

Ethernet – második rész

Moldován István

2022. október 10.



Budapest University of Technology and Economics

**Department of
Telecommunications and Media Informatics**



- 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

A VLAN által nyújtott előnyök és hátrányok



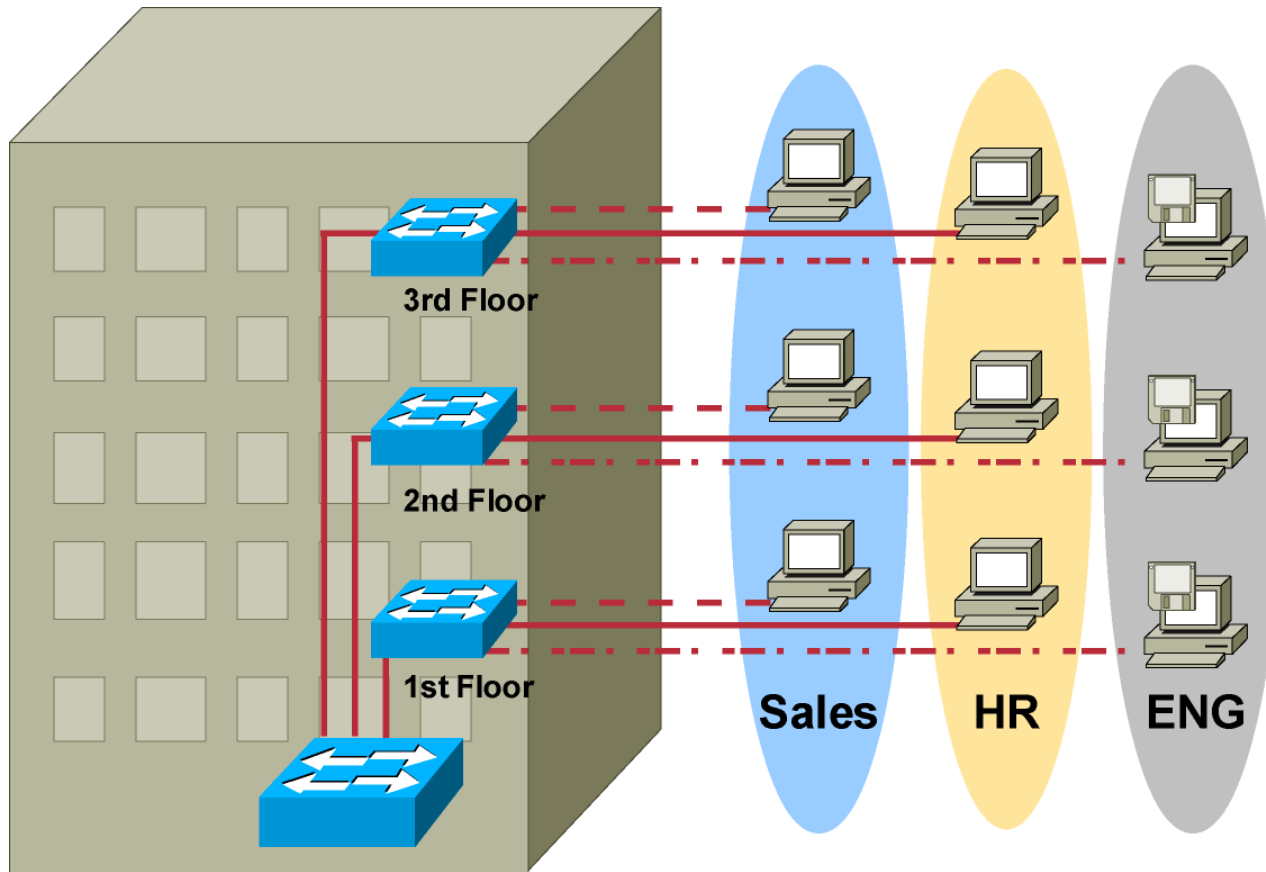
BME-TMIT

- Előnyök:
 - könnyebb kezelni a felhasználók helyváltoztatását (mobilitás)
 - szórt adás kiterjedésének csökkentése
 - felhasználók virtuális elkülönítése
 - hatékonyabb topológia (esetleg átlapolódás is a VLAN-ok között)
 - biztonság nő
 - virtuális munkacsoportok
- Hátrányok:
 - a virtuális munkacsoportoknál túl gyakorivá válhat a tagság változása
 - Adminisztrációs problémák
 - WAN-ra kiterjedő VLAN-nál a szórt adás már főbb vonalakat is terhelhet

VLAN Áttekintés



BME-TMIT



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

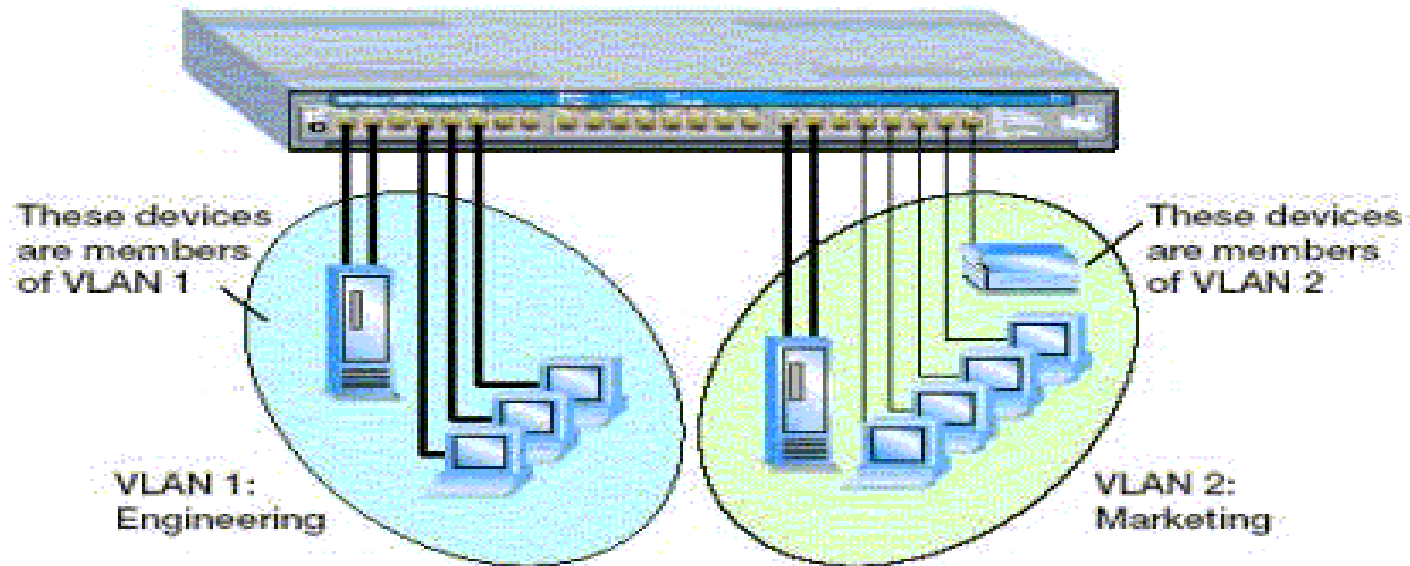
1 VLAN = 1 Broadcast Domain = 1 Logikai hálózat (Subnet)

- 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

Megosztott kapcsoló példa



BME-TMIT



1. VLAN: 2., 4., 6., 9. port

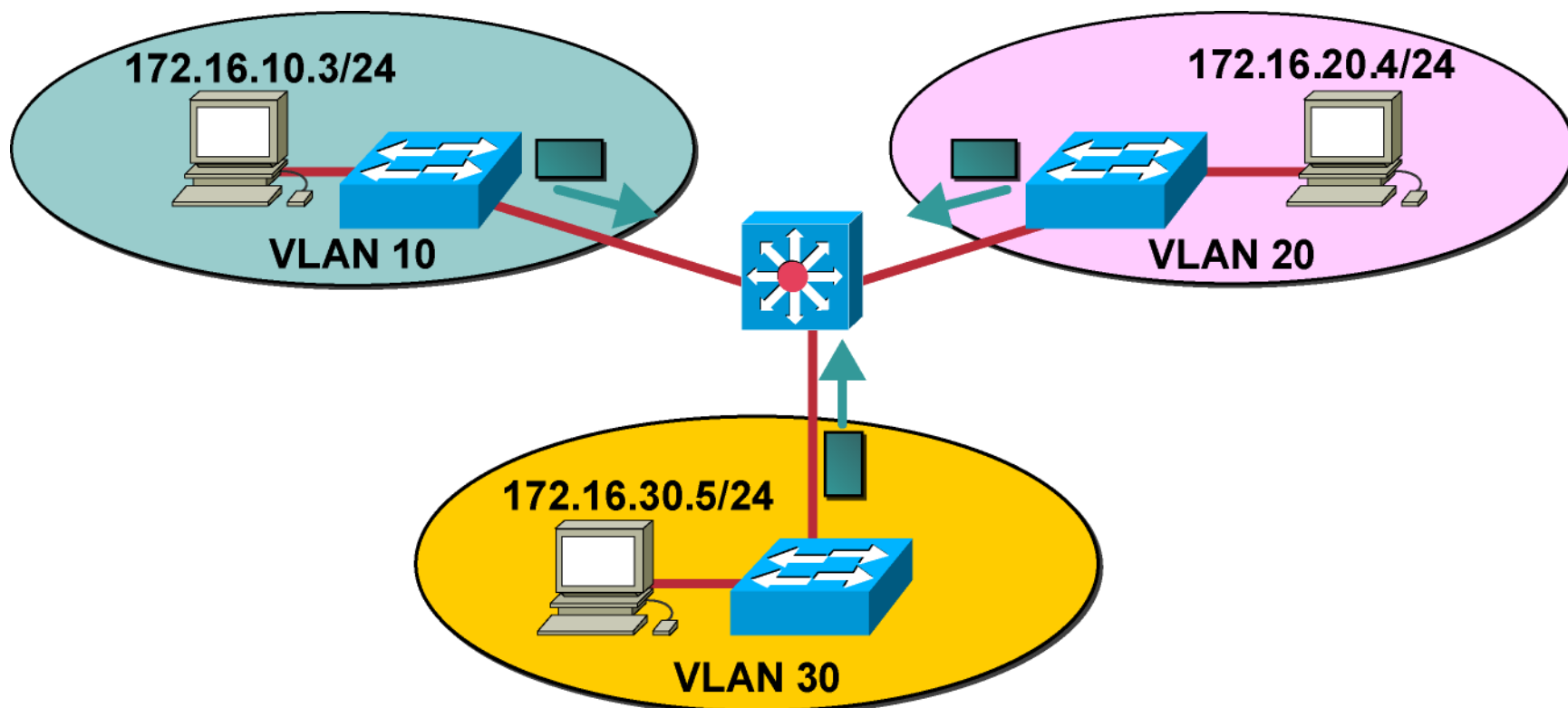
2. VLAN: 17., 19., 21., 23. port

Egymás forgalmát nem látják!

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

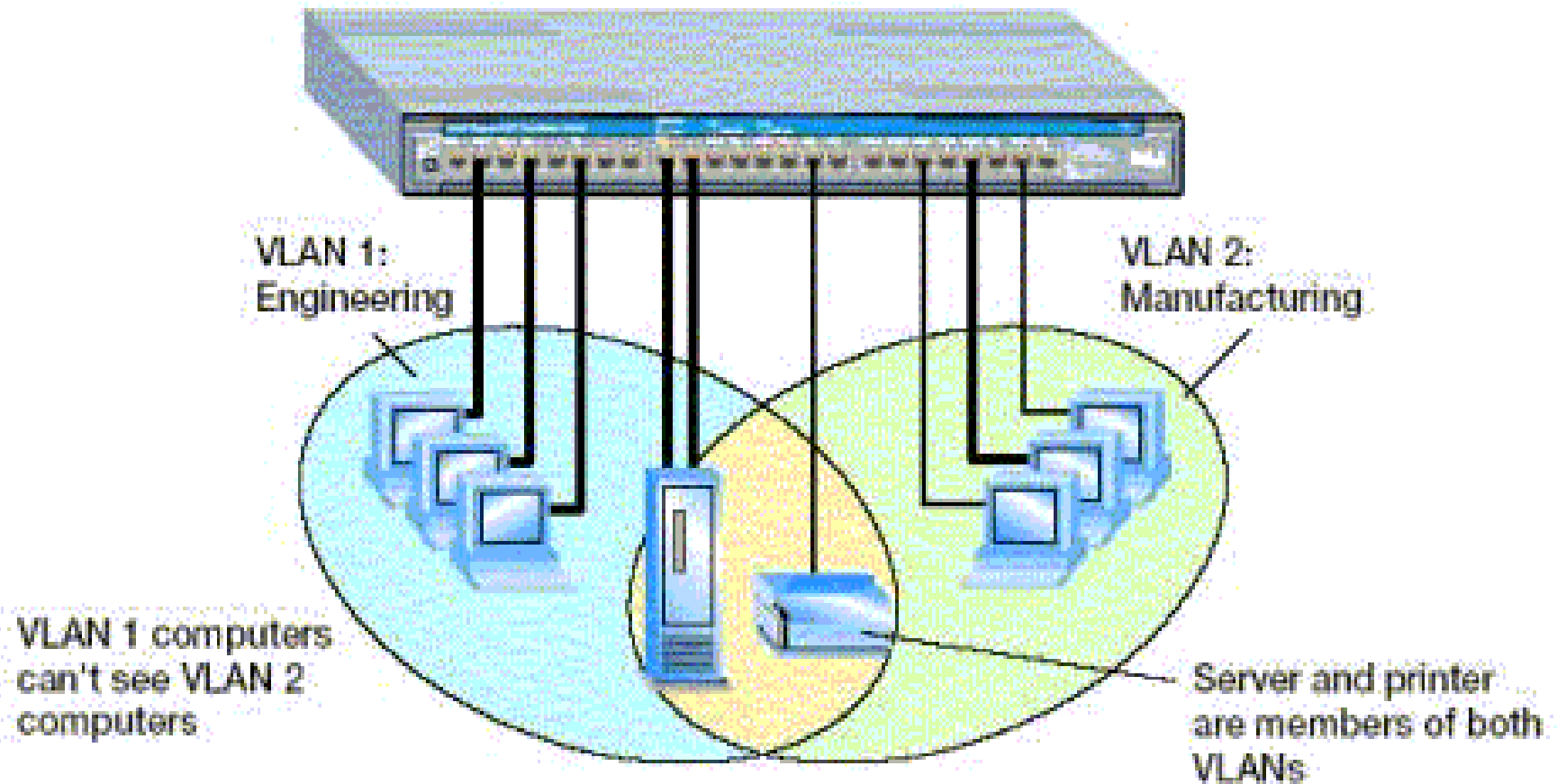
- minden IEEE 802 LAN MAC protokoll felett használható
- könnyű adminisztráció (létrehozás, tag hozzáadása, stb.)
- két különböző VLAN között nincs forgalom (adatkapcsolati szinten)
- egy LAN-on belül több csoport is elkülöníthető
- jól megválasztott csoportok esetén forgalomcsökkenés érhető el

- 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

VLAN-ok átfedése



BME-TMIT

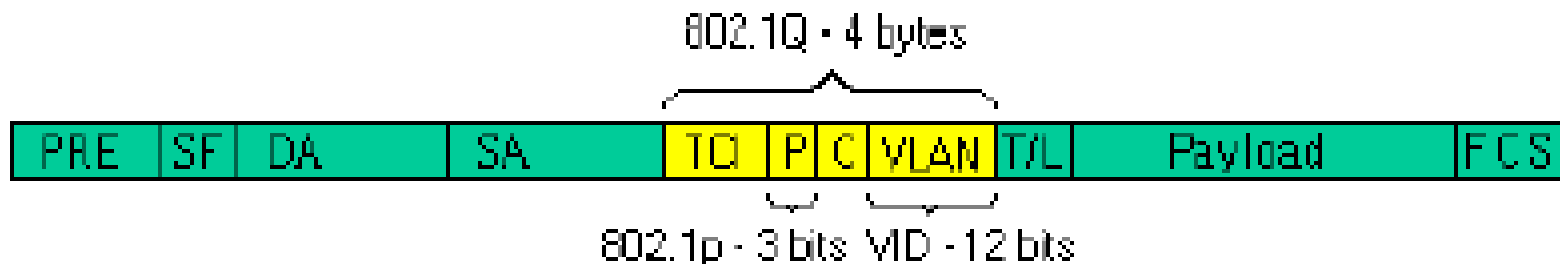


.1Q VLAN keretformátum



BME-TMIT

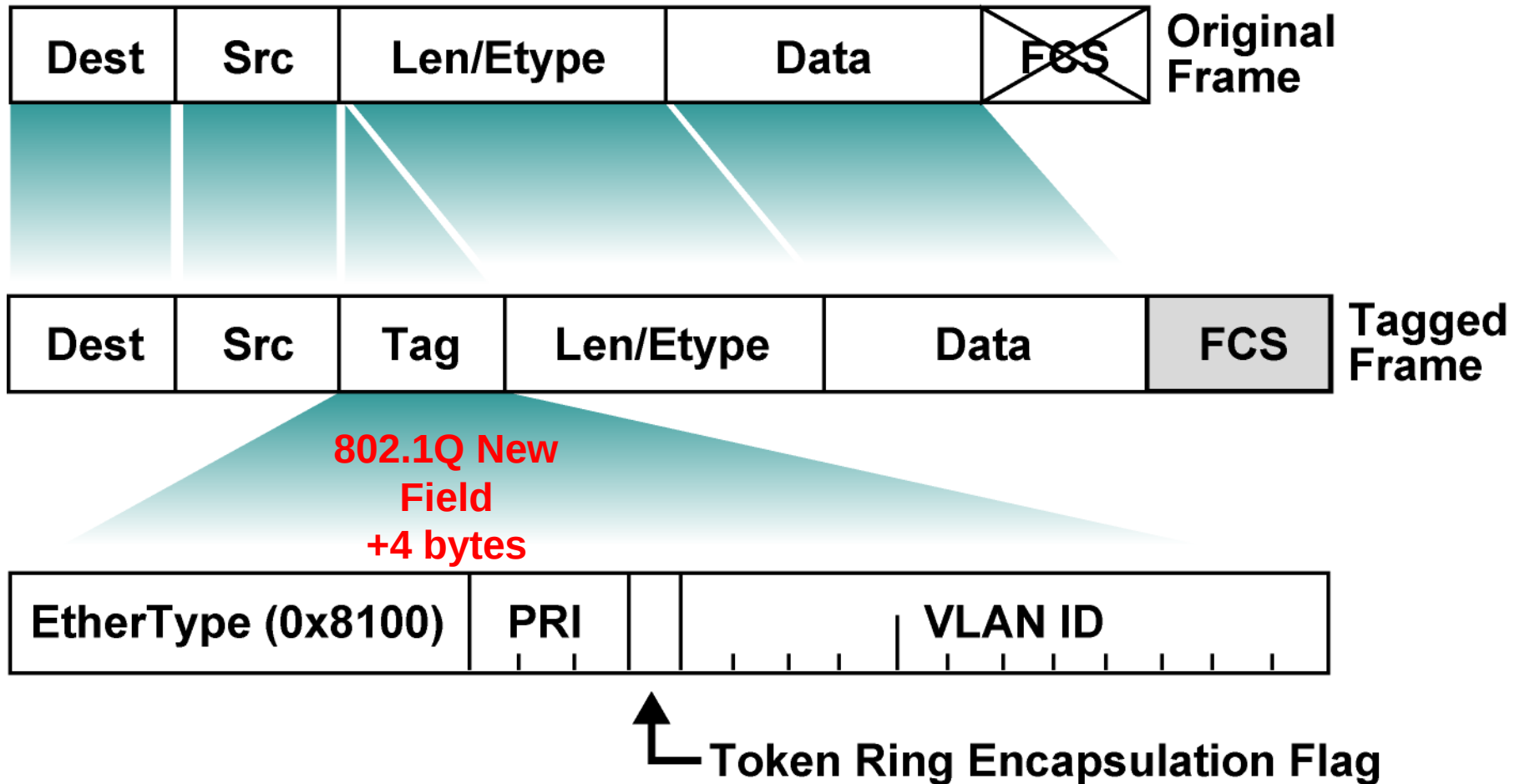
- A VLAN tag tárolásához új mezők az Ethernet-keretben
 - 4 bájtal nő az Ethernet keret
- Helye közvetlenül a forrás MAC cím után
- Lehetővé teszi a minőségbiztosítást is
 - 802.1p prioritás bitek



802.1Q Tag Formatum



BME-TMIT

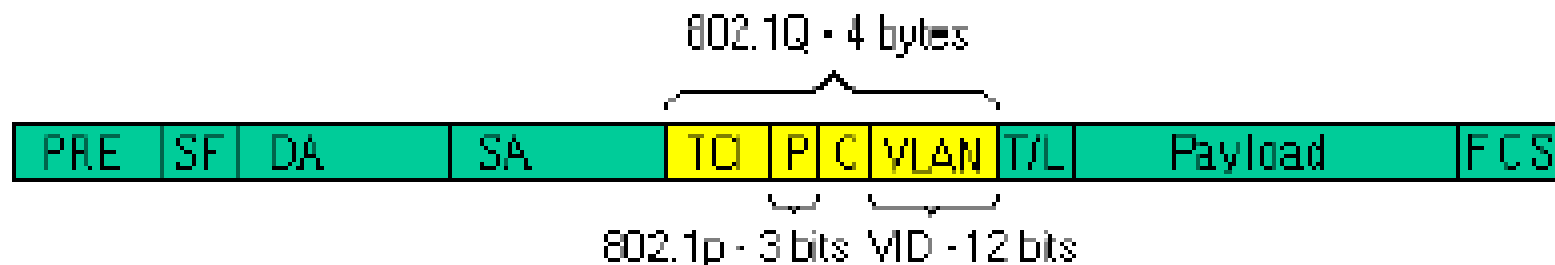


Új keretformátum – 2.



BME-TMIT

- 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)



- Régi berendezések:
 - A TCI mező értéke 0x8100, melyet típusként értelmeznek
 - Ha nem támogatja, nem tudja értelmezni tehát eldobja a keretet
- megoldás: az új, tag-el rendelkező kereteket támogató eszközök csatlakoztatásánál a régi típusúak felé csatlakozó portokon a tag leválasztása

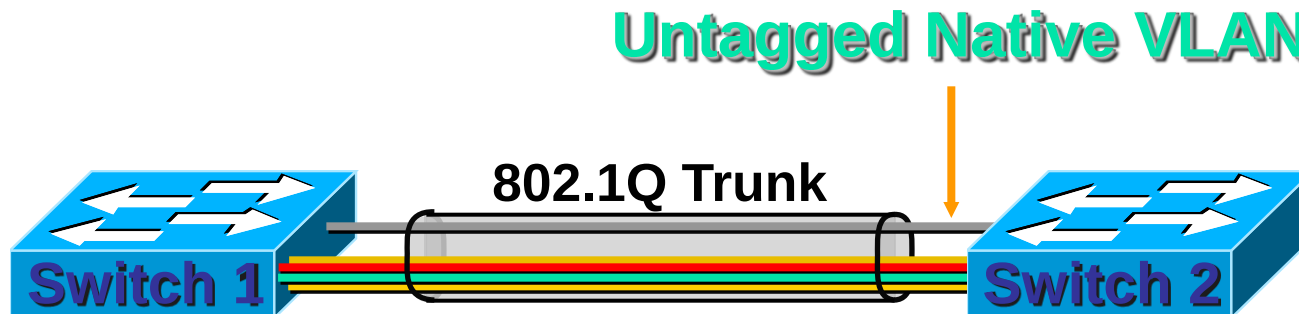
- VLAN Identifier
- 0-4095 tartomány
- 0: alapérték
 - ha a keret eredetileg tag nélküli volt, ezt kapja meg
- 4095: fenntartva, az ilyen VID-jű kereteket eldobjuk
- lehetőség van rá, hogy a tag nélküli keret 0-tól különböző értéket kapjon (port-based VLAN, Port VID)
 - Port VID: a switch minden portjának van, azt mutatja, hogy a tag nélküli keretet melyik VLAN-ba továbbítsák

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 fejléct
- 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)

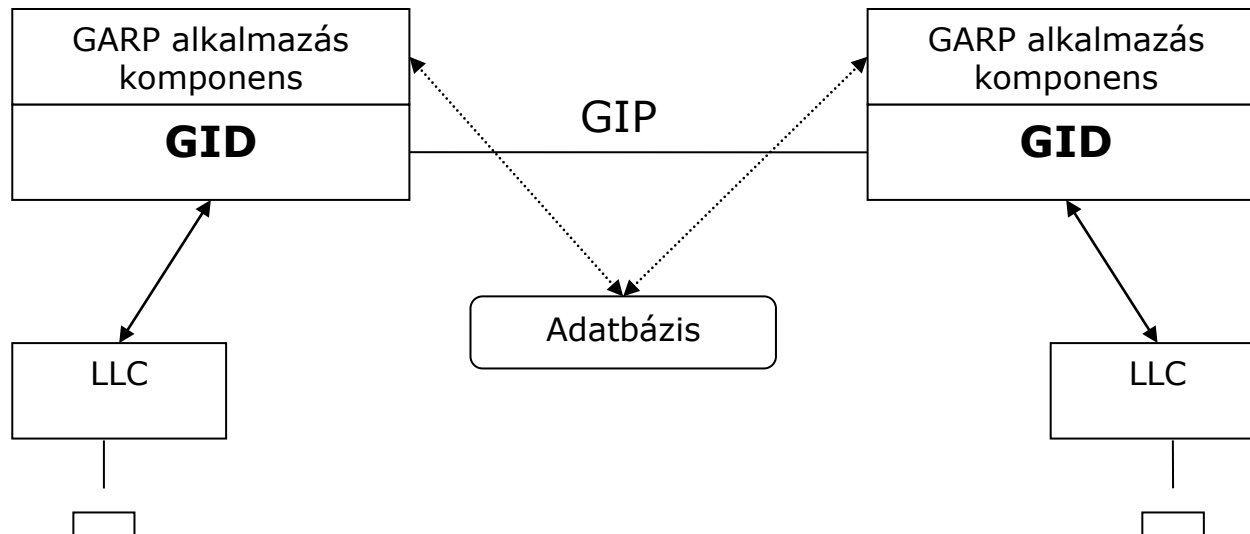
- a legegyszerűbb megoldás
- a switch egyes portjaihoz hozzárendeljük a megfelelő VLAN azonosítóját
- egy porthoz legfeljebb egy azonosító tartozhat
- a VLAN változtatásakor csak a switch-hez kell nyúlni – a felhasználó számára átlátszó

- 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)

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

- *Statikus:*
a VLAN tagság információk manuálisan állíthatóak, a dinamikus terjesztés protokolljai tiltva vannak.
- *Dinamikus:*
GVRP (GARP VLAN Registration Protocol) használatával az információ dinamikusan terjed, ha valami változás történik.
- *Vegyes:*
egyes nyilvántartott VLAN-ok információi csak statikusan, másoké csak dinamikusan változtathatóak.

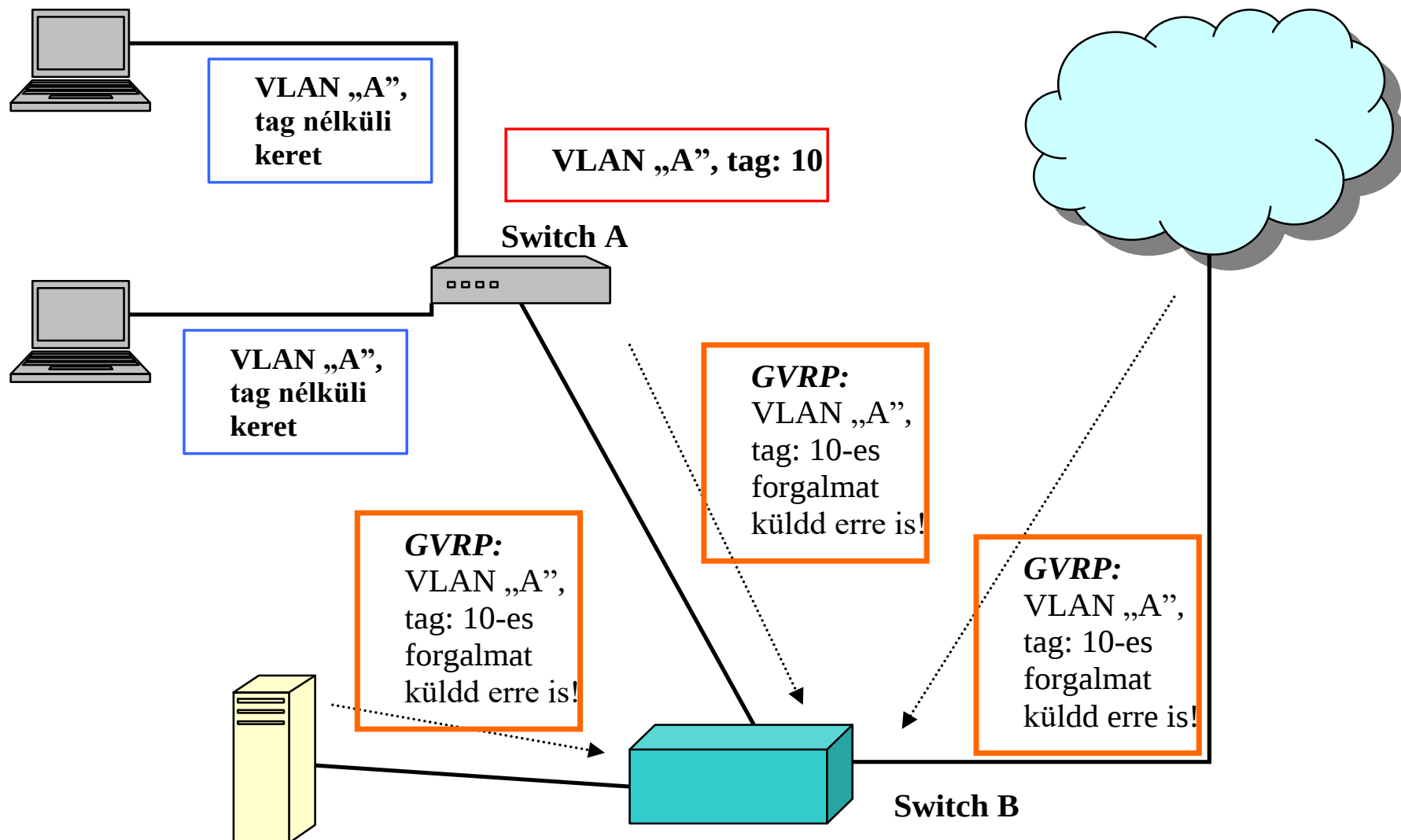
- Alapja a GARP (Generic Attribute Registration Protocol).
 - GARP alkalmazás komponens
 - GARP Information Declaration (GID)
 - GARP Information Propagation (GIP)



GVRP – GARP VLAN Registration Protocol

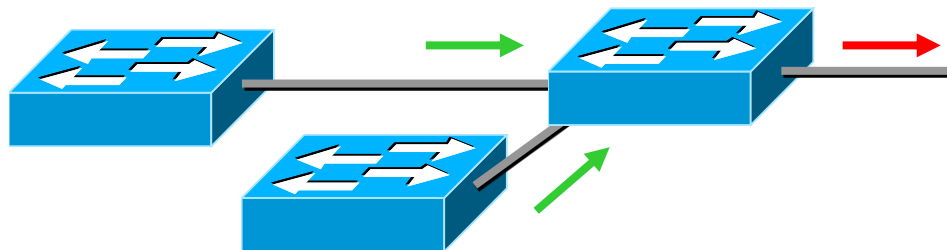


BME-TMIT



- 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

- IP QoS/ToS Mechanizmusok
 - Transzparens módon használhatók a TAG-al ellátott vagy anélküli linkeken
 - Ethernet szintű torlódás esetén az IP QoS nem garantált
 - Ethernet szintű torlódás:
- Mapping functionalitás szükséges az Ethernet CoS és IP ToS együttműködéséhez
- Az QoS/CoS aktuális megvalósítása QoS/CoS a kapcsoló architektúrájától függ és változó lehet
 - Nem egyértelműen szabványosított

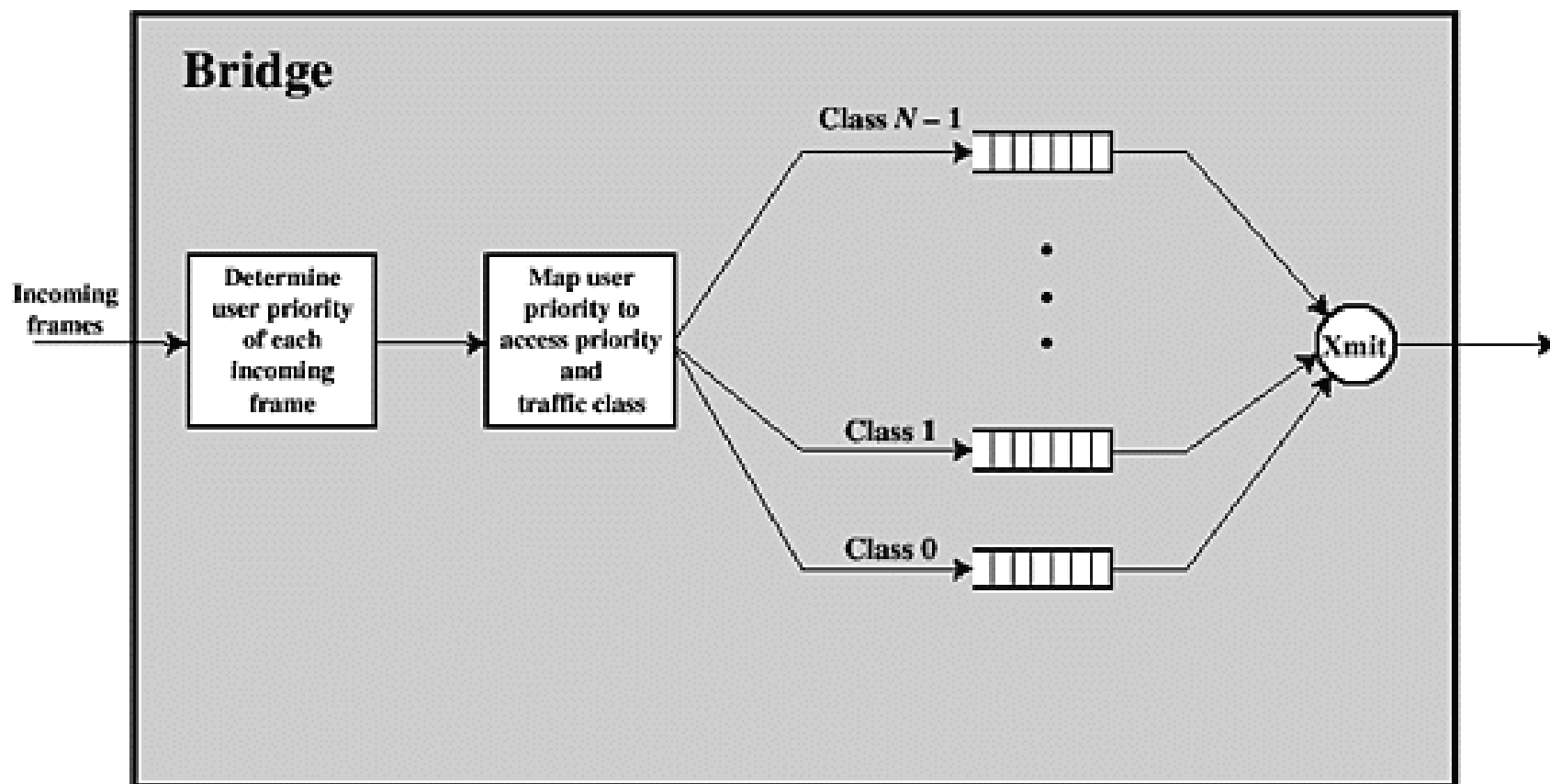


- **Network Control:** legnagyobb prioritás
- **Voice:** kisebb mint 10 ms késleltetés
- **Video:** kisebb mint 100 ms késleltetés
- **Controlled Load:** fontosabb alkalmazások
- **Excellent Effort:** fontosabb előfizetők BE forgalma
- **Best Effort:** alap prioritás
- **Background:** letöltések, játékok, stb

IEEE 802.1D forgalmi osztályok kezelése



BME-TMIT

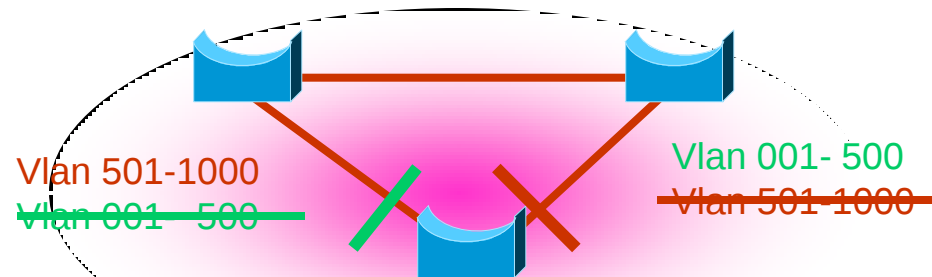


- Az RSTP hátránya: rossz hálózati kihasználás
- Cisco: PVST (Per-VLAN feszítőfa)
 - Minden VLAN: egy RSTP
 - Sok VLAN – nem skálázható, fölösleges
- IEEE: MSTP
 - Lehetővé tesz több feszítőfát
 - A VLAN-ok a feszítőfákhoz vannak rendelve

PVST vs. 802.1Q vs. 802.1s

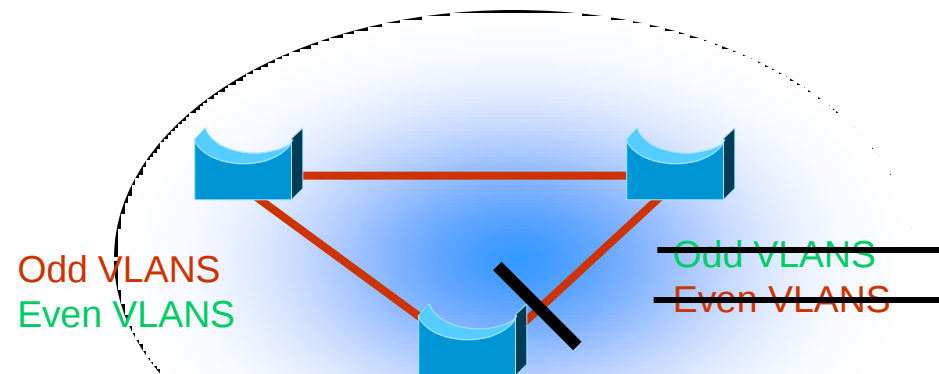


BME-TMIT



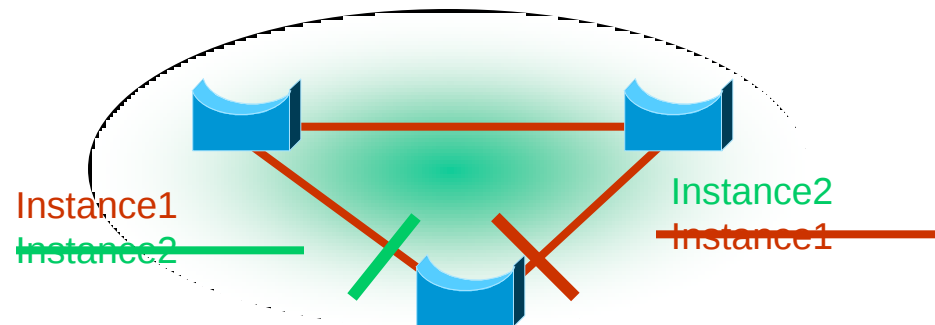
Prop. PVST egy STP per VLAN

Skálázhatóság 1000 nagyságrendű Vlan-ra (SPT!) nagy kihívás



802.1Q egyetlen SPT

Load sharing nem lehetséges



802.1s több SPT

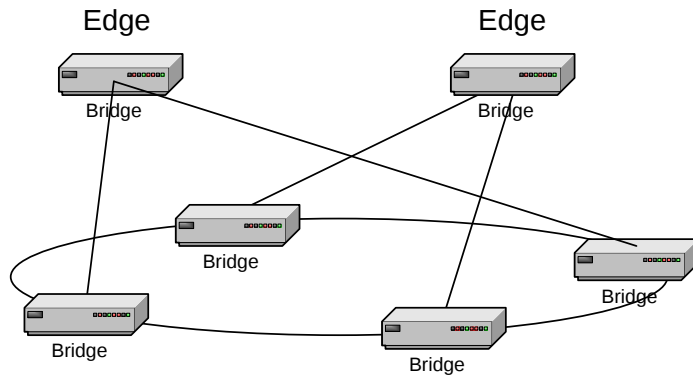
HATÉKONY Load sharing lehetséges

- 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!

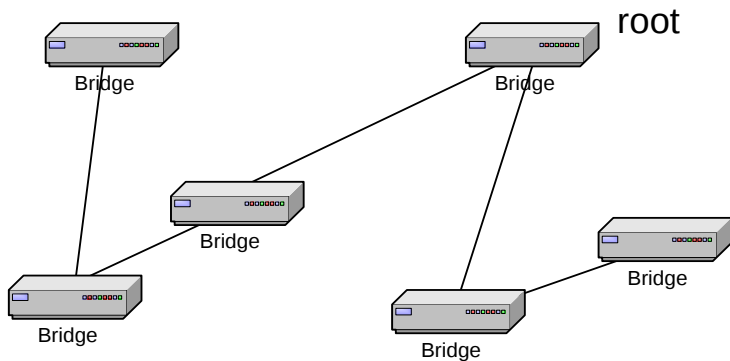
MSTP előnyei



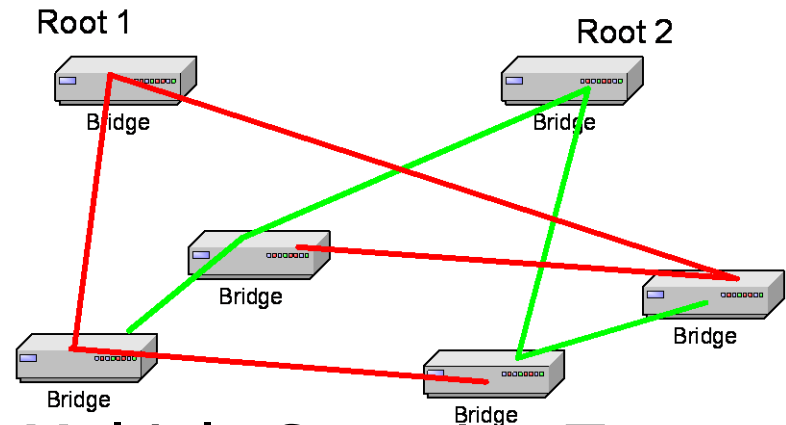
BME-TMIT



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



- STP: Egy feszítőfa



- Multiple Spanning Tree
 - 2 feszítőfa

- **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

MST régiók - 2



BME-TMIT

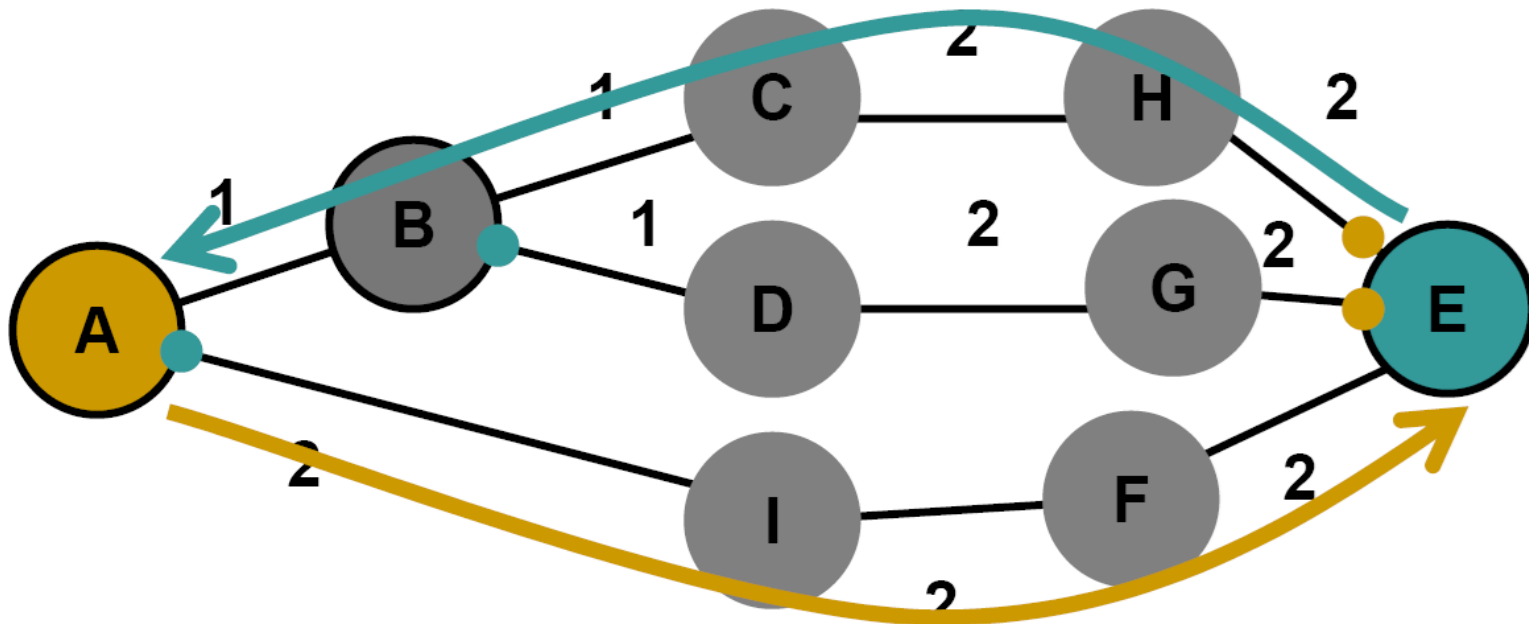
- Miért használjunk régiót?
 - Különböző adminisztratív vezérlés az L2 hálózat különböző részei között
 - Nem minden switch támogat/futtat MSTP-t – különböző STP-k felosztják a hálózatot STP régiókra
 - Az MST előnyei régióon belül érvényesülnek azon kívül egyetlen példány (topológia) minden VLAN számára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

Shortest Path Bridging



BME-TMIT

- 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



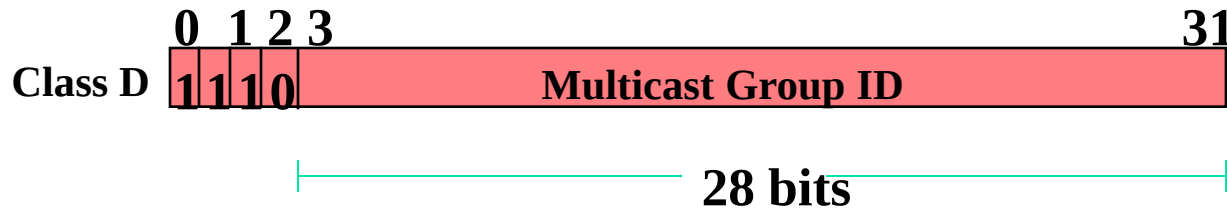
BME-TMIT

- 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!

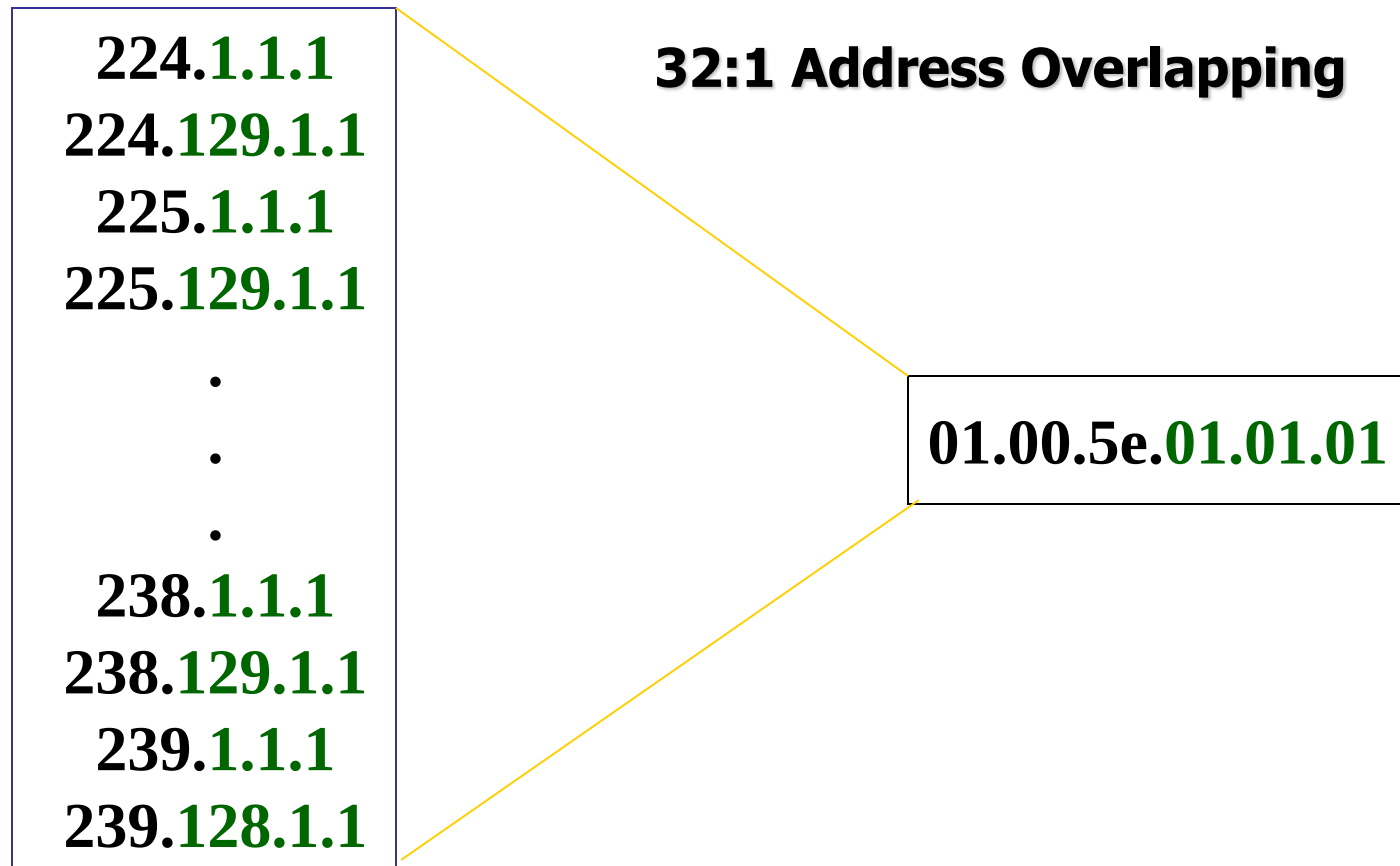
Multicast címzés



BME-TMIT



- 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

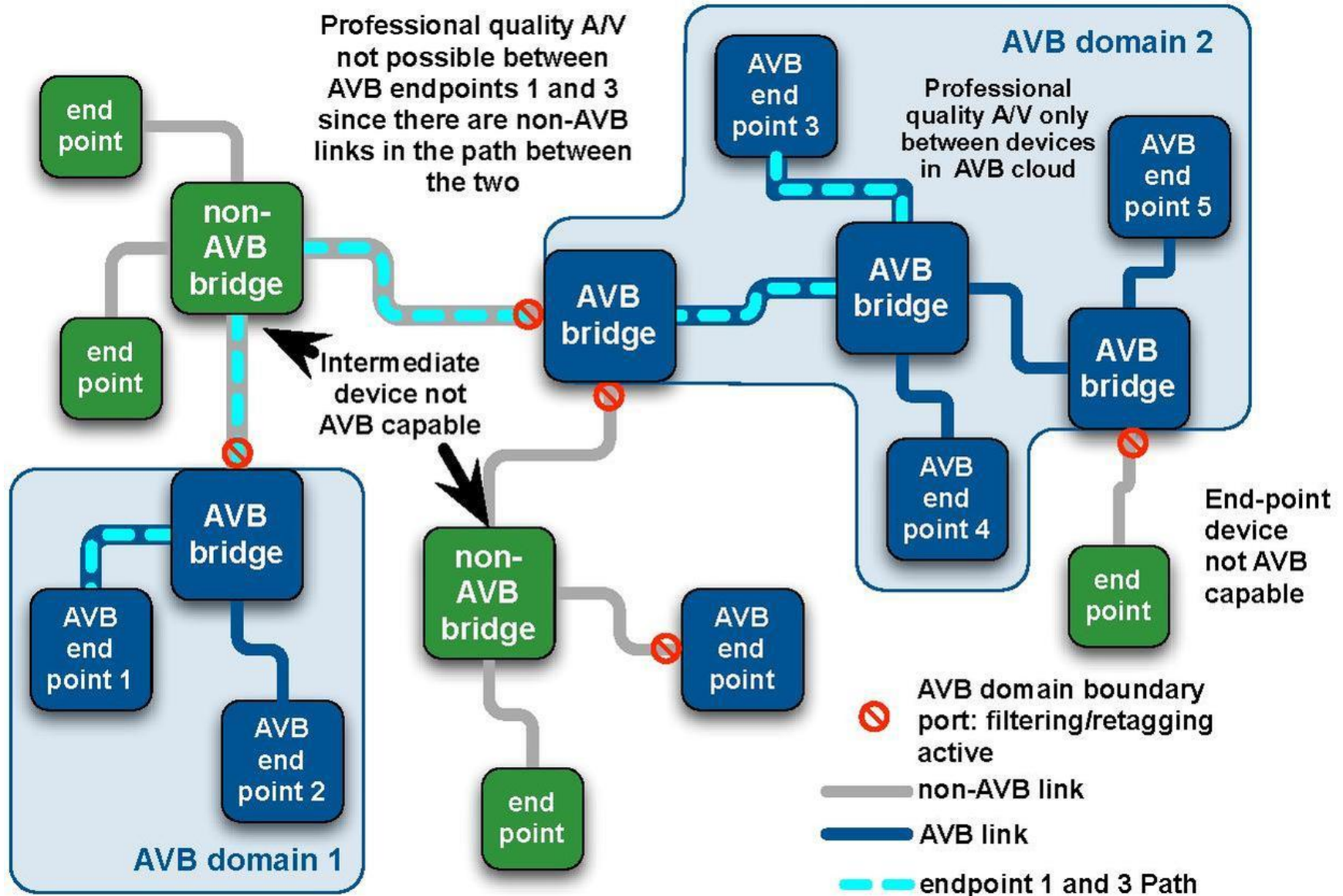




- A broadcast jelleg miatt nagy a veszély
- Támadható pontok/területek
 - SPT DOS
 - ARP
 - MAC címek kicserélése
- A C-VLAN használata leszűkíti támadó lehetőségeit

- 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

AVB – Audio Video Bridging



- 802.1AS – idő szinkron
- 802.1Qav – továbbítás
- 802.1Qat – Erőforrás foglалás
- 1722 - beágyazás

AVBTP network stack.

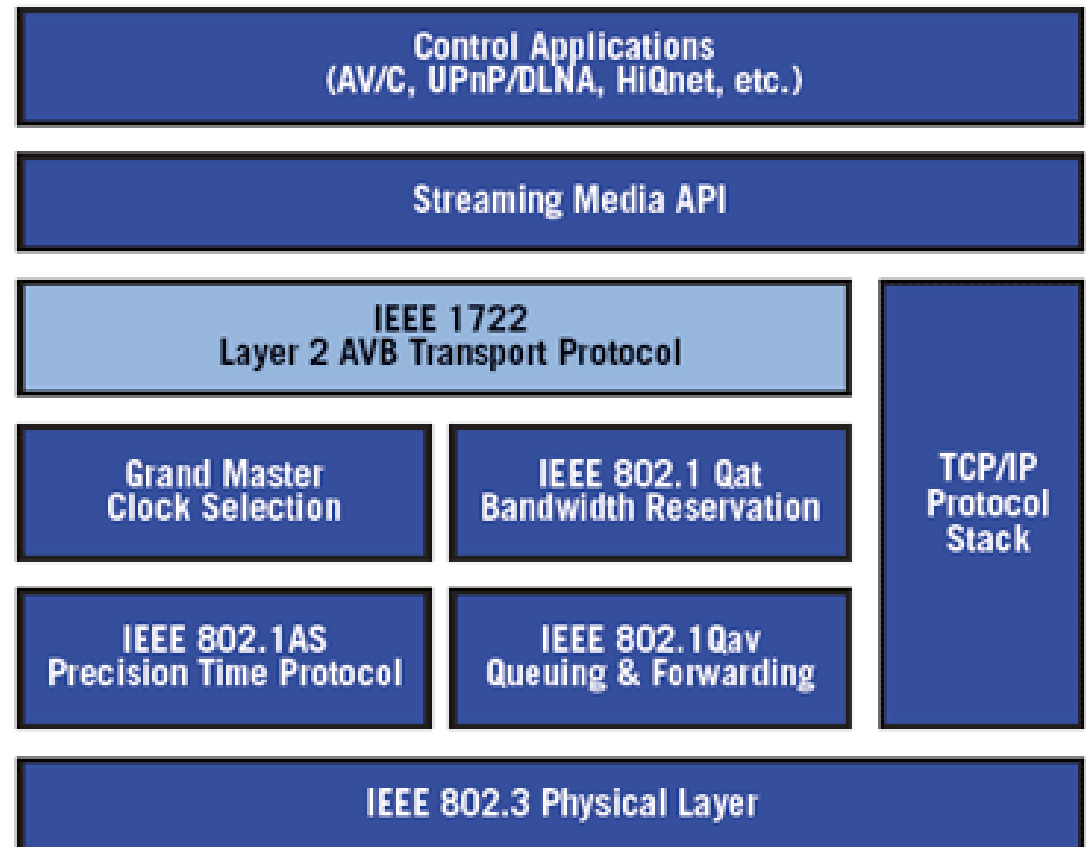


Figure 1

- Az AVB „utódja” – átnevezés
- Tágabb felhasználási terület
 - Ipar
 - Autók
 - Stb.
- A szabványosítás jelenleg is folyik
 - Új szabványok

- › P802.1Qbu – Frame Preemption – ready
 - › P802.1Qbv – Enhancements for Scheduled Traffic – ready
 - › P802.1Qcc – Stream Reservation Protocol (SRP) Enhancements and Performance Improvements
 - › P802.1Qci – Per-Stream Filtering and Policing
 - › P802.1Qch – Cyclic Queuing and Forwarding
 - › 802.1Qcj – Auto-attach to PBB services
 - › P802.1AS-Rev – Timing and Synchronization – Revision
 - › P802.1CB – Frame Replication and Elimination for Reliability
 - › P802.1CM – Time-Sensitive Networking for Fronthaul
- related
- related to each other

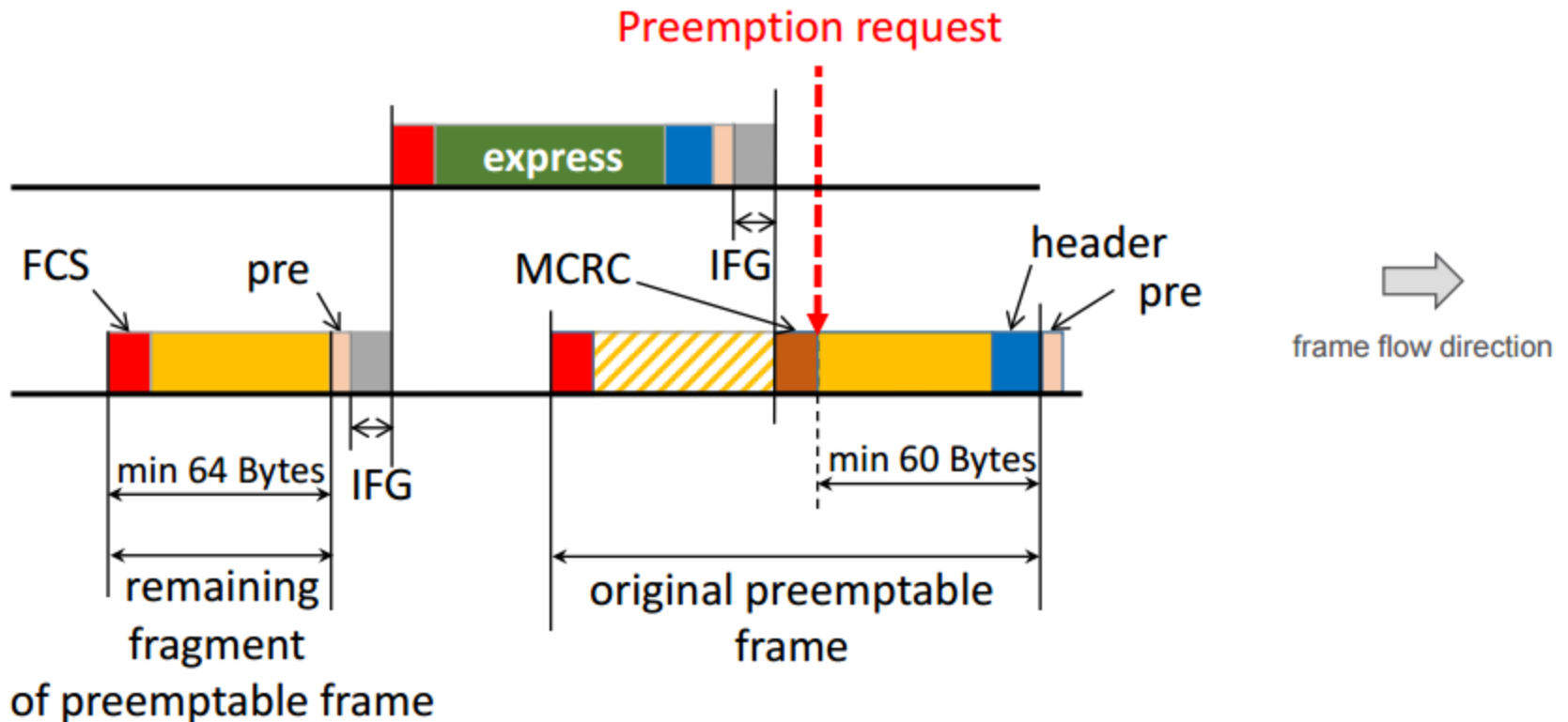
Frame Preemption



BME-TMIT

2. 802.1Qbu – Frame Preemption

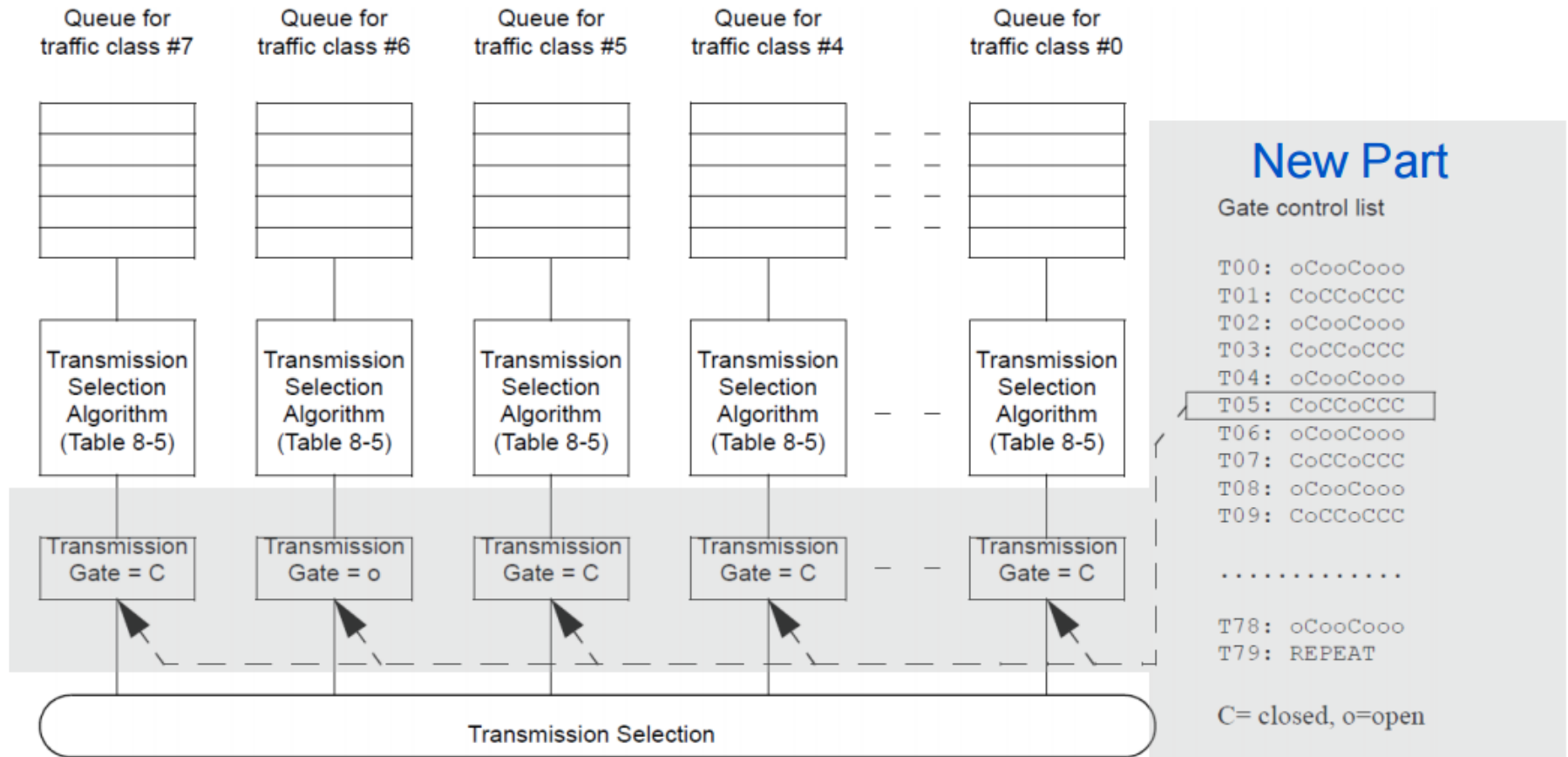
1. 802.3br – Interspersing Express Traffic (IET)



802.1Qbv – Time Gated Queuing



BME-TMIT

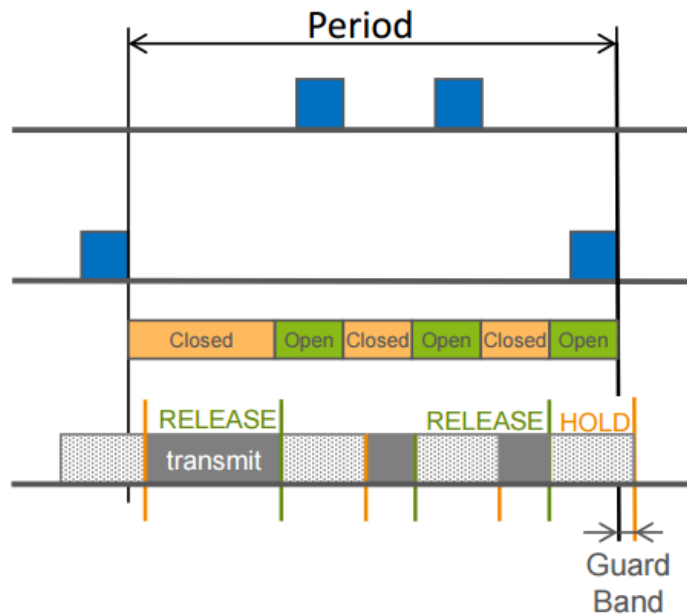


Time Gated Queuing – Működés



BME-TMIT

Example 1



Legend

Express From Port 1

Express From Port 2

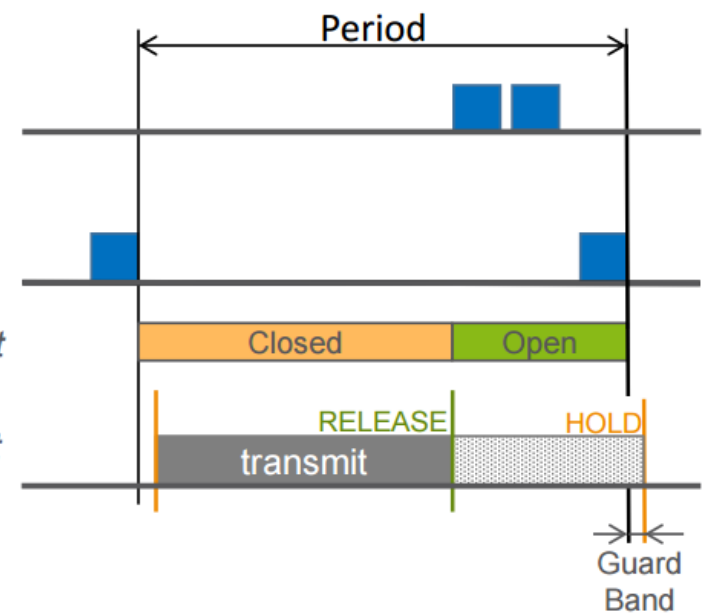
Express Gate at egress port

Preemptable at egress port



frame flow direction

Example 2



Köszönöm a figyelmet

- Vége -



Budapest University of Technology and Economics

**Department of
Telecommunications and Media Informatics**

