

Ethernet

Moldován István



Budapest University of Technology and Economics



Department of
Telecommunications and Media Informatics

- A *lokális hálózat* azonos szinten elhelyezkedő gépek összességét jelenti.
 - Ezek az adatkapcsolati szintű működés szempontjából azonos jogú egységek. – logikai szinten
- Ezeket szokás *többszörös hozzáférésű hálózatok*nak is nevezni, mert több, azonos joggal rendelkező egység fér hozzá egy adott, közös elérésű erőforráshoz.
 - Ez például a sín topológia esetén maga a sín.
- Annak érdekében, hogy ehhez az elosztott erőforráshoz mindenki igazságosan tudjon hozzáférni, *elosztott protokollok* alkalmazása szükséges.

Az Ethernet őse: Aloha



BME-TMIT

- Hawai szigetek közti rádiózásra fejlesztették
- Több állomás egymással való beszélgetésére
- Algoritmus:
 - Ha van adat, elküldi
 - Vár a nyugtára. A vevők minden csomagot nyugtáznak
 - Ha nem jön ACK, az ütközést jelent. Random idő múlva újraküldi a csomagot

Az Ethernet fejlődése



BME-TMIT

Aloha

Az ősz.

Slotted Aloha

Újítás: csak adott időpontokban küldhet (slots)

CSMA

CSMA = Carrier Sense Multiple Access
Újítás: Először ellenőrzi, hogy van-e adás, és csak akkor küld ha nincs

CSMA/CD

CD = Collision Detection

Újítás: Leállítja a küldést ha ütközést észlel (ilyen az Ethernet)

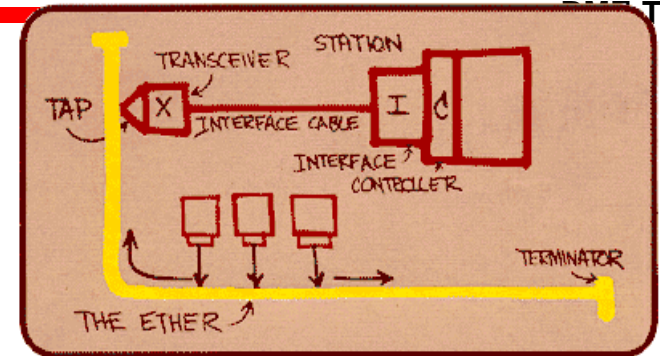
Hogyan kezdődött...



- 1972 Dr Robert Metcalfe

1976 az Ethernet nevet először használták

- Az eredeti DIX Ethernet V2 standard
 - 1982 (DEC-Intel-Xerox)
- Az IEEE 802.3
 - 10Base-5 - 1983
 - 10Base-2 - 1988
 - 10Base-T - 1990



Az első Ethernet ábra

- Ethernet fejlődés –10 Mega után
 - 100BASE-TX (Fast Ethernet)
 - IEEE 802.3u: 1995
 - 1000BASE-X (Gigabit Ethernet)
 - IEEE 802.3z: Június 1998
 - 1000BASE-T (Gigabit on Copper)
 - IEEE 802.3ab Június 1999
 - 10 Gigabit Ethernet (IEEE 802.3ae)
 - IEEE 802.3ae 2002 nyarán

- Az Ethernet által lefedett rétegek:
 - Physical Layer (Layer 1) – teljesen lefedi
 - Data Link layer (Layer 2) – részlegesen lefedi

IEEE	Leírás
802.2	Logical Link Control (LLC) szabvány. Egy általános interfészt határoz meg a hálózati réteg (IP, IPX,...) és az adatkapcsolati réteg (Ethernet, Token Ring,...) közt
802.3	CSMA/CD hálózat specifikáció. Meghatározza a csomag formátumot, kábelezést és a jelzési rendszert.

IEEE 802 Csoportok

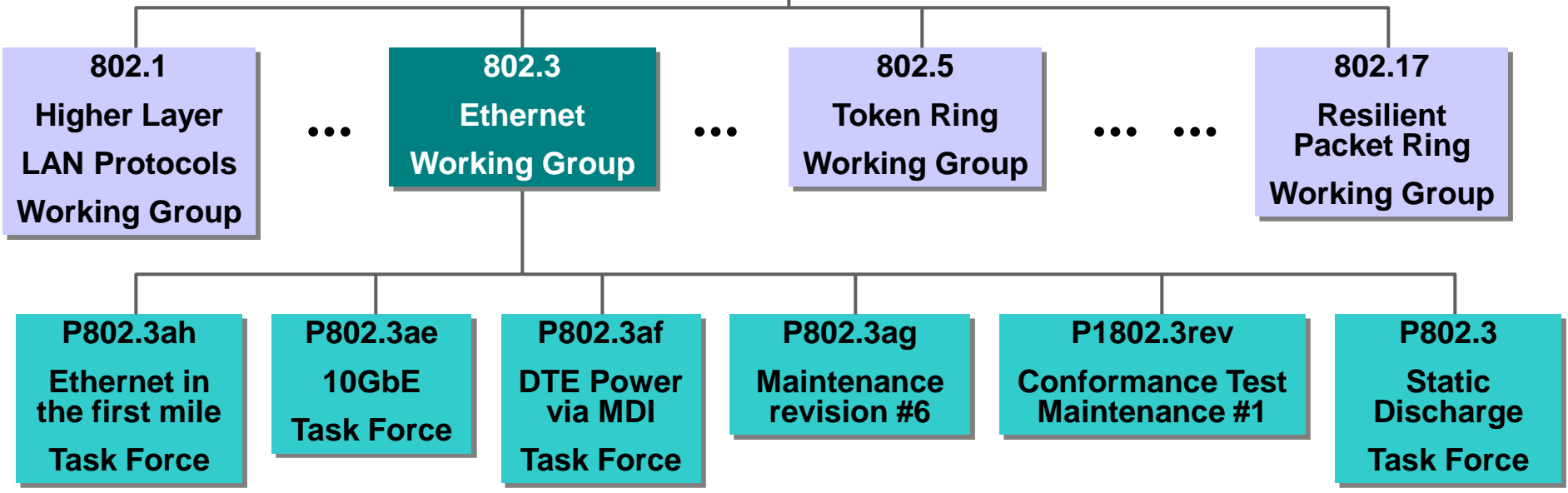


BME-TMIT



IEEE
Standard Boards

IEEE 802
LAN/MAN
Standard Committee

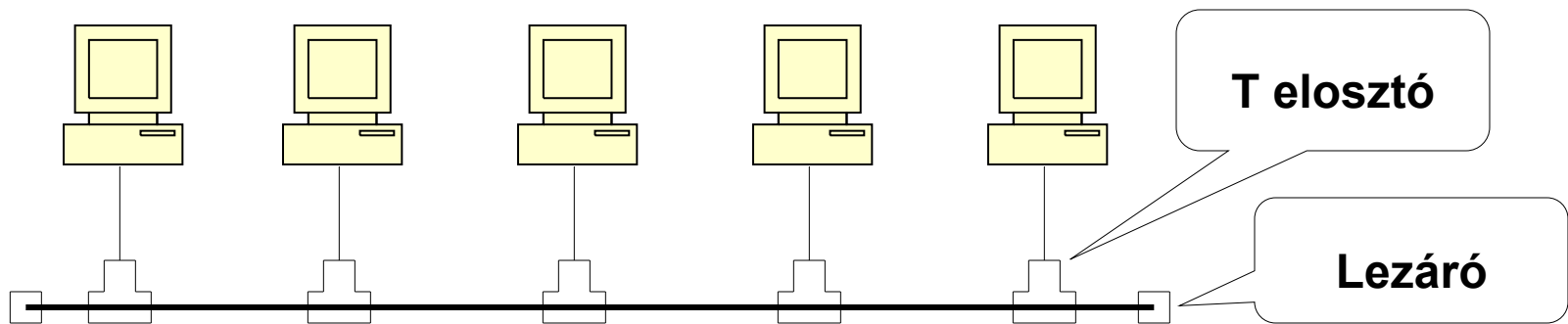


Fizikai kapcsolat típusok - 1



BME-TMIT

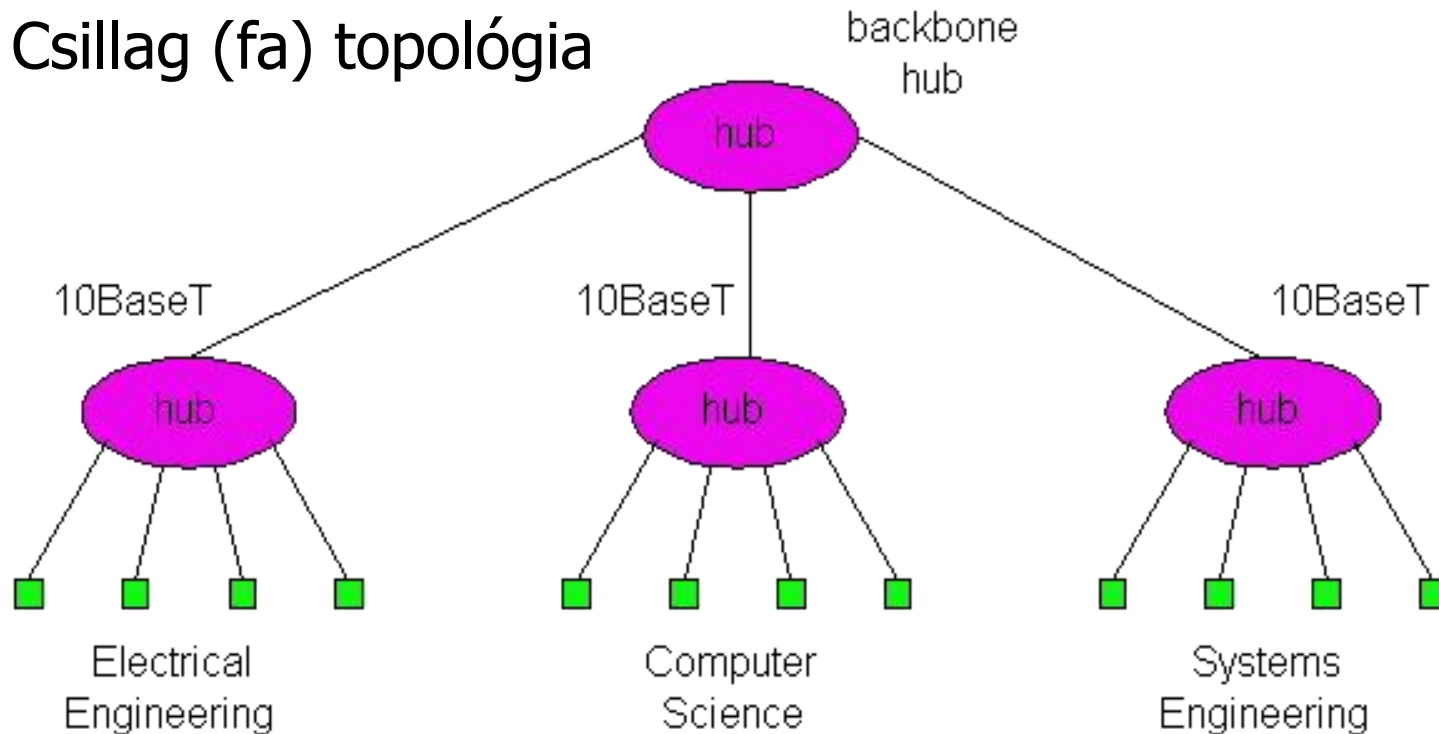
- Koax, vagy 10base2
 - 10: 10Mbps; 2: 200 méter max kábel hossz
 - Vékony koax kábelt használt, busz topológia
- Nagyobb távolság áthidalása:
 - repeater



Fizikai kapcsolat típusok - 2



- 10BaseT és 100BaseT
 - 10 vagy 100 MBps
 - T: Twisted Pair, csavart érpár
 - Csillag (fa) topológia



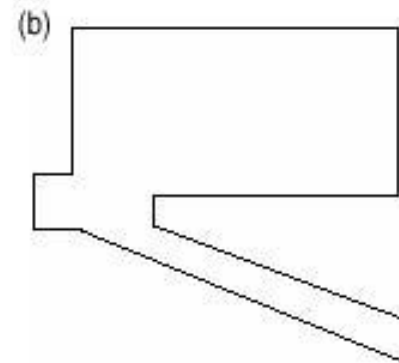
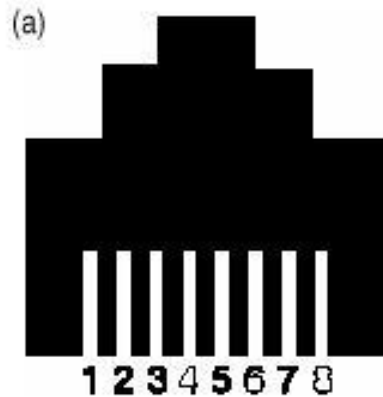
- GE: Gigabit
 - TX – csavart érpár
 - SX/LX/FX – üvegszál, különböző távolságok áthidalására
- 10GE
 - Csak üvegszál
- 802.11: WLAN
 - Ethernet az is!

UTP – Category 5



BME-TMIT

- RJ-45 dugasz



- **Láb kiosztás (10/100)**

- 1 TD+ (Transmit Data)
- 2 TD- (Transmit Data)
- 3 RD+ (Receive Data)
- 4 Nem használt

- 5 Nem használt
- 6 RD- (Receive Data)
- 7 Nem használt
- 8 Nem használt

- A GE mind a 8 szálát használja!

- Direkt kábel
 - A terminálok HUB-hoz való csatolására szolgál
 - A kábel mindkét vége ugyanúgy van bekötve
 - Figyelni kell hogy X- és X+ -t hasonló szín vigye
 - (pl. TD+ narancs-fehér, TD- fehér-narancs)
- Cross kábel
 - Két gép egymással csak keresztkábelrel tud kommunikálni
 - A TD kivezetések az RD lábakra kell legyenek kötve

- Előnye a nagyobb távolságok áthidalásának lehetősége
 - Olcsóbb, gyors
 - Kiterjeszti a LAN hálózatot 100m –nél távolabbra
- Pont-pont típusú kapcsolat
- FX interfész, csatlakoztatás:
 - média átalakító
 - Bővíthető kapcsoló
- GE: GBIC/SFP

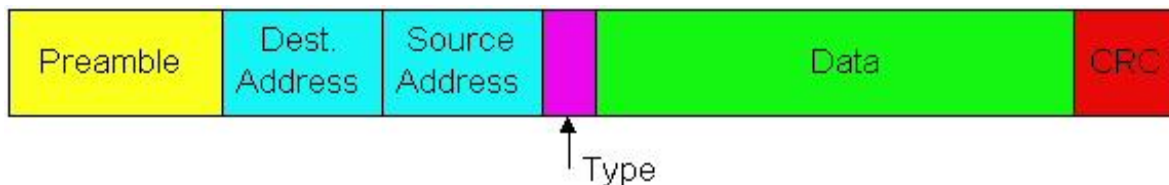
- Standard Ethernet formátumot használ
- Point-to-point és megosztott broadcast működést támogat
- Megosztott módban CSMA/CD-t használ
 - Csak rövid távolságot hidal át (<100m réz esetén.)
- Full-Duplex 1 Gbps sebességgel point-to-point linkeken
 - Általában üvegszálás média, nagyobb táv

- Általában a GE-képes eszközökben kiválasztható a fizikai médium
 - TX (réz), SX/LX/FX (üveg)
- GigaBit Interface Converter
 - Cserélhető, hot-swappable modul
- Small Factory Plug
 - Kisebb méretű átalakító

Csomag formátum



- Ethernet csomag fejlődés
 - I, II, 802.3 (802.2 SNAP az Ethernet II kompatibilitás miatt)
- IEEE 802.3 Data Link Control (DLC)



- A Preamble és CRC mezőket a hardver kezeli:
 - 7 bájt 10101010 melyet egy 10101011 bájt követ (szinkronizáció céljából szükséges)
- Az IEEE 802.3 kasznál LLC és SNAP keretezést

Csomag formátum - 3



BME-TMIT

- Címek: 6 bájtosak
 - A csomagokat minden állomás fogadja, de eldobja ha nem neki címezték
- Type mező: 2 bájt
- CRC: 4 bájt, a vevő ellenőrzi és eldobja a csomagot, ha hibát detektál
- Data: maximum 1500 bájt, minimum 46 bájt
 - Maximum 9000 bájt GE esetén

Csomag formátum - 3



BME-TMIT

E.g. 0800 IPv4
86DD IPv6
0806 ARP
...

MTU	FR	4470
	FDDI	4500
	ATM	9180
	Ethernet	1500

Ethernet V2



Octets 7 4 1 6 6 2 from 46 to 1500 9.6 μ sec

IEEE 802.3



802.2 LLC
802.2 SNAP

Megkülönböztethető a V2 és 802.3

Maximum Frame Size az 1518 (decimal), vagy 0x05EE Hex
EthernetV2 Ethertype mindig nagyobb mint 0x05EF

<http://www.iana.org/assignments/ethernet-numbers>

- **Logical Link Control (LLC) Feladatai:**
 - **MAC szintű protokoll multiplexálás/demux**
 - **opcionálisan flow control, csomagvesztés esetén újraküldés kérések**
- **Service Access Point (SAP) mező szerinti szétválasztás**
 - Source és Destination SAP
 - Control
 - **Több működési mód**
- **Subnetwork Access Protocol (SNAP)**
 - Még több protokoll multiplexálására (8 bit nem elég)
 - Az 0xAA és 0xAB SAP SNAP fejléct jelent
- Mivel az LLC/SNAP 8 byte overhead-et jelent, az IETF szabvány kimondja, hogy az IP/ARP csomagokat Ethernet esetében Ethernet II keretformátummal kell küldeni

Keret továbbítás



BME-TMIT

Egyedi MAC címek

0000.0012.3456

VENDOR Code „OUI“
24 Bits

Egyedi számok
24 Bits

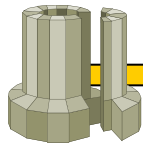
E.g. Alcatel: 00-11-3F
Xerox: 00-00-00

Burned-In Address (BIA):

- Locally Administered Address (LAA)
- Universally Administered Address (UAA)

Elméletileg ez 281,474,976,710,656 cím
Mindenkire 56,000 MAC cím jut!

Direkt címzés: **UNICAST**



FRAME

0000.0000.0001

A PC MAC címére
címezve

0000.0000.0002

*Kivétel:
NIC promiscuous módban*

FRAME

0000.0000.0002

Ez nekem
szól...

http://coffer.com/mac_find/
<http://standards.ieee.org/regauth/oui/index.shtml>

- HUB
 - Fizikai szintű ismétlő
- Switching HUB
 - Tanul, nem mindenhova továbbít
- Bridge
 - Szabványos elnevezés
- Switch
 - Menedzselhető
 - Nem menedzselhető

- Link Layer eszközök: megvizsgálják a MAC fejléceket és szelektíven továbbítanak
- Elválasztják az ütközési zónákat:
 - pufferelek a csomagokat
 - Csak a megfelelő szegmensre továbbítanak
- A célszegmensen CSMA/CD-t használnak a hozzáférésre
- A pufferelés lehetővé teszi különböző médiák/sebességek összekapcsolását

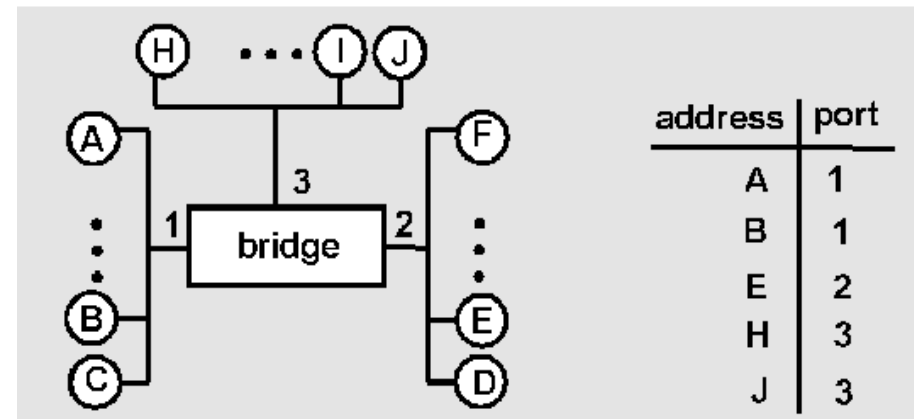
- Cél: traszparens működés
 - Automatikus, plug-n-play működés
 - Automatikus konfigurálás
 - A létező LAN-okkal való együttműködés
- Három fő funkcionális:
 1. Csomag továbbítás
 2. MAC cím tanulás
 3. Hurok elhárítás: Spanning Tree algoritmus

- Megtanulják, hogy mely MAC címet melyik porton érik el: szűrési táblák
 - A beérkező csomagnak kiolvassa a forrását
 - Bejegyzi a szűrési táblába a megfelelő port-al
- Minden bejegyzéshez tartozik egy időbélyeg
 - {MAC cím, port, idő}
 - A bejegyzések az idő lejártával törlődnek
- Működés:
 - Ha van bejegyzés, oda továbbít
 - Ha ugyanaz az interfész, eldobja a csomagot
 - Ha nincs bejegyzés, broadcast

MAC cím tanulás - példa



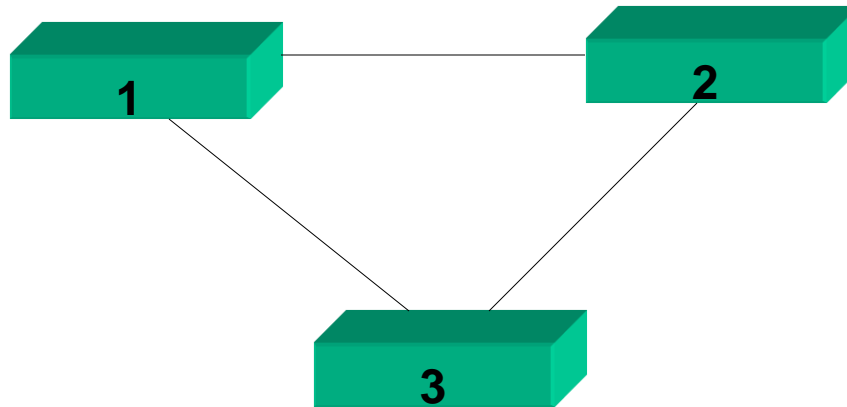
- C küld D-nek
 - A bridge broadcast-ol a 2 és 3 interfészeken
 - A 3. interfészen mindenki eldobja
- D válaszol
 - A bridge már tudja C helyét, csak az 1.-es szegmensre küldi



Redundancia - hurok



BME-TMIT



1. Az első bridge kap egy csomagot. Továbbítja 2 es 3 felé
2. 2 a csomagot továbbítja 3 felé,
3. ugyanakkor 3 továbbítja 2 felé
4. 2 es 3 a csomagokat továbbítják 1 felé
 - ez egy hurok, végtelen körforgás

- Célja a hurok elkerülése
 - Induláskor fa topológiára korlátozza a fizikai topológiát
- Tanuló bridge alapú
- A csomagok kizárólag a fa mentén közlekednek
 - a gyökér irányában, ameddig a cél MAC cím egy más interfészhez nem tartozik
- 802.1d

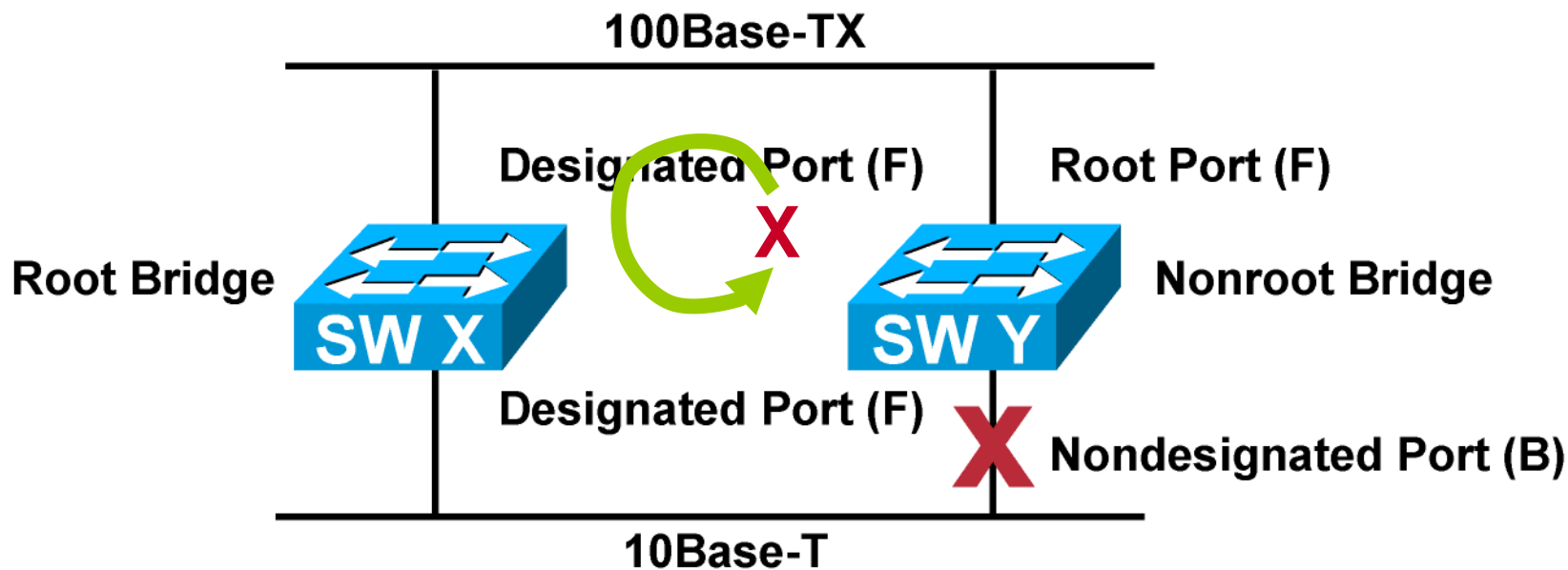
Spanning Tree Alapok



BME-TMIT

Hurok mentes

- Egy root bridge egy hálózatban
- Egy root port minden nem-root bridge-n
- Egy „designated port” minden szegmensre
- Az összes többi port blokkol



STP algoritmus - 1



- A kapcsolók először kiválasztanak egy gyökeret (*Root Bridge*)
 - a legkisebb MAC címmel vagy ID-vel rendelkezőt
- a gyökérből kiindulva kiépítik a fát
 - minden port rendelkezik egy árral (*Port Cost*)
 - a fa kiépítésekor a legkisebb árral rendelkező útvonalat választja
- a fa kiépülése után megtanulja a címeket
 - 15 másodperc tanulási idő

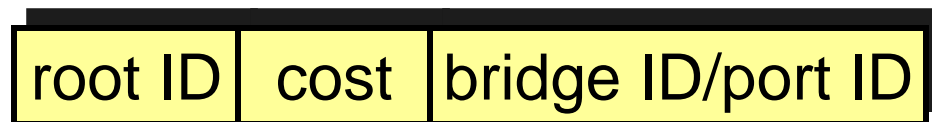
- Bridge ID
 - Alapértelmezett értéke a MAC cím
 - állítható

- Portonkénti ár (**Port Cost**)
 - Alapértéke a sebességtől függ
 - Manuálisan beállítható

STP algoritmus - 2



- Először minden bridge azt feltételezi hogy ő a root
 - BPDU üzenetet küld a következő tartalommal:



Root bridge ID (amit gondol)

Root cost

Saját bridge ID

- Első BPDU: (B, 0, B)

STP algoritmus - 3

- A Root bridge a legkisebb ID-vel rendelkező bridge lesz.
 - Ha egy kapcsoló kisebb ID-vel rendelkező BPDU-t kap R-től, elfogadja root-nak, és a következő BPDU-t továbbítja:



- Ahol B a saját ID és cost a *Port Cost*-ok összege R felé
- 15 másodperc van a topológia kialakítására

STP algoritmus - 4



- Az interfész amelyen a Root Bridge-t éri el, a *Root Port* lesz
- Az a bridge, amely egy LAN-t szolgál ki a root fele, a LAN *designated bridge*-e lesz
 - A designated bridge portja *forwarding state*-be kerül
- Az összes többi, topológiában részt nem vevő interfész blokkolni fog (*blocking state*)
- Létezik egy adminisztratív kikapcsolt állapot is, a *disabled state*

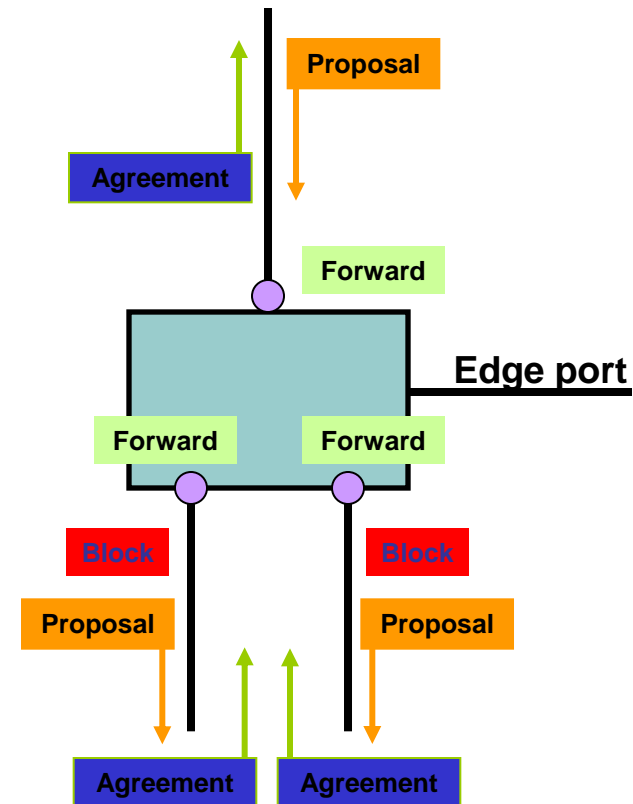
- Minden porton periodikusan HELLO üzeneteket küldenek
- 2 HELLO üzenet elmaradása hibát jelent
 - A bridge-ek újraszámolják a topológiát
 - Ha van blokkolt port akkor azt fogja használni
- Az új topológia kialakítására van 15 sec
- Következik a MAC címek megtanulása a portokon
- 30 másodpercen belül újra működőképes a rendszer

802.1w - Rapid STP alapok

- Újabb IEEE protocol (802.1w)
Kompatibilis a 802.1D-1998-al
- Gyorsabb konvergencia & Timer független
 - CSAK point-to-point FDX Link esetén
 - CSAK ha az edge portok helyesek
 - CSAK ha 802.1D együttműködés nem kell
- Gyártók egyedi megoldásait tartalmazza
- Újítások:
 - új Port Role
 - Más BPDU
 - BPDU kezelés
 - Gyors port állapotváltás
 - Új topologia kialakítás
 - PVST+/802.1D kompatibilitás



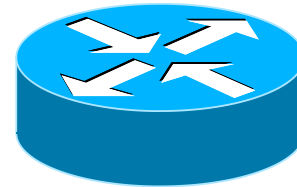
- Proposal érkezés
 - Blokkol minden nem edge port
- Visszaküld egy agreementet
 - Az új port forwarding állapotba kerül
- A többi porton proposal küldés
- Agreementek fogadása
 - Portok forwarding módba



- Az új topológia kialakulása nem timer függő, de topológia függő
 - Nincs korlát – csak az időzítő (STP-ből)
 - Nagy topológia esetén lassú lehet
- Terhelés megosztás továbbra sem lehetséges
- A tanulási fázis nem csökkent le
 - Bár a táblák ürítésére megoldást ad

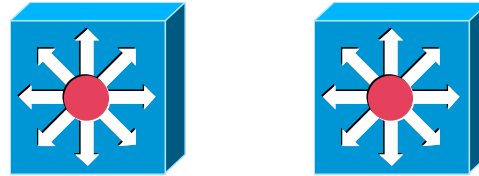
- A nagyobb teljesítményű kapcsolók egyben bridge-ek is
 - Támogatják az STP protokollt
- Típusok
 - Nem menedzselhető:
 - irodai célokra, HUB-ok összekapcsolására kiváló
 - Nem támogatja az STP protokollt, sem a VLAN-okat (jövő óra)
 - Menedzselhető
 - VLAN és STP támogatás
 - Menedzsment interfész
 - L2/L3

- Hierarchikusan



Router

Nagy teljesítményű,
multiservice kapcsoló



SWITCH, Bridge



HUB

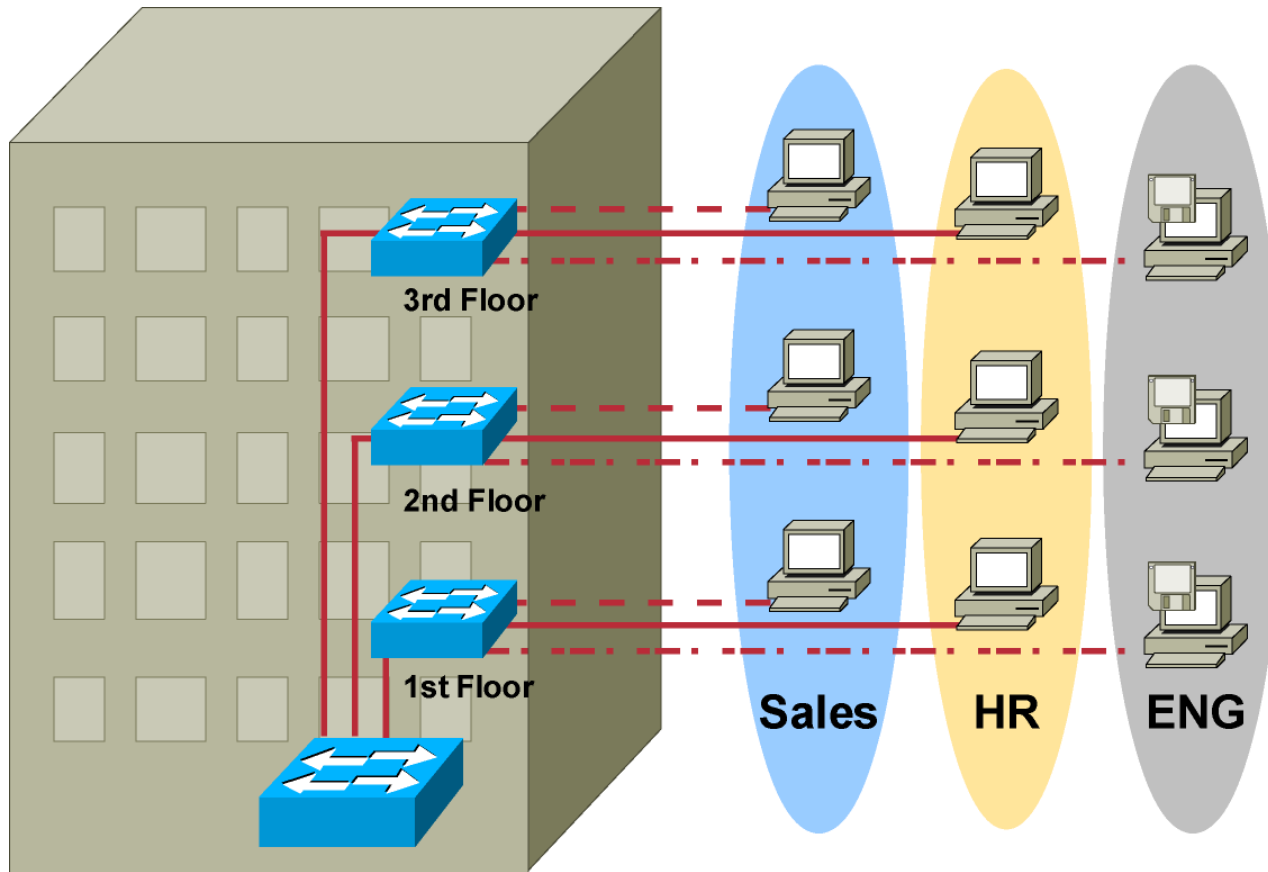


- LAN (Local Area Network): broadcast tartomány
 - a tartományon belül mindenki megkapja a szórt üzenetet
 - kívül senki
 - a LAN határait a kábelezés szabja meg
 - kifelé router kell a kommunikációhoz
 - másik gép megtalálásához is szórt adás kell (ARP)
- VLAN (Virtual LAN): adminisztratív úton létrehozott broadcast tartomány
 - a rendszer adminisztrátora határozza meg, ki van benne
 - a határok itt nem fizikaiak, csak virtuálisak
 - a különböző VLAN-ok nem látják egymás forgalmát

VLAN Áttekintés



BME-TMIT



- Layer 2 connectivity
- Logikai elrendezési flexibilitás
- Egyetlen broadcast domain
- Management
- Biztonság

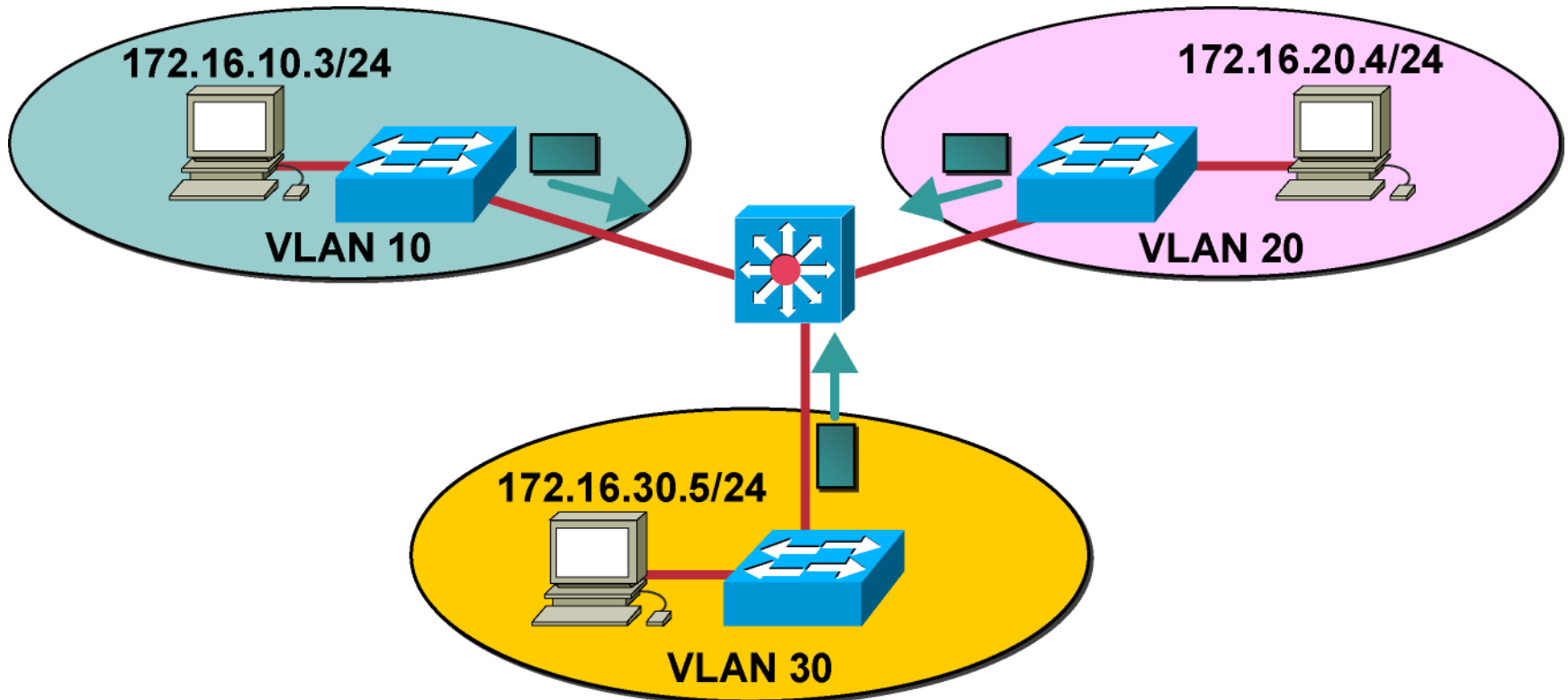
1 VLAN = 1 Broadcast Domain = 1 Logikai hálózat (Subnet)

- Megosztott kapcsolók
 - Csak kapcsolón belül értelmezett
 - Lehet port alapú, MAC alapú
- IEEE 802.1Q szabvány
 - Az Ethernet szabvány kiterjesztése
 - Új mező az Ethernet fejlécben
 - Egy LAN-on belül értelmezett

Átjárás VLAN-ok között



BME-TMIT



- Probléma: elkülönített Broadcast Domain
 - Természetüktől fogva a VLAN-ok tiltják a VLAN-ok közti kommunikációt
 - A VLAN-ok közti átjárás 3. szintű eszközt igényel: L3 SW vagy Router

IEEE 802.1Q



BME-TMIT

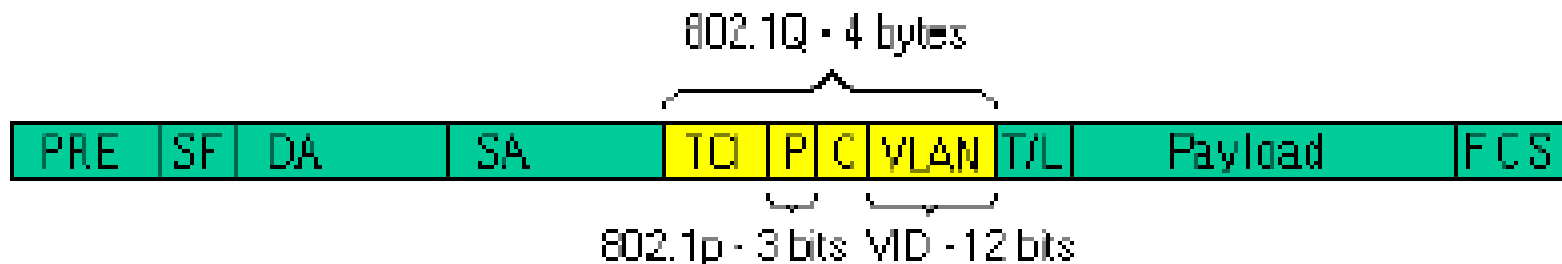
- minden IEEE 802 LAN MAC protokoll felett használható
- könnyű adminisztráció (létrehozás, tag hozzáadása, stb.)
- két különböző VLAN között nincs forgalom (adatkapcsolati szinten)
- egy LAN-on belül több csoport is elkülöníthető
- jól megválasztott csoportok esetén forgalomcsökkenés érhető el

- minden VLAN-nak van egy azonosítója: VID
- a switch nyilvántartja, melyik porthoz melyik VLAN-ok tartoznak
- egy felhasználó több VLAN-nak is tagja lehet
- egy port több VLAN-hoz is tartozhat
- a VLAN több switchre is kiterjedhet
- csökken a szórt adás által felemészített kapacitás, biztonság nő

.1Q VLAN keretformátum



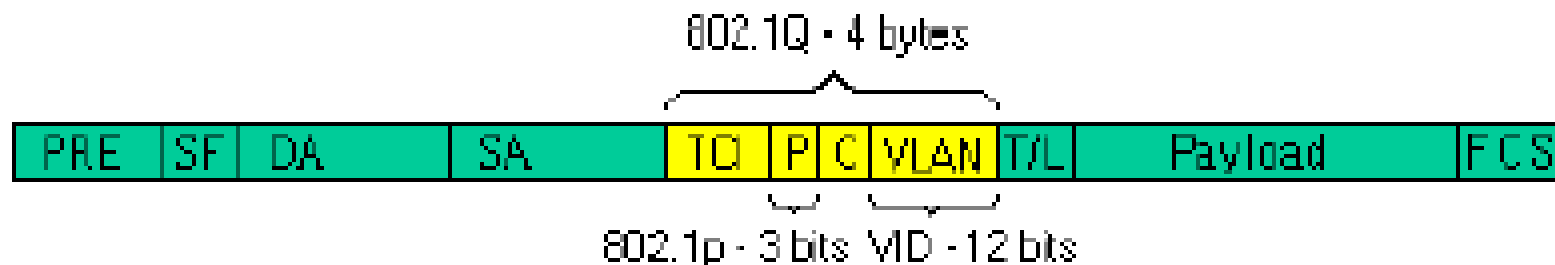
- A VLAN tag tárolásához új mezők az Ethernet-keretben
 - 4 bájtal nő az Ethernet keret
- Helye közvetlenül a forrás MAC cím után
- Lehetővé teszi a minőségbiztosítást is
 - 802.1p prioritás bitek



Új keretformátum – 2.



- TCI (Tag Control Info): 8100-as értéke mutatja a 802.1p és Q használatát
- P: prioritás (0..7)
- C (Canonical Indicator): megmutatja, hogy kanonikus formátumban vannak-e a MAC-címek
- VLAN: a VID-t tárolja (0..4095)

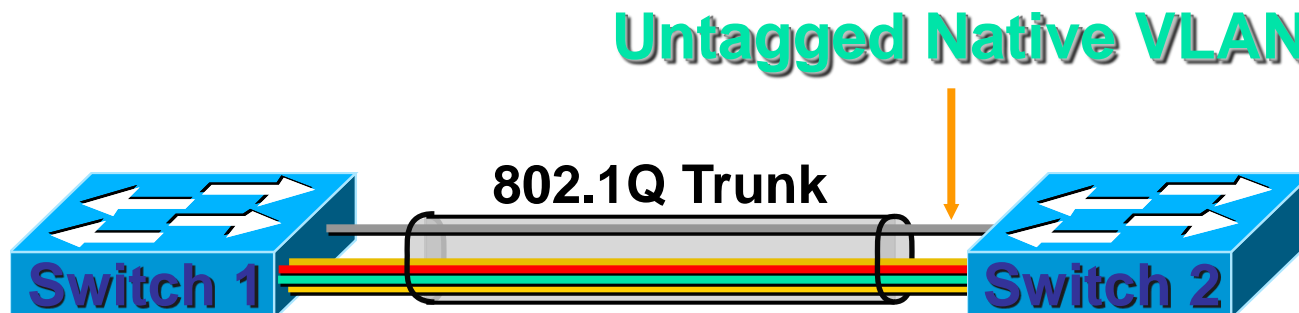


A Natív VLAN és a 802.1Q



BME-TMIT

- Egyetlen nem-csomagolt VLAN – nincs Tag
- Általánosan elterjedt menedzsment célokra
- Meghatározva és kötelező a 802.1Q -ban
- Bármely VLAN lehet, nem feltétlen a VLAN 1
- Egy hálózati tartományban egységes



- megnézzük a fejléctet
- ha nincs tag:
 - VID=0 értékkel teszünk bele
 - ha port alapú VLAN-t használunk, a port PVID-je lesz a VID
- ha van tag, szűrés:
 - megnézzük, kik a tagjai a VID által mutatott VLAN-nak
 - ha a fogadó port nincs a VLAN-ban, eldobjuk a keretet
 - egyébként megnézzük, a cél is tagja-e a VLAN-nak
 - ha igen, továbbítjuk

- megnézzük, a másik oldal támogatja-e a tagelt kereteket
 - ha nem, levesszük a taget
 - ha igen, továbbküldjük
- Átjárás VLAN-ok között csak routeren keresztül
 - Ha egy porton több VLAN van, a router virtuális interfészekként kezeli
 - Átjárás csak IP szinten!

VLAN-ok hozzárendelése



BME-TMIT

- Port-based VLANs: fizikai interfészenként
- MAC-based VLANs: a kapcsoló rendelkezik egy MAC-VLAN listával
- Protocol-based VLANs: a kapcsolóban be van állítva hogy milyen protokoll milyen VLAN-hoz tartozik
- IP subnet alapú (nem elterjedt)

Port alapú VLAN



- a legegyszerűbb megoldás
- a switch egyes portjaihoz hozzárendeljük a megfelelő VLAN azonosítóját
- egy porthoz legfeljebb egy azonosító tartozhat
- a VLAN változtatásakor csak a switch-hez kell nyúlni – a felhasználó számára átlátszó

- a switchben egy lista van, ez tartalmazza az egyes VLAN-okhoz tartozó eszközök MAC-címét
- előny:
 - ha egy felhasználó portot változtat a switch-en belül, az nem igényel semmilyen beavatkozást
- hátrányok:
 - általában nehezebb az adminisztráció (mindenki MAC-címét ismerni kell)

Protokoll alapú VLAN

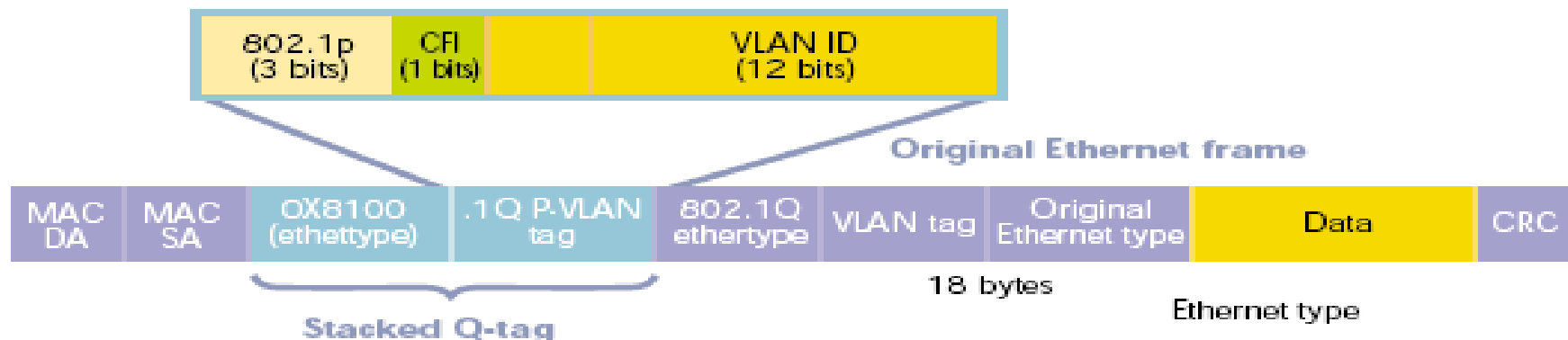


- Különböző protokoll típusokhoz más-más VLAN tag lesz rendelve
- Feltételezi, hogy a kapcsoló megnézi az IP fejléceket
- Nem felhasználót azonosít, hanem szolgáltatást

Q-in-Q (VLAN trönk)



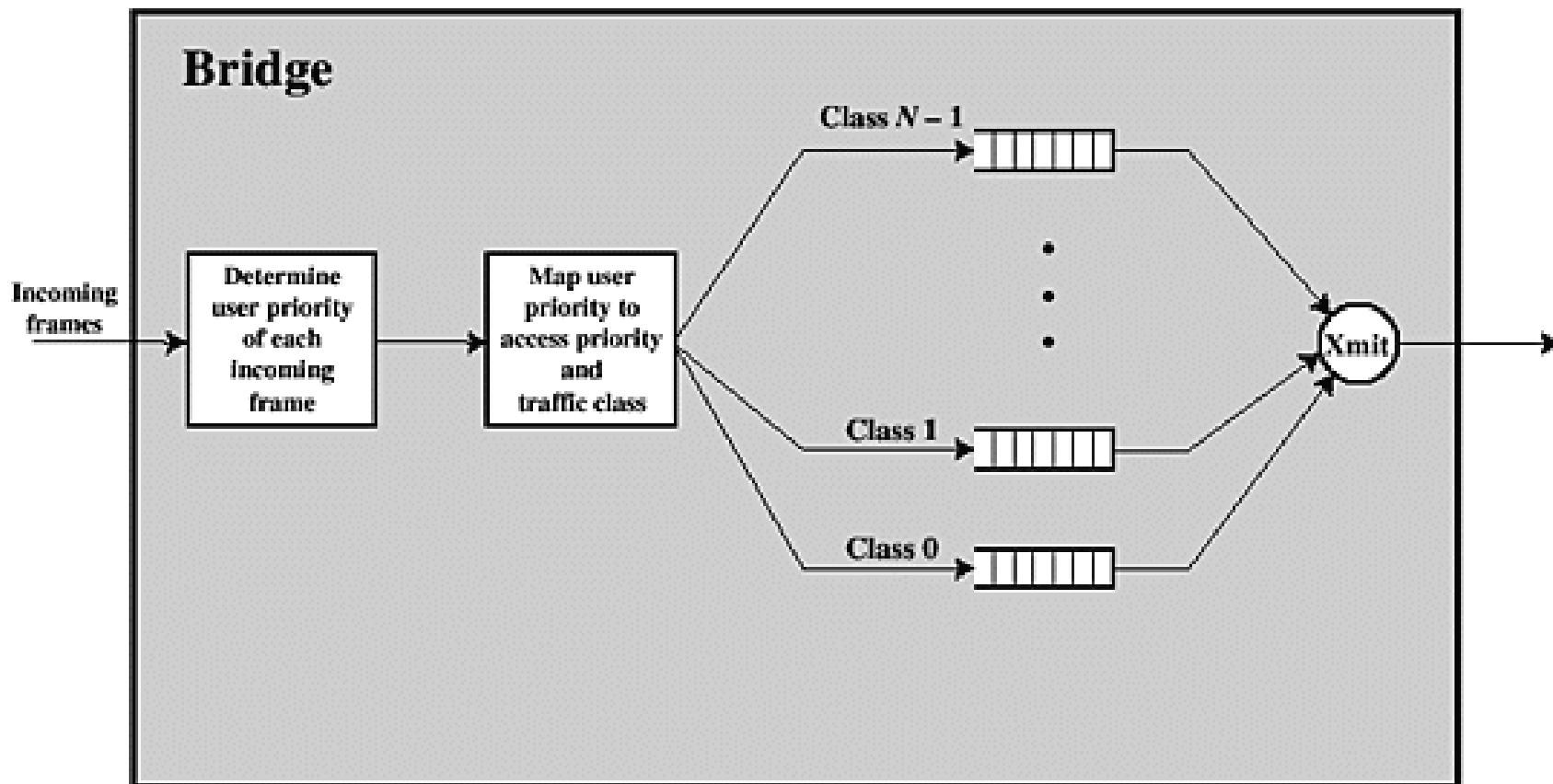
- 4096 VLAN nem elég egy nagyobb hálózatban (>4095 felhasználó)
 - A felhasználók azonosítására használva: C-VLAN
- Bevezetnek egy szolgáltatói VLAN tag-et
 - S-VLAN



- Előnye hogy a VLAN –ok száma megnő
- Léteznek más megoldások is:
 - MAC-in-MAC
 - V-MAN tag bevezetése
 - MPLS tunnel
- A IEEE 802.1ad provider bridge szabvány a QiQ-t támogatja

- Prioritás kezelés a 802.1Q VLAN tag alapján
 - 3 prioritás bit = 8 osztály
 - Ez azt jelenti hogy QoS-hez 802.1Q VLAN-okat kell használni
- A prioritás bitek értelmezését a 802.1P szabvány adja meg
 - A VLAN prioritás és az IP TOS hasonló
 - Jelen Ethernet kapcsolók nem mind támogatják a 8 osztályt

IEEE 802.1D forgalmi osztályok kezelése



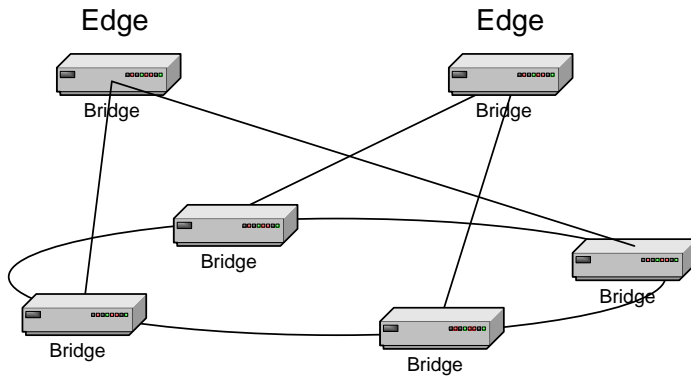
- Az RSTP hátránya: rossz hálózati kihasználás
- Cisco: PVST (Per-VLAN feszítőfa)
 - Minden VLAN: egy RSTP
 - Sok VLAN – nem skálázható, fölösleges
- IEEE: MSTP
 - Lehetővé tesz több feszítőfát
 - A VLAN-ok a feszítőfákhoz vannak rendelve

- RSTP alapú, a szabvány továbbfejlesztése
- Max. 64 fa (MST instance)
- Minden fának beállíthatjuk
 - A gyökerét
 - A link cost-okat
 - A hozzá tartozó VLAN-okat
- Egy VLAN csak 1 fához tartozhat!

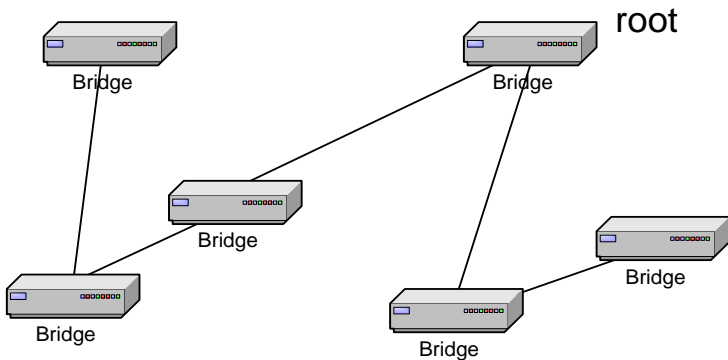
MSTP előnyei



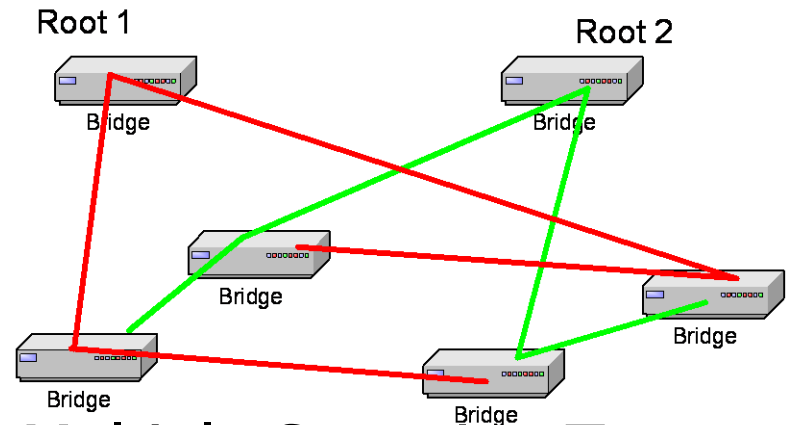
BME-TMIT



- Hálózati topológia: 2 kijárat
- A gyűrű redundanciát jelent
 - Nagyobb megbízhatóság



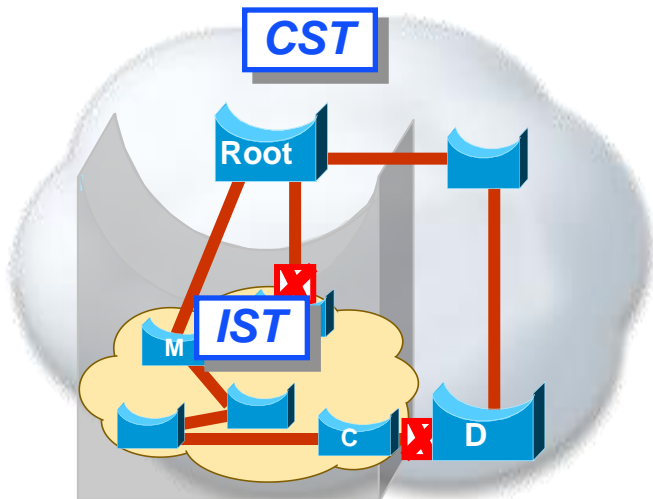
- STP: Egy feszítőfa



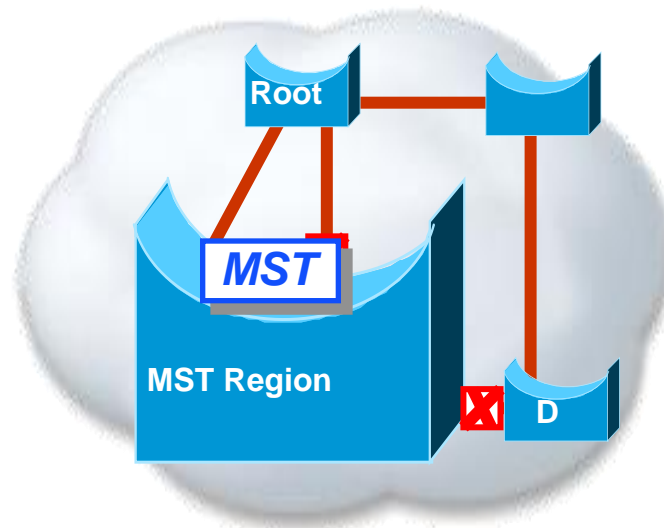
- Multiple Spanning Tree
 - 2 feszítőfa

802.1s: CST, IST, MST – Sok fa

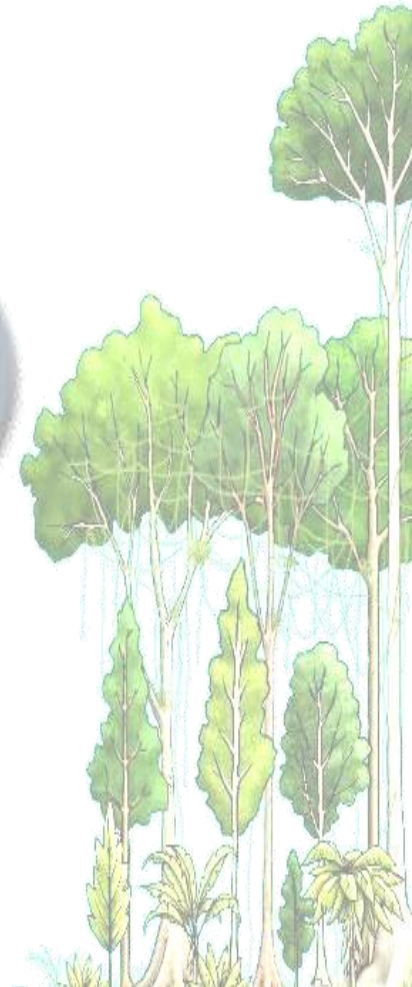
Belső nézet



Külső nézet



- **CST 802.1Q Common SPT** => Egyetlen fa
- **IST 802.1s Internal SPT** => a külső világ számára az MST-t egyetlen CST kapcsolónak mutatja
- **MST 802.1s Multiple SPT** => több VLAN egyetlen MST Instance-ba való összefogása



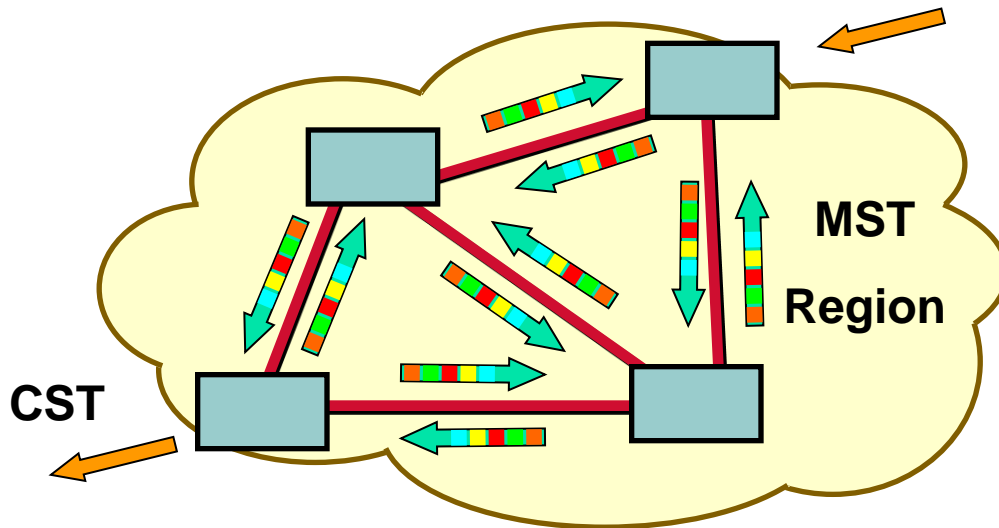
- Az MSTP lehetőséget nyújt régiók kialakítására
- A régiókat egymástól adminisztratív módon választhatjuk el
 - RG mező
- Előnyök:
 - egy régió belüli hiba nem zavarja a többi régió működését
 - Negy hálózat felbontása régiókra javítja a skálázhatóságot
 - A VLAN-ok lokális jelentőséget kapnak

- Miért használjunk régiót?
 - Különböző adminisztratív vezérlés az L2 hálózat különböző részei között
 - Nem minden switch támogat/futtat MSTP-t – különböző STP-k felosztják a hálózatot STP régiókra
 - Az MST előnyei régió**n belül érvényesülnek** azon kívül egyetlen példány (topológia) minden VLAN számára
- Az MST régió egy csoport összekapcsolt MST switch amely ugyanolyan MST konfigurációt használ
- Régió**n belül**: több példány
 - **IST** – Internal Spanning Tree (instance 0), mindig jelen van minden porton
 - **MSTI** - Multiple Spanning Tree Instance
- Régió**n kívül**: egy példány

MST instance-ok



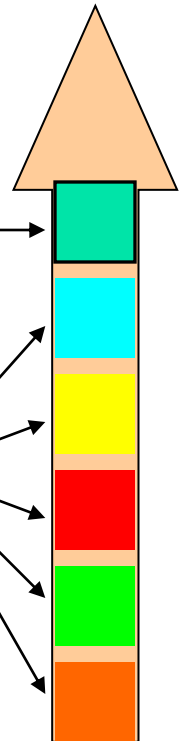
- Az MSTI-k STP példányok amelyek **csak a régió belül** értelmezettek
- Az MSTI-k nincsenek kapcsolatban a régió kívüli eszközökkel
- Az MST egyetlen BPDU-t küld az összes példánynak egy M-rekorddal példányonként
- Egyetlen példánynak van timer-alapú paramétere (az IST instance)
- Az MST BPDU-k **minden porton kiküldődnek**
- **A BPDU-k mindkét irányban küldődnek** ellentétben a 802.1D-vel, ahol csak a designated bridge küld



Protokoll információ az IST számára

Protokoll információ az MST példányoknak

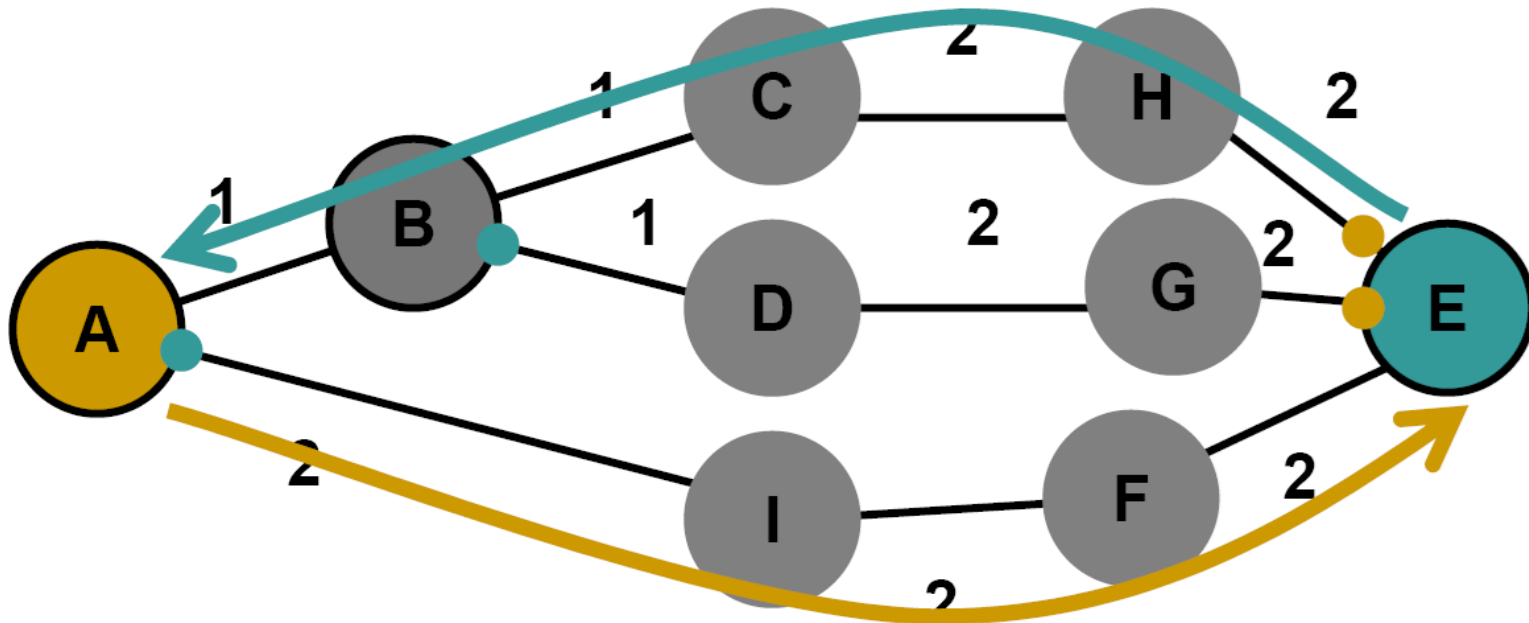
MST BPDU



Shortest Path Bridging



- IEEE 802.1aq
- Több fa, gyökerek a bridge-ekben
 - Mindegyik a legrövidebb utat használja
- Megoldandó
 - Szimmetrikus útvonalak...



- Speciális Multicast MAC címek
- Kevesebb mint IPv4 multicast
 - Mapping kell
- GMRP – Multicast regisztráció
 - GMRP és IGMP együttműködés szükséges

Multicast – IGMP snooping



BME-TMIT

- A kapcsoló figyeli az IGMPv2 üzeneteket
- Minden IGMP join üzenetre hozzáad egy bejegyzést a bridge által megtanult címekhez
 - Így a következő multicast csomag csak azon a porton fog megjelenni
- Az IGMP leave üzenet törli a bejegyzést
- Megszűnik a multicast broadcast jellegű továbbítása
- IGMPv3 – még nem széles körben támogatott!

Multicast címzés



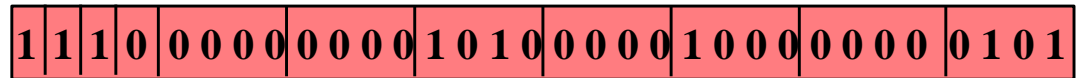
- Internet Assigned Numbers Authority (IANA)
- 224.0.0.1-224.0.0.255-->Reserved
- **224.0.1.0-238.255.255.255-->Multicast Group**
- 224.0.0.1: All multicast-capable hosts group
- 224.0.0.2: All multicast routers group
- 224.0.0.4: All DVMRP routers

Address Mapping



Class D Address 224 . 10 . 8 . 5

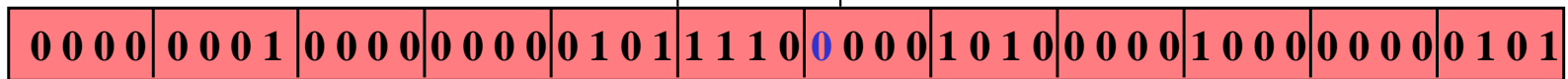
E 0 0 A 0 8 0 5



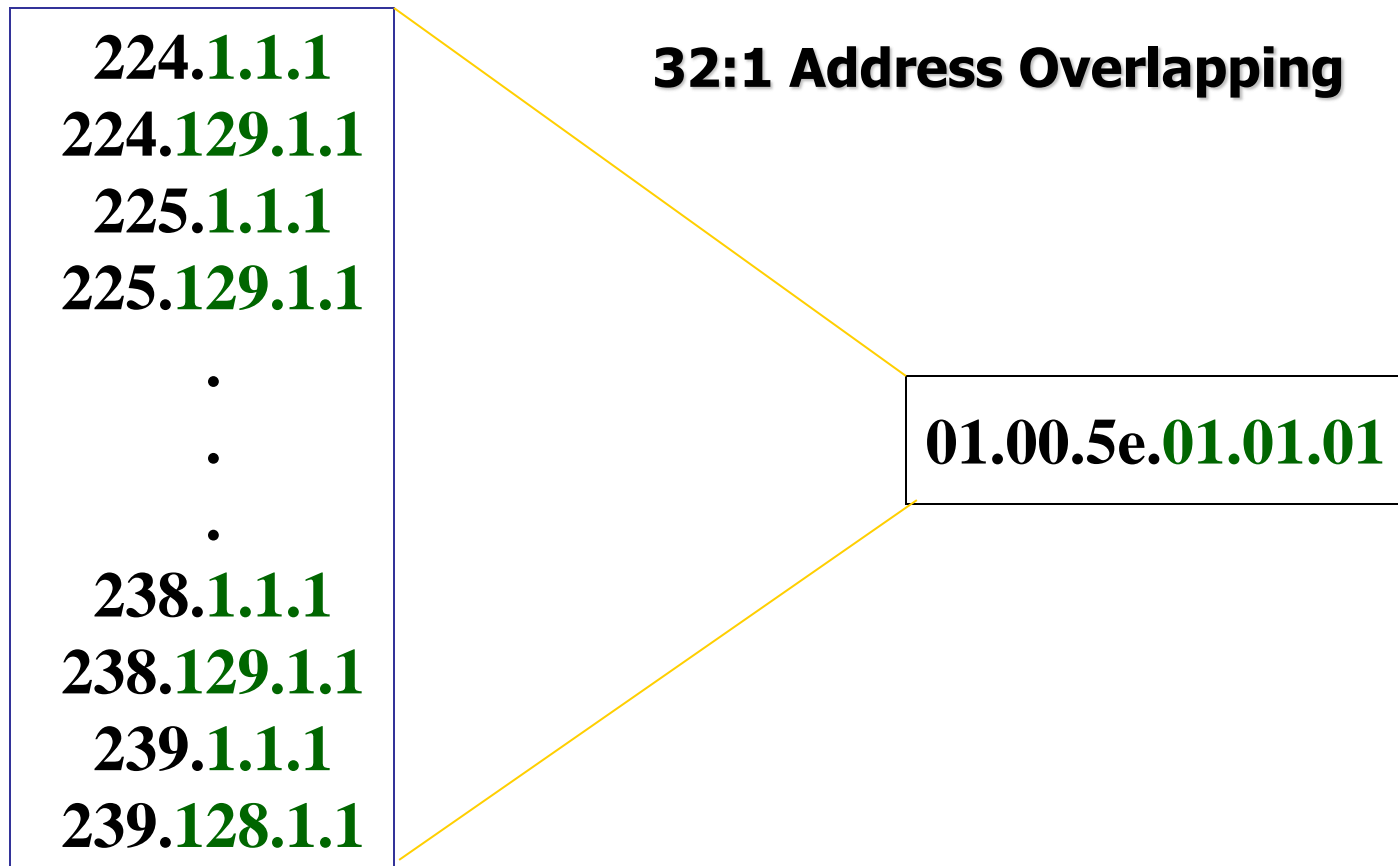
Ethernet Multicast Address

Not used

Low-ordered 23-bits mapped



0 1 0 0 5 E 0 A 0 8 0 5



- A broadcast jelleg miatt nagy a veszély
- Támadható pontok/területek
 - SPT DOS
 - ARP
 - MAC címek kicserélése
- A C-VLAN használata leszűkíti támadó lehetőségeit

- IPoE specifikus
 - DHCP snooping használata
 - Dinamikus ARP figyelés
 - ARP proxy
- Védekezni kell
 - BPDU szűrés – STP támadás ellen
 - PVLAN használata a trónk portokon
 - Traffic policing – a broadcast stormok ellen
 - A MAC címek limitálása egy porton

- O'Reilly ***Ethernet: The Definitive Guide***
 - by Charles E. Spurgeon
- IEEE 802.3 szabvány
- Cisco – Understanding STP, RSTP

Kérdések?



Budapest University of Technology and Economics



Department of
Telecommunications and Media Informatics