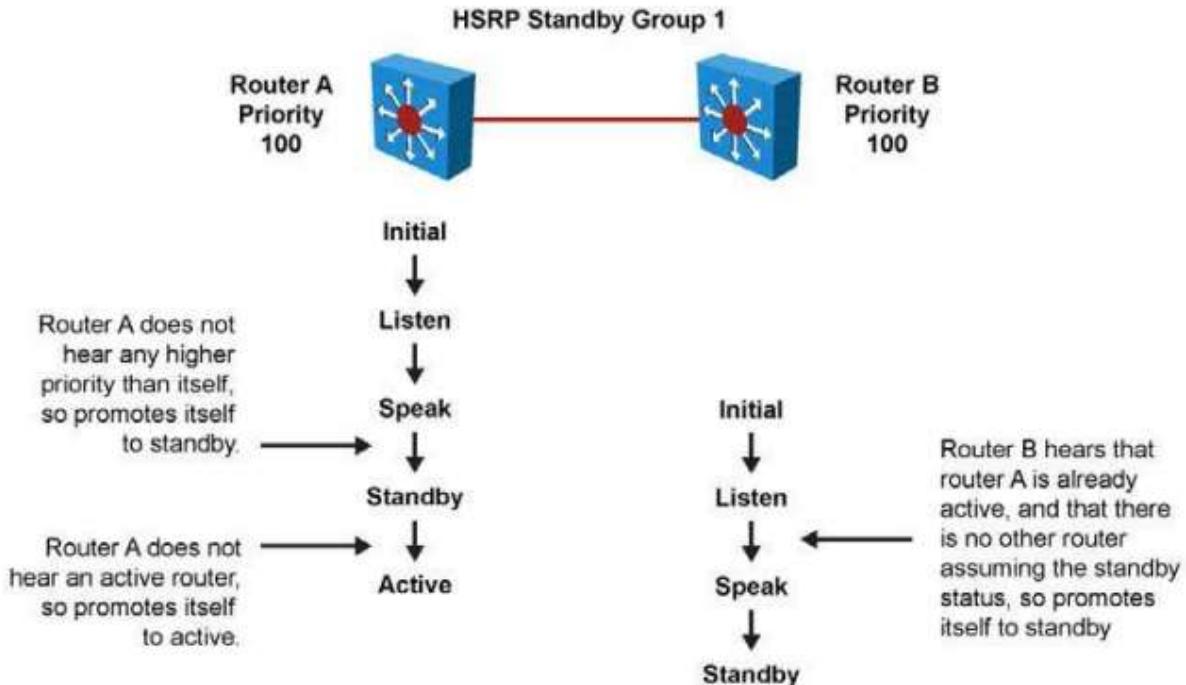
- HSRP active and standby routers send hello messages to multicast address 224.0.0.2 UDP port 1985.
- Hello messages used to communicate between routers within the HSRP group.
- All routers in HSRP group need to be L2- adjacent
- All routers in an HSRP group have specific roles and interact in specific ways:
 - Virtual router
 - Active router
 - Standby router
 - Other routers

HSRP States

State	Definition
Initial	The beginning state. The initial state indicates that HSRP does not run. This state is entered via a configuration change or when an interface first comes up.
Listen	The router knows the virtual IP address, but the router is neither the active router nor the standby router. It listens for hello messages from those routers.
Speak	The router sends periodic hello messages and actively participates in the election of the active or standby router. A router cannot enter speak state unless the router has the virtual IP address.
Standby	The router is a candidate to become the next active router and sends periodic hello messages. With the exclusion of transient conditions, there is, at most, one router in the group in standby state.
Active	The router currently forwards packets that are sent to the group virtual MAC address. The router sends periodic hello messages. With the exclusion of transient conditions, there must be, at the most, one router in the active state in the group.

HSRP State Transition

- Router A starts. As it is the first router for standby Group 1 in the subnet, it transits through the listen and speak states and then becomes the active router
- Router B starts after Router A. While Router B is in listen state, Router A is already assuming the standby and then the active role. As there is already an existing active router, Router B assumes the standby role



HSRP Active Router and Spanning Tree Topology

- In a redundant spanning-tree topology, some links are blocked. The spanningtree topology has no awareness about the HSRP configuration. There is no automatic relationship between the HSRP active router election process and the Spanning Tree Root Bridge election.
- When configuring both spanning tree and HSRP (or any other first hop redundancy protocol), you must make sure that the active router is the same as the root bridge for the corresponding VLAN. When the root bridge is different from the HSRP active router, a suboptimal path can result, as illustrated.

HSRP Versions

- HSRP version 1 is the default in IOS and it enables group numbers up to 255. Because one can have up to 4095 VLANs, one has to reuse the same HSRP group number on multiple interfaces if needed. This is allowed even though it might cause some confusion.
- HSRP version 2 has been added to IOS since 12.2 46SE or later and it enables group numbers up to 4095. This enables you to use the VLAN number as the group number.

- With HSRPv2, the MAC address of the virtual router and the multicast address for the hello messages has been changed. The virtual MAC address is 0000.0C9F.FXXX (XXX=HSRP group), and hello packets are sent to multicast address 224.0.0.102
- Also, HSRPv2 has a different packet format from HSRPv1. Ensure that the same version is configured on all routers in a HSRP group. Otherwise hello messages are not understood. Version 1 is the default.

EtherChannel Technology

- Up to 8 physical links can be bundled into a single logical EtherChannel link.
- Usually EtherChannel is used for trunk links.
- Configuration applied to port channel interface affects all physical interfaces assigned to the port channel.
- Load balancing takes place between the physical links in an EtherChannel.
- EtherChannels can be L2 or L3 interfaces.

EtherChannel Management Protocols

- Port Aggregation Protocol (PAgP)** is a Cisco-proprietary protocol that aids in the automatic creation of Fast EtherChannel links.
 - When an EtherChannel link is configured using PAgP, PAgP packets are sent between Fast EtherChannel-capable ports to negotiate the forming of a channel. (30 sec)
 - When PAgP identifies matched Ethernet links, it groups the links into an EtherChannel. Spanning tree adds the EtherChannel as a single bridge port
- Link Aggregation Control Protocol (LACP)** is part of an IEEE specification (802.3ad) that also enables several physical ports to be bundled together to form an EtherChannel.
 - LACP enables a switch to negotiate an automatic bundle by sending LACP packets to the peer
 - It performs a similar function as PAgP with Cisco EtherChannel
 - Because LACP is an IEEE standard, you can use it to facilitate EtherChannels in mixed-switch environments. In a Cisco environment, both protocols are supported

26. KÜLSŐ ÁTJÁRÓ PROTOKOLL

- **Interior gateway protocol (IGP)**
 - AS-en (Autonomous System) belül működik
 - RIP, OSPF, IS-IS, EIGRP
- **Exterior gateway protocol (EGP)**
 - Különböző autonóm rendszerek között működik

Autonomous Systems (AS)

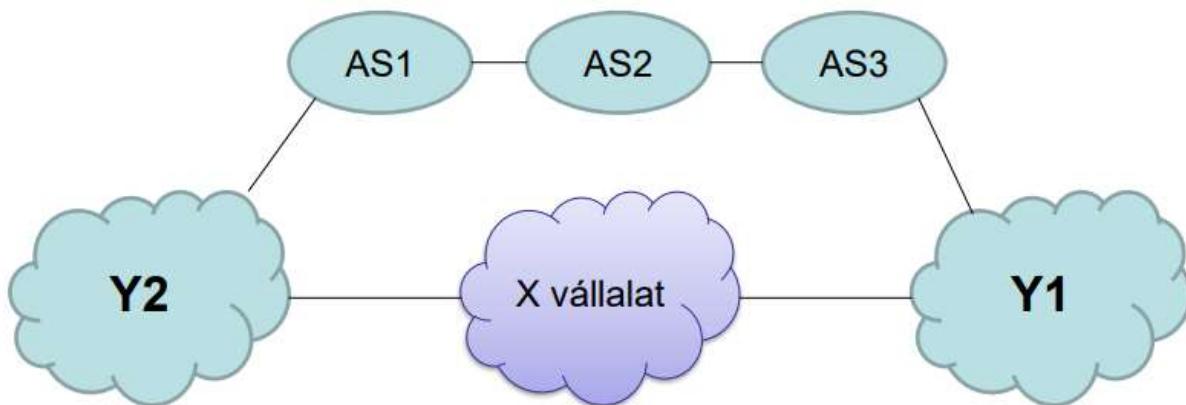
- Közös adminisztrációs és forgalomirányítási szabályozás alá eső forgalomirányítók (hálózatok) csoportja
- Általában egyetlen szervezethez tartozik (ISP, vállalat, stb.)
- Internet Assigned Numbers Authority (IANA) felügyeli

AS Numbers

- 1 - 65,535
 - RIR-ek kezelik 1 - 64,512.
 - 64,512 - 65,535 privát
 - Kevésnek bizonyult
 - IETF BGP kiterjesztések definiál, amiket a 4893-as és az 5398 RFC ír le és az AS számot 16 bitesről 32 bitesre terjeszt ki

Miért van rá szükség?

- Házirend alapú
- Redundancia esetén kezeli a kapcsolatokat



Connection Redundancy

- Single-homed
- Multihomed
- Dual-homed
- Dual-multihomed

Using BGP in an Enterprise Network

- External BGP (EBGP) különböző AS forgalomirányítói között
- Internal BGP (IBGP) azonos AS forgalomirányítói között

EBGP szomszédság követelményei

- Szomszédság felépítése:
 - TCP kapcsolat kell hozzá
 - Nem automatikus (manuálisan kell konfigurálni)
- Elérhetőség:
 - Általában közvetlen csatlakozás van közöttük
- Különböző AS szám

IBGP szomszédság követelményei

- Szomszédság felépítése:
 - TCP kapcsolat kell hozzá
 - Nem automatikus (manuálisan kell konfigurálni)
- Elérhetőség:
 - A szomszédoknak IGP-n keresztül kell elérhetőnek lenni (nem közvetlenül!)
 - Loopback IP cím az azonosító
- Azonos AS szám:
 - IBGP neighbors must have the same AS number

BGP jellemzők

- Külső átjáró protokoll, RFC 4971
- 4-es verzió van érvényben
- TCP 179-es port
- CIDR és VLSM támogatás
- Útvonal vektor (path vector) alapú ~ távolság vektor
 - Útvonal-paramétereket használ → attribútumok
- Házirend-alapú (policy-based)
- Nem rendel költséget az útvonalakhoz, hanem az attribútumok segítségével leírja
- Hurokmentes forgalomirányatás
 - Látóhatár megosztás (split horizon)
 - Útvonalmérgezés (route poisoning)

BGP működés – üzenetek

- Szomszédsági viszonyokra épül, amit manuálisan kell beállítani (neighbors vagy peer)
- TCP felett épül ki → a BGP egyszerűbb, nem foglalkozik az összeköttetéssel és a nyugtákkal
- OPEN üzenettel bemutatkoznak (verzió, AS szám, azonosító, időzítő, stb.)
- A terjesztésre szánt útvonalaiat megosztják egymással (UPDATE)
- Eseményvezérelt frissítéseket küldenek
- Hiba esetén NOTIFICATION üzenetet küldenek
- Ha nincs más üzenet, ébrenláti üzeneteket küldenek (KEEPALIVE üzenet)

BGP Tables

- Neighbor table
 - List of BGP neighbors
- BGP table (forwarding database)
 - List of all networks learned from each neighbor
 - Can contain multiple paths to destination networks
 - Contains BGP attributes for each path
- IP routing table
 - List of best paths to destination networks

BGP Üzenet típusok

Open Message

16	2	1	1	2	2	4	1	7
Marker	Length	Type	Version	AS	Hold Time	BGP ID	Optional Length	Optional

TCP felépülése után az első üzenet → „bemutatkozás”

- Verzió: verziószám (4-es)
- AS: saját AS szám
- Hold Time: milyen időközönként kell a szomszédtól üzenetet kapni (sec)
- ID: BGP forgalomirányító azonosítója
- Opt. Length: opcionális paraméter mező hossza
- Opt: opcionális paraméterek listája

Update Message

16	2	1	2	Variable	2	Variable	Variable
Marker	Length	Type	Unfeasible Routes Length	Withdrawn Routes	Attribute Length	Path Attributes	NLRI

- A BGP ezt használja útvonalak hirdetésére vagy kivonására
- Segítségükkel feltérképezi a hurokmentes AS-ek közötti kapcsolatokat reprezentáló gráfot
- Egy üzenet egy útvonalra vonatkozó attribútumokat tartalmazza
- Az alábbi információkat tartalmazhatja
 - Elérhetetlenné vált útvonalak
 - Útvonal attribútumok
 - Network-layer reachability information (NLRI)
 - Azoknak az IP prefixeken a lista, amelyek az adott útvonalon elérhetők

Notification Message

16	2	1	1	1	Variable
Marker	Length	Type	Error Code	Error Sub-code	Diagnostic Data

- A BGP notification message is sent when an error condition is detected
 - The BGP connection is closed immediately after this is sent
- Notification messages include an error code, an error subcode, and data related to the error

Keepalive Message Type

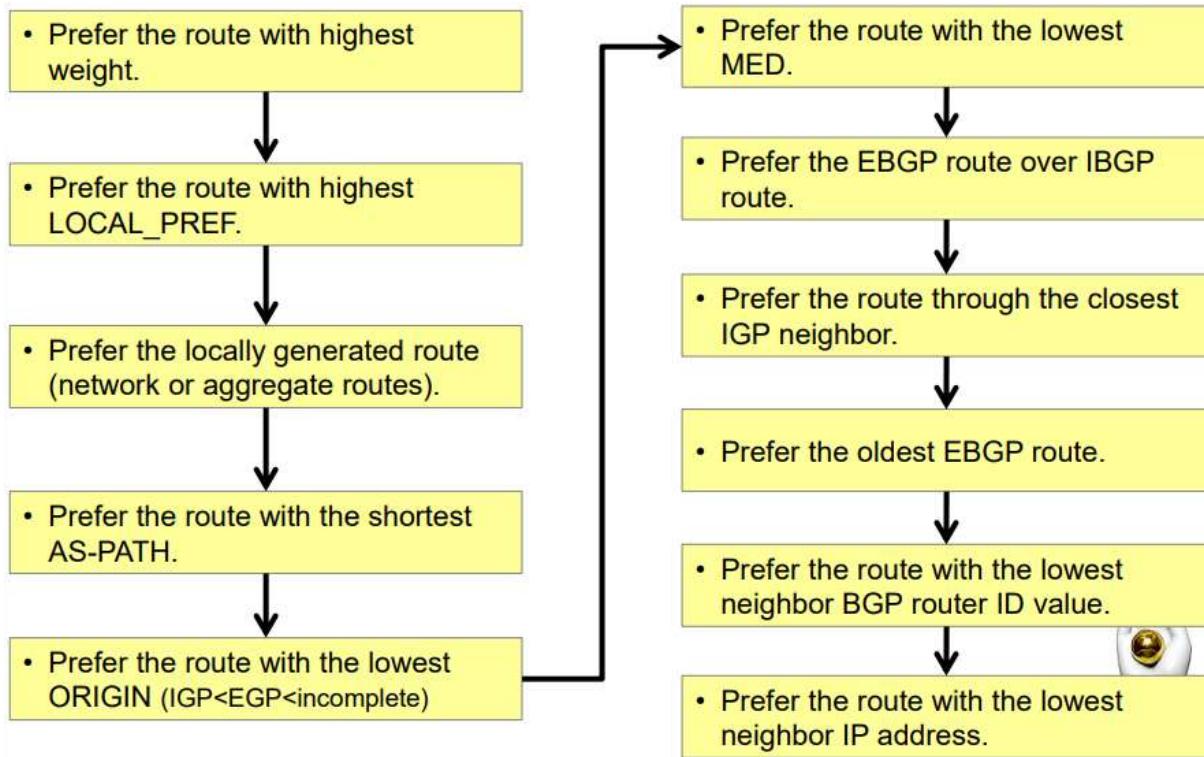
16	2	1
Marker	Length	Type

- Keepalive messages are sent between peers every 60 seconds (by default) to maintain connections
- The message consists of only a message header (19 bytes)
 - Hold time is three times the KEEPALIVE timer of 60 seconds
 - If the periodic timer = 0, no keepalives are sent
 - Recommended keepalive interval is one-third of the hold time interval

Útvonal attribútumok

- A legjobb útvonal kiválasztásához szükséges
- Egy útvonal vektor kötelező attribútumai:
 - ORIGIN: azt tárolja, hogyan értesültek először az útvonalról (IGP-től, EGP-től vagy egyéb), értékét az első BGP router állítja be, aki az útvonalat a többiekkel megosztotta
 - AUTONOM SYSTEM PATH: Egy adott hálózathoz vezető teljes útvonalon az összes AS száma
 - NEXT-HOP: a következő forgalomirányító IP címe

BGP útválasztás folyamata



BGP States

- BGP is a state machine that takes a router through the following states with its neighbors:
 - Idle
 - Connect
 - Open sent
 - Open confirm
 - Established
- The Idle state begins once the neighbor command is configured

27. SZOLGÁLTATÁSMINŐSÉG

Előzmény

Jó minőségű szolgáltatás érdekében eddig torlódáskezelési és hálózati teljesítőképesség növelési mechanizmusokat használtunk

Réteg	Politikák
Szállítási	<ul style="list-style-type: none">• Újraadási politika• Sorrenden kívül érkezett csomagok tárolási politikája• Nyugtázási politika• Forgalomszabályozási politika• Időzítés meghatározása
Hálózati	<ul style="list-style-type: none">• Az alhálózaton belül virtuális áramkörök vagy datagramok• Csomag-sorbaállítási és kiszolgálási politika• Csomageldobási politika• Forgalomirányító algoritmus• Csomagélettartam menedzselés
Adatkapcsolati	<ul style="list-style-type: none">• Újraadási politika• Sorrenden kívül érkezett csomagok tárolási politikája• Nyugtázási politika• Forgalomszabályozási politika

Probléma

Egy hálózat fontosabb mérőszámai:

- Sávszélesség (Mbit/s)
- Késleltetés (ms)
- Csomagvesztés (megbízhatóság)
- Késleltetés ingadozás – jitter

Ezeket az átviteli közeg, az áthidalandó távolság és a hálózati eszközök együttesen határozzák meg (szűk keresztmetszet)

Nem érint minden szolgáltatást, (pl. file átvitelnél vagy böngészés), de valós idejű alkalmazásoknál nagyon fontos: VoIP, IPTV, TelePresence

Túlméretezés (overprovisioning)

A szolgáltatásminőség biztosításának szempontjai

1. Milyen alkalmazásokra van szüksége a hálózatnak?
2. Hogyan szabályozható a hálózatba belépő forgalom?
3. Hogyan tarthatók fenn erőforrások az útválasztón a teljesítőképesség garantálásához?
4. Biztonságosan tud-e fogadni a hálózat további forgalmat?

Queuing – Várakozási sorok

Amikor a forgalom nagyobb, mint amit egy hálózat továbbítani tud, az eszközök várakozási sorokba rendezik a csomagokat és szükség szerint várakoztatják mindaddig, míg szabad erőforrás nem lesz a továbbításhoz

- Nő a csomagok késleltetése
- Ha a sorok megtelnek, csomagvesztés lép fel

Torlódási pontok

Egy interfészen torlódás lép fel, amikor nagyobb a forgalom, mint amennyit az interfész továbbítani tud

- késleltetés
- késleltetés ingadozás
 - a torlódási pontokon QoS mechanizmus szükséges

A csomagkésleltetés különböző okai

Delay	Description
Code delay	The fixed amount of time it takes to compress data at the source before transmitting to the first internetworking device, usually a switch.
Packetization delay	The fixed time it takes to encapsulate a packet with all the necessary header information.
Queuing delay	The variable amount of time a frame or packet waits to be transmitted on the link.
Serialization delay	The fixed amount of time it takes to transmit a frame from the NIC to the wire.
Propagation delay	The variable amount of time it takes for the frame to traverse the links between the source and destination.
De-jitter delay	The fixed amount of time it takes to buffer a flow of packets and then send them out in evenly spaced intervals.

QoS nélkül...

... a hálózati eszközök a csomagokat érkezésük sorrendjében dolgozzák fel. Torlódás esetén a forgalomirányítók és a kapcsolók eldobják a csomagokat.

- TCP, UDP?
- TIME SENSITIV TRAFFIC? → RTP (Real-time Transport Protocol)

QoS eszközök

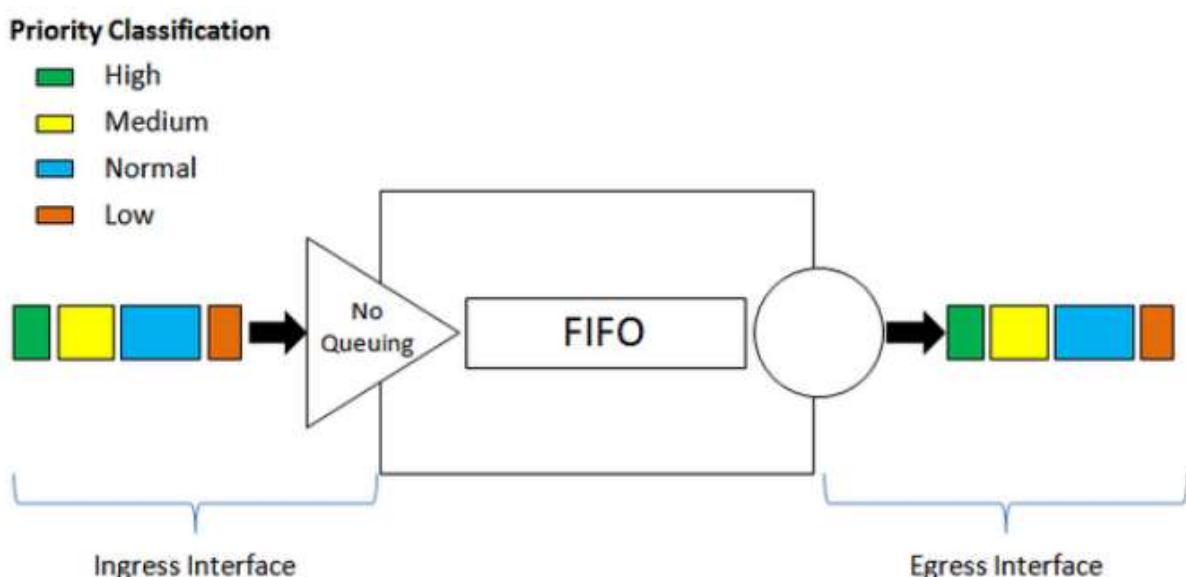
- Sorbanállási algoritmusok – Queuing algorithm
- Forgalomformálás – Traffic shaping
- Osztályozás és megjelölés – Classification and marking
- Belépés-engedélyezés – Admission Control
- Rendfenntartás – Policy

Queuing algorithm – várakozási sor kezelő algoritmusok

A QoS szabályok – melyeket a hálózat üzemeltetője előzetesen beállított – akkor lépnek életbe, amikor a hálózat egy pontján torlódás jelentkezik. Az egyik torlódás kezelő mechanizmus a várakozási sorok használata, melyekbe a csomagokat besorolják, prioritást kaphatnak és szükség esetén újra rendezhetik őket a továbbítás előtt.

- First-In, First-Out (FIFO)
- Weighted Fair Queueing (WFQ)
- Priority Queueing (PQ)
- Class-Based Weighted Fair Queueing (CBWFQ)
- Low Latency Queueing (LLQ)

FIFO



Fair Queuing (WFQ)

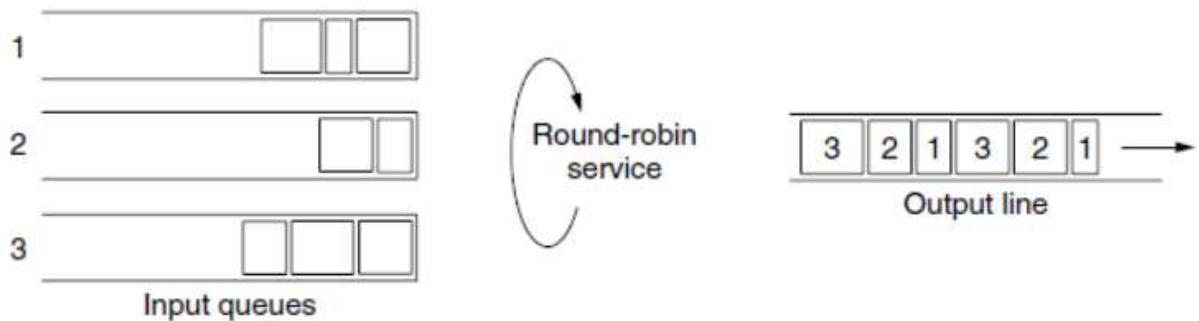
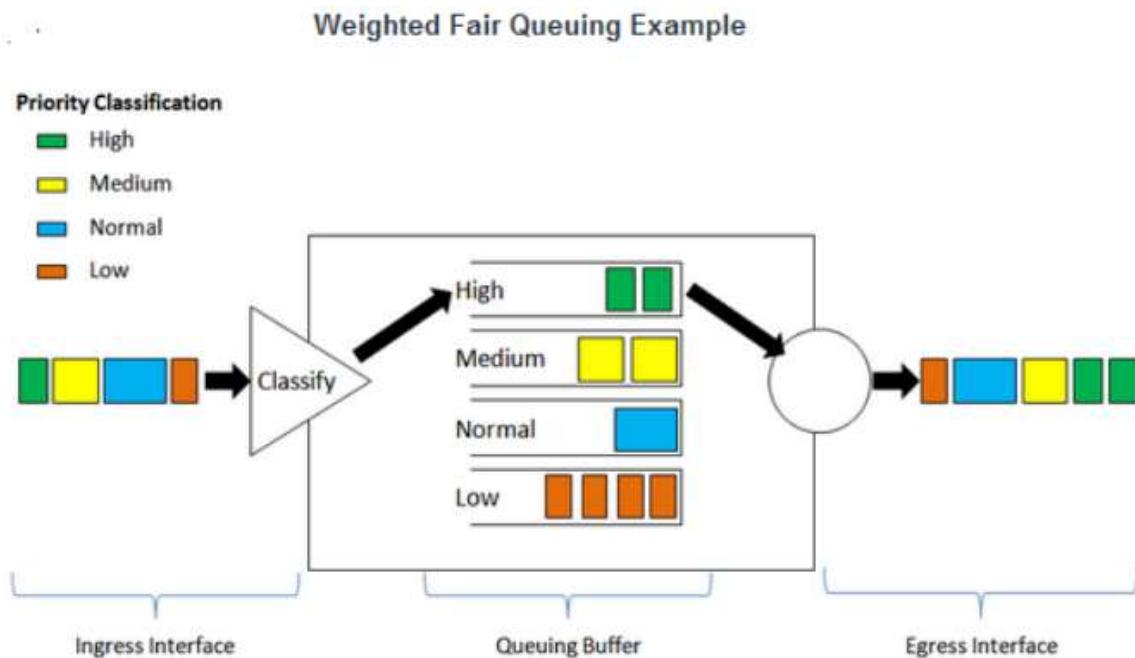


Figure 5-30. Round-robin fair queuing.

Weighted Fair Queuing (WFQ)

Priority Queuing (PQ)



Class-Based Weighted Fair Queuing (CBWFQ)

Először az adat a felhasználó által definiált osztályok szerint csoportosítva lesz, majd az osztályokon belül súly szerint sorba lesznek állítva

Low Latency Queuing (LLQ)

Az előző mellett van egy fontos sor is.

Lyukas és Vezérjeles Vödör - Leaky and Token Buckets

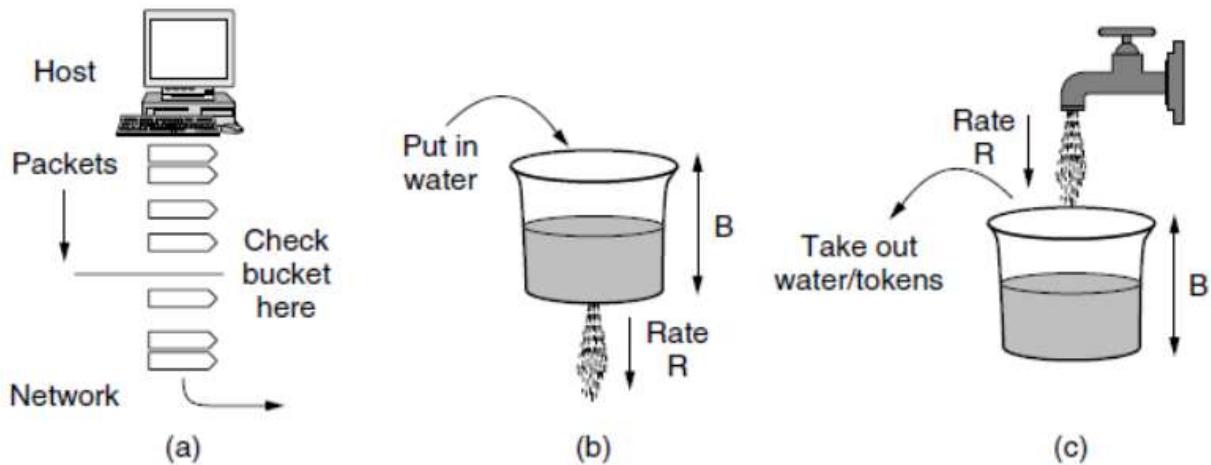


Figure 5-28. (a) Shaping packets. (b) A leaky bucket. (c) A token bucket.

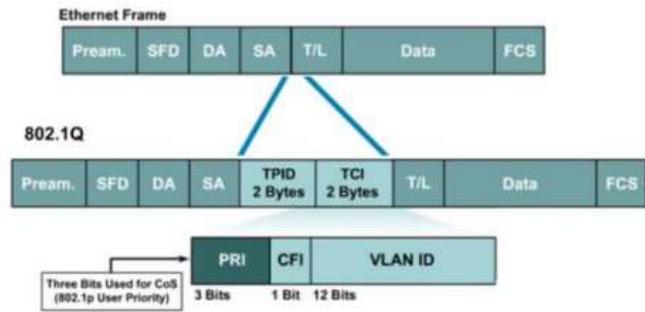
Classification and Marking

- Layer 2 marking of frames can be performed for non-IP traffic
- Layer 2 marking of frames is the only QoS option available for switches that are not “IP aware”
- Layer 3 marking will carry the QoS information end-to-end

L2 marking

Ethernet Class of Service (CoS) Values

Value	Description
7	Reserved
6	Reserved
5	Voice bearer (voice traffic)
4	Videoconferencing
3	Call Signaling
2	High-Priority Data
1	Medium-Priority Data
0	Best-Effort Data



L3 marking

- IPv4: Type of Service
- IPv6: Traffic Class

Congestion Avoidance

RED – Random Early detection

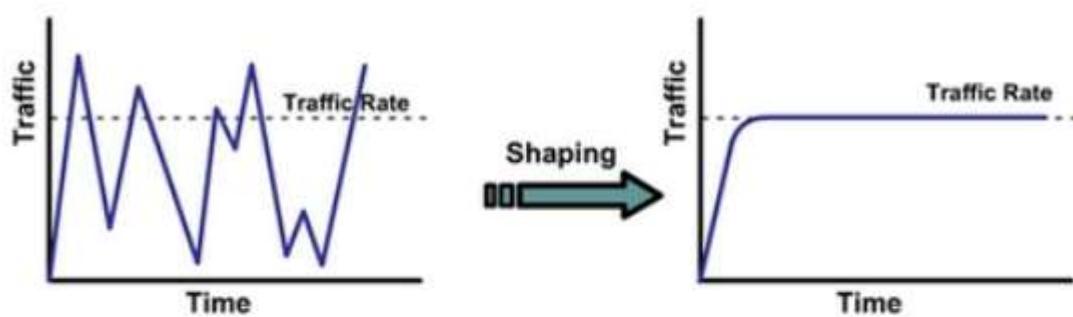
véletlenszerűen dobja el a csomagokat még komolyabb torlódás kialakulása előtt

WRED – Weighted Random Early Detection

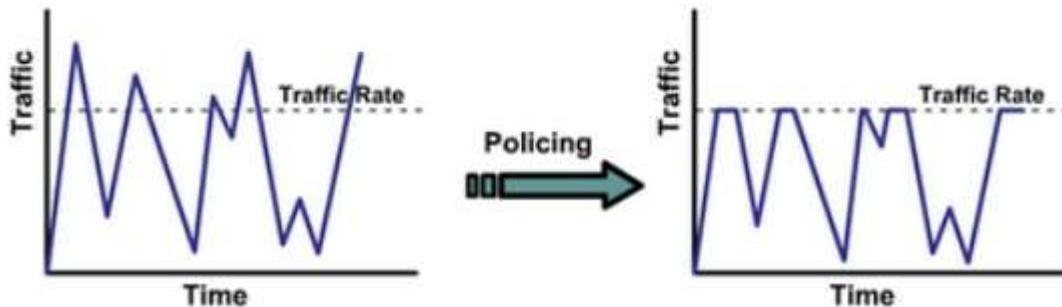
IP precedenciával kiegészített RED

Forgalomformálás (Shaping) és rendfenntartás (policing)

Shaping Traffic Example



Policing Traffic Example



QoS models

Best-Effort

Benefits	Drawbacks
<ul style="list-style-type: none">The model is the most scalable.Scalability is only limited by bandwidth limits, in which case all traffic is equally affected.No special QoS mechanisms are required.It is the easiest and quickest model to deploy.	<ul style="list-style-type: none">There are no guarantees of delivery.Packets will arrive whenever they can and in any order possible, if they arrive at all.No packets have preferential treatment.Critical data is treated the same as casual email is treated.

IntServ - Integrated Services (Integrált szolgáltatások)

- Végpontól-végpontig terjedő QoS szolgáltatás, amit az alkalmazások tudnak igénybe venni
- Hozzáférési hálózatban működik
- Összeköttetés alapú
- Feladatai:
 - Erőforrás-lefoglalás – RSVP – Resource Reservation Protocol
 - kijelöli az útvonalat a hálózatban a forrástól a célig és szállítja a QoS paramétereket
 - Befogadás-engedélyezés (Admission Control)
 - meghatározza a hálózati eszközökön fellépő erőforrás-igények kielégíthetőségét
 - Forgalomszabályozás (Traffic Control)
 - kikényszeríti a lefoglalt minőségi paramétereket

A teljes útvonalon minden eszköznek támogatnia kell az RSVP-t a lefoglaláshoz, különben a kapcsolat nem épül fel!

RSVP - Resource Reservation Protocol

- L4 protokoll
- Forrás kezd – path
- Cél – reserve

Az internetes forgalom leírására az IntServ (és az RSVP) három szolgáltatási osztályt határoz meg:

- Guaranteed Service – garantált szolgáltatás
- Controlled Load Service – ellenőrzött terhelésű szolgáltatás
- Best Effort Service – legjobb szándékú szolgáltatás

Ellenőrzött terhelésű szolgáltatás

Biztosítja, hogy az elsőbbséget élvező csomagok minimális várakozási idő elteltével sorra kerüljenek az útválasztó sorokban, így viszonylag gyorsabban át tudnak haladni a hálózaton. A csomagkésleltetési idő és a csomagvesztés kicsi, viszont a kiválasztott csomagok szempontjából a Controlled Load Service ugyanolyan, mint a Best Effort. Erős forgalom esetén, ahol több nagyobb elsőbbséget élvező csomag is sorban áll és a kisebb prioritású csomagok elenyészően kevesen lettek (mert már „fel lettek áldozva”), még a nagy elsőbbséget élvező csomagok is elveszhetnek.

Garantált szolgáltatás

A garantált szolgáltatás kizárolag csak a maximális késleltetés értékét biztosítja. Ezt úgy kell érteni, hogy a szolgáltatási szint nem szabályozza sem a minimális-, sem az ingadozó (jitter) késleltetést. Az erőforrás lefoglalást végző RSVP protokoll lefoglalja a sávszélesség egy adott részét, és addig nem ejt ki egyetlenegy csomagot sem, amíg a forgalom túl nem lépi a lefoglalt sávszélesség szabta határokat. Így tudja a késleltetést biztosítani a csomagok számára. A teljes körű szolgáltatás megvalósításához a hálózati forgalomban részt vevő összes elemnek támogatnia kell a szolgáltatást, ellenkező esetben a garancia nem tartható.

Előnyök és hátrányok

Benefits	Drawbacks
<ul style="list-style-type: none">• Explicit end-to-end resource admission control• Per-request policy admission control• Signaling of dynamic port numbers	<ul style="list-style-type: none">• Resource intensive due to the stateful architecture requirement for continuous signaling.• Flow-based approach not scalable to large implementations such as the Internet.

DiffServ – Differentiated Services (Megkülönböztetett szolgáltatások)

- Osztályalapú szolgáltatásminőség
- Egy adminisztratív körzetbe tartozó forgalomirányítók kínálhatják
- Működés:
 - Minőségi osztályokat definiál
 - A különböző osztályokhoz kiszolgálási elveket határoz meg
- viselkedési csoportok (BA, Behaviour Aggregate)
 - ugyanazzal a DSCP-vel rendelkező csomagokat gyűjtő össze
- ugrásonkénti viselkedés (PHB, Per Hop Behaviour)
 - szolgáltatási osztályok → továbbítási szabály

PHB Category	Description
Default Best effort	<ul style="list-style-type: none"> • Used for best-effort service. • Left-most DSCP bits equal 000xxx
Expedited Forwarding (EF) Gyorsított továbbítás	<ul style="list-style-type: none"> • Used for low-delay service providing a low-loss, low-latency, low-jitter, and assured bandwidth service for applications such as voice and video. • Left-most DSCP bits equal 101xxx
Assured Forwarding (AF) Biztosított továbbítás	<ul style="list-style-type: none"> • Used for guaranteed bandwidth service. • It defines 4 sub-classes (AF1, AF2, AF3, and AF4). • Left-most DSCP bits equal 001xxx, 010xxx, 011xxx, or 100xxx
Class Selector Csoport választó	<ul style="list-style-type: none"> • Used for backward compatibility with non-DiffServ-compliant devices • Bits 2 to 4 of DSCP equal xxx000.

www.uni-obuda.hu

Az Edge/Border router folyamonkénti (per flow) forgalommenedzselést végez. Fő feladatai:

- Befogadás-engedélyezés
- Megjelölés (marking): a beérkező csomagokat megjelölése;
- Rendtartás (policing): a szerződésekben lefektetettek betartatása

Az Interior/core router osztályonként menedzseli a forgalmat:

- A széleken megjelölt prioritásnak megfelelően továbbítja a csomagokat

Benefits	Drawbacks
<ul style="list-style-type: none"> • Highly scalable • Provides many different levels of quality 	<ul style="list-style-type: none"> • No absolute guarantee of service quality • Requires a set of complex mechanisms to work in concert throughout the network

28. HÁLÓZATFELÜGYELET

nem láttam, hogy le lett volna adva

Bevezetés a hálózatfelügyeletbe

Minél több hálózati erőforrás érhető el a felhasználók számára, annál bonyolultabbá válik a hálózat, és karbantartása is egyre nehezebb lesz.

Feladatok

- A hálózat elérhetőség figyelése
- Az automatizálás fokozása
- A válaszidő figyelése
- Biztonsági funkciók nyújtása
- A forgalom átirányítása
- Helyreállítási lehetőségek
- Felhasználók regisztrálása
- **A vállalati vagyon ellenőrzése**
- **A bonyolultság kézben tartása**
- **A szolgáltatások továbbfejlesztése**
- **A különböző igények kiegyensúlyozása**
 - A felhasználóknak különféle alkalmazásokat kell biztosítani, meghatározott támogatási szinttel, illetve megadott teljesítménybeli, rendelkezésre állási és biztonsági elvárásokat teljesítve.
- **A leállási idők csökkentése**
 - Megfelelő redundancia betervezése
- **A költségek kézben tartása** elfogadható költség mellett is kielégítő szintű szolgáltatások

Alapvető fogalmak

- SNMP: Az egyszerű hálózatfelügyelő protokoll az IETF szabványa a hálózati erőforrások felügyeletére
- MIB: A felügyeleti információs adatbázis egy felügyelt objektum adatdefiníciója és struktúrája
- RMON: A távoli felügyelet egy MIB/ügynök specifikáció, amely távoli készülékek figyeléséhez definiál funkciókat.

Az OSI és a hálózat felügyeleti modell



SNMP (Simple Network Management Protocol)

- SNMP a hálózatfelügyeleti szabványok egész gyűjteménye
- alkalmazott protokollra, adatbázis szerkezetének megadására, az adatobjektumok leírására egyaránt kiterjed
- Az SNMP-t 1989-ben fogadták el. SNMP 2c 1993-ban a központosított és az elosztott hálózatfelügyeleti módszereket egyaránt támogatja
- SNMPv3 biztonsági kérdések megoldása érdekében a hálózaton keresztül továbbított csomagok hitelesítésével és titkosításával foglalkozik

Az SNMP működése

Alkalmazási rétegbeli protokoll –feladata a felügyeleti adatcserék lebonyolítása

- Felügyelő állomás (NMS)
- Felügyeleti ügynökök
- Felügyeleti információs bázis (MIB)
- Hálózat-felügyelő protokoll

Az NMS általában egy különálló munkaállomás, de több rendszerre is kiterjedhet network management application, NMA szoftvert futtat. Válaszol a felhasználó parancsaira, és a hálózaton keresztül utasításokkal látja el a felügyeleti ügynököket.

Az ügynökök válaszolnak az NMS-től érkező információkérésekre fontos, adott esetben kérés nélkül továbbított adatokkal, például csapdákkal látják el az NMS-t.

Az ügynök lehetőségei:

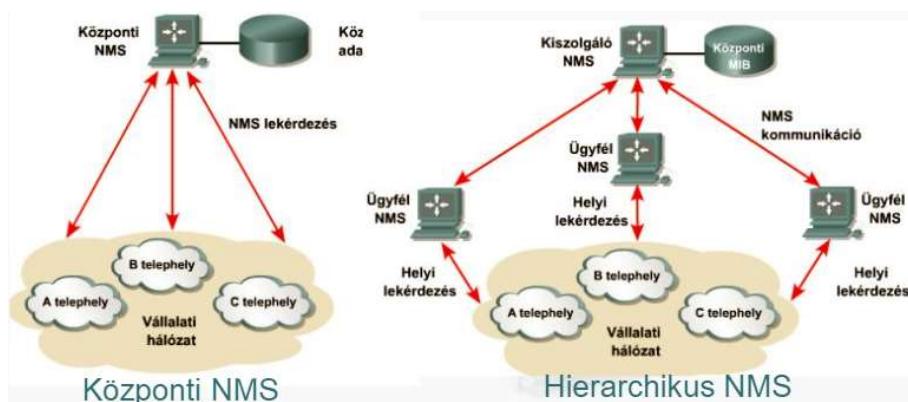
- Saját virtuális áramköreinek száma és állapota
- Megadott típusú beérkező hibaüzenetek száma
- A készülék által elküldött és fogadott bajtok száma
- Forgalomirányítók és más hálózat-összekapcsoló készülékek esetén a kimeneti várakozási sor maximális hossza
- Elküldött és fogadott szórásos üzenetek
- A hálózati interfések leállása és elindulása
- A felügyelő és az ügynökök közötti kommunikáció egy alkalmazási rétegbeli felügyeleti protokoll segítségével folyik. Az SNMP UDP-t használ, az üzenetek küldését és fogadását a 161-es és a 162-es porton keresztül végzi
- Get (Lekérdezés)–Segítségével a felügyelő állomás MIB objektumok értékeit kérdezheti le az ügynöktől.
- Set (Beállítás)–Segítségével a felügyelő állomás beállíthatja az ügynök által kezelt MIB objektumok értékeit.
- Trap (Csapda)–Segítségével az ügynök értesítheti a felügyelő állomást a fontosabb eseményekről

Agent szerepe:

- Amikor a hálózat felügyeletét végző állomás egy egyedi felügyeleti felülettel rendelkező készülékkel szeretne kommunikálni, akkor egy proxy ügynök segítségét veszi igénybe
- A felügyelő SNMP kérését fordítja le a célrendszer által fogadható formába
- A hálózat-felügyeleti alkalmazások bizonyos felügyeleti funkciókat gyakran egy távoli felügyeleti (remote monitor, RMON) szondának adnak ki
- Az RMON szonda helyben gyűjt felügyeleti adatokat, ezek összegzését a hálózat-felügyelő rendszeres időközönként lekérdezi tőle

Felügyeleti állomás (NMS)

- Az NMS egy normál munkaállomás, amely valamelyen hétköznapi operációs rendszert futtat.
- A hálózat-felügyeleti alkalmazás a gazda operációs rendszer szolgáltatásaira és kommunikációs képességeire támaszkodik
- Az elosztott NMS-ek ügyfél-kiszolgáló rendszerben működhetnek

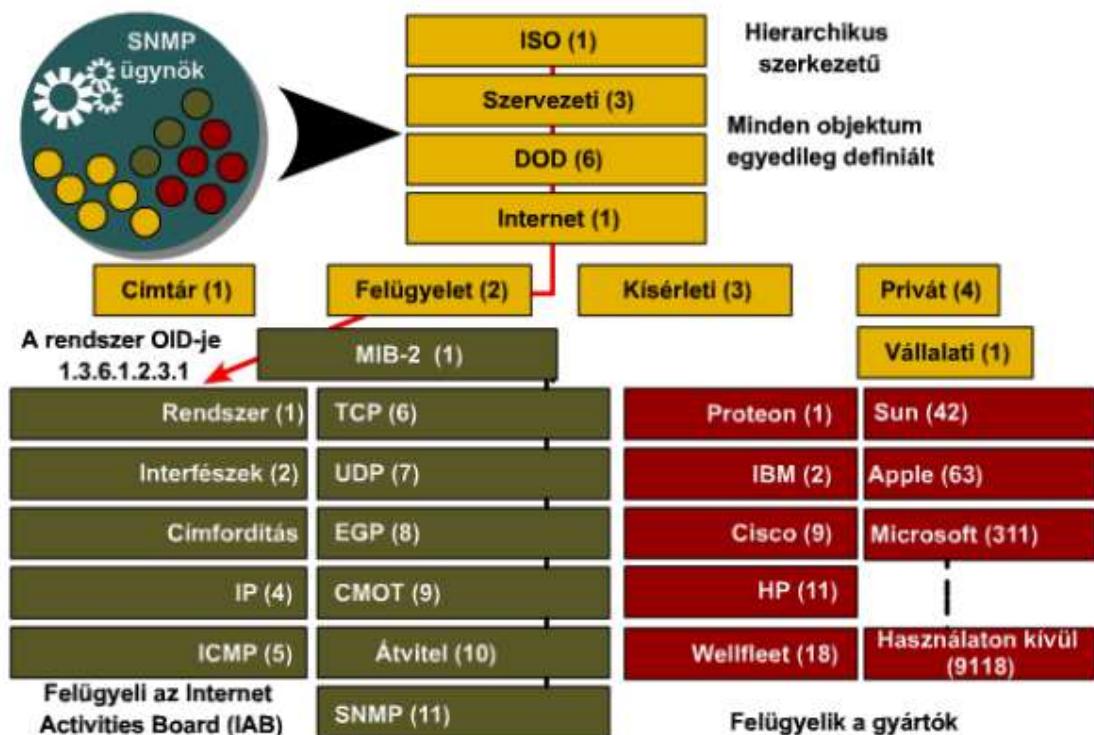


A felügyeleti információk és a MIB-ek szerkezete

- A MIB feladata a hálózati elemeket és a jellemzőiket leíró strukturált információk tárolása. (A struktúrát az SMI szabvány írja le)
- Az SMI megadja, az adattípusokat, az objektumok elnevezését, illetve hogyan kell a hálózati átvitel előtt kódolni őket. A MIB-ek az egyes készülékekéről erősen strukturált adatokat tárolnak



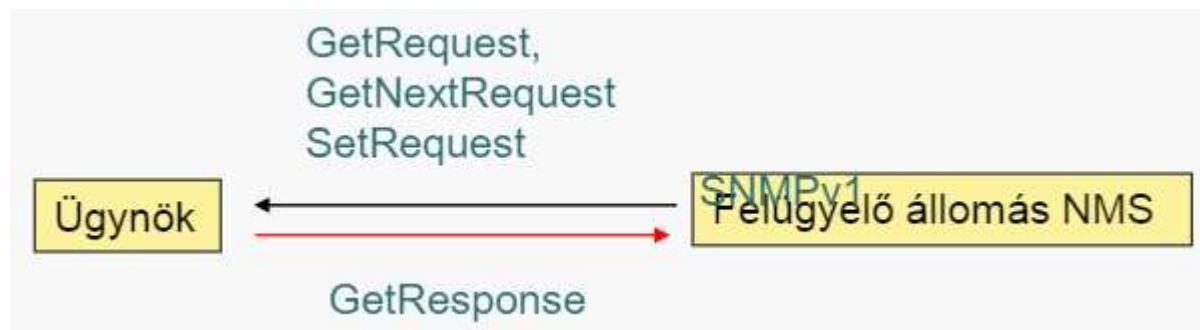
Minden felügyelt objektuma egy hierarchikus szerkezetbe, fa struktúrába kerül.



az ábra alján jelennek meg, a ténylegesen felügyelt objektumok. A felügyelt objektumok pontozott formában írt egyedi azonosítókkal rendelkeznek. A MIB-definíciók közzététele minden gyártóról elvárható.

Az SNMP protokoll

- Probléma
 - Ügyfelek szórással keresnek DHCP kiszolgálót
 - Ügyfél és kiszolgáló nem ugyanazon szórási tartományban van
- Megoldás
 - minden szegmensbe DHCP kiszolgáló telepítése
 - Segédcím használata
- Segédcím szerepe
 - UDP alapú szolgáltatások szórásos kéréseinek fogadása, majd egyedi címzésű továbbítása
- Használható forgalmak
 - Idő, TACACS, DNS, BOOTP/DHCP, TFTP, Netbios
- Az ügynök egy szoftveres funkció, amely a legtöbb hálózati készülékben megtalálható. Felelős a felügyelőtől érkező SNMP-kérések feldolgozásáért, feladata a MIB-ekben található változókat karbantartó eljárások futtatása
- A felügyelő és az ügynök közötti párbeszéd lebonyolítása az SNMP segítségével történik. A simple szó az elnevezésben arra utal, hogy a protokoll eredeti specifikációjában csak korlátozott számú üzenettípus definíciója szerepel.

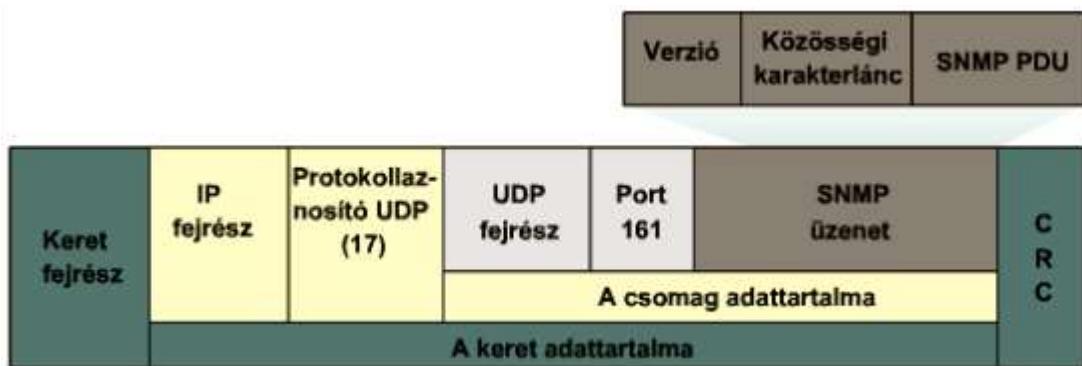


Az NMS-ek nevében háromféle SNMP-üzenetet lehetett elküldeni, ezek a GetRequest, a GetNextRequest és a SetRequest.

Az ügynökök mindenkorban mindenütt egy GetResponse üzenettel nyugtázzák SNMPv2c GetBulkRequest bevezetését MIB 64 bites számlálókkal való bővítése volt.

- A 64 bites számlálók bevezetése a nagysebességű, például Gigabit Ethernet összeköttetések esetében volt problémás
- A felügyeleti entitást felügyelőnek vagy NMS-nek nevezzük. Feladata az ügynökök adatainak lekérdezése
 - A kapott adatok későbbi elemzés céljából naplózhatók
 - grafikus segédprogrammal megjeleníthetők
 - illetve előre meghatározott értékekkel összevethetők; utóbbi annak ellenére alkalmas, hogy megadott feltételek teljesülnek-e
- A felügyeleti funkciók képesek bizonyos beállítási értékeket megváltoztatni

- Így a rendszergazda távolról konfigurálhatja az eszközöket



- A túl agresszív megfigyelési módszerek kedvezőtlenül befolyásolják a hálózat teljesítményét
- Általános szabály, hogy a lehető legkevesebb információt és a lehető legritkábban kell lekérdezni
- Minden SNMP-üzenet tartalmaz egy nyílt szövegben továbbított karakterláncot, ez a közösségi karakterlánc -egyfajta jelszóként viselkedik
- A protokollkészlet minden mezője nyílt szöveget tartalmaz, kivéve a hitelesítési és titkosítási funkciókat
- Minden SNMP alapú felügyeleti alkalmazásban be kell állítani a megfelelő közösségi karakterláncot!

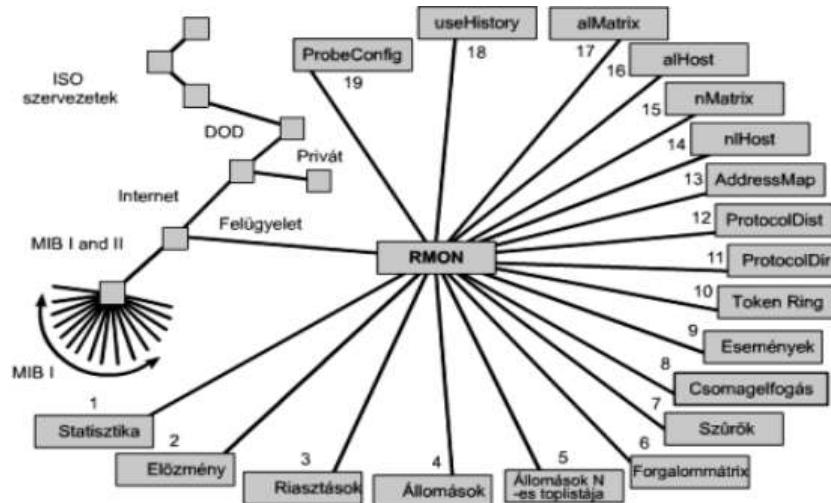
RMON

Az RMON egy távoli felügyelő MIB-et definiál, amely a MIB-II kiegészítéseként szolgál, és fontos információkkal látja el a rendszergazdát a hálózattal kapcsolatban.

Minden készüléken külön SNMP ügynök fut.

A felügyelő lekérdezheti az ügynökök értékeit de a MIB-II segítségével nem tud átfogó képet alkotni róluk.

A felhasználók által definiált riasztások hozhatók létre, amelyeket a RMON-nak adnak át, segítve ezzel a statisztikák központi létrehozását.



A szondák a központi felügyeleti állomással, az ügyféllel SNMP-n keresztül tartják a kapcsolatot.

- Statisztikai csoport–A megfigyelt alhálózat vagy szegmens használati és hibastatisztikáit tartalmazza. Ide tartozik például a sávszélesség használata, a szórásos és a többes címzéses forgalom, a CRC-hibák, a töredékek stb
- Előzmény csoport–Szabályos időközönként mintákat vesz a statisztikai csoport adataiból, és későbbi visszakeresés céljából tárolja őket. Ide tartozik például a kihasználás, a hibaszám és a csomagszám
- Riasztás csoport–Segítségével a rendszergazda mintavételezési időközöket és küszöbértékeket adhat meg az ügynök által vizsgált értékekhez. Példaként abszolút és viszonylagos értékek és emelkedési vagy csökkenési határértékek említhetők
- Állomás csoport–A hálózathoz csatlakozó állomásokról kiinduló és a hozzájuk befutó forgalom mérését határozza meg. Ilyen például az elküldött és a fogadott csomagok, a hibák, a szórásos és a többes címzéses csomagok száma
- Állomások N toplistája–N állomásból álló toplista, amely az állomás csoport statisztikái alapján áll elő
- Forgalommátrix csoport–A hálózat egymással forgalmazó állomás páraihoz tartozó hiba- és használati statisztikákat tárolja. Példa: hibák, bájtok és csomagok
- Szűrő csoport–Szűrőmotor, amely a felhasználó által megadott mintával egyezést mutató csomagokból külön adatfolyamot állít elő
- Csomagelfogó csoport–Megadja, hogy a szűrési feltételek megfelelő csomagok belső pufferelése hogyan történjen
- Esemény csoport–Lehetővé teszi az események, más néven a létrejött csapdák időponttal és dátummal együtt történő naplázását a felügyelő számára. Példa: a riasztás típusa alapján testreszabott jelentések

Syslog

- A rendszeresemények naplázása általában a rendszer konzoljára történik, amíg ezt a funkciót le nem tiltjuk
- A syslog protokoll segítségével a Cisco készülékek ilyen kérés nélkül továbbított üzeneteket küldhetnek egy megadott hálózatfelügyelő állomásnak
- minden syslog üzenet egy időbélyeggel, egy berendezésnévvel, egy fontossági mérőszámmal és egy szöveges üzenettel kiegészítve kerül naplózásra
- A fontossági szint azt jelzi, hogy a hibaüzenet mennyire komoly hibáról tájékoztat. A fontossági szintet egy 0 és 7 közötti szám adja meg
- Cisco IOS alapesetben a 6-os fontossági szintet használja
- A syslog használatát konfigurálni kell!

Fontossági szintek

1. Vész helyzet
2. Riasztás
3. Kritikus
4. Hiba
5. Figyelmeztetés
6. Értesítés
7. Tájékoztatás
8. Hibakeresés

29. A HÁLÓZATI ESZKÖZÖK EGYEDI VÉDELME

Hálózatbiztonság „definiálása”

- Jogosulatlan hozzáférés észlelése és megakadályozása a hálózati eszközök, ill. hozzájuk csatlakozó rendszerekhez és végberendezésekhez
- Ez minden magában foglal: Jogosulatlan hozzáférés kapcsolók portjaihoz , vagy akár jogosulatlan forgalom akár bentről akár kinatról, rosszindulatú programok, stb...

Tudásmegosztás

- indicators of compromise (IOC) – egy támadás egyedi, megkülönböztető leírója
- Indicators of attack (IOA) egy támadás startégiájának egyedi, megkülönböztető leírója

Biztonsági alapelvek

Hálózati biztonsági alapelvek:

- Confidentiality – adatok kiszivárgásának megakadályozása → titkosítás
- Integrity – Sérültlenség → integritást védő algoritmusok
- Availability – rendelkezésre állás
 - Hálózati eszközök és adatok elérhetősége
 - Authentication – hitelesítés

Védekezési technikák

Határvédelem (perimeter defence)

Régi gondolkodásmód, elavult eljárás

Ma már nem elég, ha a rendszerünk határán ellenőrizzük milyen hálózati forgalom engedélyezett vagy blokkolt

Mélységi védelem (defence in dept)

A mai kornak jobban megfelel ez a koncepció, amely szerint többrétegű biztonsági ellenőrzéseket kell üzembe helyezni az egész informatikai rendszerben

például: antivirus, kétfaktoros authentikáció, DMZ, tűzfalak, behatolás érzékelő és megelőző rendszerek, naplózó és ellenőrző rendszerek, fizikai védelem, VPN, homokozó, proxy, biometria, idő alapú hozzáférés, stb...

→ Security operation Center

A biztonság (védelem) megteremtése

- Hitelesítés, Jogosultságkezelés, naplózás
- Titkosítás
- Tűzfalak
- IDS, IPS
- VPN-ek
- Sérülékenységek javítása
- Log- és forgalomelemzésen alapuló behatolás detektálás

A támadás fajtái

Aktív

A támadás folyamán aktívan beavatkozik a hálózati forgalomba. Belebeszél, módosít, esetleg csomagokat eltávolít.

- Spoofing (átejtés)
- DoS támadások
- DDoS támadások
- Jelszavakat érintő támadások
- Man-in-the-Middle attack
- Kártékony kódok

Olyan alkalmazások, programok, scriptek, amelyek megsértik a biztonsági házirendet és a rendszer sérülékenységéhez vezethetnek, akár a felhasználó tudta és beavatkozása nélkül.

- Vírusok
- Férgek
- Trójaiak
- Spywarek
- Keyloggerek
- Backdoorok
- Botnetek

Passzív

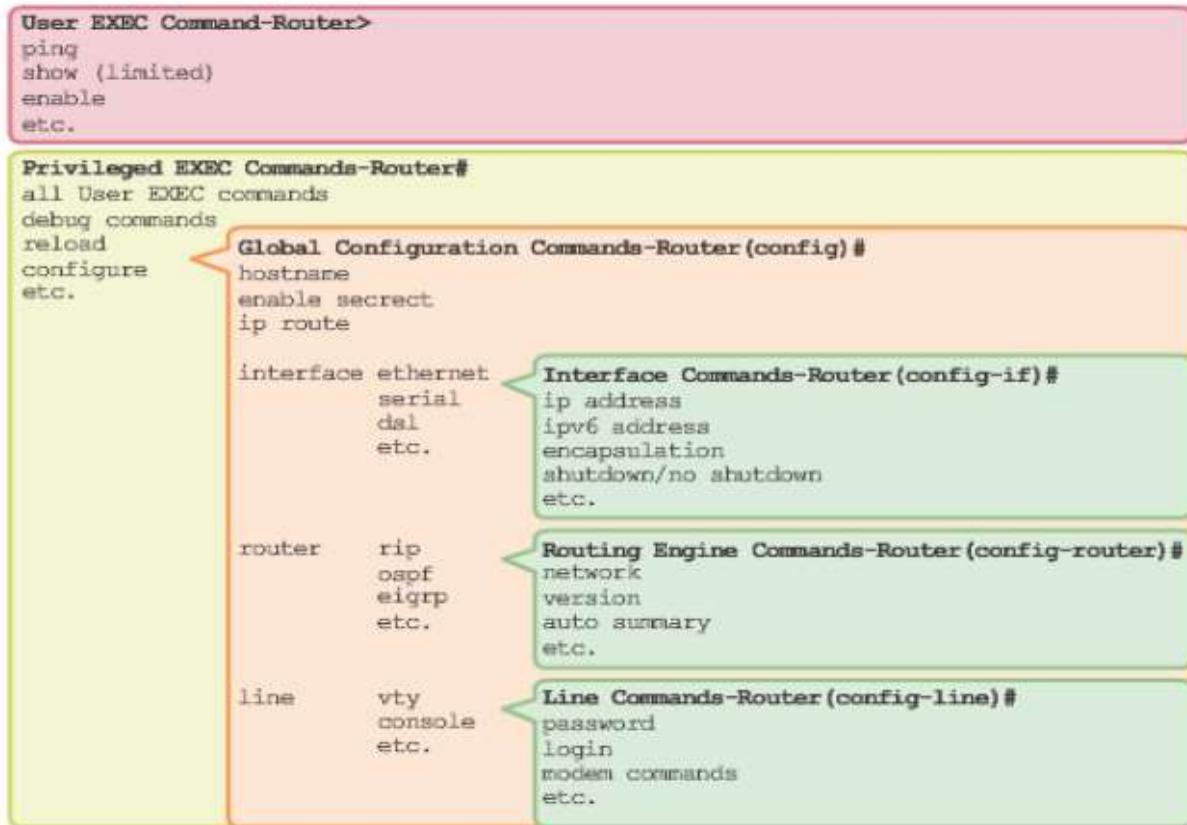
A támadás folyamán egyáltalán nem avatkozik bele a hálózati forgalomba.

Felderítéses támadások (reconnaissance)

- social engineering, reverse social engineering, dumpster diving
- ping (ping sweep), whois, nslookup, arp requests
- packet sniffers (wireshark)
- port scanners (nmap)
- network vulnerability scanners (openvas, nessus, nexpose)
- application vulnerability scanners (acunetix vws, ibm appscan, hp webinspect)

A forgalomirányítók operációsrendszere

IOS Mode Hierarchical Structure



A forgalomirányító védelmének három területe

1. Fizikai védelem

- Zárható helységben történő tárolás, ahol
 - Illetéktelen felhasználó nem férhet hozzá
 - Nincs EMI és RFI
 - Megfelelő a tűzvédelem
 - Megfelelő Hőmérséklet és páratartalom szabályozó van
- Szünetmentes tápegység van

2. Operációs rendszer védelme

- Maximális memória (DoS támadások ellen)
- Legfrissebb stabil IOS
- Biztonsági másolat az IOS-ról és a Config file-ról

3. Router hardening

- Adminisztratív hozzáférés védelme
- A használaton kívüli portok és interfések lekapcsolása
- A szükségtelen szolgáltatások kikapcsolása

A megelőzés érdekében

- Dedikált management hálózat
- Titkosított forgalom használata (SSH, HTTPS)
- Csomagszűrés alkalmazása, hogy csak engedélyezett állomásokról engedélyezett protokollokkal lehessen hozzáférni
- VPN kapcsolaton keresztül

Adminisztratív hozzáférés védelme

- Az eszköz hozzáférhetőségének korlátozása
 - Portok, interfések, távoli elérések korlátozása
- A hozzáférések dokumentálása és „logolása”
- Hitelesített hozzáférés
 - Hibás bejelentkezések korlátozása
- Jogosultságok korlátozása
 - Adott személyek meghatározott műveleteket hajthatnak végre
- A bizalmas adatok védelme

A forgalomirányító jelszavai

Helyi és távoli hozzáférések, illetve protokollok korlátozása

Erős jelszavak kényszerítése

- Hossz
- Karakterek típusa
- Ne tartalmazzon személyes adatokat
- Password helyett Passphrase

Jelszavak biztonságos tárolása

Nem használt (várakozó) kapcsolatok lekapcsolása

Helyi adatbázis használata

Felhasználónévvel és jelszóval történő hitelesítés

Jelszavak titkosítása

Többszöri próbálkozások korlátozása

Telnet tiltása, SSH v2 engedélyezése

Banner üzenetek beállítása

- A rendszer helyes használatának meghatározása
- Figyelemfelkeltés és monitorozás, stb.

Jogosultságok kezelése

- Privilege levels
- Role-Based CLI

Privilege Levels

- A konfiguráció különböző szinteken történhet
 - Különböző jelszókkal védhetők a különböző szintek
 - 16 különböző szint van
-
- **Level 0:**
 - Előre definiált felhasználói szintű hozzáférés
 - Ritkán használt, öt parancs érhető el: disable, enable, exit, help, logout
 - **Level 1(User EXEC mode):**
 - The default level for login with the router prompt Router>
 - A user cannot make any changes or view the running configuration file
 - **Levels 2 –14:**
 - May be customized for user-level privileges
 - Commands from lower levels may be moved up to a higher level, or commands from higher levels may be moved down to a lower level.
 - **Level 15 (Privileged EXEC mode)**
 - Reserved for the enable mode privileges (enable command)
 - Users can view and change all aspects of the configuration

Hátrányok

- hierarchikus - Egy szinten definiált parancsok a magasabb szinten mind elérhetők
- hierarchikus – A magasabb szinten definiált parancsok az alacsonyabb szinten nem lesznek elérhetők
- Ha több parancsszóból álló parancsot definiálunk egy szinthez, minden parancs alkalmazható lesz az adott szinten, amiben az adott parancsszavak valamelyike megtalálható (pl. A show ip route parancs esetén az összes show és show ip parancs is elérhető lesz)
- Nem lehet kezelní (korlátozni) az egyes felhasználók meghatározott porthoz vagy interfészhez történő hozzáférését

Role-based CLI access – szerep-alapú CLI hozzáférés

- Un. VIEW -kat (nézeteket/láthatóságot) hoz létre
- A view-k nem hierarchikusan szerveződnek
- A parancsok specifikusabban rendelhetők a VIEW-hoz
- Root view is the highest administrative view
 - Creating and modifying a view or ‘superview’ is possible only from root view
 - The difference between root view and privilege Level 15 is that only a root view user can create or modify views and superviews
- Role-Based CLI views require AAA new-model
 - This is necessary even with local view authentication
- A maximum of 15 CLI views can exist in addition to the root view

Root View

- Root View is required to defines Views and Superviews
- Views contain commands
- A command can appear in more than one view

30. HÁLÓZATOK CENTRALIZÁLT VÉDELME

Hogyan csináltuk eddig?

- A lokális és távoli hozzáférés legegyszerűbb hitelesítési módszere login és password konfigurációja a console, vty és aux line-okon
 - Könnyű implementáció, de nem biztonságos megoldás
 - Bárki a jelszó birtokában hozzáférhet az eszköz konfigurációjához és megváltoztathatja azt.
- Telnet, SSH (biztonságosabb és accounting is van) (lokális adatbázis esetén felhasználónév is kell!, naplózza a rendszer)
 - Biztonságosabb, de minden eszközön helyileg kell konfigurálni és nem biztosít tartalék megoldást

Hogyan lehetne jobban?

- Jobb megoldást nyújt
 - Ha tudunk tartalék/alternatív megoldásokat konfigurálni
 - Ha minden eszköz egy központi szerveren eltárolt adatbázisra épít
 - Egyszerre lehet kezelní a hitelesítést és a jogosultságkezelést

AAA lehetőséget nyújt felügyelni, hogy

- Ki érheti el a hálózatot (authentication),
- Mit tehet a hálózaton (authorization),
- Milyen tevékenységeket tett a hálózaton (accounting).

AAA komponensek

AAA egy keretet biztosít a hozzáférés felügyeletére

- Authentication – Hitelesítés
 - Hitelesítés megvalósítható felhasználónév jelszó párokkal, kihívás és válasz üzenetekkel, token alapú hitelsítéssel vagy smart cards használatával, stb....
 - Bizonyítani lehet, hogy ki vagyok
 - "I am user 'student' and I know the password to prove it."
- Authorization – Jogosultságkezelés
 - Jogosultságkezeléssel meghatározható, hogy mely erőforrásokhoz férhetnek hozzá a felhasználók és milyen műveleteket végezhetnek rajtuk
 - "User 'student' can access host serverXYZ using SSH only."
- Accounting – Könyvelés
 - Naplózza, hogy mit csinált a felhasználó, beleértve, hogy milyen erőforrást és mennyi ideig ért el, mit változtatott.
 - "User 'student' accessed host serverXYZ using SSH for 15 minutes."

Authentication

Local AAA Authentication

- Felhasználóneveket és jelszavakat lokálisan a Cisco forgalomirányítókon tárolja, és ez alapján hitelesíti a felhasználókat
 - Ideal for small networks
-
1. A kliens kapcsolatot létesít a forgalomirányítóval
 2. Az AAA router felhasználónevet és jelszót kér
 3. A router hitelesíti a felhasználót és a jelszavát a lokális adatbázis alapján
 4. Az adatbázisban tárolt információ alapján a felhasználó jogosult a hálózat használatára

Server-Based AAA Authentication

- A központi AAA szerver tárolja a felhasználóneveket és jelszavakat minden felhasználó számára
 - Több hálózati eszközött is tartalmazó hálózat esetében ez az előnyösebb
-
1. A kliens kapcsolatot létesít a forgalomirányítóval
 2. Az AAA router felhasználónevet és jelszót kér.
 3. A router hitelesíti a felhasználót és a jelszavát a távoli szerveren tárolt információ alapján
 4. A szereveren tárolt információ alapján a felhasználó jogosult a hálózat használatára

AAA Authorization

- Hitelesítés után a felhasználó által kért szolgáltatásokra engedélyt kér a forgalomirányító a szerverről:
 - Milyen erőforrásokat ér el?
 - Milyen műveleteket hajthat végre?
 - Privilege level-höz és a role-based CLI-hez hasonlóan jogokat biztosít bizonyos parancsokhoz,
 - AAA authorization is egy nevesített listával konfigurálható, melyet interfészhez kell rendelni.
 - Általában szerver alapú jogosultságkezelést valósítunk meg
 - Automatikus a végrehajtása hitelesítés után
-
1. A felhasználó hitelesítése után egy viszony alakul ki a router és a szerver között
 2. Amikor a felhasználó megpróbál privilegizált EXEC módba lépni, a router visszaigazolást kér az AAA szerverről, hogy a felhasználó valóban rendelkezik a megfelelő jogokkal
 3. Az AAA szerver visszaküld egy “PASS/FAIL” választ.

AAA Accounting

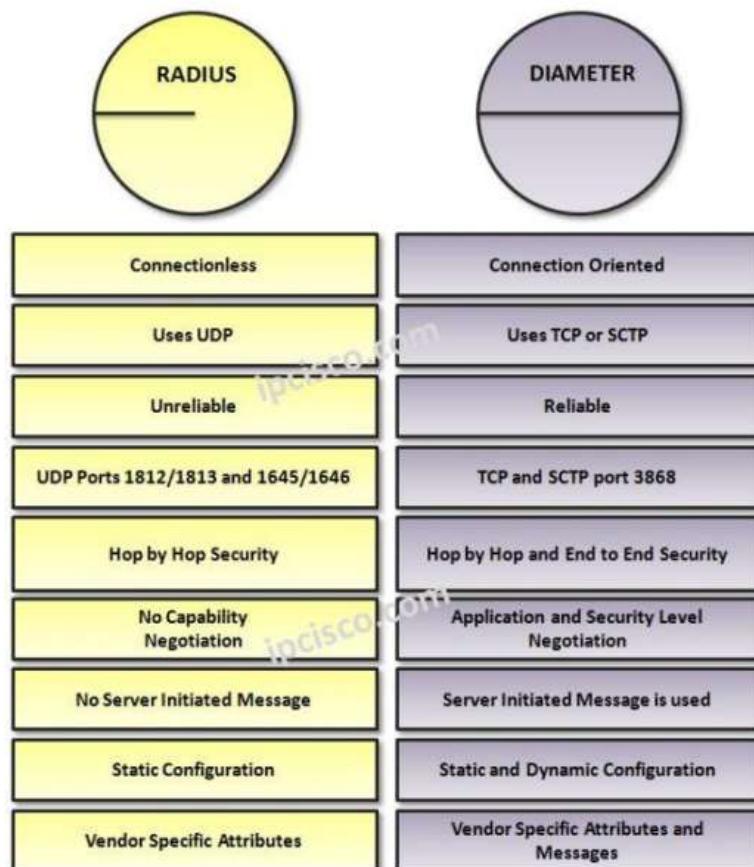
1. A felhasználó hitelesítése után az AAA accounting (könyvelés) folyamata egy start üzenetet generál, melyet követően a könyvelés megkezdődik
 2. A kijelentkezést egy stop üzenet követi, mellyel lezárul a könyvelés folyamata
-
- Összegyűjti és jegyzőkönyvezi a használt adatokat (kezdés és végzés időpontja, végrehajtott parancsok, küldött és fogadott csomagok száma, ...)

AAA előnyei

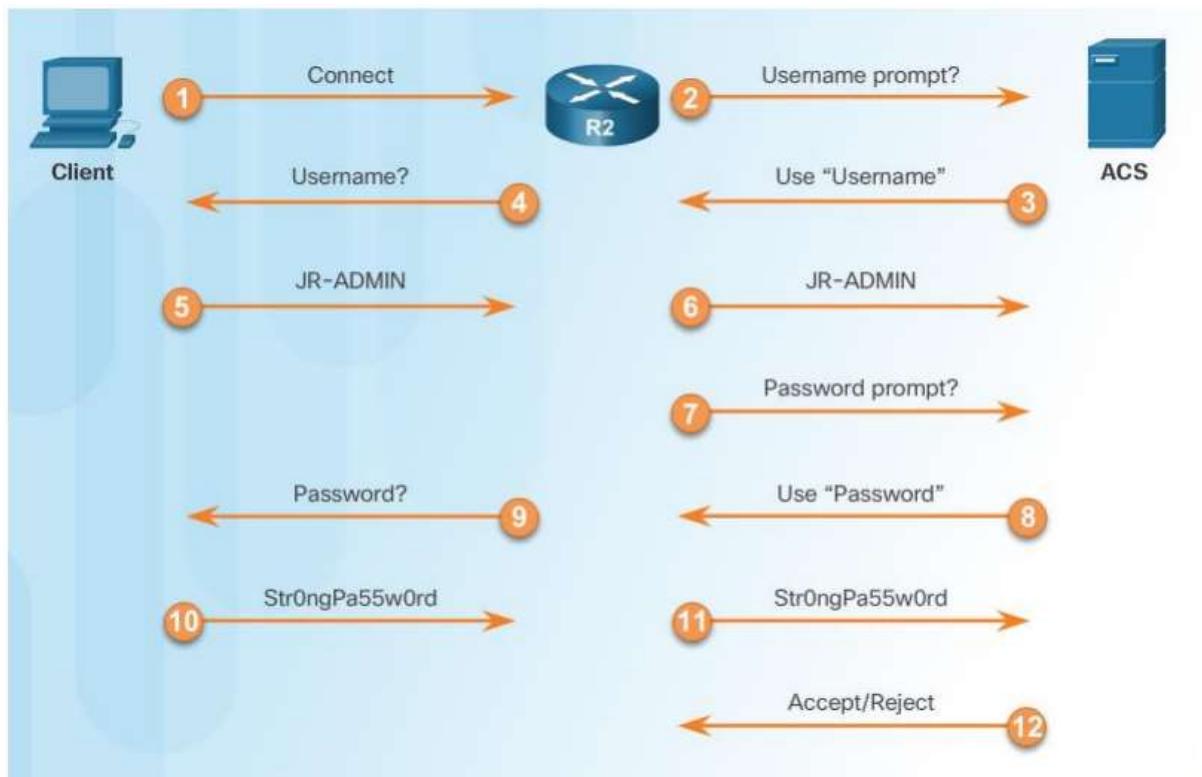
- A hozzáférés rugalmásabb konfigurálása
- Skálázhatóság – központilag kell konfigurálni ellenértben a lokális adatbázissal, amit routerenként kell
- Több backup rendszer használata – hiba esetén más hitelesítési módszerek, Pl.: radius szerver kiseik - > local database
- Szabványos hitelesítési módszerek használata
 - RADIUS - Remote Authentication Dial-In User Service
 - TACACS+ - Terminal Access Controller Access Control System Plus
 - Diameter

Szerver alapú hitelesítés

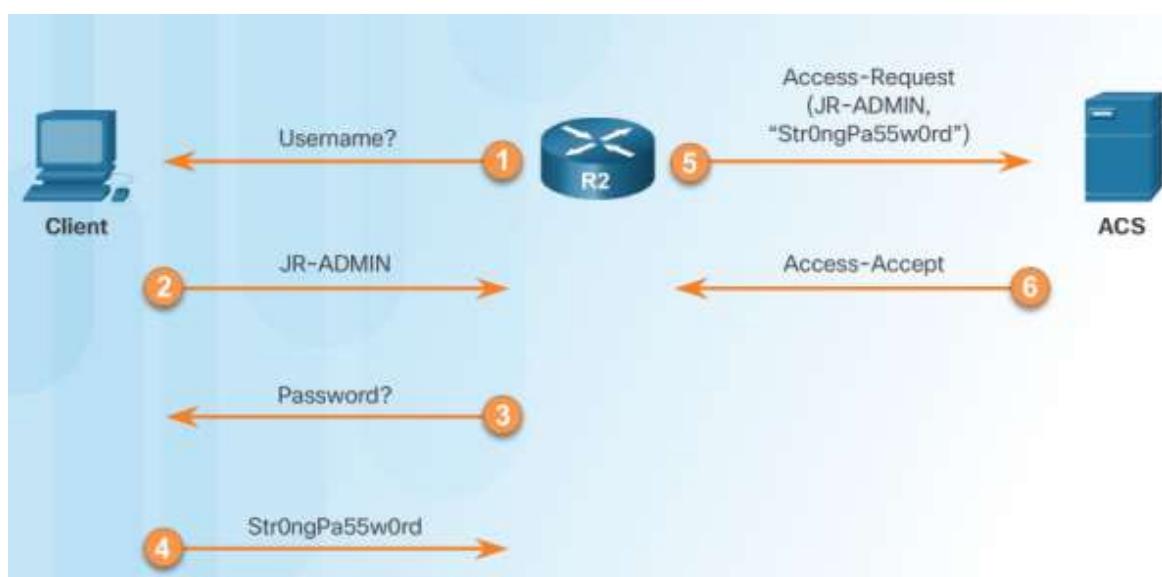
- A TACACS+ és RADIUS a két legelterjedtebb protokoll, amit az eszközök támogatnak szerver-alapú AAA megvalósítására
 - TACACS+ - Terminal Access Control Access Control Server Plus
 - RADIUS - Remote Dial-in User Services



TACACS+ Authentication



RADIUS Authentication



Jogosultság-kezelés

- Egy felhasználó által elérhető szolgáltatások korlátozására szolgál
- Lokális adatbázisból vagy a szerveren található adatbázisból ellenőrzi a felhasználó jogosultságait
 - A felhasználó ezután engedélyt kap (vagy nem) a kért szolgáltatás elérésére

Ha AAA jogosultság-kezelés nincs implementálva, minden felhasználó teljes hozzáférést kap

Könyvelés/számlázás

- Hasonlóan kell konfigurálni, mint hitelesítést vagy jogosultságkezelést
- Meg kell adni a számlázás módjait sorrendben

31. TÜZFALAK

Defining Firewalls

Tüzfal definíciója: Olyan szoftveres vagy hardveres hálózatbiztonsági eszköz, amely a rajta áthaladó (általában: bejövő és kimenő) hálózati forgalmat ellenőrzi a szabályrendszere alapján.

A célja, hogy akadályt képezzen egy megbízható belső biztonságos hálózat és egy másik külső, nem megbízható hálózat (pl.: internet) között.

Firewalls characteristics

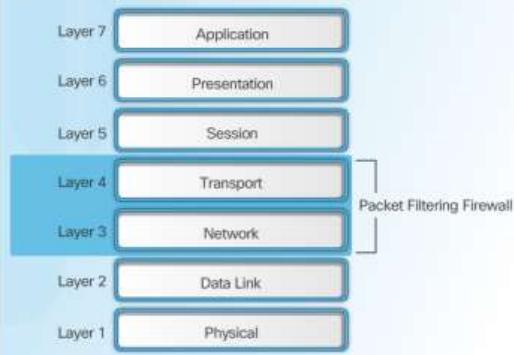
- minden forgalom az internet és a belső hálózat között keresztül halad a tüzfalon, ezért szabályozható, hogy milyen forgalmat engedünk
- A biztonságra vonatkozó döntések fókuszpontja
- Általában más védekezési mechanizmusokkal együtt kell használni
- A tüzfalnak hátrányai is vannak: költséges, fáradtságos az elkészítése, és gyakran bosszantó korlátozásokkal jár a hálózat belső használói számára is

Firewalls do not provide

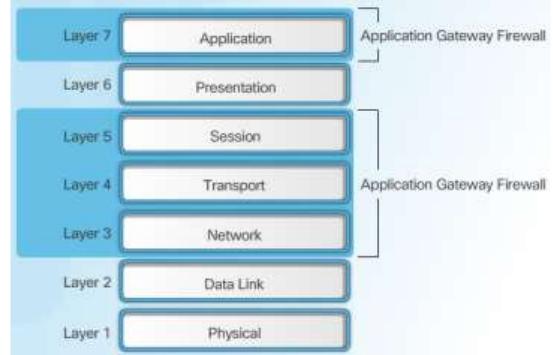
- A tüzfal nem védi a rosszindulatú belső felhasználók ellen
- A tüzfal nem védi olyan kapcsolatot, amelyek nem mennek rajta keresztül
 - Telefonos vagy vezeték nélküli kapcsolat is létesíthető a belső hálózat és az internet között
- A tüzfal nem meg egészen újfajta fenyegetésekkel szemben
- A tüzfal nem örökre készítjük, időnként felül kell vizsgálni. Időnként újfajta támadások bukkannak elő, amelyeket korábban nem ismertünk
- A tüzfal nem minden esetben védi vírusok ellen
- Az áthaladó csomagokban a vírusok felismerése korlátozott
- Titkosított forgalom vírus-ellenőrzése nehéz vagy lehetetlen

Firewall Type Descriptions

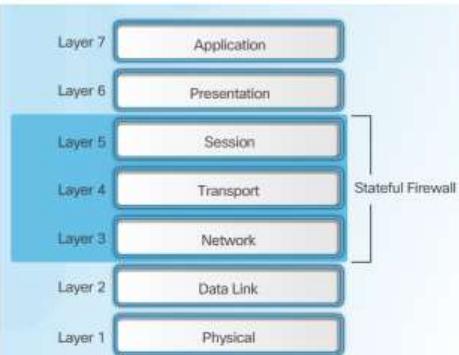
Packet Filtering Firewall



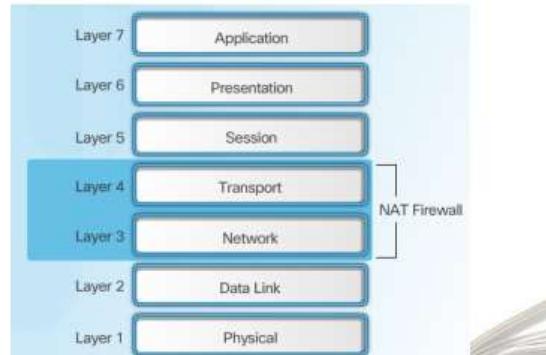
Application Gateway Firewall



Stateful Firewall



NAT Firewall



1st generation – packet filtering firewall

- Hálózati rétegen működik (OSI 3.)
- A kibővített verziója a szállítási réteget is figyeli (OSI 4.)
- Döntését az alábbiakra alapozza:
 - Forrás / cél MAC címe
 - Forrás / cél IP Címe
 - IP csomagba beágyazott protokoll (TCP, UDP, ICMP, stb.)
 - forrás / cél port száma
- A csomag fejlécében lévő információt összeveti a tűzfalban megadott szabályok sorozatával a megadott sorrendben!
- Ha a csomag illeszkedik valamelyik szabályra, a szabályban rögzített műveletet elvégzi (továbbítja, elutasítja)
- Ha nem illeszkedik egyetlen szabályra sem, az alapértelmezett műveletet hajtja végre (többnyire elutasítja). White List vs. black List...

Benefits & Limitations

- A hálózati és a szállítási rétegen működik, adattartalmat nem figyel
- Nem kezeli a kapcsolatállapotot
- Alacsony szintű biztonságot nyújt, mert nem vizsgálja a csomag tartalmát
- Komplex konfiguráció
- A kétirányú forgalmat (kérés és válasz) külön-külön szabályokkal kell megadni
- Sok protokoll (pl. FTP) dinamikusan választ portot az ügyfél oldalon, így a rendszergazdának egy egész port-tartományt engedélyeznie kell

2nd generation - Stateful Firewalls

- Az állapotszűrő (stateful filter) más néven áramkör szintű (circuit-level) tűzfalak az első generációs egyszerű csomagszűrő (packet filter) tűzfalakhoz hasonló tartalmakat vizsgálnak, de már figyelembe veszik a felépített kapcsolatokat
 - pl.: élő TCP kapcsolat, vagy TCP kapcsolat kiépítése, a TCP sequence number folytonossága, ICMP azonosítók ellenőrzése, stb...
- Figyeli, az összes áthaladó csomagot és hogy azok közül melyik csomag kezdeményez új kapcsolatot, melyik már egy meglévő kapcsolat része és melyik csomag nem része egyik kapcsolatnak sem és ez alapján képes a döntéseket hozni. Ezt nevezzük „stateful packet inspection”-nak.
- A leírtakból következik, hogy az OSI modell 5. rétegében is dolgozik
- Kapcsolatállapotot kezel, különbséget tesz az új és a már felépített kapcsolat között
- A felépített kapcsolat információt gyorstárolóban tárolja
- A kapcsolat további csomagjait a gyorstárolóban lévő bejegyzésekkel hasonlítja össze, ezért nagyon hatékony
- Figyeli a dinamikus protokollok állapotát (FTP passive ports) és dinamikusan módosítja a szabályokat, így nem kell teljes port tartományokat nyitva tartani

Előnyei:

- Jobban le lehet írni a hálózati szabályokat (állapotokat)
- Nagyobb biztonságot nyújt, mint a csomagszűrő tűzfalak, a sorszámokat folyamatosan követi

Hátrányai:

- Osztozik a csomagszűrő tűzfalak hátrányiban
- Az állapotok kezelése jelentős teljesítménynövekedést eredményez
- Az adattartalommal nem foglalkozik, ezért alacsony szintű biztonságot nyújt

Application level firewall

Két alkategóriája van:

- Proxy tűzfalak (Proxy Firewalls)
- Mély csomag ellenőrző (Deep Packet Inspection)

Az OSI protokoll alkalmazás rétegében működik.

Előnyei:

- Nagy fokú biztonságot nyújt
- Egyszerűbb konfigurálni, mint a csomagszűrő tűzfalakat
- Figyeli a protokoll fejléc mezőinek hosszát, így ellenáll a puffer túlcsordulás típusú támadások egy részének

Hátrányai:

- Nagy terhelést ró a tűzfal processzorára. Gyakran több processzorral érik el a kívánt teljesítményt
- Nem megfelelő megvalósítás esetén gyenge teljesítményt nyújt
- A gyártóknak követniük kell az új protokollokat
- A transzparencia hiánya

Proxy firewalls

- Proxy alkalmazásokat futtat, amelyek külön-külön kapcsolatot létesítenek a két kommunikáló fél között
- A közvetlen kapcsolat megszakad, a továbbítandó csomagot újra előállítja, átmásolva az összes protokollréteg szükséges mezőit
 - „Vírusos kliensről jövő csomagot újra előállítja bullshit nélkül.”
- minden alkalmazástípusra külön-külön proxy alkalmazás szükséges. Pl.: egy HTTP proxy csak a HTTP forgalom mezőit másolja, továbbítja és szűri
- Alkalmazás szinten képes a parancsok szűrésére. Pl.: egy FTP proxy használatakor parancsonként és felhasználónként lehet szűrni

Deep Packet Inspection Firewalls

- Transzparenlesen működik, nem épít fel külön kapcsolatot a két kommunikáló fél között
- Képes egyszerre az OSI modell minden a 7 réteget szűrni.
- Figyeli a protokollnak nem megfelelő csomagokat és szűri azokat
- A csomagokat az alkalmazásoknak megfelelően osztályozza
 - Skype, Webex, BitTorrent, stb...

Next generation firewalls

- A következő generációs tűzfal elnevezés több hálózatbiztonsági technológia együttes integrációjára utal.
- Olyan megoldás, amely DPI tűzfalat, IDS/IPS eszközöket, Antivirus átjárót, Proxy megoldást, VPN kiszolgálót, SSL/SSH kapcsolat szűrést, Loadbalancing technológiát, Tartalom szűrést, QoS és sávszélesség menedzsmentet biztosít, hogy a lehető legjobban kielégítse a mai kor igényeit
- Granular identification, visibility, and control of behaviors within applications
- Restricting web and web application use based on the reputation of the site
- Proactive protection against Internet threats
- Enforcement of policies based on the user, device, role, application type, and threat profile
- Use of an IPS

Firewall architectures

- Dual-Homed (screening router, two leg perimeter)
- Single-Homed (screened-host, screened subnet, bastion)
- Multi-Homed (three leg perimeter, DMZ)

Dual-homed

- Két interfésszel rendelkezik, amelyek külön-külön hálózatba csatlakoznak és közöttük szűri a hálózati forgalmat.
- A tűzfal lehet SPI, DPI, Proxy, stb...
- Two Leg Perimeter
- Speciális esete:
 - router a tűzfal: screening router

Single-homed – screened host

- Ez az architektúra úgy biztosítja a szolgáltatásokat, hogy a szolgáltatást nyújtó (Bástya) gép csak a belső hálózatra csatlakozik
- Az elsődleges biztonságot a csomagszűrő forgalomirányító (screening router) adja, amely megakadályozza, hogy a felhasználói gépek közvetlenül hozzáférjenek az internethez
- A csomagszűrő forgalomirányítót úgy konfigurálják, hogy az internet gépei csak a bástya géppel léphetnek érintkezésbe
- A bástya gép biztonsága elsőrendűen fontos
- A bástya gép proxy-ként működik
- A screening router akár úgy is konfigurálható, hogy bizonyos szolgáltatások közvetlenül is elérhetők legyenek, míg más szolgáltatások csak a proxy szerveren keresztül működtethetők

Előnye:

- A screened host architektúra nagyobb biztonságot nyújt, mint a dual-homed host architektúra
- Nincs Single Point Of Failure

Hátránya:

- ha egy támadónak sikerül betörnie a bástya gépre, már semmi sem állja útját a belső hálózat többi gépe felé...
- Ebből a szempontból a screened subnet architektúra biztonságosabb

Single-homed – screened subnet

- A screened-subnet architektúra egy újabb biztonsági réteget helyez el az internet és a belső hálózat közé.
- Ez a határ (perimeter) hálózat.
- A bástya gép sebezhető, ezt támadják leginkább. Ha a támadó bejut a bástya gépre, még minden útját állja a belső forgalomirányító!

Perimeter hálózat:

- Ha a támadó bejut a bástya gépre, csak a perimeter hálózat forgalmát tudja lehallgatni, a belső hálózat forgalmát nem láthatja
- A perimeter hálózaton megy keresztül a bástya gépre és közvetlenül az Internetre irányuló forgalom, de két belső gép egymás közötti forgalma nem

Bástya gép:

- A bejövő forgalom kezelésének helye (bejövő SMTP, FTP, DNS WWW, stb.)
- A kifelé irányuló szolgáltatások két módon is kezelhetők:
 - a belső és a külső forgalomirányítók csomagszűrő szabályainak beállításával
 - proxy szerverek futtatásával a bástya gépen. Ekkor is megfelelően kell beállítani a csomagszűrőket

Belső router (Choke router):

- Szabályozza, hogy a belső hálózatról mely szolgáltatások érhetők el közvetlenül: pl. Telnet, FTP, Http, stb.
- Szabályozza a belső hálózat és a bástya gép közötti forgalmat. Ezt a forgalmat is lehetőleg kevés számú protokollra (SMTP, DNS, WWW) és kevés számú belső gépre kell redukálni, hogy a bástya gépről minél kevesebb belső gép legyen támadható

Külső router (Access router):

- Védi a perimeter és a belső hálózatot az internet felől
- Általában minden forgalmat kienged a perimeter hálózatról. A belső hálózat védelmét biztosító csomagszűrési szabályok minden forgalomirányítón azonosak
- Csak azon szabályok különlegesek, amelyek a bástya gépet védi az internet felől

Multi-homed

- Három vagy több interfésszel rendelkezik (vagy interfészenként több IP cím – trönk vonal), amelyek külön-külön hálózatba csatlakoznak és közöttük szűri a hálózati forgalmat.
- A tűzfal lehet SPI, DPI, Proxy, stb...
- Three Leg Perimeter

Demilitarized Zone – DMZ

- Perimeter hálózatnak is szokták nevezni
- Olyan hálózati szegmens, amely szolgáltatásokat nyújt a külső hálózat (általában internet) irányába
- A célja, hogy egy további réteget adjon a hálózati topológiához, ugyanis így egy külső támadó nem fér hozzá egyből a bizalmas belső hálózathoz, hiszen a DMZ és a belső hálózat között lesz még egy (másik) tűzfal, ami blokkolhatja a támadó forgalmát.
- A megbízható belső hálózat is használhat DMZ-beli kiszolgálókat
- Speciális esete, amikor a Bánya gép is a DMZ-ben van, ugyanis az már Screen-Subnet architektúra

Forgalomirányítón megvalósítható tűzfalak – CBAC

1. Access Control List

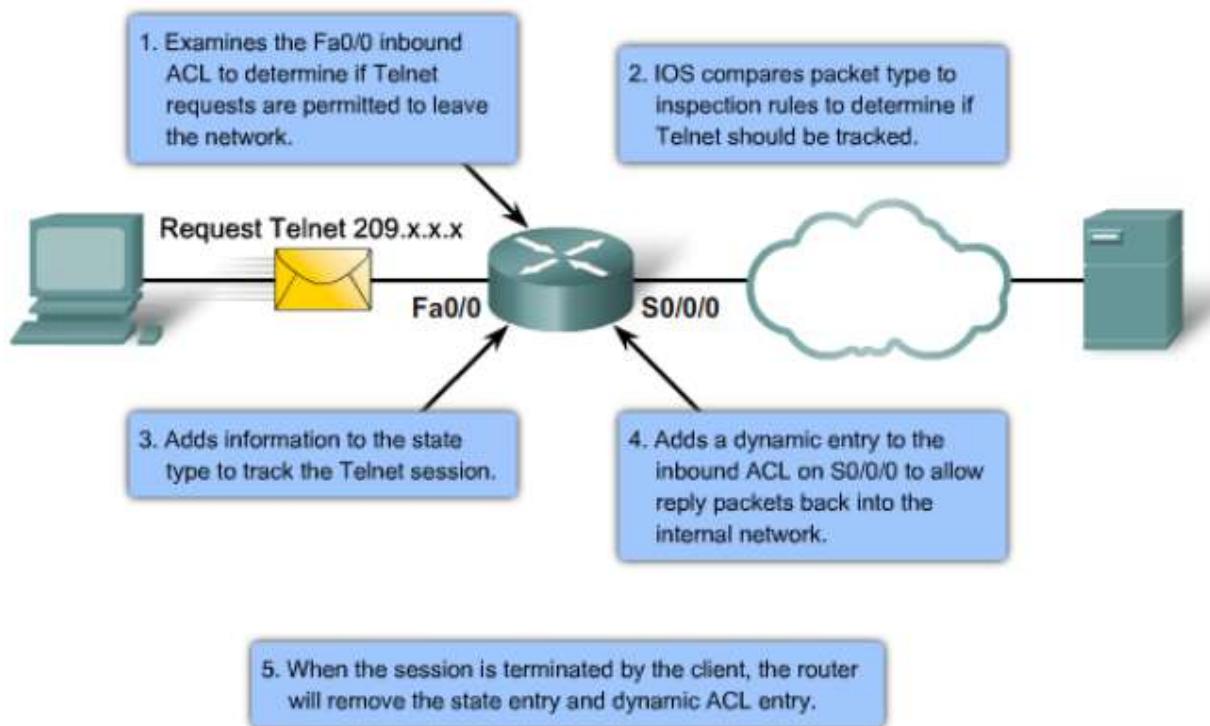
- Legegyszerűbb, első generációs tűzfal
- Állapotmentes
- 3. Illetve 4. rétegen működik

2. CBAC - context-based access control

Fő funkciói:

- Állapottartó szűrés (stateful packet filtering) - nem csak hálózati réteg, szállítási réteg információk alapján, hanem alkalmazási réteg információt is vizsgál, hogy megállapítsa a viszonyok állapotát
- Forgalom figyelés, vizsgálat (traffic inspection) – SYN flood attacks, TCP sorszámozást figyel és gyanúsakat eldobja
- Behatolás érzékelés (Intrusion detection) - syslog üzenetek átvizsgálásával bizonyos smtp támadások, SYN flood attacks, sajátosságait ki lehet szűrni, ezeket a kapcsolatokat eldobja és riasztást, értesítést küld a rendszernek, Cisco IOS tűzfal 3 küszöbértéket is figyel a TCP alapú DoS támadások kivédésére:
 - A félig megnyitott TCP kacsolatok száma
 - A félig megnyitott TCP kacsolatok száma adott intervallumban
 - A félig megnyitott TCP kacsolatok száma egy adott host-tól
- Naplázás, értesítés (audits and alerts)
- CBAC csak azon protokollok alapján szűr, amelyeket az adminisztrátor konfigurál
- Csak azokat a csomagokat szűri, amelyek áthaladnak a routeren

CBAC működés



- Monitors TCP connection setup
 - Tracks TCP sequence numbers
 - Monitors UDP session information
 - Inspects DNS queries and replies
 - Inspects common ICMP message types
 - Supports applications that rely on multiple connections
 - Inspects embedded addresses
 - Inspects Application Layer information
-
- TCP, UDP és ICMP kapcsolatokról információt tárol az állapot táblában (state table)
 - Állapot tábla alapján dinamikus ACL-t hoz létre a visszajövő csomagok számára – IOS 12.3(4)-ig
 - CBAC ideiglenes „nyílásokat” hoz létre megadott viszonyhoz, kapcsolathoz, melyek beengedik az amúgy bokkolt forgalmat
 - Az állapottábla automatikusan frissül a forgalom áramlásának megfelelően
 - Hasonló a reflexive ACL-ekhez

CBAC konfigurálása

- 1. lépés: Interfész kiválasztása : belső interfész ahonnan indulhat egy viszony felépítés
- 2. lépés: ACL konfigurálás az interfészen: milyen típusú forgalmat engedélyezünk az interfészen
 - Alap konf: internal network to external network minden
 - external to internal semmit
 - Engedélyezzük azt a forgalmat amit meg kell vizsgálni a CBAC-nak
 - Implicit deny-t tegyük explicitté – naplózás miatt
- 3. lépés: Inspection rule megfogalmazása a vizsgált forgalomra
- 4. lépés: Alkalmazás a megfelelő interfészen

Forgalomirányítón megvalósítható tűzfalak – ZPF (33. téTEL)

Benefits of ZPF

- ACL-től független.
- Alapfelfogás: minden tiltunk, amíg külön nem engedjük
- Könnyen olvasható, értelmezhető
- One policy affects any given traffic, instead of needing multiple ACLs and inspection actions

Zone-based policy firewall

- Zone-based policy firewall configuration model (ZPF or ZBF or ZFW) 2006 –ban vezették be a Cisco IOS Release 12.4(6)T-nél
- Zóna alapú tűzfal konfiguráció esetén az interfések zónához vannak rendelve és a szabály a zónák közötti forgalmat szabályozza
 - CBAC-al ellentétben alapfelfogás, hogy minden tiltsunk, amit engedni akarunk azt kell konfigurálni
 - Mindazt tudja amit az eddigi tűzfalak: alkalmazás rétegbeli vizsgálat, URL szűrés, DoS támadások kiszűrése
- Jól struktúrált
- Könnyű használni
- CBAC és ZPF nem használható együtt ugyanazon az interfészen!

Basic ZPF Zone Topology

- Ha új interfészt adunk a Private zónához, akkor az összes állomás, mely az interfészhez csatlakozik kommunikálhat a zóna összes állomásával
- Az új interfész örökli a Private zóna más zónákkal meghatározott kommunikációs szabályait

3 Actions of ZPF

- Inspect
 - Cisco IOS SPI (Stateful packet inspection) (egyenértékű az ip inspect parancssal).
 - Automatikusan beengedi a válasz forgalmat
 - Támogatja azokat a protokollokat, melyek több párhuzamos kapcsolat felépítését igénylik (FTP or H.323)
- Pass
 - Hasonló egy ACL permit állításához
 - Nem követi a kapcsolat állapotát
 - Csak egy irányban engedi át a forgalmat
 - Megfelelő szabályt kell alkalmazni a válaszforgalom beengedésére
- Drop
 - Hasonló egy ACL deny állításához
 - A blokkolt csomagok naplázására lehetőség van

ZPF, ZBF Szabályok

- Egy zónát először konfigurálni kell, mielőtt egy interfész hozzárendelhetünk
- Egy interfész egy biztonsági zónához rendelhető
- Egy zónához tartozó interfészek közötti forgalom engedélyezett (implicitly)
- Különböző zónák közötti forgalom engedélyezéséhez policy-t kell konfigurálni
- Egy zónabeli és egy nem zónabeli interfész között a forgalom nem engedélyezett
- Zónák között a mehet (pass), vizsgál (inspect) és nem mehet (drop) események definíálhatók
- Nem zónához tartozó interfészen CBAC-ot lehet konfigurálni
- Ha egy interfész nem akarunk zónához rendelni, akkor is szükség lehet arra, hogy egy minden átenged policy-vel konfigurált zónába tegyük

The Self Zone

- The ZPF szabályok eltérnek abban az esetben, ha a router, a forrása vagy a célállomása egy forgalomnak
 - Ha egy interfész az egyik zónához rendelünk, akkor az interfészhez csatlakozó állomások kerülnek a zónába
 - A forgalomirányítónak vagy a forgalomirányító által küldött forgalom nem része a zónák között értelmezett szabályoknak
 - Alapértelmezett beállításként a router interfészei a SELF zóna tagjai
- Forgalmeszabályok definíálhatók akkor is ha a zónapár egyik tagja a SELF zóna
 - A self zóna egy rendszer által definiált zóna
 - Nem kell konfigurálni az interfészeket, hogy tagja legyenek
- The SELF zone is the router itself!
- The SELF zone is the only exception to the default deny all policy!

ZPF konfigurálás

1. Hozzuk létre a tűzfal zónákat!
zone security
2. Definiálunk forgalmi osztályokat!
class-map type inspect
3. Határozzuk meg a tűzfal policy-t!
policy-map type inspect
4. Alkalmazzuk a tűzfal policy-t megfelelő zónapárok között!
zone-pair
5. Rendeljük az interfészket a zónákhoz!
zone-member security

32. ÁLLAPOT MENTES TŰZFALAK

Az ACL elve

- Csomag szűrés vagy más néven statikus csomagszűrés hálózati hozzáférést képes kontrollálni a bejövő és kimenő csomagok elemzésével majd azok engedésével vagy eldobásával
- A forgalomirányító csomagszűrőként viselkedik, amikor továbbítja vagy eldobja a csomagokat
- Egy ACL (Hozzáférési lista) permit és deny állítások (ACE) sorrendezett listája

ACL működése



An inbound ACL filters packets coming into a specific interface and before they are routed to the outbound interface.

An outbound ACL filters packets after being routed, regardless of the inbound interface.

Az ACL utolsó állítása mindenkor implicit deny. Ez az állítás mindenkor ott van a végén, még akkor is ha fizikailag nincs ott. Ez minden forgalmat blokkol. Az implicit deny miatt minden olyan ACL amelyben nincs permit állítás, minden forgalmat blokkol.

Az ACL típusai

- Számosztott
 - Standard → 3. rétegbeli szűrés
 - Extended (kiterjesztett) → 3. és 4. rétegbeli szűrés
- Named (nevesített)

Kiterjesztett ACL

Wildcard maszk használata

Wildcard mask és subnet mask az 1-esek és 0-k értelmezésében különböznek:

- Wildcard mask bit 0 – a cím megfelelő bitjeit hasonlítja
- Wildcard mask bit 1 – a cím megfelelő bitjeit figyelmen kívül hagyja

Konfigurálási szabály

A három P szabály:

- **One ACL per protocol** – Az interfészen értelmezett minden protokollhoz külön lista kell
- **One ACL per direction** – ACL-ek egyszerre csak egy irányban vizsgálják a forgalmat. Egy interfészen a kimenő és bemenő irányban két külön ACL kell.
- **One ACL per interface** – ACL-ek egy adott interfészen értelmezendők

ACL elhelyezése a hálózatban

Minden ACL-t oda kell helyezni, ahol a legnagyobb hatékonysággal képes szűrni.

- Extended ACLs – A lehető legközelebb a forgalom forrásához
- Standard ACLs – Mivel a standard ACL nem határozza meg a célcímet, ezért amennyire csak lehet, a célállomáshoz közel kell helyezni

IPv6 ACL

Although IPv4 and IPv6 ACLs are very similar, there are three significant differences between them.

- Applying an IPv6 ACL
 - IPv6 uses the ipv6 traffic-filter command to perform the same function for IPv6 interfaces
- No Wildcard Masks
 - The prefix-length is used to indicate how much of an IPv6 source or destination address should be matched.
- Additional Default Statements
 - permit icmp any any nd-na
 - permit icmp any any nd-ns

IPv6 ACL konfigurálás

1. From global configuration mode, use the ipv6 accesslist name command to create an IPv6 ACL
2. From the named ACL configuration mode, use the permit or deny statements to specify one or more conditions to determine if a packet is forwarded or dropped
3. Return to privileged EXEC mode with the end command

34. BEHATOLÁS ELLENI VEDELEM

- A mai rendszereket, hálózatokat nagy biztonságtechnikai kihívások terhelik
- Az eszközökhöz való hozzáférés korlátozása, az AAA technikák, access listák, és tűzfalak alkalmazása még nem elegendők a mai gyorsan változó vírusok, férgek általi veszélyekre
- Már nem elegendő egy-két helyen védekezni, az egész rendszert átfogó, újfajta szemléletmódra van szükség
- Egy nagyon fontos oka ennek a Zero-Day Attack. Ez a fajta támadás egy olyan sebezhetőséget használ ki, ami még nem ismert, vagy nem elismert a szoftver készítője által

Lehetséges Megoldások

- Behatolás Detektálás (Intrusion Detection)
- Behatolás Megelőzés (Intrusion Prevention)

A biztonsági célok és a megvalósítás lépései

Biztonsági célok:

- Titkosság
- Integritás
- Rendelkezésre állás

A biztonsági célok megvalósításának öt legfontosabb lépése:

1. **Védelem:** a biztonsági politika kialakítása, megvalósítása megfelelő technológia alkalmazásával
2. **Érzékelés:** a támadások észlelése
3. **Elhárítás:** megfelelő válaszlépés megtétele. Ez az intézményi „Computer Security Incident Response Team” feladata
4. **Értékelés:** a kockázatelemzés elvégzi az eset jövőbeli előfordulása kockázatának vizsgálatát, a lehetséges ellenintézkedéseket és a költség/haszon elemzést, hogy mely ellenintézkedéseket érdemes megvalósítani
5. **Javítás:** a kiválasztott ellenintézkedések megvalósítása

Behatolás érzékelő (IDS) és megelőző (IPS) rendszerek

A behatolás a számítógépek és a számítógép hálózat illetéktelen használata

Behatolás érzékelő eszközöknek a hálózat kritikus forgalmat átbocsátó pontjaira helyezésével a nem kívánt vagy jogosulatlan forgalom érzékelhető, és akár valós idejű beavatkozás is elvégezhető

- A behatolás érzékelő (IDS) és megelőző (IPS) rendszerek érzékelik
 - a gyanús, szabványtól eltérő csomagokat
 - az illegális tevékenységre utaló adattartalmakat
 - a normálistól eltérő forgalom mintákat
 - a küszöb értékeket meghaladó mennyiségű csomagokat
- A behatolás érzékelő rendszerek (IDS) jelzik a behatolás tényét
- A behatolás megelőző rendszerek (IPS) valós időben ellenintézkedéseket tesznek támadások megelőzésére

Behatolás Detektálás

- A Behatolás Detektálása a hálózati forgalom figyeléséből áll
- Passzívan figyeli a forgalmat -> nem tudja azonnal megakadályozni a behatolást, csak észreveszi
- Ahogy a következő ábra is mutatja, a behatolást figyelő eszköz lemosolja a hálózati forgalmat, és elemezi azt. A lényeg, hogy nincsen beépülve a hálózati forgalomba, és nem real-time figyeli az eseményeket, ezért nem is tud real-time reagálni.

Előnyei:

- Nem érinti negatívan a hálózati forgalmat

Hátrányai:

- Rosszul skálázható
- A rosszindulatú csomag célba jutását nem tudja megakadályozni

IDS típusok

A behatolás érzékelők típusai:

- Állomás (Host IDS: HIDS)
- Hálózat (Network IDS: NIDS)

HIDS rendszerek:

- Az adott számítógépen futnak, és a számítógépet érintő behatolásokat érzékelik
- Vizsgálják a beállításokat, jelzik a beállítások megváltozását, bizonyos fájlok megváltozását, amelyek illetéktelen hozzáférést jelentenek
- Jelzik a már bekövetkezett eseményeket

NIDS rendszerek:

- Figyelik a rosszindulatú hálózati forgalmat
- Jelzik a folyamatban lévő támadásokat

A két rendszer együttes alkalmazása célszerű

Behatolás Megelőzés

- Real-time figyeli a forgalmat és így azonnal tud reagálni (pl.: letiltani a forgalmat), így az esetleges veszélyes forgalom nem jut be a hálózatba
- A 3-as és 4-es rétegekben figyel. A csomagok tartalmát, és a payload-ját is figyeli
- Több eljárást is használ: signature-based, profile-based detektálást. Ezzel azokat a csomagokat is el tudja kapni ami egy átlagos tűzfalon átjutna

Előnyei:

- Meg tud állítani single-packet támadásokat is. (mivel detektálás után nem engedi tovább)

Hátrányai:

- Negatívan érinti a hálózati teljesítményt (latency, jitter)
- Kiesés esetén megszakad a forgalom

Implementálás:

- Router amin Cisco IOS IPS szoftver van
- Dedikált eszköz IDS vagy IPS szolgáltatással
- Egy hálózati modul amit Adaptive Security Appliance (ASA)-re telepítettek

IDS és IPS közötti hasonlóságok

- külön szenzor (eszköz vagy szotver) telepítését igényli
- mintákat/jeleket használ a rosszindulatú hálózati forgalom detektálására
- atomi jeleket is képesek detektálni (single-packet)

IDS és IPS közötti különbségek

- Míg az IDS passzív, nem in-line kialakítású, ezért nem képes real-time reagálni a veszélyre, addig az IPS már az első rosszindulatú csomagot is képes megfékezni
- Az IDS-el ellentétben az IPS negatívan érinti a hálózati forgalmat (latency, jitter).
- Eszköz kiesésnél csak az IDS nem okoz hálózati problémát.

Host-based IPS

- Behatolás Detektálás/Megelőzés főként két szegmensben létezik. Hálózati és egyedi számítógépes (host-based).
- A lényege, hogy a kliensre egy szoftvert telepítenek ami monitorozza a gépen végzett tevékenységet(felhasználói, bejövő, kimenő forgalom).

Előnyei:

- Az operációs rendszerre tipikus támadásokat figyeli
- A szokásostól eltérő műveleteket is tudja detektálni (pl.: registry update)

Hátrányai:

- Csak lokális
- – minden gépen implementálni kell (minden operációs rendszerre is)
- Nem ismeri az egész hálózatot, csak a legvégén van

Hálózati IPS szenzorok (network-based IPS)

- A host-based szenzorok önmagukban a hálózatot még nem tudják megvédeni, ezért fontos hálózati szenzorok alkalmazása is
- Ezen szenzorokat a hálózat megfelelő pontjaira kell telepíteni, a maximális biztonság elérése céljából
- Szenzorok fő hardver implementációs követelményei:
 - **NIC** – muszáj hogy képes legyen a hálózathoz csatlakozni
 - **Processzor** – a behatolás analízis, és minta keresés nagyon CPU igényes feladat
 - **Memória** – minta keresésnél kritikus a megfelelő memória mérete, ez befolyásolja hogy meddig képes egy adott esetleges behatolást figyelni, hogy tényleg negatív forgalom-e

Előnyök:

- Költséghatékony
- Hálózaton transzparens
- Alacsony szintű hálózati eseményeket is látja (host-based –el ellentétben)

Hátrányok:

- Titkosított forgalmat nem látja
- Nem tudja egy támadás sikeres lett-e vagy sem

Port Mirroring

- A hálózati forgalom figyelésére használhatunk különböző csomag analizáló/packet sniffer tool-okat.
- Ennek elősegítésére van a port mirroring. Lényege, hogy a bejövő csomagokat nem csak tovább küldi a cél felé, de le is másolja és elküldi egy meghatározott portján az analizáló eszközünk felé
- Ennek a Cisco SPAN(switched port analyzer) egy cisco implementációja

Cisco SPAN (Switched Port Analyzer)

- Kétféle port definiálása:
 - **Source** (SPAN) port: azon portok amelyeken átmenő forgalmat tovább küldi a Destination port -ra
 - **Destination** (SPAN) port: a lemasolt forgalmat erre küldi, a másik oldalán egy csomag ellenőrző gép/szoftver van
- A source és destination portok asszociációja egy SPAN session, és több session is lehet
- Source port lehet egy port, vagy akár egy VLAN is, de minden hozzá tartozó port source lesz)

Signatures (szignatúrák, minták)

- AIDS, IPS eszközök a rosszindulatú hálózati forgalom észlelésében az egyes minták segítik
- Ezek a minták azonosítanak egyedi férgeket, vírusokat, rosszindulatú forgalmakat
- minden támadásnak megvan az egyedi jele amiben eltér a megszokottól. (hibás csomag, furcsa hálózati aktivitás, stb.)

Minták

A minták attribútumai:

- Típus
- Kiváltó (trigger)
- Akció

Minták típusai:

- Atomi
- Összetett

Atomi minták

- Az atomi minták a legkisebb egységek. Lehet egyetlen csomag vagy akár esemény
- Detektálás után a megfelelő ellenlépéseket megtesz a rendszer
- Detektálásuk kevés erőforrást igényel
- Pl.: LAND támadás: helytelen TCP SYN csomag: forrás és cél is a gép címe → magával kezd el kommunikálni folyamatosan

Összetett Minták (állapotteljes)

- Több csomag, események figyeléséből következtethető a támadás
- A limitált erőforrás miatt configurálni kell milyen sokáig figyeljen egy eseménysorozatot, ha annak eleje egy támadás mintájára hasonlít
- Minta fájlok: cisco által kiadott minták fájlja amit az IPS eszközre fel lehet tölteni
- Ahhoz hogy az IDS, IPS eszközünk hatásosan tudjon lenni, gyakran frissítenünk kell a minta-gyűjteményét
- A Cisco kiad egy minta fájlt, ami az általa ismert összes támadási mintát tartalmazza

Signature micro-engine, SME

- A hatékony figyelés érdekében a cisco signature microengine (SME) –el kategóriákba csoporthozzájárulva a mintákat
- Motorok: (függ az eszköztől, az IOS-tól, és a minta fájltól is)
 - Atomi: csak egyes csomagokat figyel
 - Service: a különböző service-eket figyeli
 - String: minták amik reguláris kifejezéseket használva figyelnek
 - Multi-string: flexibilis mintakeresést tesz lehetővé
 - Other

A behatolás érzékelők fajtái

- Amint bebizonyosodik a behatolás/támadás a megfelelő ellenlépéseket megtesz a rendszer vagy a megfelelő személy.
- Többféle képen tudhatjuk biztosra a behatolás tényét:
 - Minta alapján
 - Anomália alapján
 - Policy alapján
 - Mézesbődön alapján

Pattern-matching detection (minták illesztésén alapuló érzékelés)

- Előre definiált mintákat keres a forgalomban. Atomi és összetett mintákat is felismer. Az egyes mintákat gyakran egyes portokhoz rendelik, és csak ha azon át folyik az a forgalom akkor jelez hibát. Ez probléma olyan rendszerekben ahol nem használnak jól meghatározott portokat.
- Előnyei:
 - Könnyen konfigurálható
 - Kevesebb hibás pozitív eredmény
- Hátrányai:
 - Eddig nem ismert mintát nem tud felismerni
 - Kezdetben sok a hibás pozitív eredmény
 - A mintákat folyamatosan karban kell tartani, updatelni

Anomaly detection (rendellenes viselkedés érzékelése)

- Létre kell hozni egy „normál profil”-t. Meg kell határozni mi a normális működés, és minden ami attól eltér negatív
- Előnyei:
 - Egyszerű és megbízható
 - Nem kell minden támadási fajtára mintát írni, elég csak a normálist meghatározni
 - Eddig ismeretlen támadási fajta is detektálható
- Hátrányai:
 - Generikus, általános kimenet (nem mondja meg pontosan milyen támadás történik)
 - Meg kell határozni a normál működést
 - Nem minden riasztás támadás
 - A tanulási időszakban biztosan támadásmentesnek kell lenni a hálózatnak, különben az lesz a normális

Policy-based

- A minta alapján történő –re hasonlít, de nem mintákat határoz meg, hanem viselkedéseket. Ezzel többféle aktivitás is lefedhető egyszerre. Például egy minta ami riadoztat, ha egy e-mail kliens a cmd.exe –t meghívja. Az adminisztrátorok ezt nem kell mindenhez hozzárendelnie, mert mindenre alkalmazódik ami egy e-mail klienst imitál. Pl.: ha új klienst telepít a felhasználó arra is érvényes lesz.
- Előnyei:
 - Könnyű konfigurálás
 - Képes ismeretlen támadásokat detektálni
- Hátrányai:
 - Nehéz profilkba kategorizálni a hálózati forgalmat nagy hálózatokon
 - Nem változhat a hálózati forgalom profilja

Honey pot – „mézes bődön”

- Ál-szervereket állít a hálózatba, hogy azt támadják
 - Adatokat gyűjt a különböző támadásokról, hogy azokat felhasználva finom hangolják a hálózat IDS, IPS szenzorait. Production environment –ben nem szokták használni, inkább a biztonsági cégek szokták használni kutatás céljából
- Előnyei:
 - Egy ablak a támadásokra
 - Megtéveszti, lelassítja a támadókat
 - Információkat gyűjt a támadásról
- Hátrányai:
 - Dedikált szervert/eszközt igényel

Riasztások fajtái

- **False positive:** elvárt, de nem kívánt riadó
- **False negative:** amikor a rendszer nem ismeri fel a támadást
- **True positive:** helyesen ismeri fel a támadást
- **True negative:** helyes működésnél nem generál riadót

Észlelés után

- Miután észleltük a támadó/normálistól eltérő viselkedést, többféle lépést is tehetünk:
 - Figyelmeztetés
 - Logolás
 - Aktivitás megszakítása/letiltás
 - Reset TCP kapcsolat
 - Jövőbeni kapcsolatok blokkolása (a riasztások alapján új ACL-eket hoz létre)
 - Engedélyezés

Riasztás menedzselése

- **Atomi riasztás:** Pár esetben hasznos, de a támadó képes ezzel direkt a konzolt elárasztani, hogy ne vegyük észre az igazi támadást. Ezért érdemesebb ezeket inkább logolni és később átnézni
- **Összefoglaló riasztás:** A konzol elárasztása ellen az egyes riasztásokról típus szerint összefoglalva kapunk jelentést

Logolás

- Ha az adminisztrátornak nincsen ideje valós időben figyelni, vagy később is meg akarja vizsgálni, az események logolása fontos
- Mit logolni:
 - Támadó csomagokat
 - Áldozat (IP címét tartalmazó) csomagokat
 - Páros csomagokat (előző kettőt együtt)

Aktivitás megszakítása/letiltás

- **Támadó letiltása:** csak a támadót tiltja le. Listát tart fenn a támadókról, amiket később tudunk szerkeszteni
- **Támadó csatlakozásának letiltása (TCP kapcsolatot letiltja)**
- **Csomagok letiltása** (mindent)

Reset TCP kapcsolat

- **Reset TCP connection**
- **Request block connection:** kérelmet küld egy blokkoló eszköznek a kapcsolat blokkolására
- **Request block host:** kérelmet küld egy blokkoló eszköznek a host blokkolására
- **Request SNMP trap**

Figyelembe kell venni

- **Menedzsment metodika:** kis hálózatokon lehet egyesével is konfigurálni az eszközöket, de nagyobb hálózaton már központosítani kell.
- **Esemény összefüggés:** fontos az események helyes időbélyegzése, hogy a későbbi analízis során meg tudjuk állapítani a támadás külön helyen történő, de összefüggő eseményeit.
- **Biztonsági személyzet:** a hálózathoz mérten megfelelő számú személyzet kell a biztonsági riasztások vizsgálatára
- **Válaszlépési terv:** sikeres támadás esetén mi a teendő: eszközök visszaállítása, támadás mélységének, céljának meghatározása, stb.

35. PUBLIKUS HÁLÓZATOKON HALADÓ INFORMÁCIÓ VÉDELME

A széles körben alkalmazott kriptográfiai eljárások rendszerezése és feladatai

- minden titkosítás egy algoritmust használ, aminek cipher a neve, az üzenet titkosítására és feltörésére.
- A tranzpozíciós cipherek esetében a betűknek csak a sorrendje van felcserélve. A helyettesítési cipherek esetében a betűk le vannak cserélve egy szabály szerint.
- A one-time pad cipherek csak egyszer használatos kulcsokat alkalmaztak amik random számokból álltak.
- Számos eljárás létezik -> cél: minél hosszabb ideig tartson a feltörés (mivel visszafejthetetlen titkosítás nincs csak kevés idő)

Hitelesítési és integritásvédelmi megoldások elve, megvalósítása, alaptípusai, alkalmazása

Hitelesítés és integritás védelem

Ezt többet használnánk mint gondolnánk. Hiszen egy-egy weboldalra való bejelentkezés esetén vagy online ügyintézés vagy bankolás esetén is alkalmazzuk.

- Partnerazonosítás: a küldő biztosítja, hogy csak a címzett olvashassa el az üzenetet
- Digitális aláírás és időpecsét: az üzenetet hitelesíti és képes bizonyítani eredetiségét, illetve annak keletkezésének idejét is bizonyítja, így véd az újra kibocsátás elől
- Username + password authentikáció
- Több lépcsős azonosítások

Authenticity (hmac-sha-256)

- A HMAC kulcsot úgy számolják, hogy a hashelt értéket és egy titkos kulcsot kombinál.
- Csak a küldő és a fogadó ismerik a kulcsot. Így az output csak a hash-től és a kulcstól függene.
- Így csak az nyithatja fel az üzenetet, aki megvan a kulcs, ez véd rengeteg támadástól, pl man-in-the-middle.
- Mivel csak a két félnek van meg az adott kulcs, ha az egyik kap egy üzenetet az garantálja, hogy az üzenet a másik féltől jött.
- Mind a SHA és MD5 használható HMAC-el. Ezzel is fix hosszúságú a kimenet, ez a hash és a kulcs hosszától függ eredetileg

Integrity (SHA-256)

- A hash-eket az integritás miatt használják.
- A hash segítségével bármilyen hosszú adatból egy fix hosszúságú reprezentálást hoz létre
- Az egésznek egy olyan matematikai átalakítás az alapja, amit könnyű megvalósítani, de relatívan nehéz visszafejteni.
- Gyakorlatilag lehetetlen két olyan üzenetet találni, amik ugyanazt a hash-t eredményezik, tehát ezek egyediek.
- Ilyen algoritmusok:
 - MD5 (128-bit hash)
 - SHA-224 (224 bit)
 - SHA-256 (256 bit)
 - SHA-384 (384 bit)
 - SHA-512 (512 bit)
- Az SHA-1 egy 160- bites hasht eredményez, ami mára már nem biztonságos.
- A 256- bitestől minősülnek next-gen algoritmusoknak, ezeket érdemes használni, ha lehet.
- Sha 256 egy kulcs alapján az adatot egy 256 bit hosszú kóddá alakítja, amit csak a kulcs segítségével lehet visszafejteni

A kulcskezelés lényege, problémái, elterjed megoldásai, működése és beállítása

Confidentiality

- Használják az üzenetek forrásának igazolására, mivel csak a két félnek van meg az adott kulcs.
- Emiatt is ilyen fontos maguknak a kulcsoknak a kezelése, ha illetéktelen kezekbe kerül aláássa az egész rendszert.
- Az IPSec VPN-ek is a HMAC-et

Fontos a megfelelő kulcshosszt megválasztani, hiszen minél hosszabb a kulcs annál több idő feltörni pl brute-force támadással, viszont akkor a továbbítandó adatok is hosszabbak, jobban terhelik a rendszert a nagyobb és hosszabb csomagok.

- Kulcsok kezelése:
 - igen kényes téma, hiszen nem mindegy, hogy hogyan juttatjuk el a kulcsot a másik félhez, az biztos:
 - az interneten keresztül átküldeni nem a legjobb ötlet
 - előre legeneráltatni a két helyen a megbeszéltek szerint nem igazán életszerű

DH (Diffie-Hellman),

- ez az alapja a legtöbb mai kulcs cserélő módszernek.
- Ez nem egy titkosítási mód, ez egy biztonságos mód a kulcsok cseréjére, ami titkosítja majd az adatokat.
- Ez egy matematikai algoritmus, ami segítségével a két fél generálhat egy egyező titkos kulcsot bármilyen kommunikáció nélkül.
- Mivel az aszimmetrikus kulcsok nagyon lassúak, ezért használják azokat általában csak a kulcsok cseréjére és onnan magukat az adatokat szimmetrikus kulcsokkal titkosítják.

Szimmetrikus és aszimmetrikus titkosítási megoldások jellemzői, beállítás

Szimmetrikus algoritmusok

- Ezek az algoritmusok egy előre megosztott kulcsot használnak, secret key, az üzenetek titkosítására és visszafejtésére
- Bármilyen adat elküldése előtt minden félnek megvan már a kulcs, ebből adódóan használhatnak rövidebb kulcsokat, ami gyorsabb továbbítást eredményez
- **DES** (Data Encryption Standard)
 - szimmetrikus titkosító
 - blokkos módban operál (64 bit)
 - hossz már rövidnek minősül ezért nem szabad ezt alkalmazni
 - inkább 3DES, ugyanazon permutációs és helyettesítő eljárásokat elvégzi háromszor
- **AES** (Advanced Encryption Standard)
 - sokkal hosszabb kulcsot használ, mint a DES és kevésbé erőforrás igényes, mint a 3DES
 - Inkább használatos ott, ahol sok az adat és alacsony a késés tűrése a rendszernek

Aszimmetrikus algoritmusok

- Ezek az algoritmusok nem használnak egy előre megosztott kulcsot
- hanem külön kulccsal titkosítják és fejtik vissza az üzeneteket
- Emiatt van szükség hosszabb kulcsok használatára, ebből adódik a lassabb továbbítás. (IKE, SSL, SSH, PGP)

Nyilvános és titkos kulcsok

- A titkos kulcs titokban tartandó, míg a nyilvános kulcs széles körben terjeszthető. A kulcsok matematikailag összefüggnek, ám a titkos kulcsot gyakorlatilag nem lehet meghatározni a nyilvános kulcs ismeretében. Egy, a nyilvános kulccsal kódolt üzenetet csak a kulcspár másik darabjával, a titkos kulccsal lehet visszafejteni

Vannak block és stream cipherek, a block esetében az adatokat blokkonként titkosítja, a stream esetében a plain-text adatokat byte-onként titkosítja

SEAL (Software-Optimized Encryption Algorithm)

- Egy stream cipher ami 160 bites kulcsot használ
- Mivel az adatokat folyamatosan titkosítja nem vár, mint a blokkos ezért összességében gyorsabb azoktól
- Összességében kisebb terhelést ró a CPU-ra, de az inicializálási fázisa hosszabb a nagy táblákat generál SHA-val

RC {2,4,5,6}

- ezek széleskörben használt titkosítási algoritmusok hálózati applikációknál a nagy sebességük miatt és változtatható kulcs hosszuk miatt

Digitális aláírás, nyilvános kulcsú infrastruktúra (PKI), tanúsítvány alapú működés

Digitális aláírás

A digitális aláírással együtt minden aláíró kap egy megbízható hitelesítésszolgáltató (CA) által kiállított, tanúsítványalapú digitális azonosítót, az aláírást pedig nyilvános kulcsú infrastruktúra (PKI) védi. Ennek köszönhetően a digitális aláírások ideális megoldást jelentenek a korszerűbb hitelesítést igénylő tranzakciókhoz.

Az SSL-tanúsítvány egy digitális tanúsítvány, amely megerősíti a webhely tartományának azonosságát. Az SSL webhelyén való megvalósításához SSL-tanúsítványt kell vásárolnia a domainhez egy SSL-tanúsítvány-szolgáltatótól.

Tanúsító hatóságok

- Amikor a számítógépek HTTPS-en keresztül próbálnak csatlakozni egy webhelyhez, a webböngésző ellenőrzi a webhely biztonsági tanúsítványát, és ellenőrzi, hogy az érvényes-e, és egy megbízható tanúsító hatóságtól (Certificate Authority -CA) származik-e
- Ez igazolja, hogy a webhely azonosítása igaz.
- A digitális tanúsítványt a webböngésző helyileg menti, majd felhasználja a további tranzakciókban
- A webhely nyilvános kulcsa szerepel a tanúsítványban, és a webhely és az ügyfél közötti jövőbeni kommunikáció ellenőrzésére szolgál.

A digitális aláírásnak két formája van

- **Code signing** – Szoftver kódok integritását és eredetiséget jelölik. Igazolja, hogy az adott kód attól van, akitől állítják, hogy van. Biztosítja, hogy a kód a kiadótól van és nem lett módosítva, és hogy maga a kiadó akarta kiadni a kódot/szoftvert
- **Digital Certificate** – Ezek segítségével tudnak a hostok, felhasználók és szervezetek biztonságosan információt cserélni az interneten. Vagyis authentikálja a személyt/szervezetet, hogy tényleg az küldi a valamit, akinek mondják, hogy küldi.
- Digitális aláírásokat lehet generálni három algoritmussal: DSA (privát és publikus kulcs párok), RSA (aszimmetrikus algoritmus), ECDSA

A PKI

- egy olyan infrastruktúra, ami segítségével könnyebb azonosítási információkat cserélne az interneten
- Tehát a felek elfogadják egy harmadik fél véleményét, aki nyilván tartja szervezetek és felhasználók azonosságát, és az azonosítja őket, amit utána a felek igaznak fogadnak el.
- Úgy működik, hogy támogatják a széleskörű szétosztását különböző publikus kulcsoknak az interneten azért, hogy azonosíthassák az adott feleket
- A PKI megkövetel egy bizonyos biztonsági szintet a felektől
- Tehát a PKI biztosítja az authentikálást
- A PKI keretrendszer a hardverből, szoftverből, emberekből, policykból és procedúrákból áll azért, hogy kezeljen, tároljon, szétoszson és visszavezgyen digitális aláírásokat
- A PKI szükséges a nyilvános titkosítási kulcsok nagyszabású terjesztésének és azonosításának támogatásához. A PKI keretrendszer nagymértékben méretezhető bizalmi kapcsolatot tesz lehetővé

PKI (Public Key Infrastructure)

- Szerepek, irányelvek, eljárások sorozata, amely szükséges ahhoz, hogy létrehozzuk a, kezeljük, használjuk, tároljuk és visszavonjuk a digitális tanúsítványokat, illetve kezeljük a nyílt kulcsú titkosítást
- Nagyobb szintű biztonság esetén van rá szükség
- Felépítése:
 - **CA:** amely tárolja, kiosztja és megjelöli a digitális tanúsítványokat
 - **RA:** amely az azonosító hatóságnál tárolt digitális tanúsítványok alapján az egységek beazonosítását igazolja
 - **központi könyvtár:** ahol biztonságos módon tárolják és jelölnek a kulcsokat
 - **tanúsításirányítási rendszer:** amely a tárolt tanúsítványok hozzáférését irányítja, illetve a tanúsítványokat elosztja
 - **tanúsítási irányelvek:** melyek leírják a PKI-rendszer folyamataival szemben támasztott követelményeket

36. VIRTUÁLIS MAGÁNHÁLÓZAT (VPN) – L3

Virtual Private Networks

- Virtual private networks (VPNs) to create end-to-end private network connections
- A VPN is virtual in that it carries information within a private network, but that information is actually transported over a public network
- A VPN is private in that the traffic is encrypted to keep the data confidential while it is transported across the public network

VPN Benefits

- Modern VPNs now support encryption features, such as Internet Protocol Security (IPsec) and Secure Sockets Layer (SSL) VPNs to secure network traffic between sites
- Major benefits of VPNs are shown in the table:

Benefit	Description
Cost Savings	Organizations can use VPNs to reduce their connectivity costs while simultaneously increasing remote connection bandwidth.
Security	Encryption and authentication protocols protect data from unauthorized access.
Scalability	VPNs allow organizations to use the internet, making it easy to add new users without adding significant infrastructure.
Compatibility	VPNs can be implemented across a wide variety of WAN link options including broadband technologies. Remote workers can use these high-speed connections to gain secure access to corporate networks.

Site-to-Site and Remote Access VPNs

A site-to-site VPN is terminated on VPN gateways. VPN traffic is only encrypted between the gateways. Internal hosts have no knowledge that a VPN is being used.

A remote-access VPN is dynamically created to establish a secure connection between a client and a VPN terminating device.

Enterprise and Service Provider VPNs

VPNs can be managed and deployed as:

- **Enterprise VPNs** - common solution for securing enterprise traffic across the internet. Site-to-site and remote access VPNs are created and managed by the enterprise using IPsec and SSL VPNs
- **Service Provider VPNs** - created and managed by the provider network. The provider uses Multiprotocol Label Switching (MPLS) at Layer 2 or Layer 3 to create secure channels between an enterprise's sites, effectively segregating the traffic from other customer traffic.

Remote-Access VPNs

- Remote-access VPNs let remote and mobile users securely connect to the enterprise.
- Remote-access VPNs are typically enabled dynamically by the user when required and can be created using either IPsec or SSL
- **Clientless VPN connection** -The connection is secured using a web browser SSL connection
- **Client-based VPN connection** - VPN client software such as Cisco AnyConnect Secure Mobility Client must be installed on the remote user's end device.

SSL VPNs

SSL uses the public key infrastructure and digital certificates to authenticate peers. The type of VPN method implemented is based on the access requirements of the users and the organization's IT processes. The table compares IPsec and SSL remote access deployments.

Feature	IPsec	SSL
Applications supported	Extensive – All IP-based applications	Limited – Only web-based applications and file sharing
Authentication strength	Strong – Two-way authentication with shared keys or digital certificates	Moderate – one-way or two-way authentication
Encryption strength	Strong – Key lengths 56 – 256 bits	Moderate to strong - Key lengths 40 – 256 bits
Connection complexity	Medium – Requires VPN client installed on a host	Low – Requires web browser on a host
Connection option	Limited – Only specific devices with specific configurations can connect	Extensive – Any device with a web browser can connect

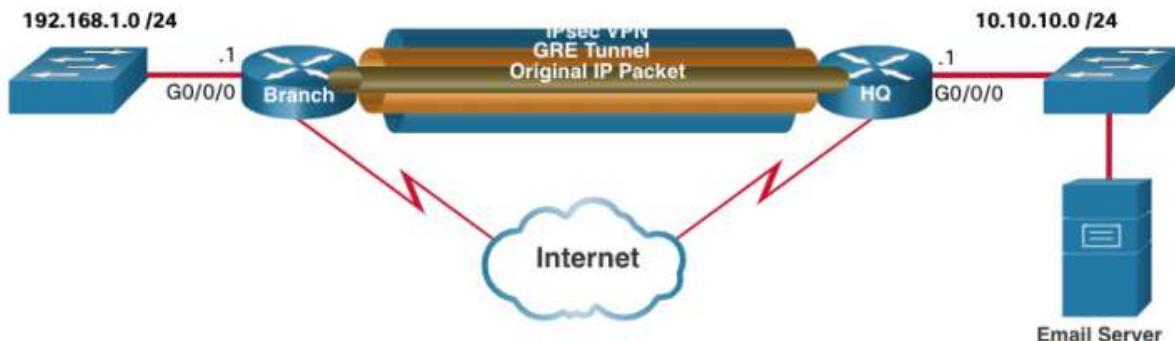
Site-to-Site IPsec VPNs

- Site-to-site VPNs connect networks across an untrusted network such as the internet.
- End hosts send and receive normal unencrypted TCP/IP traffic through a VPN gateway
- The VPN gateway encapsulates and encrypts outbound traffic from a site and sends the traffic through the VPN tunnel to the VPN gateway at the target site. The receiving VPN gateway strips the headers, decrypts the content, and relays the packet toward the target host inside its private network.

GRE over IPsec

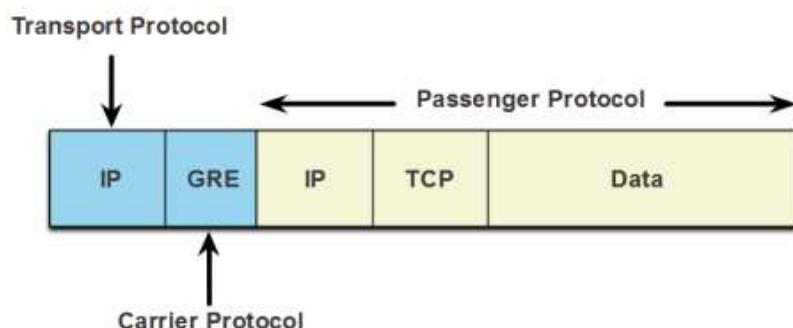
- Generic Routing Encapsulation (GRE) is a non-secure site-to-site VPN tunneling protocol.
- A GRE tunnel can encapsulate various network layer protocols as well as multicast and broadcast traffic.
- GRE does not by default support encryption; and therefore, it does not provide a secure VPN tunnel.
- A GRE packet can be encapsulated into an IPsec packet to forward it securely to the destination VPN gateway.
- Standard IPsec VPNs (non-GRE) can only create secure tunnels for unicast traffic.
- Encapsulating GRE into IPsec allows multicast routing protocol updates to be secured through a VPN.

For example, Branch and HQ need to exchange OSPF routing information over an IPsec VPN. GRE over IPsec is used to support the routing protocol traffic over the IPsec VPN. Specifically, the OSPF packets (i.e., passenger protocol) would be encapsulated by GRE (i.e., carrier protocol) and subsequently encapsulated in an IPsec VPN tunnel.



The terms used to describe the encapsulation of GRE over IPsec tunnel are passenger protocol, carrier protocol, and transport protocol.

- **Passenger protocol** – This is the original packet that is to be encapsulated by GRE. It could be an IPv4 or IPv6 packet, a routing update, and more
- **Carrier protocol** – GRE is the carrier protocol that encapsulates the original passenger packet
- **Transport protocol** – This is the protocol that will actually be used to forward the packet. This could be IPv4 or IPv6



IPsec

IPsec Technologies

IPsec is an IETF standard that defines how a VPN can be secured across IP networks. IPsec protects and authenticates IP packets between source and destination and provides these essential security functions:

- **Confidentiality** - Uses encryption algorithms to prevent cybercriminals from reading the packet contents
 - **Integrity** - Uses hashing algorithms to ensure that packets have not been altered between source and destination.
 - **Origin authentication** - Uses the Internet Key Exchange (IKE) protocol to authenticate source and destination
 - **Diffie-Hellman** – Used to secure key exchange
-
- IPsec is not bound to any specific rules for secure communications.
 - IPsec can easily integrate new security technologies without updating existing IPsec standards.
 - The open slots in the IPsec framework shown in the figure can be filled with any of the choices that are available for that IPsec function to create a unique security association (SA).

IPsec Protocol Encapsulation

Choosing the IPsec protocol encapsulation is the first building block of the framework

- IPsec encapsulates packets using Authentication Header (AH) or Encapsulation Security Protocol (ESP).
- The choice of AH or ESP establishes which other building blocks are available
 - AH is appropriate only when confidentiality is not required or permitted.
 - ESP provides both confidentiality and authentication

Confidentiality

The degree of confidentiality depends on the encryption algorithm and the length of the key used in the encryption algorithm.

The number of possibilities to try to hack the key is a function of the length of the key - the shorter the key, the easier it is to break.

The encryption algorithms highlighted in the figure are all symmetric key cryptosystems:

- DES uses a 56-bit key
- 3DES uses three independent 56-bit encryption keys per 64-bit block
- AES offers three different key lengths: 128 bits, 192 bits, and 256 bits
- SEAL is a stream cipher, which means it encrypts data continuously rather than encrypting blocks of data. SEAL uses a 160-bit key

Integrity

- Data integrity means that the data has not changed in transit
- A method of proving data integrity is required.
- The Hashed Message Authentication Code (HMAC) is a data integrity algorithm that guarantees the integrity of the message using a hash value.
 - Message-Digest 5 (MD5) uses a 128-bit shared-secret key
 - The Secure Hash Algorithm (SHA) uses a 160-bit secret key

Authentication

There are two IPsec peer authentication methods:

1. **Pre-shared key (PSK)** - (PSK) value is entered into each peer manually.
 - Easy to configure manually
 - Does not scale well
 - Must be configured on every peer
2. **Rivest, Shamir, and Adleman (RSA)** - authentication uses digital certificates to authenticate the peers
 - Each peer must authenticate its opposite peer before the tunnel is considered secure.

Secure Key Exchange with Diffie – Hellman

DH provides allows two peers to establish a shared secret key over an insecure channel.

Variations of the DH key exchange are specified as DH groups:

- DH groups 1, 2, and 5 should no longer be used.
- DH groups 14, 15, and 16 use larger key sizes with 2048 bits, 3072 bits, and 4096 bits, respectively
- DH groups 19, 20, 21 and 24 with respective key sizes of 256 bits, 384 bits, 521 bits, and 2048 bits support Elliptical Curve Cryptography (ECC), which reduces the time needed to generate keys.

IPsec működése

- Az A állomás üzenetet szeretne küldeni B-nek
- R1 és R2 között megkezdődik az IKE SA egyeztetése, hitelesítik egymást és felépítenek egy biztonságos csatornát
- R1 és R2 egyeztetik az IPsec paramétereket, aminek eredményeként fel tudják építeni az IPsec alagutat.
- Az alagút kiépült és az IPsec felek között megkezdődhet a kommunikáció
- Az IPsec tunnel befejeződik

37. HELYI HÁLÓZATOK VÉDELME

Instructions for the attacks

- It is foremost important for these attacks, that you only configure those features that is listed in the instructions!
- Carry out all the five attacks that are listed
- At first create a new topology for each attack and save it as #.start where # is the sequence number of the attack
- If the before topology is working correctly then please carry out the attack as it is described using the instructions
- Then try to configure the countermeasure for that attack and save it as #.secured.neptuncode, where neptuncode is your code
- I would like to receive these files from you, and I will try to carry out the attacks on these topologies.

CAM Table Attacks

A támadó egy eszköz segítségével megtölti a CAM táblát hamis adatokkal ezáltal, amikor az megtelik a switch minden portra kiküldi az üzenetet, mivel nem talál egyezést → a támadó megszerzi a forgalmat

Megoldás

- Port Security bekapcsolása
 - Security Violation Modes:
 - Protect
 - Restrict
 - Shutdown
- SNMP üzenetek küldése ha egy új cím megjelenik, vagy ha egy régi timeout-ol

Attack the root

Add a new switch to the topology, it is going to be the attacker, Configure spanning-tree priority to become the root on this attacker switch. You have two choices: Configure spanning tree priority on this switch to a lower value 24576, or configure spanning-tree root primary which ensures this situation. Test again the paths that packets take from PC0 to Server. They should cross the Attacker switch

- The problem with this attack is that root switch has a special role in the network, since most of the traffic is going to traverse the root switch!
- Therefore the root switch should be defended!
- An attacker that is connected to this switch with a packet sniffer can see most of the traffic

Megoldás

- Enable Root Guard
- Enable BPDU Guard
- Do not Use DTP – will see why in the next attack

Megoldások részletezése

- BPDU Guard protects the integrity of ports that are PortFast-enabled. Also protects against additional switches added to the topology
 - Configure on all portfast enabled port (If PortFast is not configured, then BPDU Guard is not activated.)
 - Apply to all end-user ports
- Root Guard is best deployed toward ports that connect to switches that should not be the root bridge. If a root-guard-enabled port receives BPDUs that are superior to those that the current root bridge is sending, that port is moved to a root-inconsistent state (≈listening state)
 - Apply to all ports which should not become root ports
- Loop Guard feature provides additional protection against Layer 2 loops. If BPDUs are not received on a non-designated Loop Guard-enabled port, the port transitions to a loopinconsistent blocking state, instead of the listening / learning / forwarding state
 - Apply to all ports that are or can become non-designated

DTP és VTP támadások

- The point of this attack is that connecting with an attacker switch shown in the topology, because of the by default enabled DTP on all ports, an attacker can form the new connection to trunk, and on trunk connection the VTP protocol can be used to propagate VLAN information. If the default settings remained on all 3 switches for VTP, then a newly connected switch can take down the connection between PC0 and Server0, because it can change VLAN information, for example it can delete the VLAN 10 from all switches
- Why is it possible? It is possible only in that case when no vtp domain were configured before on the switches
- If the attacker sets a domain name on its switch then this domain name will be propagated through the trunk links to all switches. All other switches will have the same domain name, and from that point they are in the same domain, they are all servers, so they will propagate changes and synchronize their databases

Megoldások

- Shutdown unused port, Dot1x, PortSec
- Disable DTP
- Configure Access Mode
- VTP Transparent
- VTP Authentication

Vlan Hopping támadás

- Step 1 – Double Tagging Attack
- Step 2 – Double Tagging Attack
- Step 3 – Double Tagging Attack

Dupla vlan tag esetén a trunk kapcsolat (mivel trönkön nincs vlan) ezért levesz egyet, de utána a belső érvényesítve lesz, és így a támadó hozzáfér a tulsó vlan-hoz

Megoldás

- Disable DTP (auto trunking) negotiations on non-trunking ports by using the switchport mode access interface configuration command
- Manually enable the trunk link on a trunking port using the switchport mode trunk interface configuration command.
- Disable DTP (auto trunking) negotiations on trunking ports using the switchport non-negotiate interface configuration command
- Set the native VLAN to be something other than VLAN 1 and to be set on an unused VLAN using the switchport trunk native vlan vlan_number interface configuration mode command
- Disable unused ports and put them in an unused VLAN

DHCP Starvation

Megoldás

- Use Port Security
- Use Dot1x Authentication
- DHCP snooping rate limit

DHCP Spoofing

- Hamis dhcp szerver használata
- This attack can be carried out, because the first DHCP packet originating on PC0 is a broadcast message, that means that each DHCP server is going to receive it!
- Both DHCP server will respond!
- PC0 will accept the first configuration parameters!
- Because the FAKE server is much closer than the real one, it will accept the fake's offer
- You can test it with setting IP address on PC0 as dynamic
- Check the obtained IP address!

Megoldás

- DHCP SNOOPING trust port
- DOT1x Authentication
- Port Security
- Shutdown unused ports

ARP attack

A támadó hamis ARP válaszokat továbbít

Megoldás

- Dynamic ARP Inspection
 - Dynamic ARP Inspection prevents ARP attacks by intercepting all ARP requests and responses
 - Uses the information from the DHCP Snooping Binding table. The DHCP Snooping table is built from the DHCP request, but you can put in static entries
 - Looks at the MacAddress and IpAddress fields to see if the ARP from the interface is in the binding, if not, traffic is blocked
 - DHCP Snooping had to be configured so the binding table is built
 - DAI is configured by VLAN
 - You can trust an interface like DHCP Snooping

Forgalomirányítás támadás

- If you configure RIPv2 on all routers, they will share routing information with each other
- If you have done it correctly, R1 will have two known routes to 8.8.8.0
- Because the attacker network has a lower metric because on R1 it is only 1 hop away, than it will forward all packets destined to 8.8.8.8 to the attacker server!

Megoldás

- Routing Protocol Authentication
 - RIPv1 does not support authentication
 - RIPv2 supports authentication with plaintext (default) password or with md5 hash

Összegzés

First line of defence (restrict access)

- Shutdown unused port
- Port Security
- Dot1X authentication
- DHCP Snooping

Second line of defence (protocol security)

- VTP Security
- HSRP Security
- Disable DTP
- Routing Protocol Authentication
- ACL

38. DEDIKÁLT TŰZFALAK, ÚJ GENERÁCIÓS TŰZFALAK

Általános jellemzők

- A következő funkciókat biztosítja:
 - Tűzfal (Firewall)
 - Behatolásvédelem (IPS)
 - VPN (S2S és RA)
 - Magas rendelkezésre állás (Fail-over)
- Fizikai megjelenése lehet
 - Appliance – önálló eszköz, asztali, vagy rack-be szerelhető
 - LineCard – más cisco eszközökbe kártyaként telepíthető modul
 - Virtuális entitás – akár a számítógépek/szerverek

Az ASA képességei

- Virtualizáció
 - Több, logikailag önálló Context futhat egy időben
 - minden Context saját beállításokkal, irányító táblával, stb. rendelkezik
 - Néhány funkció nem támogatott ebben a módban (Pl. VPN)
- Magas rendelkezésre állás
 - Akár a az útválasztásnál az FHRP protokollok esetén
 - Két eszköz aktív/tartalék üzemmódban
 - HW/SW azonosnak kell lennie
- Identitás tűzfal
 - Együtt tud működni a Microsoft AD-vel
 - Identitás alapú szűrésre képes IP alapú helyett
- Alapvető IPS funkciók
 - Bővítő kártyák segítségével speciális képességek (antimalware)

Tűzfal működési módok

- Irányított
 - Megjelenik a traceroute-ban
 - +1 hop
 - NAT-képes
 - IP cím szükséges interfészenként
- Transzparens
 - „Vezetékként” látszik
 - Egyszerűsíti a topológiát
 - Több technológia nem támogatott
 - VPN,QoS,DHCP relay
 - Dinamikus útválasztó protokollok

Biztonsági szintek

- minden működő interfészhez kell rendelni
 - Nevet
 - Biztonsági szintet (0 .. 100)
- Magasabb szintű zónából alacsonyabb szintű zónába alapértelmezetten engedélyezett a kommunikáció
 - Ellenkező irányban blokkolt (kivéve válaszok)
 - További kivételek ACL-ekkel szabhatóak ki

Alapértelmezett beállítások

- Factory reset: ciscoasa(config)#configurable factory-default
- Nincs alap jelszó beállítva
 - Sem konzolra, sem enable
- Egy külső interfész
 - Többi belső
- Alapvető PAT
- Elérhető ASDM számára
- DHCP in- és outside

RAS beállítás

- Telnet és SSH beállítása
 - Telnet plaintext
 - SSH preferált
 - AAA-ra figyelni

NTP beállítása

- Ugyanúgy mint a switcheken/routereken

DHCP beállítása

- Base licensz mellett max 32 IP
 - Egyszerre kifelé legfeljebb 10 kommunikálhat
 - 50 user esetén 128 cím, Unlimited esetben 256
 - Nice-to-have – nem erre találták ki ☺ SoHo esetben teszi a dolgát

Objects and Object Groups

- Az IP címeket, cím tartományokat, protokollokat, portszámokat és porttartományokat „object”-ként definiálhatunk, ezután bármely konfigurációban ezekre névvel lehet hivatkozni
- Előnye, hogy ha az Object tartalma változik, az object-et használó konfigurációkat nem kell változtatni

Network Object

- Egyetlen elemet tartalmazhat
 - IP és maszk páros, lehet host, subnet vagy range
 - Új cím felülírja a régit
 - Clear config object network – minden objectet töröl

Service Object

- Tartalmazhat protokollt, port számot vagy intervallumot
 - Szintén egyszerre csak egyet
 - Clear config object service – törli minden

Object Group és beállítása

- Több object-et csoportba lehet szervezni
 - Beállításai minden objectre vonatkoznak
 - ez nyilván akkor előny, ha ezt szeretnénk, gondos tervezést igényel

ACL

ACL-ek – hasonlóságok

- ACE-ekből épül fel (permit és deny állításokból)
- Implicit deny az utolsó rejtett sor
- Az állítások sorrendjében értékeli ki az eszköz (föntről lefelé)
- Megjegyzés (remark) soronként adható hozzá
- Interfészkenként, protokollonként és irányonként egy Acl alkalmazható („3 P szabály”)

ACL-ek – különbségek

- Alapértelmezett szabályok ACL nélkül
 - Nagyobb biztonsági szint léphet át a kisebb felé, vissza csak válasz
- Alhálózati maszk használata Wildcardmaszk helyett
 - 255.255.255.0 helyett 0.0.0.255, stb.
- Időintervallumokat lehet beállítani, mikor működjenek
- Mindig névvel vannak ellátva, nincs számozott
- Interfészhez nem lehet standard ACL-t hozzárendelni

Az ASA-n elérhető ACL-ek

- Extended
 - Egy vagy több ACE-t tartalmaz
 - Forrás+Cél cím, protokoll, port, ICMP
- Standard
 - Az IOS-nél megszokottal ellentétben cél IP címet azonosít
 - Főkén OSPF tovább hirdetésére használják
 - Nem használható forgalom szűrésre

- EtherType
 - Transzparens módban használható
- Webtype
 - Clientless SSL VPN esetén használható
- IPv6
 - IPv6 forgalom szűrése

Címfordítás

- Iránya szerint
 - Belső
 - Külső
 - Kétirányú
- Fajtája szerint
 - Dinamikus NAT
 - Címcsoportok között fordít
 - Dinamikus PAT
 - Jellemzően egy külső címhez fordít több belső címet, portok alapján
 - Statikus NAT
 - Kézzel beállított 1:1 címfordítás
 - Szabály alapú NAT
 - Szabályokat határozhatunk meg, melyek vezérlik a címfordítást

AAA

- Akárcsak a routereken/switcheken itt is használhatunk AAA-t
 - Helyi felhasználó adatbázisból csak AAA használatával tudunk authentikálni
- Teljes törlése: clear config aaa

Modular Policy Framework

- Class Maps
 - Meghatározzuk, mely forgalmat figyeljük
- Policy Maps
 - Több Class Map-et felvehetünk, melyekhez feladatokat rendelhetünk
- Service Policy
 - Policy Map alkalmazása interfészre, vagy a teljes rendszerre
- Csak egy global policy létezhet
 - Módosításához szerkeszteni, vagy cserálni kell