

Számítógép-hálózatok

Hálózatközi együttműködés

2023/2024. tanév, I. félév

Dr. Kovács Szilveszter

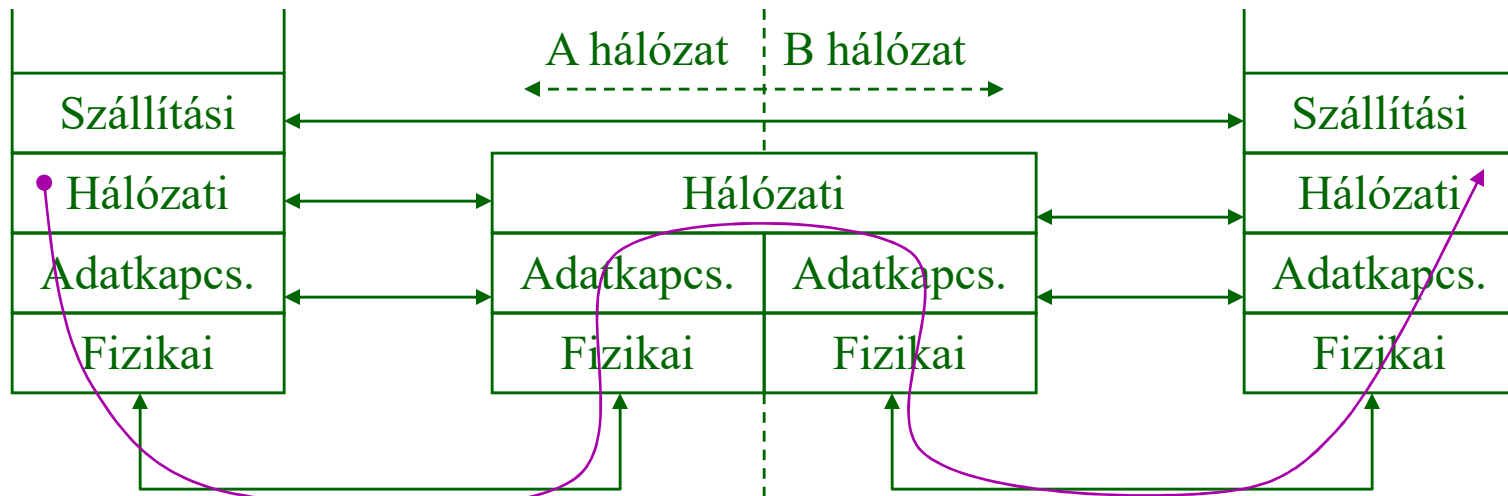
E-mail: szkovacs@iit.uni-miskolc.hu

Informatikai Intézet 106/a.

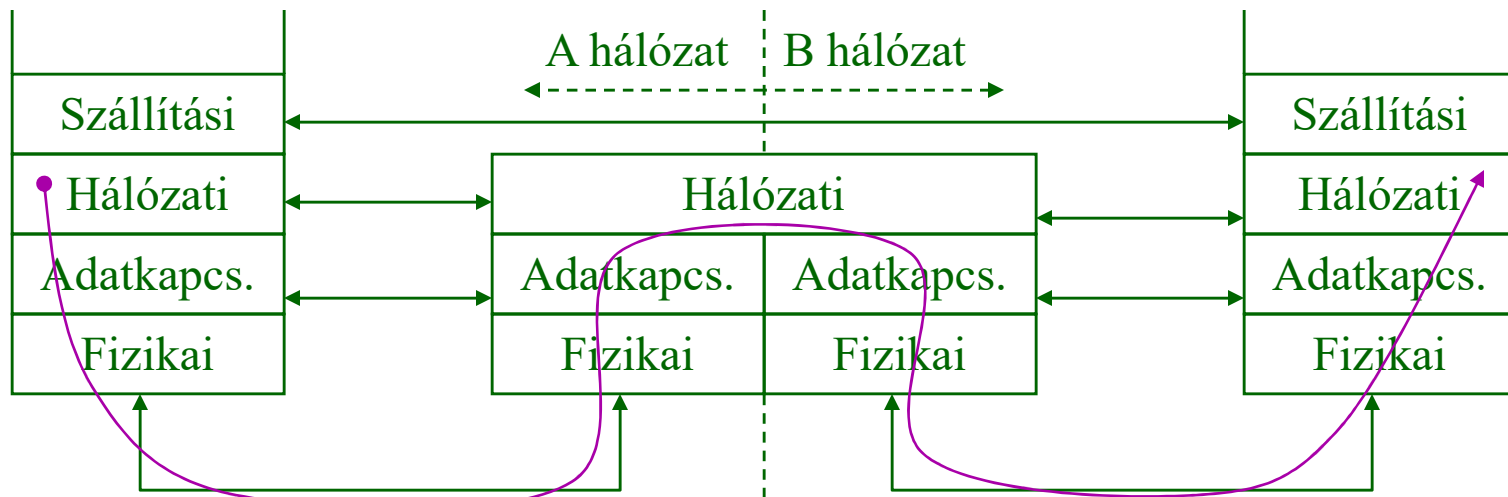
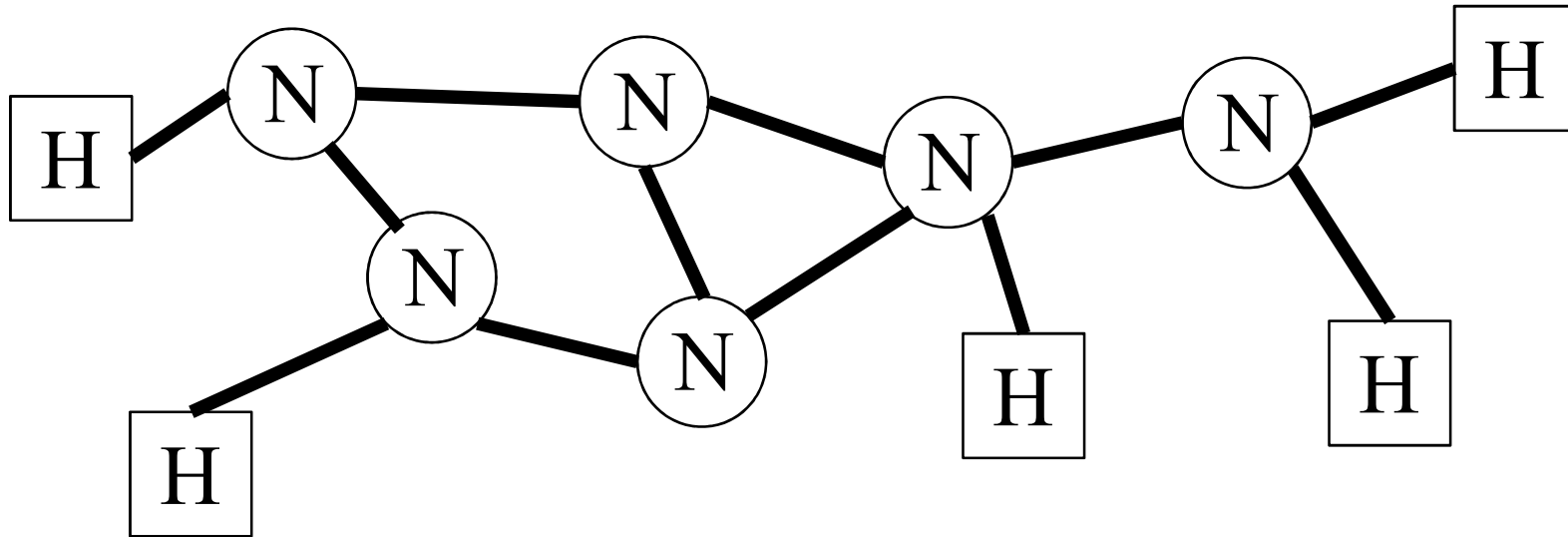
Tel: (46) 565-111 / 21-07

Motiváció

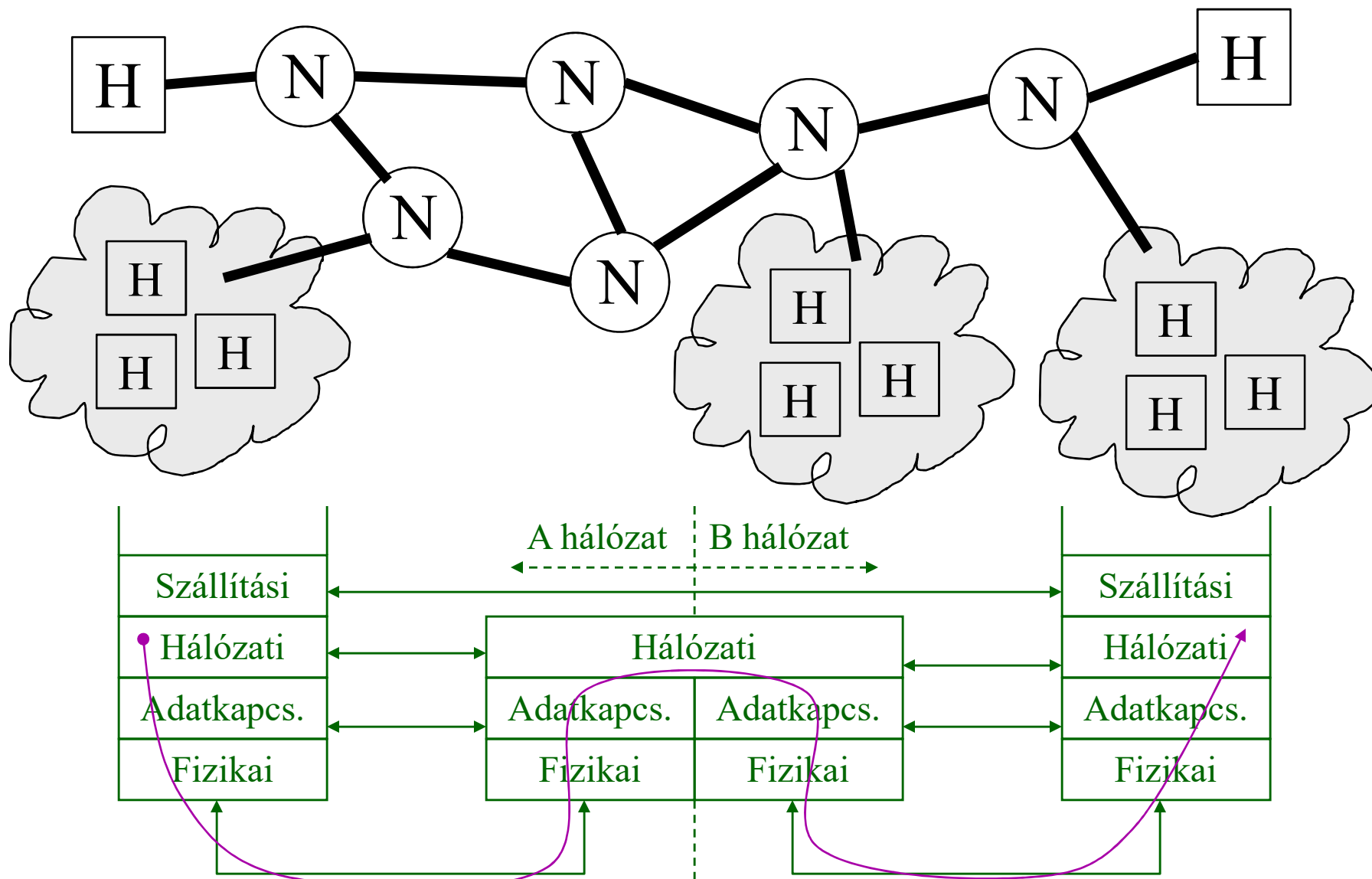
- **Különböző hálózatok összekapcsolása**
⇒ **Heterogén hálózat kialakítása**
⇒ **A hálózat (méretének) kiterjesztése**
- **Az OSI modell szerint ez csak a 3. (hálózati) rétegben történhet**
(forgalom irányítás, torlódás vezérlés)
- **A hálózatközi együttműködés OSI modellje:**



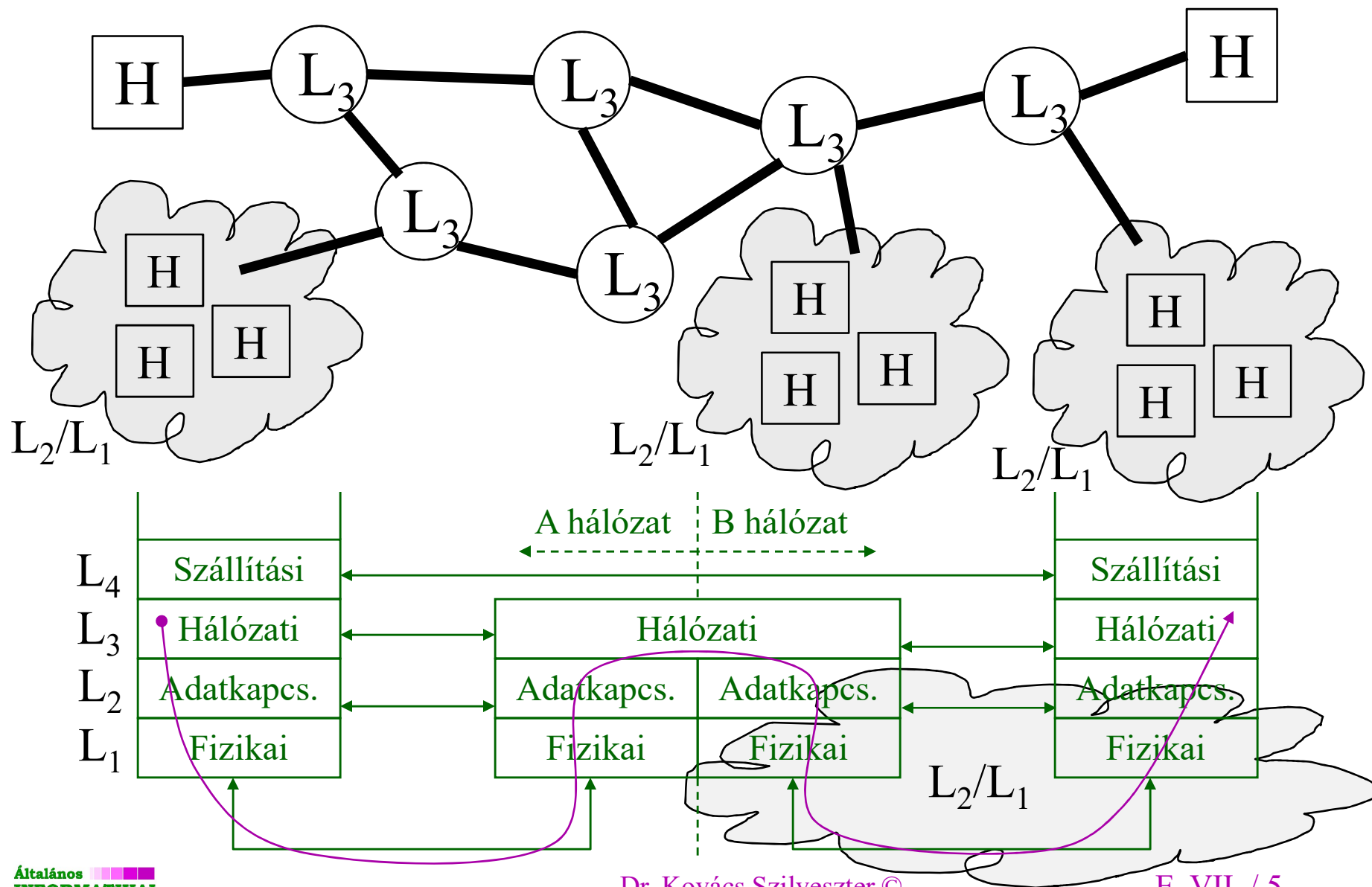
Hálózatközi együttműködés



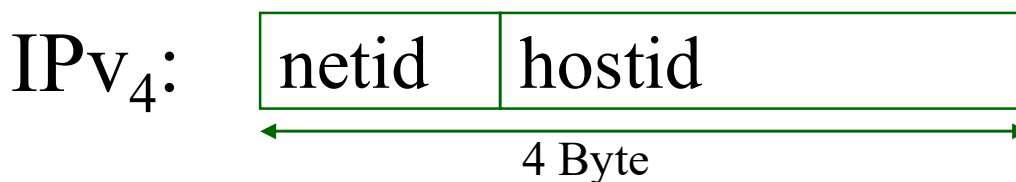
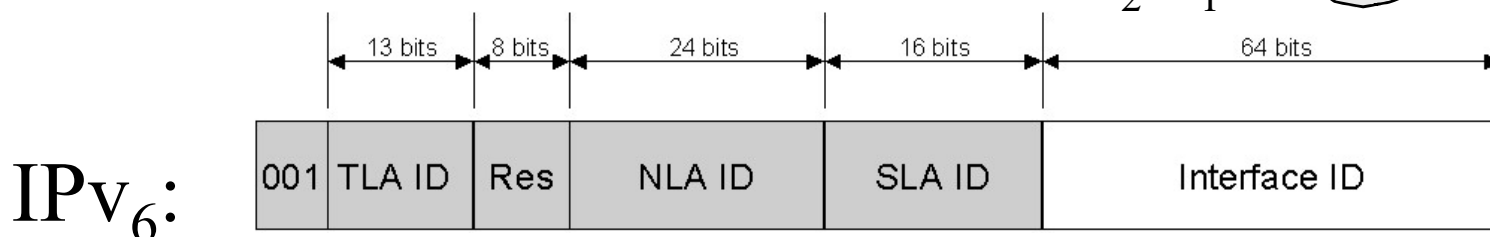
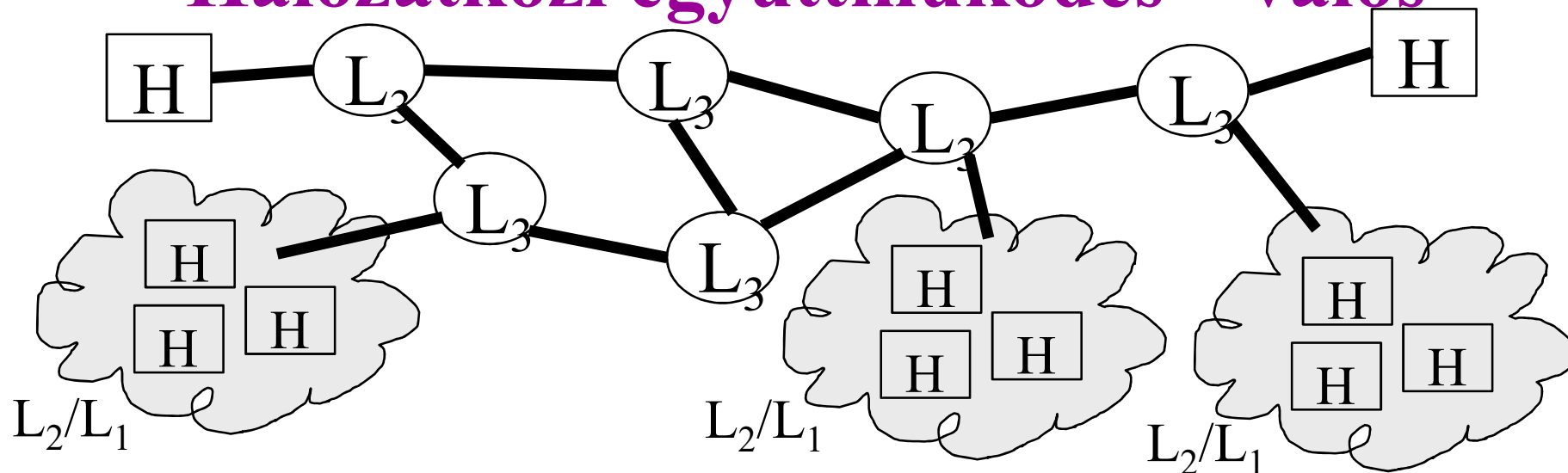
Hálózatközi együttműködés – valós



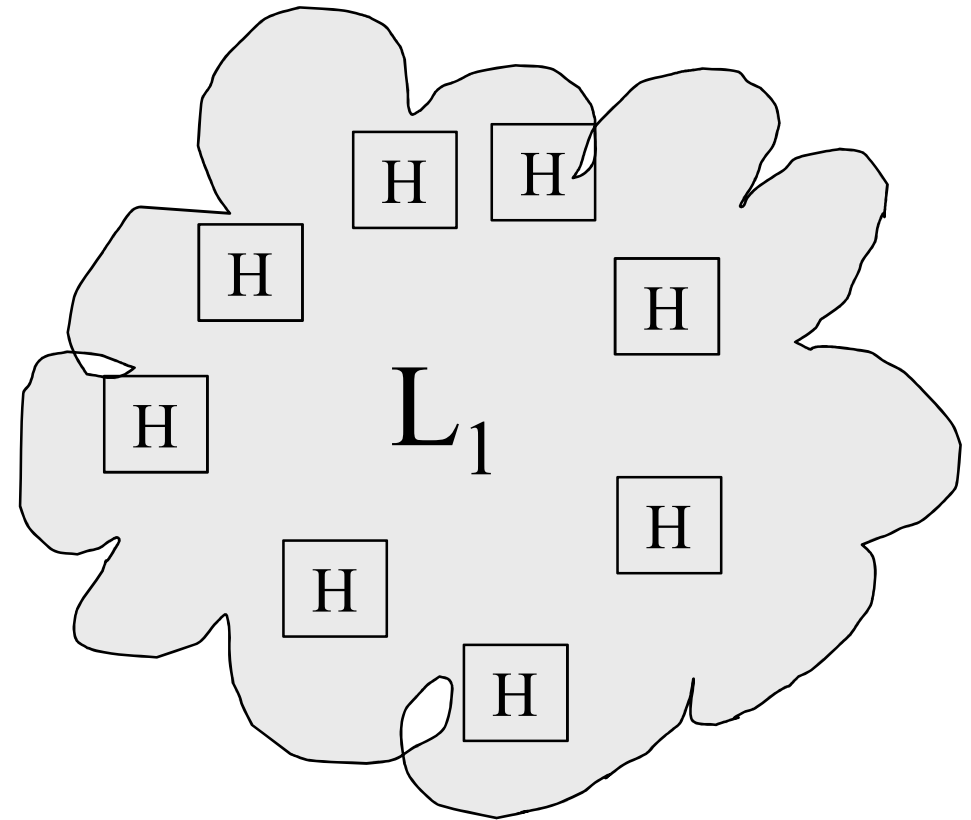
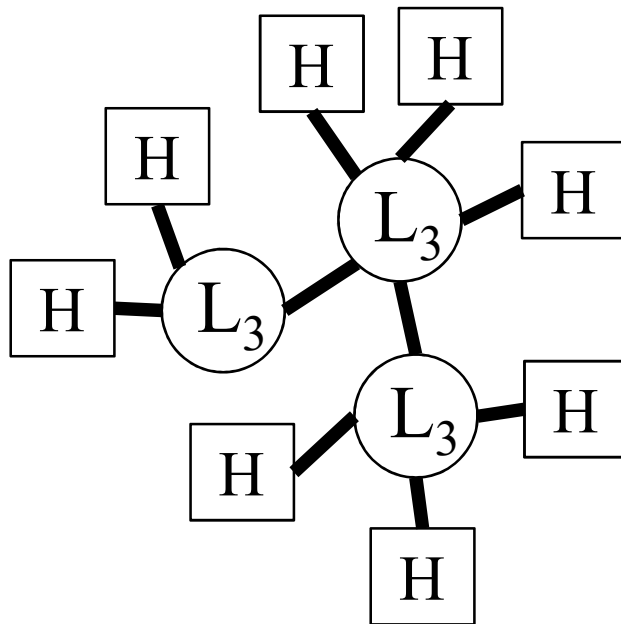
Hálózatközi együttműködés – valós



Hálózatközi együttműködés – valós

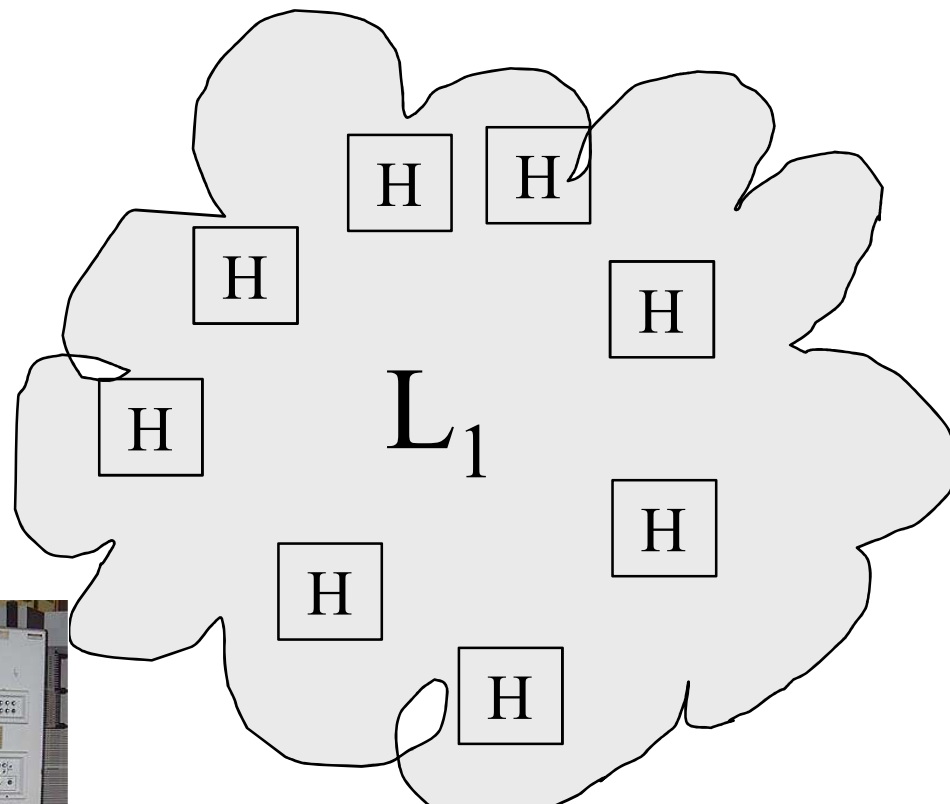
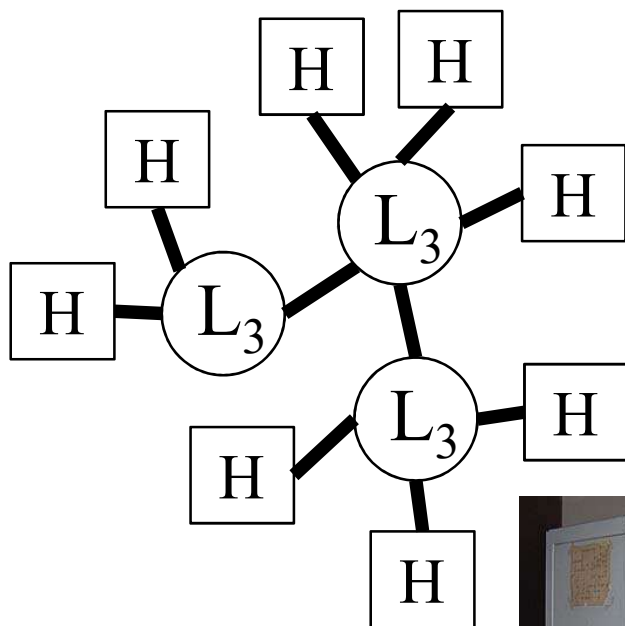


Hálózatközi együttműködés – Miért?



Az össz-áteresztőképesség szempontjából sokkal rosszabb!

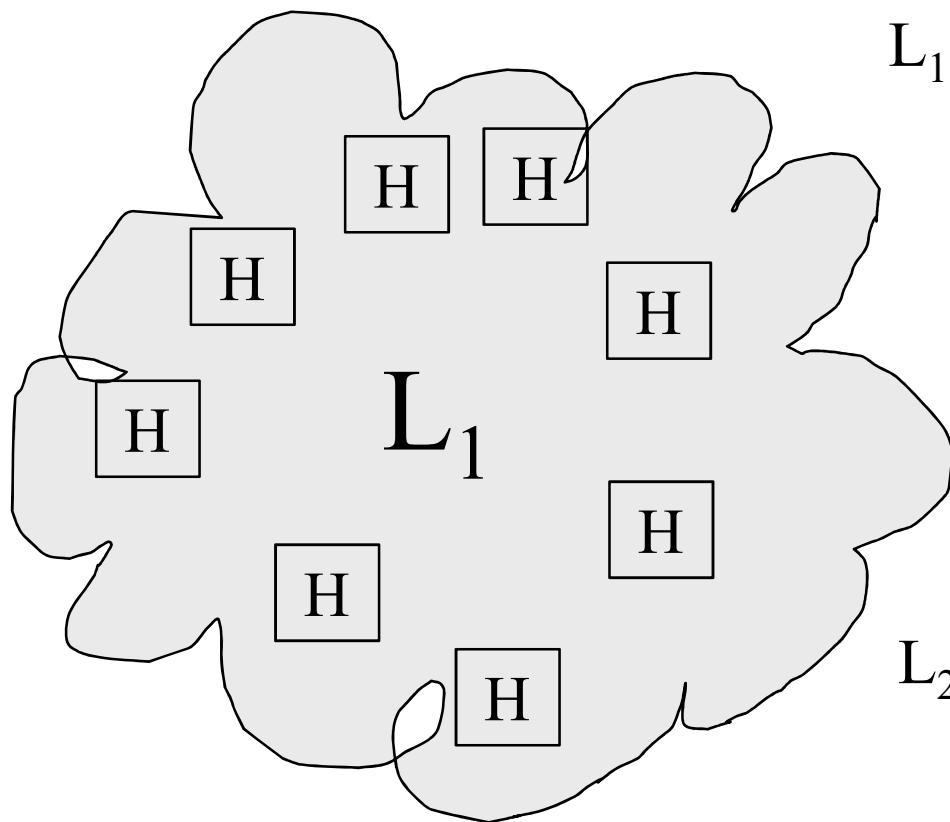
Hálózatközi együttműködés – Miért?



Ok:
IMP (1969 december)

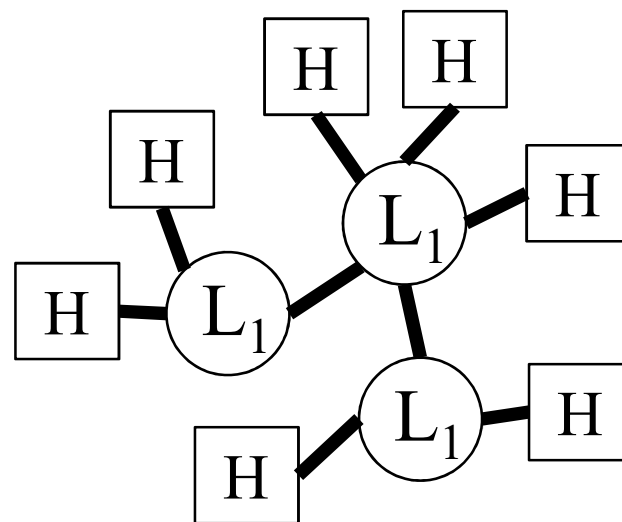


Hálózatközi együttműködés – Hogyan?

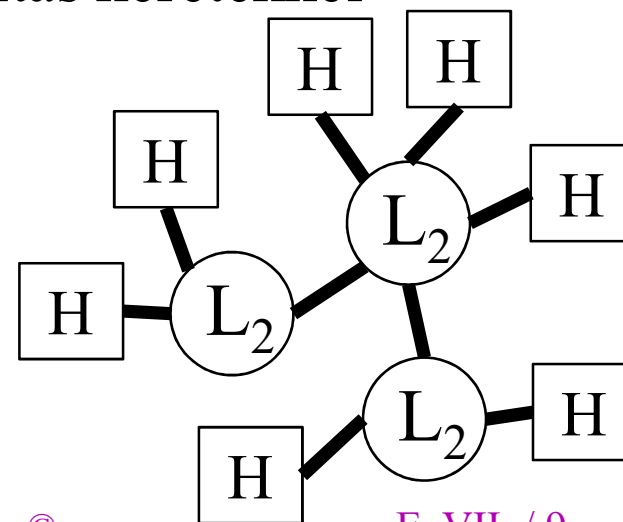


„Valódi” üzenetszórás közeg

L_1 : elárasztás bitekkel



L_2 : elárasztás keretekkel



Hálózatközi együttműködés

- **Általában a hálózatok összekötése több rétegben is lehetséges** (az összekötött hálózatok lehetnek azonos típusúak is.)
- **Hálózatok összekötésének általános célja**
⇒ **a hálózat kiterjesztése**
- **Az összekötés eszközei a rétegek szerint csoportosíthatók:**

OSI terminológia

Protokoll-konverterek {

Gateway (átjáró)

Bridge (híd)

Repeater (jelismétlő)

Stb.
Szállítási
Hálózati
Adatkapcs.
Fizikai

A gyakorlatban használatos elnevezések

Gateway (átjáró)

Router (forgalomirányító)

Bridge (híd)

Repeater (ismétlő)

Mai főbb témák

- **Jelismétlők (repeater)**

Egyéb elnevezések:

- **aktív (passzív (lásd Novell ellenállás hálózat)) hub,**
- **média konverter**

- **Hidak (bridge)**

Egyéb elnevezések:

- **Switch, illetve**
- **Layer 2 Switch**

- **Útvonalválasztók (router)**

Egyéb elnevezések:

- **Layer 3 Switch**

- **Átjárók (gateway, protocol converter) – (ma nem lesz téma)**

Egyéb elnevezések (nem pont ugyanolyan cél, de hasonló eszköz):

- **Proxy**
- **Tűzfal**

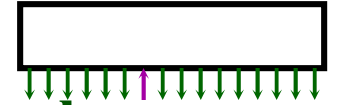
Hálózatközi együttműködés – az eszközök feladatai

- **Technológiai korlátok kiterjesztése**
(pl: max. kapcsolódó állomásszám növelése)
- **Nagyobb távolság áthidalása**
(hálózat méretének kiterjesztése)
- **Forgalom szeparálás**
(terhelés leválasztás (üzenetszórás))
- **Heterogenitás leküzdése**
(különböző típusú hálózatok összekötése)
- **Biztonsági megfontolások**
(forgalom leválasztás, forgalom szűrés, tűzfal (Proxy))

Repeater (ismétlő) – fizikai réteg

Funkciói:

- Az átviteli közeg csillapításából adódó korlátozások leküzdése.
- Több pont-pont összeköttetés egy üzenetszórásos csatornává alakítása (pl. Ethernet UTP-n).



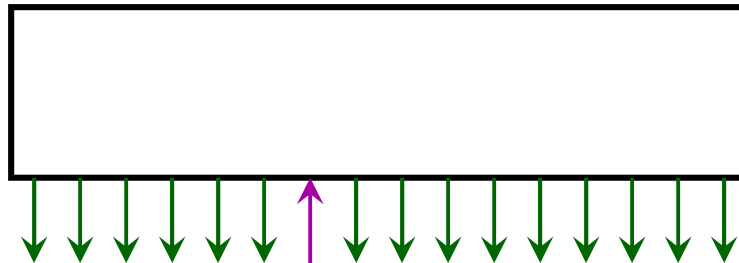
Működése:

- A vett kereteket (bitfolyam) jelfrissítés után (a vétellel azonos bitidőben – tárolás nélkül) az összes kimeneten továbbítja (kivéve ahonnan jött).
- Protokolláris, közeg-hozzáférési funkciót nem lát el (kivéve, a CSMA/CD esetén az ütközés továbbítása).
- Kettő vagy több hálózatot köthet össze.
- Alkalmas különböző fizikai közegek összekötésére (lásd mint „média konverter”).

Repeater (ismétlő) – fizikai réteg

Jellemzői:

- Különböző fizikai közegeket köthet össze, de
- csak azonos MAC (Media Access Control) eljárású hálózatokat köthet össze
(Protokolláris, közeg-hozzáférési funkciót nem lát el)
- A felsőbb protokollokra nézve transzparens

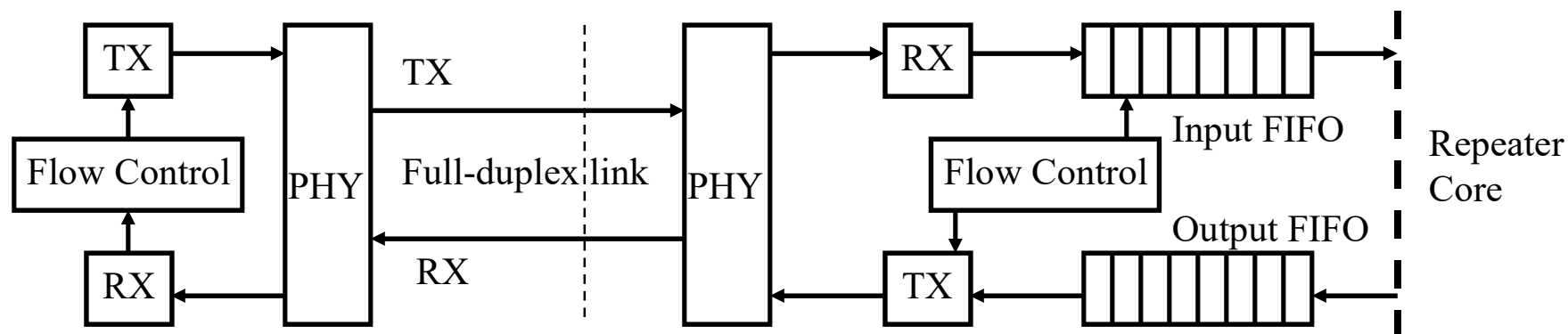


Repeater (ismétlő) – fizikai réteg

Speciális funkciók:

- **Pont-pont kapcsolatok üzenetszórások közeggé alakítása (pl.UTP)**
- **Fizikai közeg típus váltás (média konverter)**
- **Speciális biztonsági funkciók egyes ismétlőknél pl.:**
 - Portjaihoz általában 1-1 állomás kapcsolódik
 - **Egy adott port csak attól fogad el keretet (kapcsoló állomás), akinek a MAC-címét (6 byte) adminisztratív eszközökkel beállították.**
(Illetéktelen állomás csatlakoztatásának kiszűrése.)
 - **Az ismert cél című keretet csak a cél MAC-című állomásnak továbbítja eredeti formájában, a többi kapcsolódó állomásnak csak a kerettel azonos hosszúságú véletlen jelet továbbít.**
(Üzenetszórásos csatorna illetéktelen lehallgatásának kizárása – „Need to Know” security)

Repeater (ismétlő) – Full Duplex link

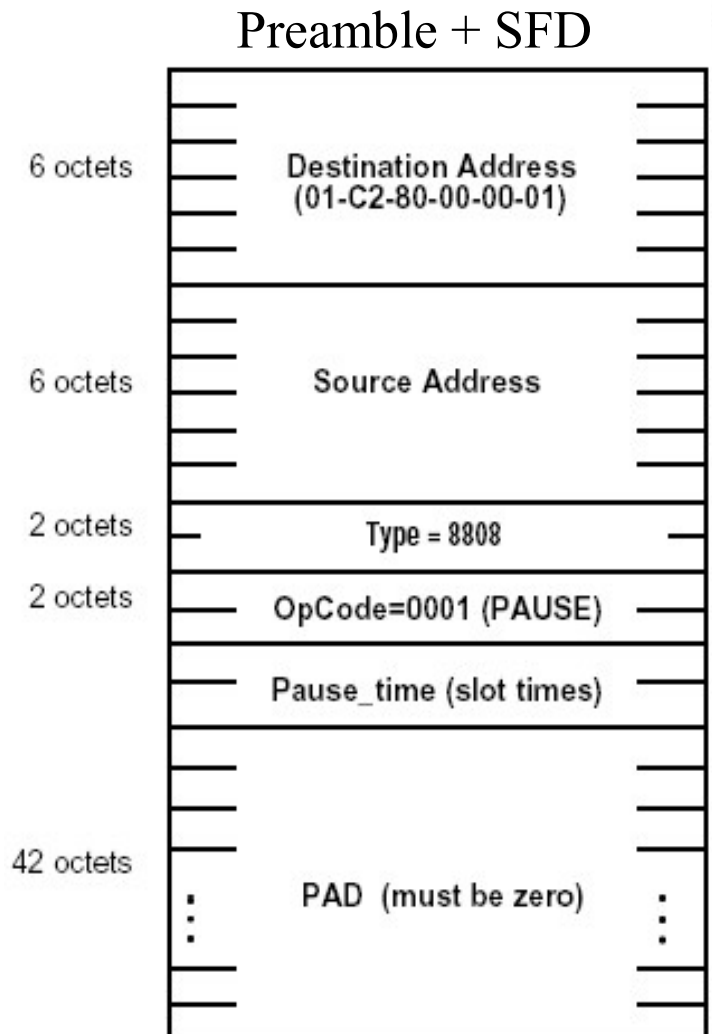


- **Buffered Distributor** (10/100/1000 Ethernet egyaránt)
- Minden portnak van Input és Output FIFO sora
- Az Input sorra érkező keretet valamennyi Output sorra továbbítja (kivéve amelyiken érkezett)
- A Buffered Distributor-on belül történik a CSMA/CD arbitráció (ütemezés) minek eredményeként a keretek az Output sorokba kerülnek.
- Mivel nincs ütközés a linkeken, ezért a linkek maximális hossz korlátja csak a fizikai közegtől függ (nincs körbejárási idő korlát).
- Mivel a küldő könnyedén el tudja árasztani a FIFO-t, ezért keret szintű adatfolyam szabályozást (802.3x – pause frame) alkalmaznak a port és a küldő állomás között.
- Viszonylag olcsó eszköz (a switch-hez képest), ami képes full duplex forgalmat kezelni a linkeken.

(802.3x – Pause Frame)

- Azok az eszközök, akik meg akarják „állítani” az adatfolyamot Pause Frame-et küldenek.
- A Pause Frame „slot time”-ban számolva tartalmazza azt az időt, amíg az adónak fel kellene függesztenie az adását.
- Ez az időtartam további Pause Frame-k küldésével módosítható (törölhető, kiterjeszthető). (A további Pause keretek felülírják az aktuális pause folyamatot.)
- **DA: 01:80:C2:00:00:01** IEEE MAC-specific Control Protocols group address
Az IEEE 802.1D bridge-k nem továbbítják
- **SA:** a keretet küldő állomás MAC címe
- **Length/Type:** 8808.
„MAC Control of CSMA/CD LANs”
- **Opcode:** 0001 - Pause
- **Parameters:** Pause_time. 0-65535 unsigned int.
512 bitidőben számolva

pl. 1000 esetén 512,000 bitidő, ami Gigabit ethernetnél 512µsec FCS
(max. $65535 \cdot 512 = 33,553,920$ bitidő, ami 33.554ms Gigabit Ethernet esetén).



Bridge (híd) – adatkapcsolati réteg

Funkciói:

- **Közeg-hozzáférési eljárások késleltetési korlátját küzdi le.**
- **Közeg-hozzáférési szempontból (MAC) független hálózatokat köt össze.**

Működése:

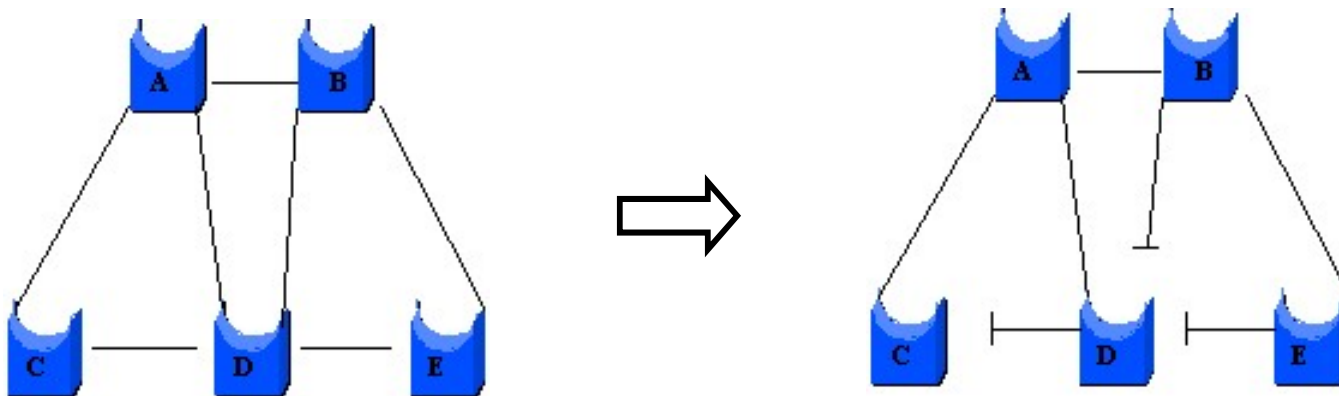
- **Két vagy több hálózatot köthet össze.**
- **Mindegyik hálózaton önálló állomásként van jelen (külön közeghozzáférés).**
- **Valamely hozzá kapcsolódó hálózaton vett keretet a többi (vagy egyik) hálózatra továbbítja.**

Típusai:

- **Transzparens hidak** (transparent bridge), vagy **feszítőfás hidak** (spanning tree bridge) – manapság ezt használják.
- **Forrás által forgalomirányított hidak** (source routing bridge) pl. IBM Token Ring – napjainkban alig használják.

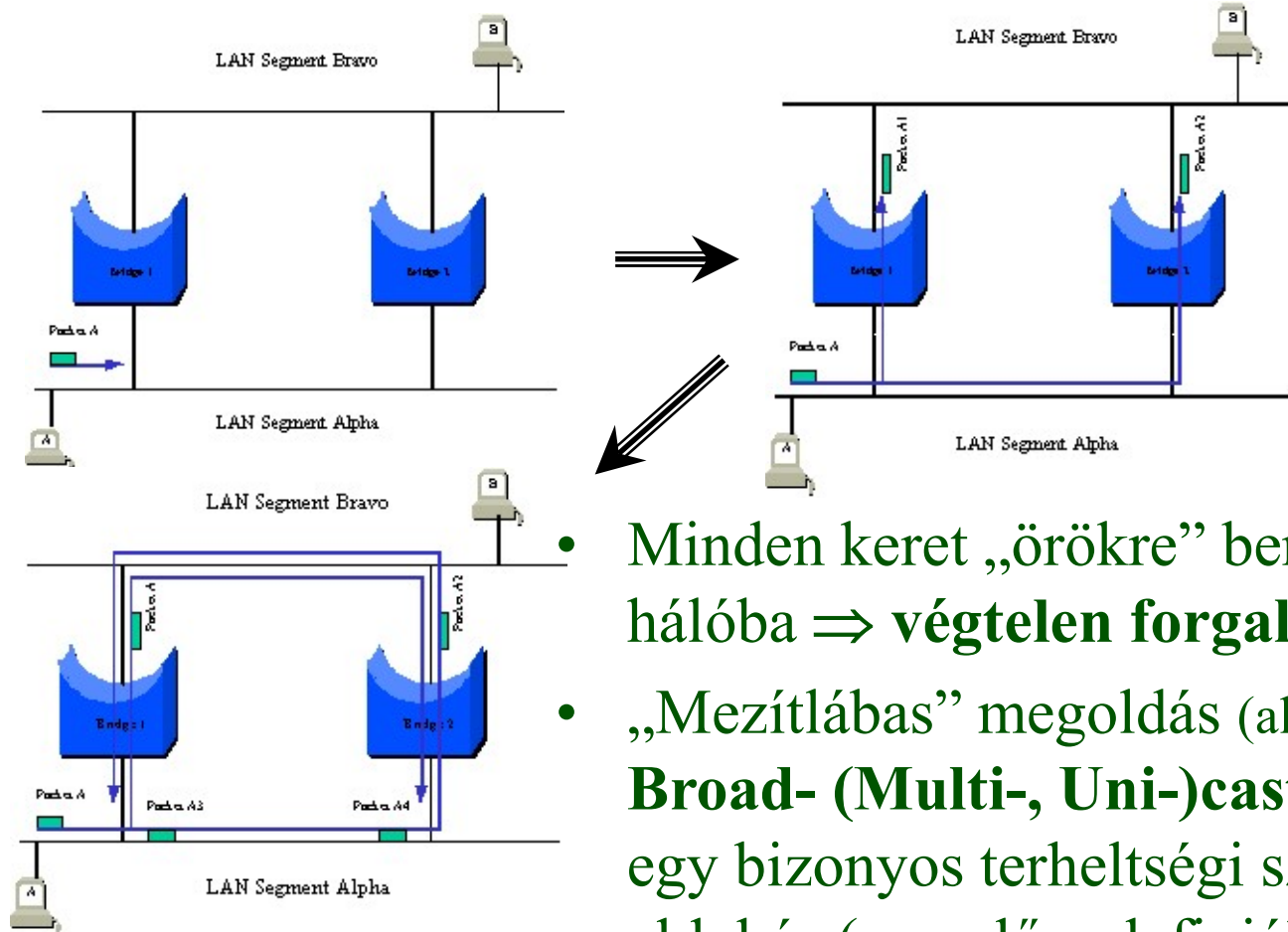
Bridge (híd) – Transzparens hidak

- (Feszítőfás hidak (spanning tree bridge))
- **Cél:** a többszörösen összefüggő hálózat egyszeresen összefüggővé alakítása
- **Megoldás:** a hálózatra egy „feszítőfát” illeszt, amely tartalmazza valamennyi csomópontot, de fa (egyszeresen összefüggő) topológia



Bridge (híd) – Transzparens hidak

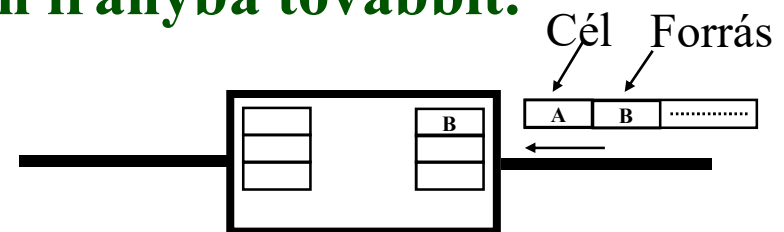
- **Redundáns topológia \Rightarrow végtelen ismételtetés**
(nincs benne pl. ugrásszámláló mint az IP-ben)



- Minden keret „örökre” benne ragad a hálóba \Rightarrow **végtelen forgalom**
- „Mezítlábas” megoldás (alkalmazott védelem): **Broad- (Multi-, Uni-)cast Storm Control** egy bizonyos terheltségi szint fölött keret eldobás (egy előre definiált ideig).

Transzparens hidak – Működésük

- Fordított (ellenirányú) tanulás
- Táblázatok (hash táblák) felhasználásával a rendeltetési helynek megfelelő irányba továbbít.
- Minden porthoz táblázatot rendel, melyek az illető porton keresztül elérhető MAC-címeket tartalmazzák.
- A táblázatokat az illető porton vett csomagok forráscímei alapján töltik ki (kezdetben üresek).
- A bejegyzések öregednek, ha az utolsó vett feladó óta x idő (néhány perc) eltelik, kitörli a táblából a bejegyzést (Pl. állomás máshova kerül).
- Ha a címzett ismeretlen, minden irányba továbbít.



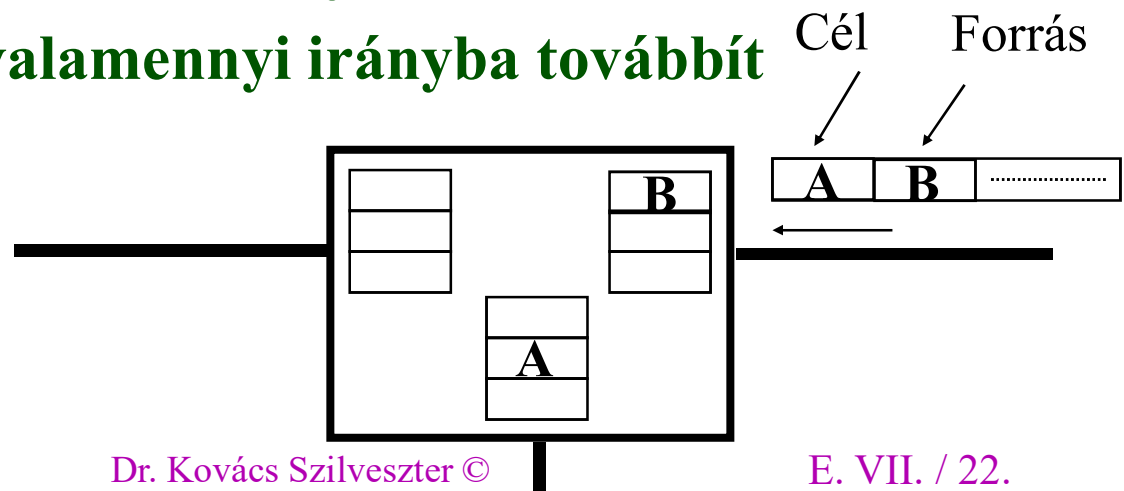
Transzparens hidak – Működésük

Két port esetén: csak azt vizsgálja, hogy a célcím benne van-e annak a portnak a hash táblájában, amelyiken az illető keretet vette

- benne van \Rightarrow nem kell továbbítani
- nincs benne \Rightarrow továbbítani kell

Több port esetén: azt is megnézi, hogy ha továbbítani kell, akkor melyik port hash táblájában van benne

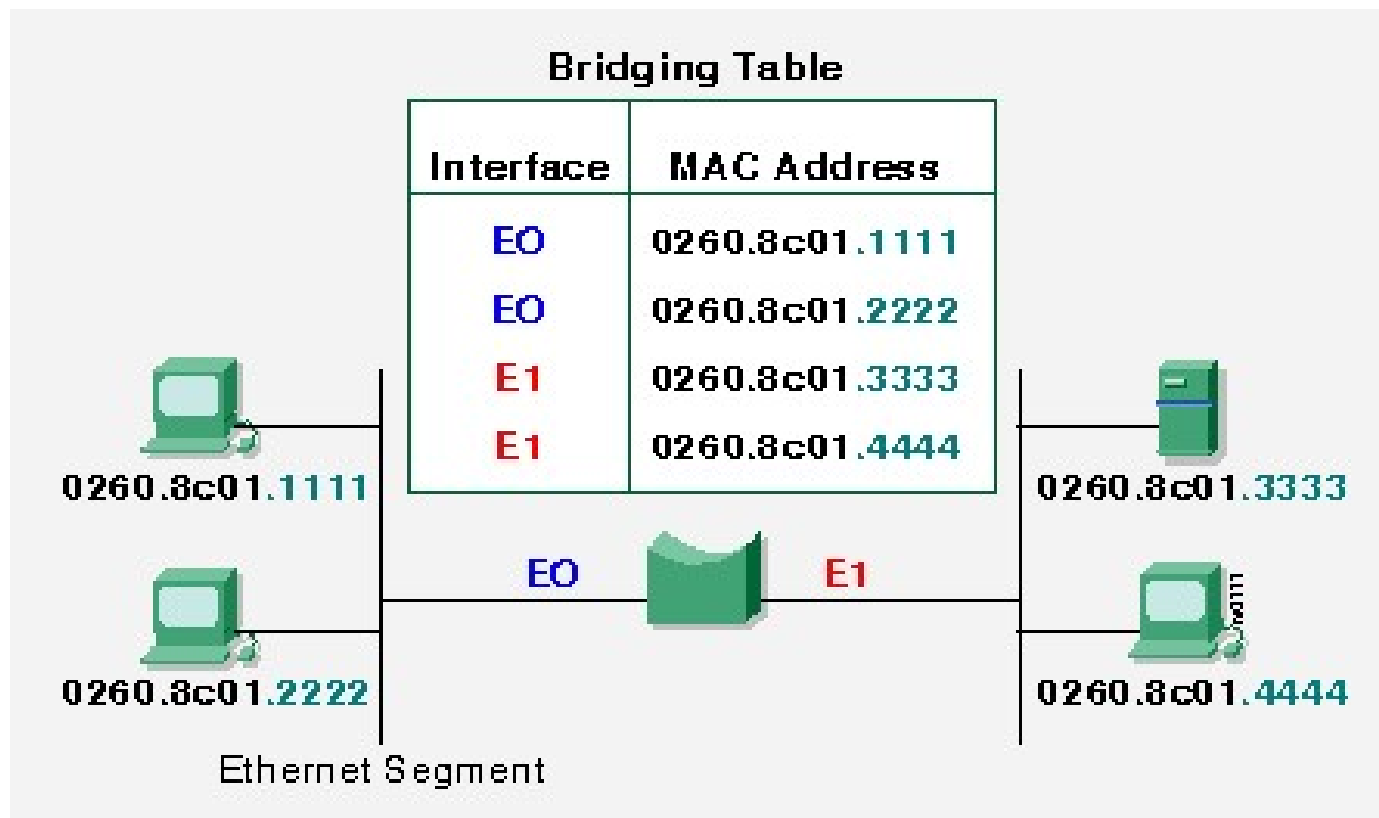
- megtalálja \Rightarrow csak arra továbbítja
- nem találja meg \Rightarrow valamennyi irányba továbbít



Transzparens hidak – Működésük

Hash táblák (CAM Content Addressable Memory):

a gyakorlatban ez csak egyetlen MAC cím – port táblázat (egy címet úgyis csak egy porthoz lehet hozzárendelni).



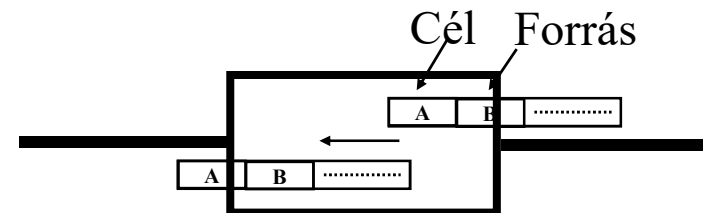
Transzparens hidak – Működési módozatok

Store-and-forward:

- a teljes keretet veszi, ellenőrzi hibátlan-e (CRC) és hibátlan esetben továbbítja.
⇒ Lassabb (nagyobb késleltetés), de kevesebb fölösleges forgalmat generál.

Cut-through:

- **Fast Forward:** a célcím vételét és a feldolgozási időt követően azonnal (átlapoltan) továbbítani kezdi. ⇒ kisebb késleltetés, de hibás csomag esetén fölösleges forgalom.
- **Fragment Free:** csak 64 bájt beolvasása után továbbít

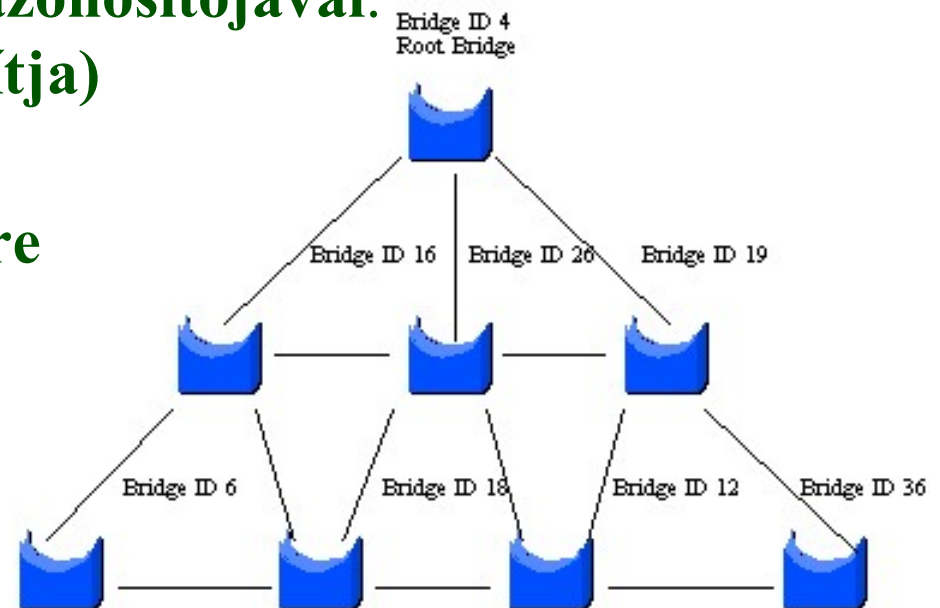


Spanning Tree Protocol (STP 802.1D)

- A transzparens hidak mindig a feszítőfa kialakításával indulnak (az esetleges hurkok olyan veszélyesek lennének)

Működése:

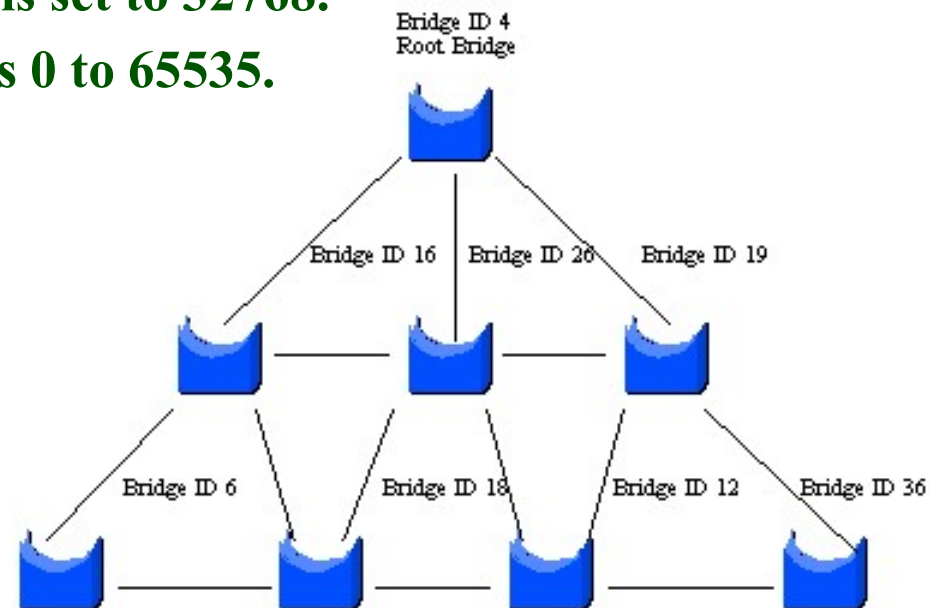
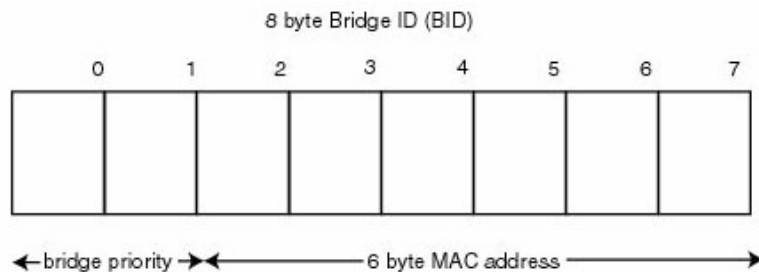
- Induláskor minden egyes bridge küld egy Bridge Protocol Data Unit-ot (BPDU DA: 01:80:C2:00:00:00 – IEEE Bridge Group address, Nearest Customer Bridge group address) valamennyi portjára a saját azonosítójával. (A BPDU-t senki sem továbbítja)
- Elosztott algoritmus eldönti, hogy ki lesz a feszítőfa gyökere (Pl. legkisebb sorszámú)
- Páronként cserélgetik a BPDU-kat, hogy ki kit gondol root-nak



Spanning Tree Protocol (STP 802.1D)

Spanning-Tree Bridge Identifier

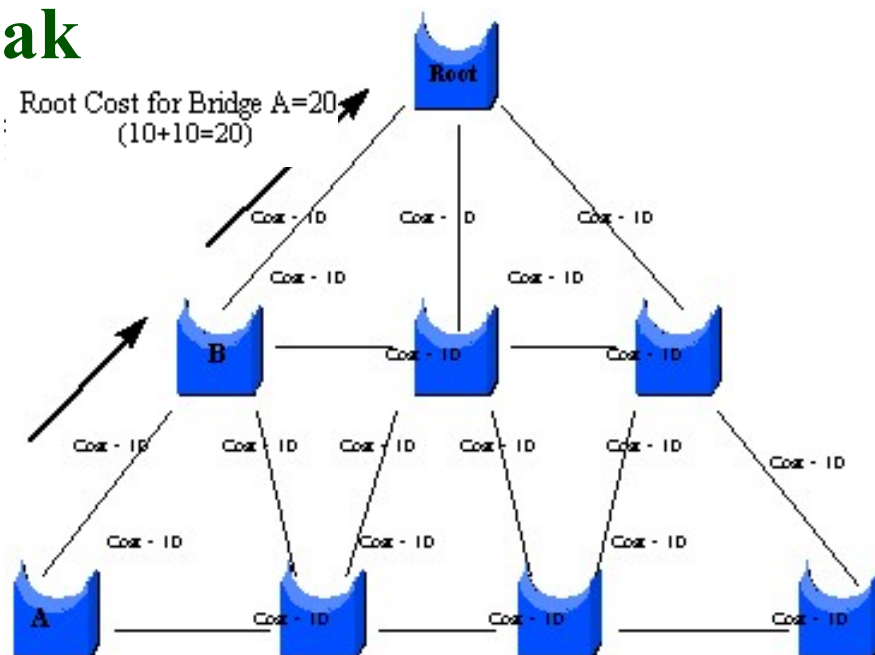
- In spanning tree, the 2-octet field is prepended to the 6-octet MAC address to form an 8-octet bridge identifier.
- The device with the lowest bridge identifier is considered the highest priority bridge and becomes the root bridge.
- By default, the bridge priority is set to 32768.
- The range for bridge priority is 0 to 65535.



- **Extended System ID:**
a prioritás alsó 12 bitje
a VLAN ID

Spanning Tree Protocol (STP 802.1D)

- Miután megvan a fa gyökere, a többi híd kiválasztja a gyökérhez vezető legrövidebb utat – mindig a szomszédjaival veti össze magát (egyezés esetén pl. a kisebb azonosítójú nyer).
- Azok a linkek, melyek nem illeszkednek a legrövidebb utakra inaktívak „blocking” lesznek, míg a legrövidebb út linkjei „forwarding” állapotba kerülnek.
⇒ Kialakul a feszítőfa.

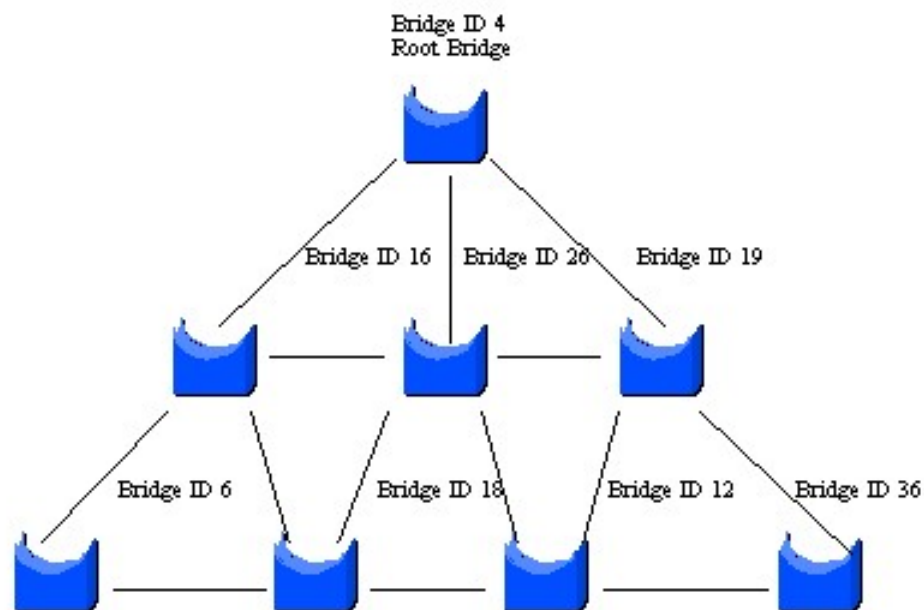


Spanning Tree Protocol (STP 802.1D)

Default **STP path cost** of an interface for a given data rate:

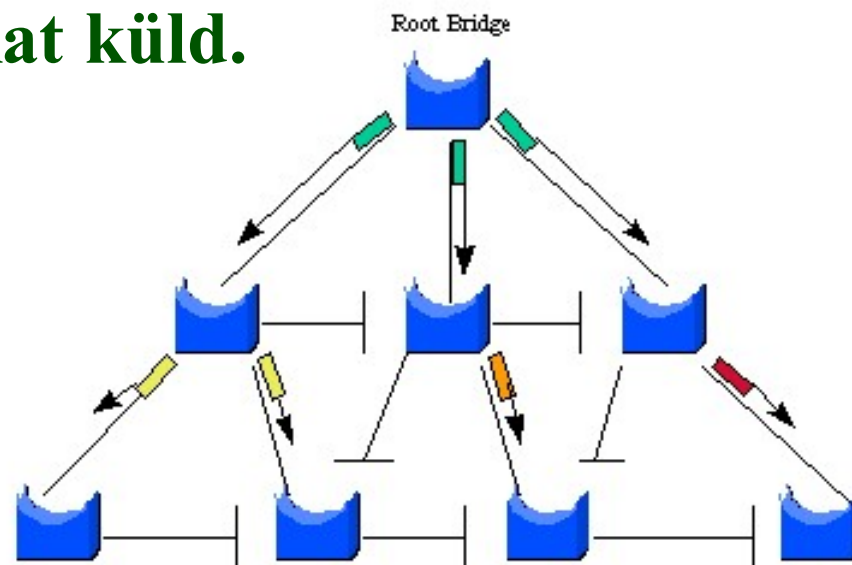
- **Data rate STP Cost**

- 4 Mbit/s 250
- 10 Mbit/s 100
- 16 Mbit/s 62
- 45 Mbit/s 39
- 100 Mbit/s 19
- 155 Mbit/s 14
- 200 Mbit/s 12
- 622 Mbit/s 6
- 1 Gbit/s 4
- 2 Gbit/s 3
- 10 Gbit/s 2



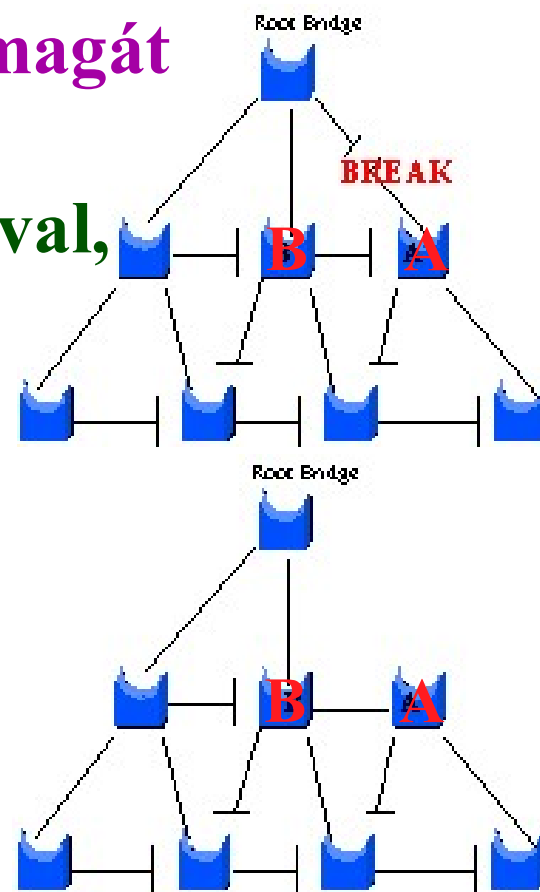
Spanning Tree Protocol (STP 802.1D)

- Miután biztonsággal kialakult a feszítőfa, csak azután kezdik a hidak a tényleges forgalmat továbbítani (forwarding).
- A root bridge rendszeres időközökben (hello time) saját konfigurációjával „hello” BPDU-kat küld.
- A többi híd ennek hatására lefelé (saját konfigur.-jával) ugyancsak „hello” BPDU-kat küld.
- Ha valaki „max age” ideig nem kap „hello”-t, akkor előlről kezdi az algoritmust. („leszakadt a fáról”)



Spanning Tree Protocol (STP 802.1D)

- Topológia változás esetén – ha egy link megszakad
- Annak akinek lejár a „hello” időzítője (**A**), törli a korábbi konfigurációját és olyan BPDU-t küld a szomszédainak, amiben **saját magát jelöli meg root-nak**.
- Ezt **B** összeveti a saját konfigurációjával, miszerint ő egy sokkal jobb root-ot lát – és ezt megküldi **A**-nak.
- **A** ezen BPDU alapján újraszámolja a konfigurációját és úgy találja, hogy a legrövidebb út a **B** felé van és a későbbiekben már ezt hirdeti.



Spanning Tree Protocol (STP 802.1D)

Port szerepek:

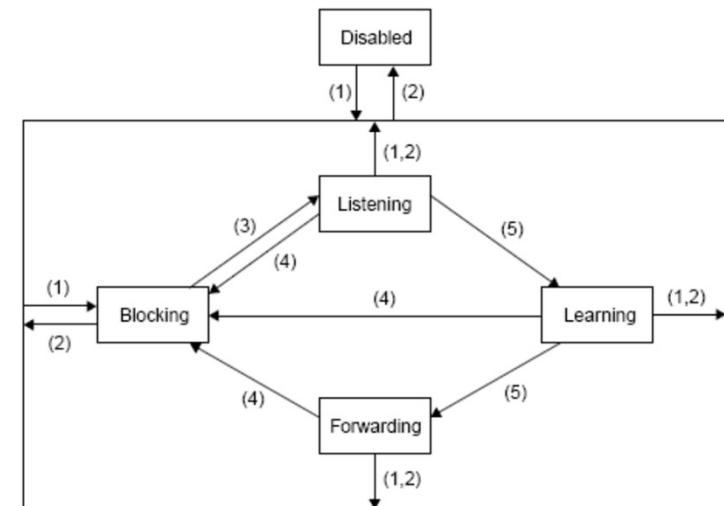
- **Root port:** the port that receives the best BPDU on a bridge is the root port. This is the port that is the closest to the root bridge in terms of path cost. The root bridge is the only bridge in the network that does not have a root port. All other bridges receive BPDUs on at least one port.
- **Designated port:** A port is designated if it can send the best BPDU on the segment to which it is connected. On a given segment, there can only be one path toward the root bridge.



Spanning Tree Protocol (STP 802.1D)

- **Port állapotok:**
A blocking és listening állapot nagyon hasonló, csak a listening egy olyan designated, vagy root port, ami nemsokára forwarding állapotban lesz.
- Learning már gyűjti a MAC címeket, de még nem forwarding.

STP(802.1D) Port State	RSTP(802.1w) Port State	Is Port Included in Active Topology	Is Port Learning Mac Addresses?
Disabled	Discarding	No	No
Blocking	Discarding	No	No
Listening	Discarding	No	No
Learning	Learning	No	Yes
Forwarding	Forwarding	Yes	Yes

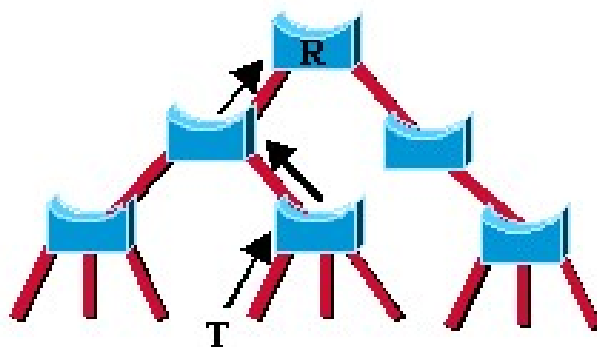


Spanning Tree Protocol (STP 802.1D)

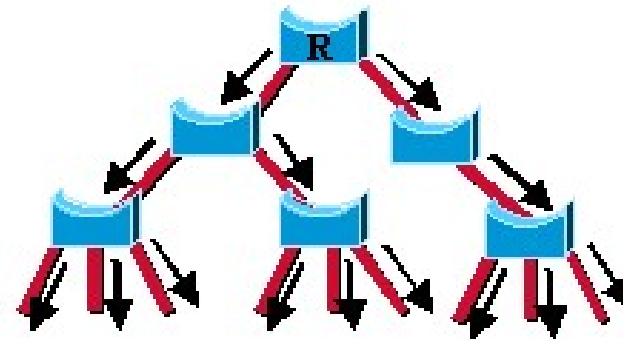
- STP időzítők:
- **Hello:** The hello time is the time between each bridge protocol data unit (BPDU) that is sent on a port. This time is equal to 2 seconds (sec) by default, but you can tune the time to be between 1 and 10 sec.
- **Forward delay:** The forward delay is the time that is spent in the **listening and learning** state. This time is equal to 15 sec by default, but you can tune the time to be between 4 and 30 sec.
- **Max age:** The max age timer controls the maximum length of time that passes before a bridge port saves its configuration BPDU information. This time is 20 sec by default, but you can tune the time to be between 6 and 40 sec.

Spanning Tree Protocol (STP 802.1D)

- Amikor egy híd változást észlel bármely portján (a figyelt portok beállíthatóak) egy Topology Change Notification (TCN) BPDU-t küld a gyöker hídnek közvetlenül (unicast) ezt addig teszi amíg nyugtát nem kap a vételről
- A figyelt portok beállíthatóak!!!! A gyöker híd ezután a konfigurációs BPDU-ban egy biten jelzi a hálózatnak (Topology Change TC bit), hogy változás történik és mindenki csökkentse a CAM (Content Addressable Memory) tábla bejegyzéseinek érvényességi idejét (Forwarding Delay-re).



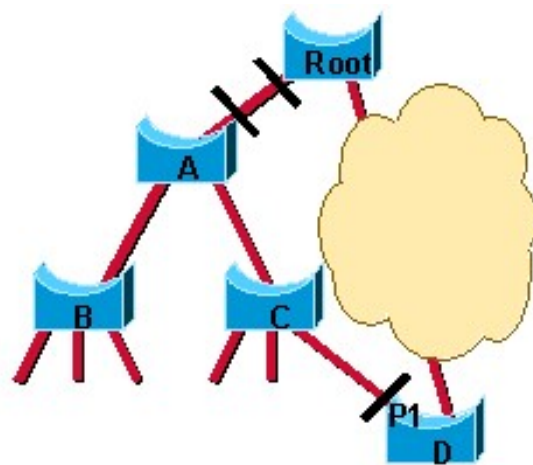
A topology change is generated on point T.
1st step: A TCN is going up to the root.



2nd step: the root advertises the TC for max-age+ forward delay.

Spanning Tree Protocol (STP 802.1D)

- Amikor egy új link jelenik meg a hálózatban (A – Root link added)
- The STA (Spanning Tree Algorithm) blocks a port and disables the bridging loop.
- First, as they come up, both ports on the link between the root and Bridge A are put in the **listening state**. Bridge A is now able to hear the root directly.
- It immediately propagates its BPDUs on the designated ports, toward the leaves of the tree.
- As soon as Bridges B and C receive this new superior information from Bridge A, they immediately relay the information towards the leaves.
- In a few seconds, Bridge D receives a BPDU from the root and instantly blocks port P1.
- **2* forward delay** (30 sec) várakozás után az új link **forwarding állapotba** kerül (addig listening/learning, amíg biztonsággal lezajlik a változás (nincs visszajelzés arról, hogy kész az új fa).



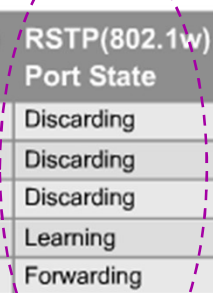
Very quickly, the BPDUs from the root reach D that immediately blocks its port P1. The topology has now converged, though, the network is disrupted for twice forward_delay.

Rapid Spanning Tree Protocol (RSTP 802.1W)

- **Problémák az STP-vel:**
 - Lassú konvergencia ($\text{MaxAge} + 2 * \text{ForwardDelay} = 20\text{s} + 2 * 15\text{s}$)
 - Minden port egyforma
- **RSTP:**
 - Kompatibilis az STP-vel
 - Van esély a gyorsabb átmenetre továbbító állapotba
 - Az edge port típus (host kapcsolat) egyből a blokkolt állapotból a továbbító állapotba léphet
 - Pont-Pont kapcsoltnál gyorsítás BPDU kézfogás segítségével

Rapid Spanning Tree Protocol (RSTP 802.1W)

- Kevesebb port állapot

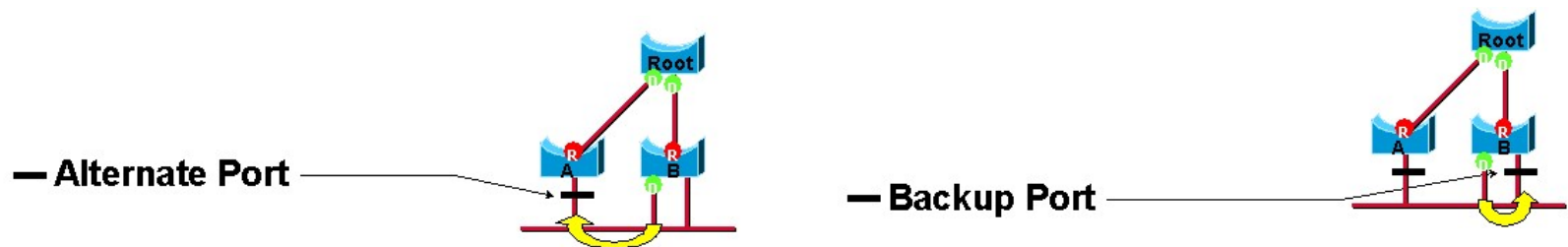


STP(802.1D) Port State	RSTP(802.1w) Port State	Is Port Included in Active Topology	Is Port Learning Mac Addresses?
Disabled	Discarding	No	No
Blocking	Discarding	No	No
Listening	Discarding	No	No
Learning	Learning	No	Yes
Forwarding	Forwarding	Yes	Yes

Rapid Spanning Tree Protocol (RSTP 802.1W)

Újabb port szerepek:

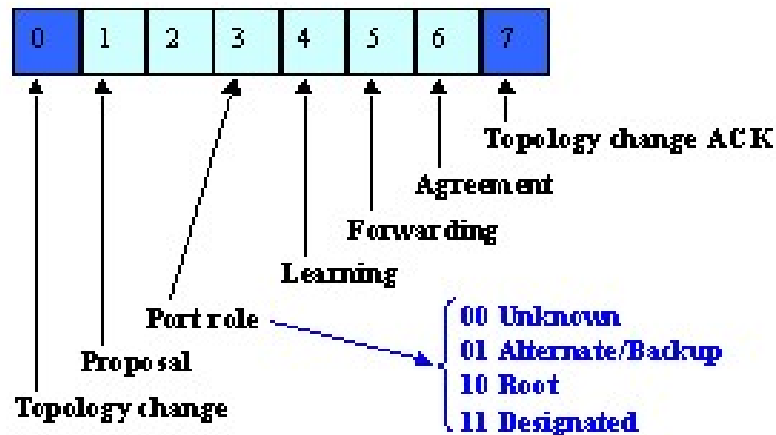
- Root port, Designated port
- Alternate port:
An alternate port receives more useful BPDUs from another bridge and is a port blocked.
- Backup port:
A backup port receives more useful BPDUs from the same bridge it is on and is a port blocked.
- Gyorsítás: Ha leszakad a gyökérről rögtön ezeket választhatja



Rapid Spanning Tree Protocol (RSTP 802.1W)

Új BPDU flag bitek:

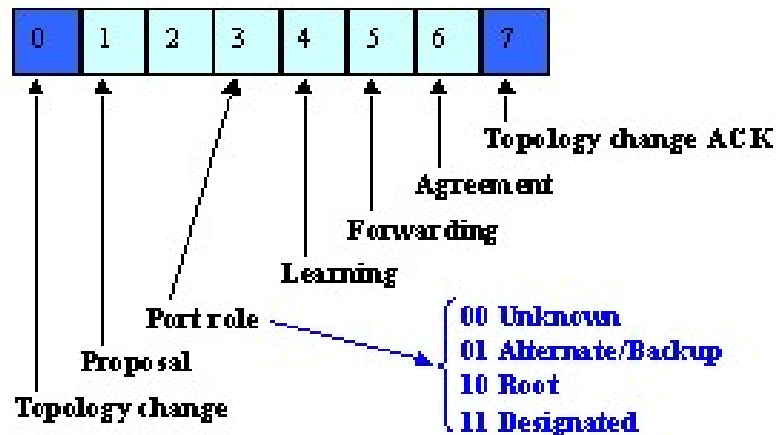
- STP-ben csak: Topology Change (TC) and TC Acknowledgment (TCA) bitek
- Encode the **role and state of the port** that originates the BPDU
- Handle the **proposal/agreement mechanism**



Rapid Spanning Tree Protocol (RSTP 802.1W)

Új BPDU kezelés:

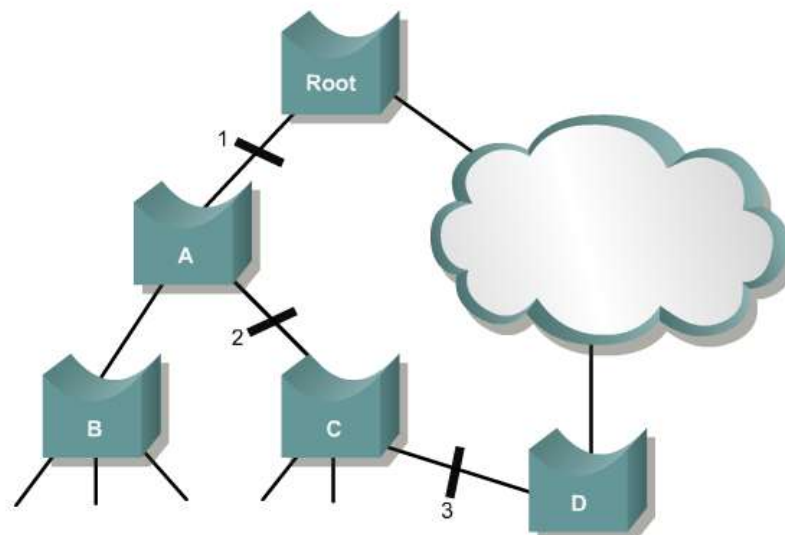
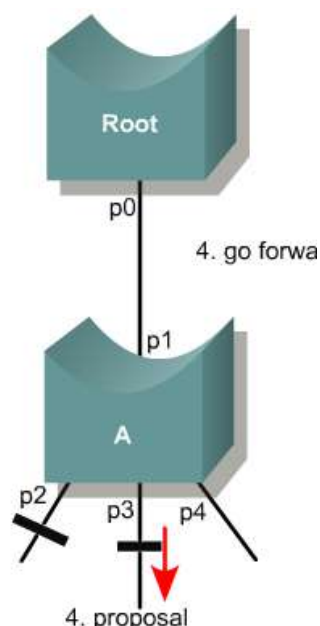
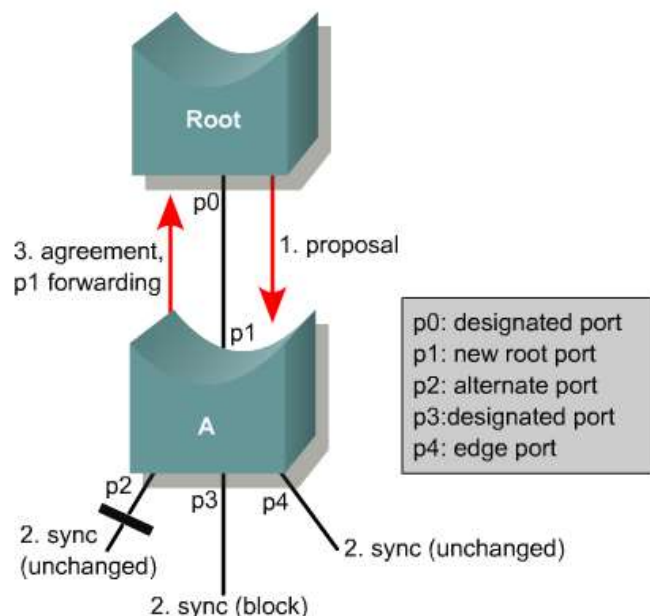
- Az STP-ben a HELLO BPDU-kat csak a Root küldi, a többi ismétli
- Az RSTP-ben a Hello időnként mindenki küld BPDU-t
- Ha 3 Hello ideig valaki nem kap BPDU-t a „kapcsolat megszakadt”



Rapid Spanning Tree Protocol (RSTP 802.1W)

Gyorsabb konvergencia – új link megjelenése
proposal/agreement szekvencia:

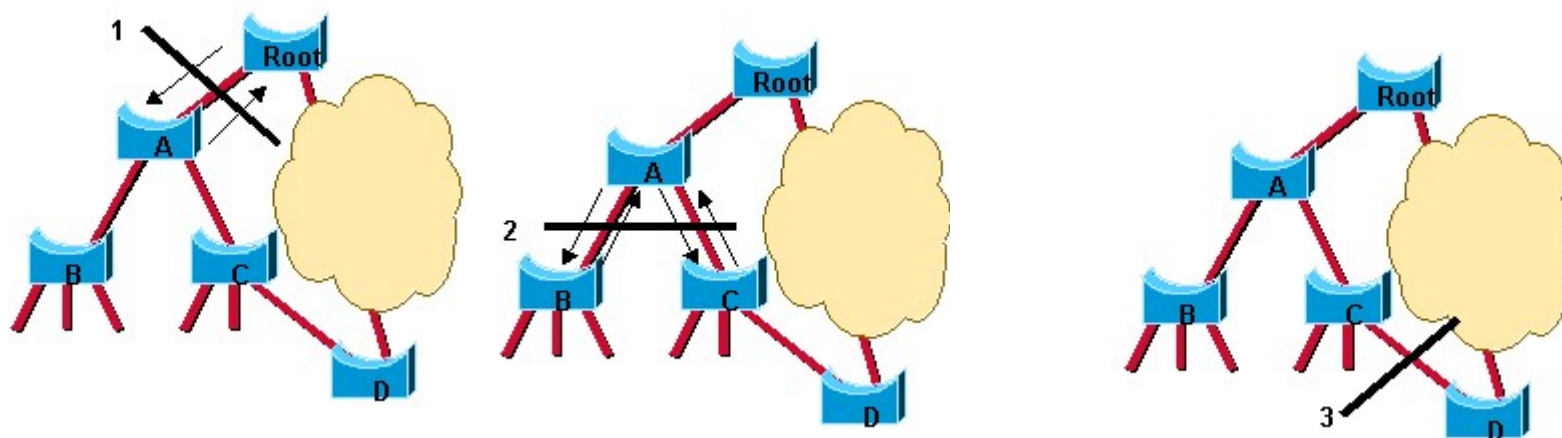
- A designated port **discarding** lesz és „**proposal**”-t küld, ha erre „**agreement**” jön (ajánlat ismétlése, csak agreement flag), akkor forward állapotba megy.
- Ha **proposal**-t kap és elfogadja, akkor a korábbi forward portját blokkolja (sync) és ezt követően **agreement**-et küld



Rapid Spanning Tree Protocol (RSTP 802.1W)

Gyorsabb konvergencia – proposal/agreement szekvencia:

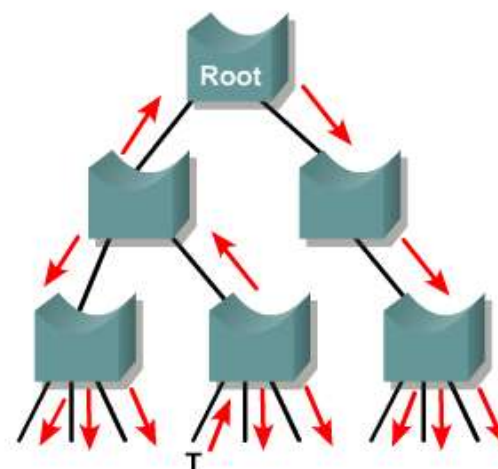
- „Kézfogás hullámot” indít el
- Sokkal gyorsabban konvergál mint az STP



Rapid Spanning Tree Protocol (RSTP 802.1W)

RSTP topológia változás:

- Csak a nem „edge” portok változása az érdekes!
- Nem csak a gyökér küld periódikusan üzeneteket, hanem minden híd
- Topológia változás hatására (változás):
 - Elindít egy időzítőt (a hello idő kétszeresét)
 - Az időzítő lejártáig minden kijelölt portján és a gyökér portján olyan BPDU-t üld ki melyben a TC bit be van állítva Ezeken a portokon kiüríti a CAM-ot
 - Aki ezt megkapta ugyanezt teszi. (a TC mindenfelé terjed)
De a bejövő porthoz tartozó CAM-ot nem üríti
 - (Nem kell elmenni a gyökérig, majd vissza STP)



Transzparens hidak – egyéb

„Dual Speed (10/100) Hub”:

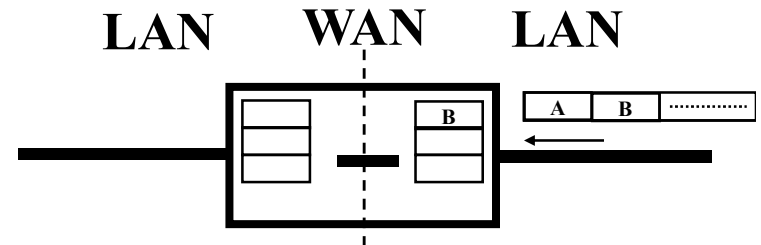
- Két repeater egy bridge-el összekötve

Remote bridge:

- Olyan kétportos bridge, amelynek csak az egyik portján van hash tábla

⇒ a másik portra nem szűr, ami onnan jön, azt mindig továbbítja (az már szűrt)

Pl.: két távoli hálózat összekötése, LAN-WAN kapcsolat



Biztonsági funkciók

- Meg lehet határozni, hogy egy porton max. hány különböző MAC cím élhessen – ha ennél több lenne akkor vagy
 - a legrégebbit törli és az újabbat megtanulja, vagy
 - az újabbakat eldobja, ilyenkor lehet úgy konfigurálni, hogy az újabb cím megjelenésekor tiltsa az érintett portot
- Disconnect Unauthorized Device (DUD)

Transzparens hidak – egyéb

A Spanning Tree tiltható

(ha a topológiai nem igényli, ne töltsse vele az időt)

Channel:

- Különböző portok „csatornába fogása” (Channel) – a csatorna portjai között terhelésmegosztást végez. (A csatorna portjai a Spanning Tree szempontjából egyetlen összeköttetésnek számítanak.)

Prioritások kezelése:

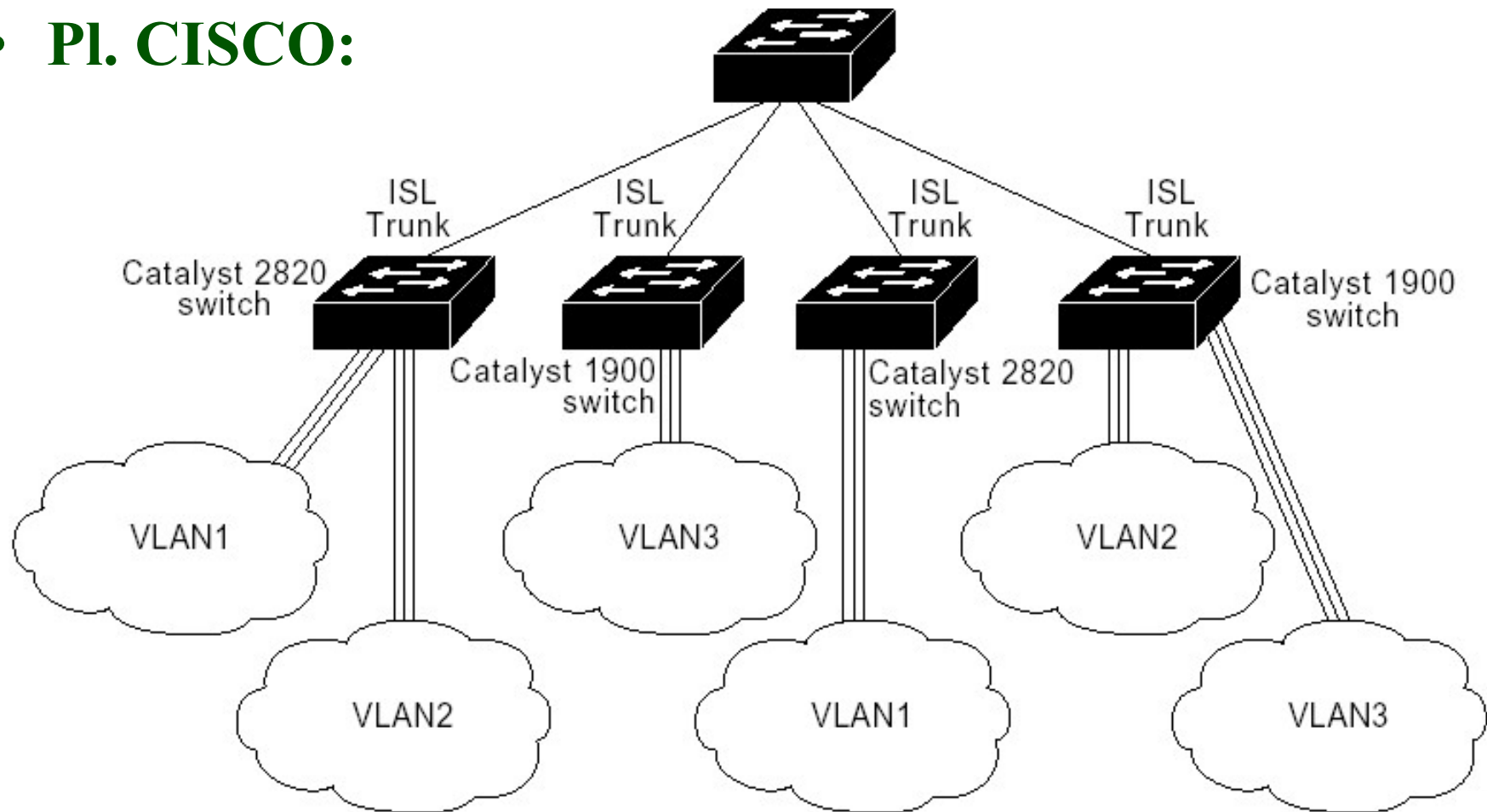
- Az egyes prioritási osztályoknak külön-külön sora lehet az egyes portokon (tipikusan kettő) és előre engedi a magasabb prioritásúakat. (Ezen a szinten lehet először prioritást kezelni – itt vannak először sorok (leszámítva a duplex repeatert).)

Transzparens hidak – VLAN

- A hidak szintjén történik a Virtuális LAN-ok (VLAN) kezelése.
- Minden portra meg lehet határozni, hogy melyik VLAN-hoz tartozzon.
- Ha egy port több VLAN-hoz is tartozik akkor a kereteken az egyes VLAN-okhoz való tartozást VLAN Tag-ok jelölik.
(Cisco: ISL, IEEE: 802.1q)
- Ha egy port csak egy VLAN-hoz tartozik, akkor a switch a porton kifelé menő keretokről leszedheti, illetve a befelé menő keretekre rárakhatja a megfelelő Tag-ot.
⇒ Az ilyen állomások számára a VLAN-ok transzparenssek.
- A táblák kialakítása és a Switching az egyes VLAN-okra külön-külön történik (virtuálisan független LAN-ok ugyanazon az infrastruktúrán)

Transzparens hidak – VLAN

- **A VLAN Tag-okkal jelölt link neve: CISCO: Trunk**
(az összefogott linkek neve: CISCO: Channel, 3COM: Trunk)
- **Pl. CISCO:**



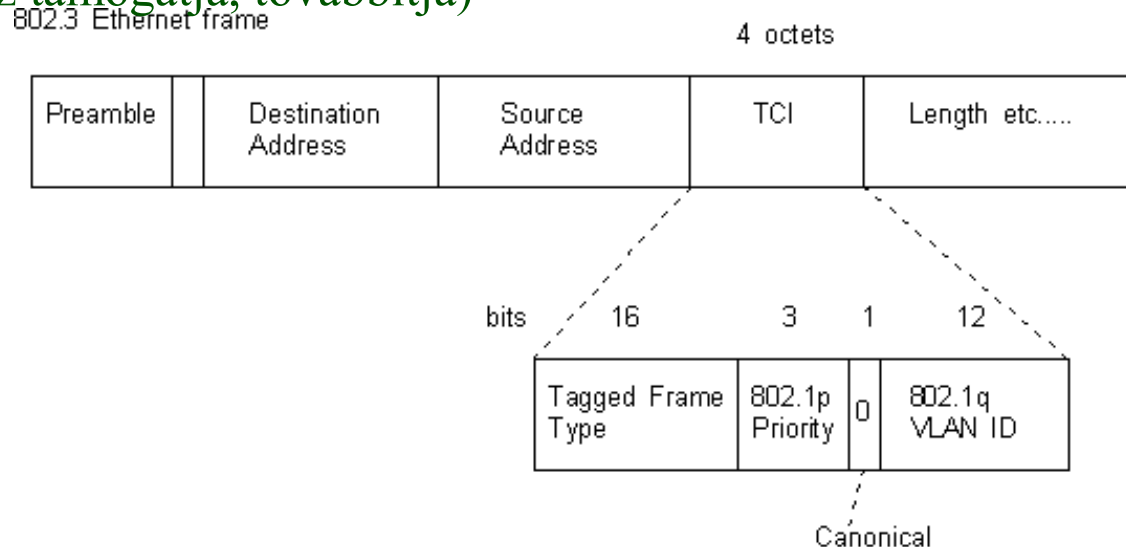
Transzparens hidak – VLAN (802.1p, 802.1q)

- **Class of Service and VLANs (802.1p, 802.1q)**

A Cisco: Inter Switch Link (ISL)
keret enkapszuláció (teljesen más)

- **Tag Control Info (TCI)**

- **Pótlólagos 4 byte csak** \Rightarrow maximális keretméret 1518 \rightarrow 1522
(nem minden eszköz támogatja, továbbítja)



- **Tagged Frame Type** – Tag típus, Ethernet keretek esetén jelenleg mindig **0x8100**.
- **802.1p Priority „Priority code point” (PCP)** – az alacsony prioritású bináris 000 (0) –tól a magas prioritású bináris 111 (7) –ig („**class of service**”)
- **Drop eligible indicator (DEI) (korábban „Canonical” 0)**
– PCP-vel együtt „class of service”, jelzi, hogy a keret torlódás esetén eldobható
- **802.1q VLAN ID** - a VLAN azonosítója a VLAN trónkökön.
- A keret végén a **CRC-t újra kell számítani**

Transzparens hidak – VLAN (ISL)

- **Inter-Switch Link (ISL) - Cisco proprietary protocol**
- **Az ISL egy Ethernet keret enkapszuláció (nem belső, hanem külső tag)**
- **ISL enkapszuláció: 26 byte header + 4-byte CRC**
- **Csak 10-bit VLAN ID**



40 bits	4 bits	4 bits	48 bits	16 bits	24 bits	24 bits	15 bits	1 bits	16 bits	16 bits	Variable length	32 bits
DA	TYPE	USER	SA	LEN	SNAP/LLC	HSA	VLAN ID	BPDU/CDP	INDX	Reserved	Encapsulated Frame	FCS (CRC)

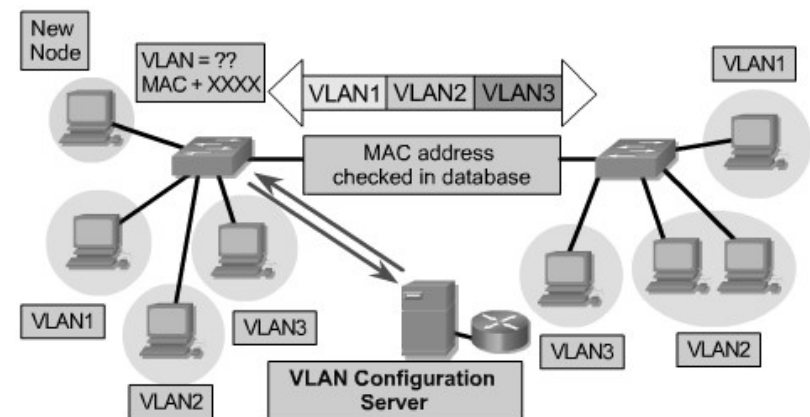
Transzparens hidak – VLAN (ISL)

Octet	Description
DA	A 40-bit multicast address with a value of 0x01-00-0C-00-00 that indicates to the receiving Catalyst that the frame is an ISL encapsulated frame.
Type	A 4-bit value indicating the source frame type. Values include 0 0 0 0 (Ethernet), 0 0 0 1 (Token Ring), 0 0 1 0 (FDDI), and 0 0 1 1 (ATM).
User	A 4-bit value usually set to zero, but can be used for special situations when transporting Token Ring.
SA	The 802.3 MAC address of the transmitting Catalyst. This is a 48-bit value.
Length	The LEN field is a 16-bit value indicating the length of the user data and ISL header, but excludes the DA , Type, User, SA, Length, and ISL CRC bytes.
SNAP	A three-byte field with a fixed value of 0xAA-AA-03.
HSA	This three-byte value duplicates the high order bytes of the ISL SA field.
VLAN	A 15-bit value to reflect the numerical value of the source VLAN that the user frame belongs to. Note that only 10 bits are used.
BPDU	A single-bit value that, when set to 1, indicates that the receiving Catalyst should immediately examine the frame at an end station because the data contains either a Spanning Tree, ISL, VTP, or CDP message.
Index	The value indicates what port the frame exited from the source Catalyst.
Reserved	Token Ring and FDDI frames have special values that need to be transported over the ISL link. These values, such as AC and FC, are carried in this field. The value of this field is zero for Ethernet frames.
User Frame	The original user data frame is inserted here including the frame's FCS.
CRC	ISL calculates a 32-bit CRC for the header and user frame. This double-checks the integrity of the message as it crosses an ISL trunk. It does not replace the User Frame CRC.

DA	40 bits
TYPE	4 bits
USER	4 bits
SA	48 bits
LEN	16 bits
SNAP/LLC	24 bits
HSA	24 bits
VLAN ID	15 bits
BPDU/CDP	1 bits
INDX	16 bits
Reserved	16 bits
Encapsulated Frame	Variable length
FCS (CRC)	32 bits

Transzparens hidak – VLAN

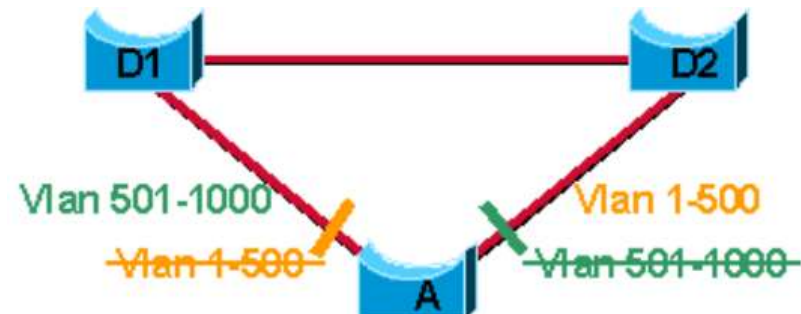
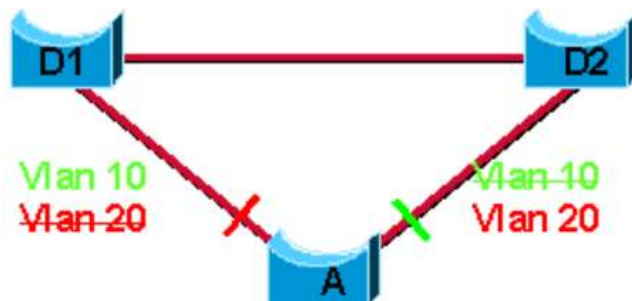
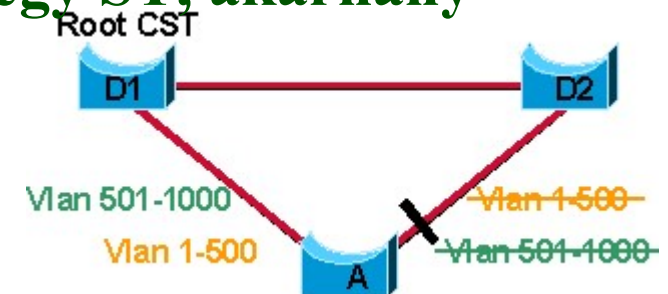
- **Statikus VLAN:**
 - Port alapú, ha nincs VLAN tag a linken, akkor a port egyértelműen tartozik valamely előre konfigurált VLAN-hoz.
- **Dinamikus VLAN:**
 - MAC cím alapú, a kapcsolódó állomás MAC címe határozza meg, hogy melyik VLAN-hoz kapcsolódik.
 - Előre konfigurálni kell egy VLAN Management Policy Server (VMPS) szerverbe a MAC-VLAN hozzárendelést.



Transzparens hidak – VLAN és STP

Gond: ha több VLAN van, jó lenne kihasználni a topológia redundanciáját.

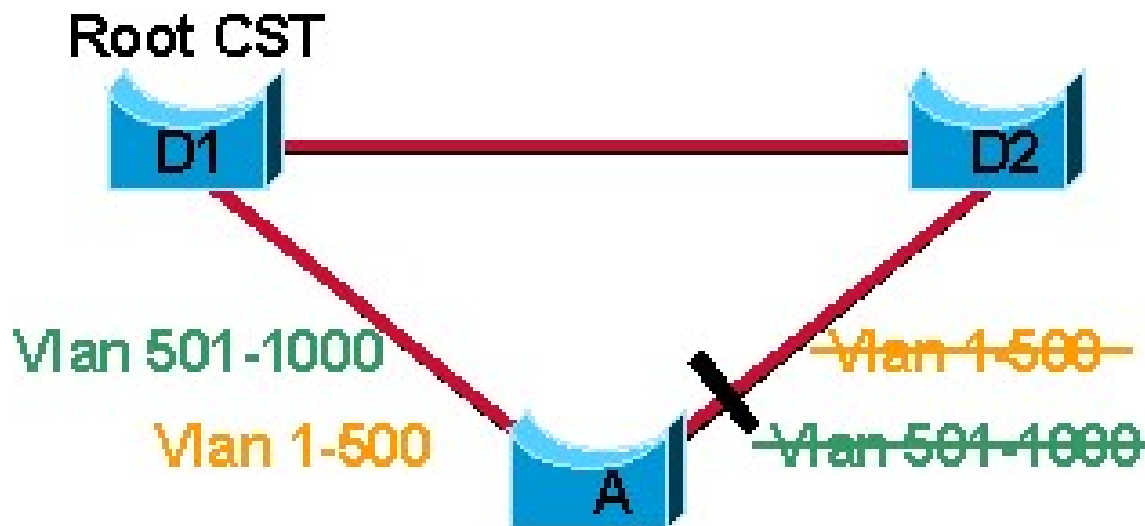
- **CST:** Common Spanning Tree csak egy ST, akárhány VLAN (802.1q default)
- **PVST:** Per-VLAN Spanning Tree annyi ST, ahány VLAN
- **MST (802.1s):** Multiple ST, annyi ST, ahány különböző lehet a topológián és ezekre vannak szétosztva a VLAN-ok



Transzparens hidak – PVST

CST: Common Spanning Tree

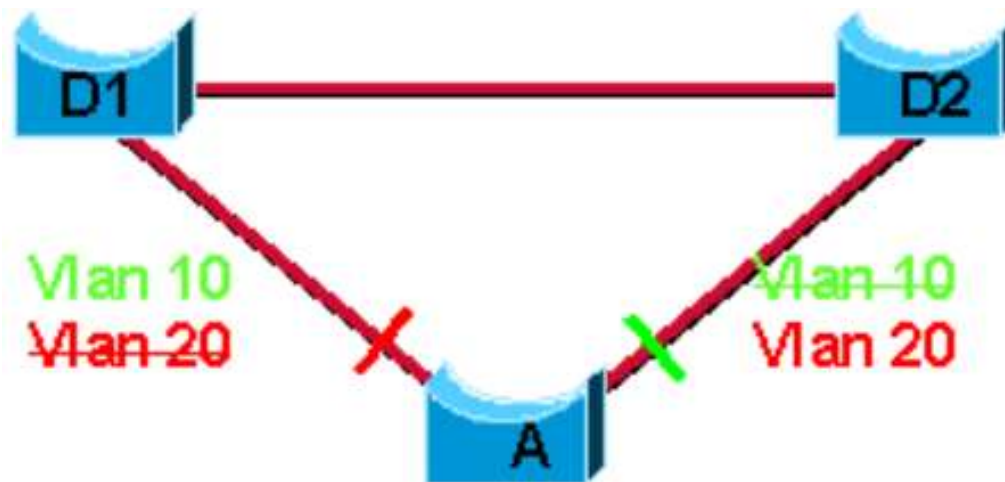
- Csak egy ST, akárhány VLAN (ez a 802.1q default)
- Nincs lehetőség a hálózati terhelés elosztásra



Transzparens hidak – PVST

PVST: Per-VLAN Spanning Tree

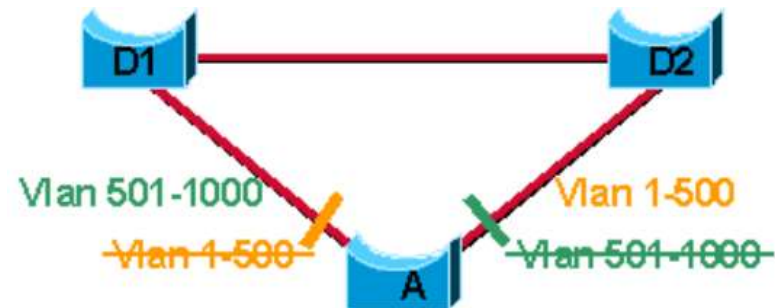
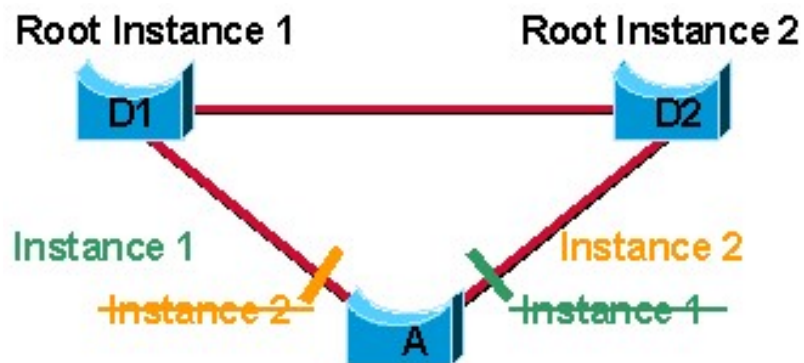
- Annyi STP, ahány VLAN
- Az egyes STP-kben más-más gyökér híd lehet
- Nagy CPU terhelés, de van lehetőség a hálózati terhelés elosztásra



Transzparens hidak – MST (802.1s)

MST (802.1s): Multiple ST

- Több ST példány (**MST instance**), annyit érdemes, ahány különböző lehet a topológián és ezekre vannak szétosztva a VLAN-ok
- VLAN csoportokat kezel
- Egy VLAN csak egy MST példányhoz tartozhat
- Egy kapcsoló több MST példány
- Kicsi CPU terhelés, hálózati terhelés elosztás lehetséges



Transzparens hidak – MST (802.1s)

Minden **MST híd** az alábbiakat tárolja:

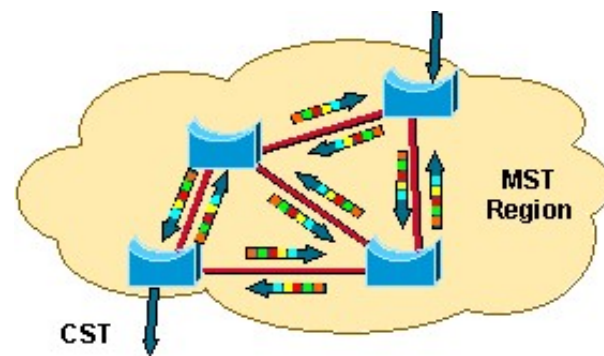
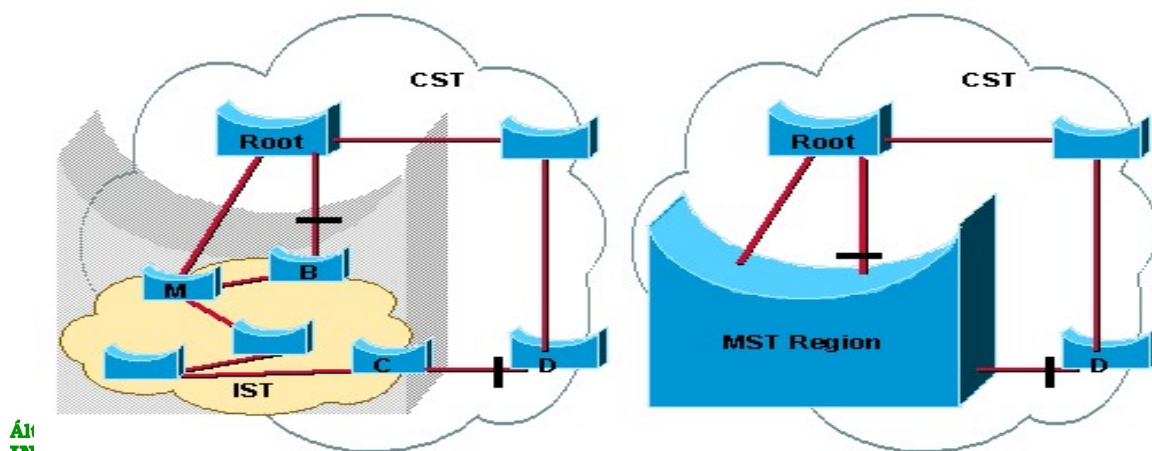
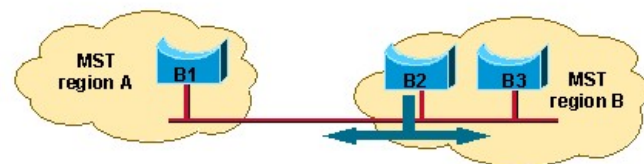
- An alphanumeric **configuration name** (32 bytes)
- A configuration revision number (two bytes)
- A **4096-element table** that associates each of the potential 4096 **VLANs** supported on the chassis to a given **MST instance** (4096 különböző VLAN lehetséges) tábla a **VLAN - MST instance (RSTP) összerendelésről**

MST régió:

- Azok a hidak, melyek ugyanazt a konfigurációt tartalmazzák ugyanahhoz a régióhoz tartoznak
- A konfiguráció elterjesztéséhez nincs ajánlás...

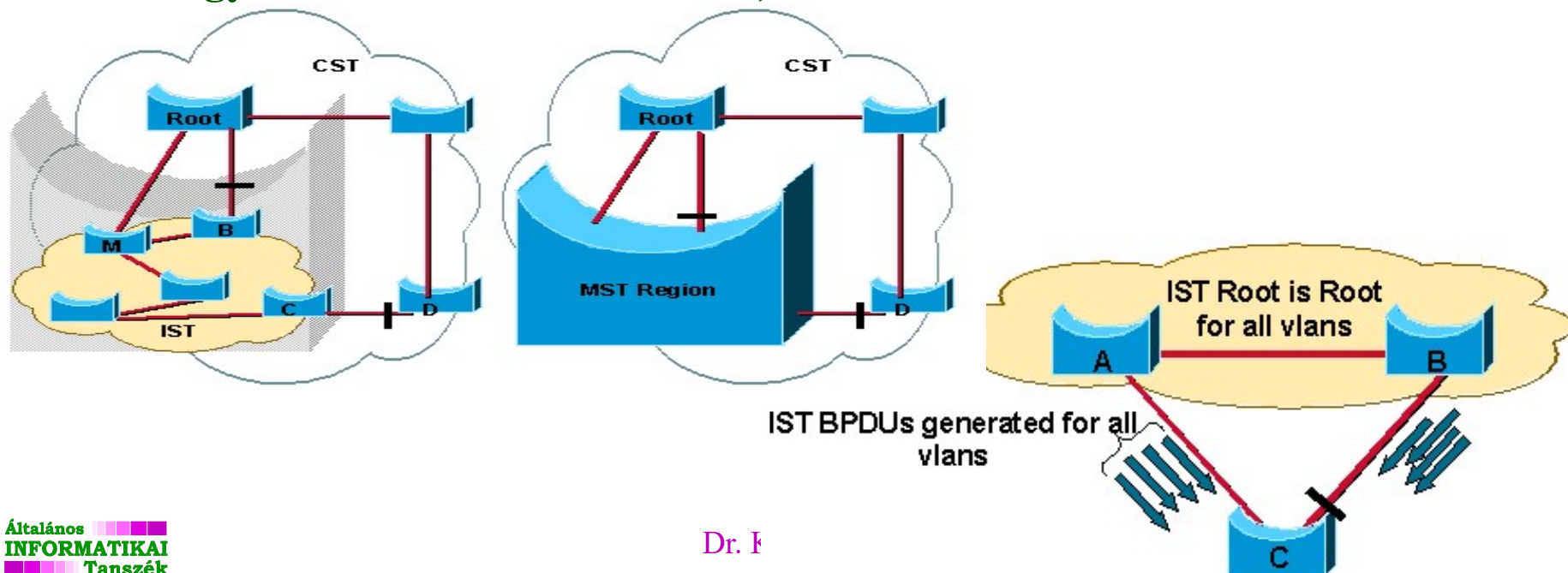
A működéshez tudni kell a pontos **határokat**:

- A **BPDU-ba** a konfiguráció kivonata is bekerül
- Ha ez egy porton a sajátjától **különbözik** akkor az a port **határ port**



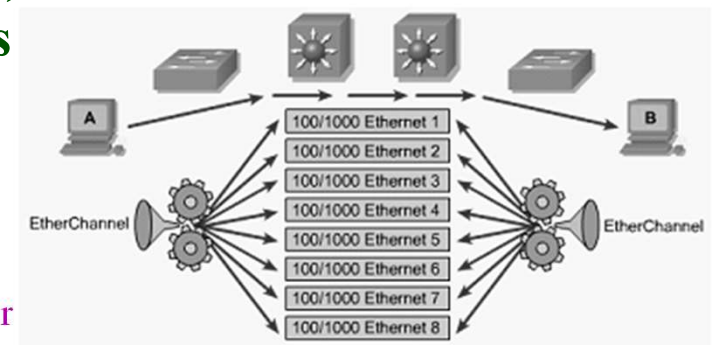
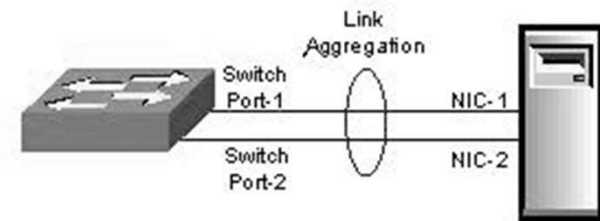
Transzparens hidak – MST (802.1s)

- Tetszőleges számú MSTI (Multiple Spanning Tree Instance)
- Az egyes MSTI-k saját ROOT-al rendelkeznek az MST régión belül
- Egy IST (Internal Spanning Tree) ez ki is jut (kívülről az egész régió egy hídként látszik, ami az IST szerint üzenet (as the MST region now replicates the IST BPDUs on every VLAN at the boundary), így kompatibilis a sima CST-vel (802.p) és a PVST-vel is
- Az IST ROOT kívül is lehet, az is lehet, hogy nem is ismeri az MST-t (az MST határokon elvész)
- Ajánlás az IST ROOT-nak legyen a legmagasabb a prioritása (így az mindegyik PVST-nél is ROOT lesz)



Transzparens hidak – Link Aggregation

- „Vonal összefogás”
- STP, RSTP, MSTP
 - A redundáns útvonalat blokkolt állapotba helyezi
 - Nincs dinamikus terhelés megosztás
- Amennyiben a linkek egy sebesség kategóriába tartoznak (10BaseT, Fast Ethernet, Giga, 10G)
 - Összefoghatunk több vonalat egy vonallá (pl. max 8)
 - Csak pont-pont összeköttetésnél használható két eszköz között
 - Csak full-duplex üzemmódban használható
- Előnyei:
 - Dinamikus terhelés elosztás
 - Nagy rendelkezésre állás
 - Gyors, automatikus rekonfiguráció (~1s)
 - A felsőbb rétegek számára transzparens
 - Determinisztikus
 - Konfigurálható



Transzparens hidak – Link Aggregation

IEEE: 802.3ad, Link Aggregation Control Protocol (LACP)

- 10,100,1000 MBit/s
- Általában pl. 3COM esetében ezt nevezik „Trunk”-nek
Cisco: „Channel”, Linux: „Bonding”

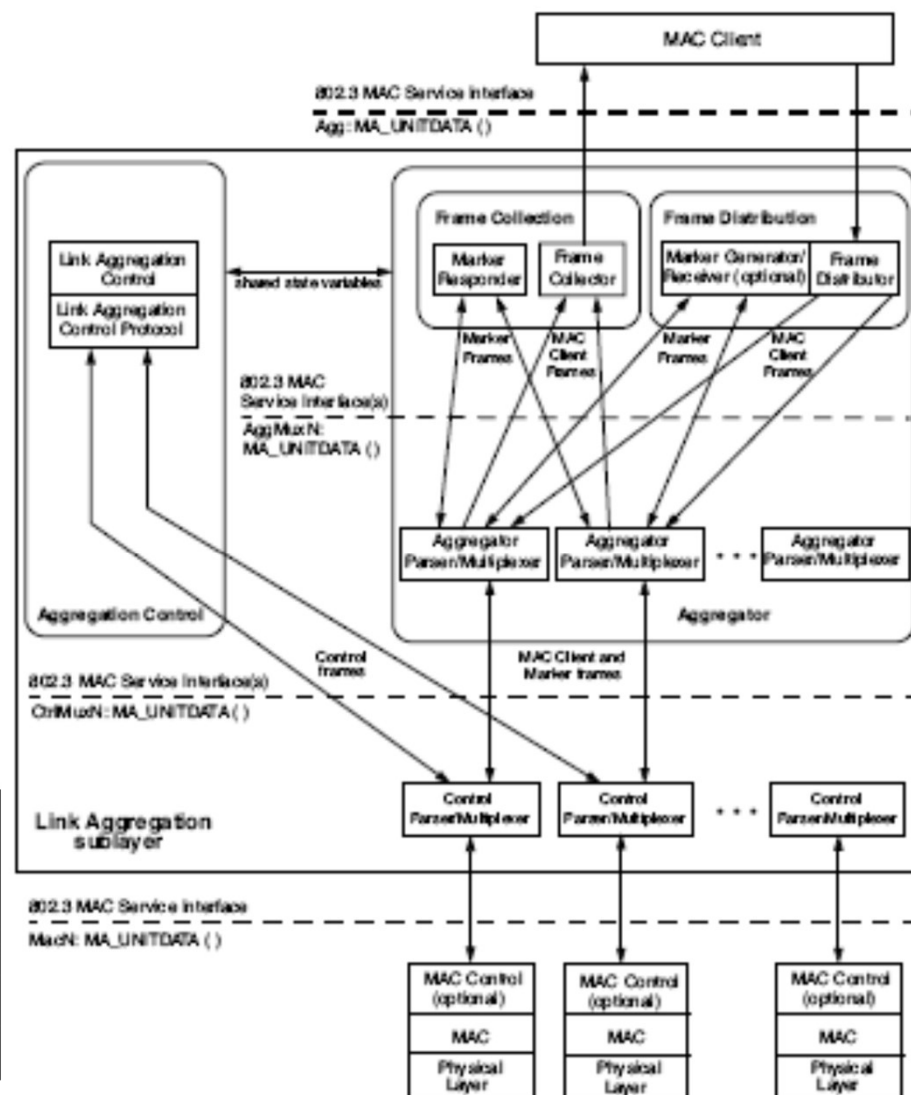
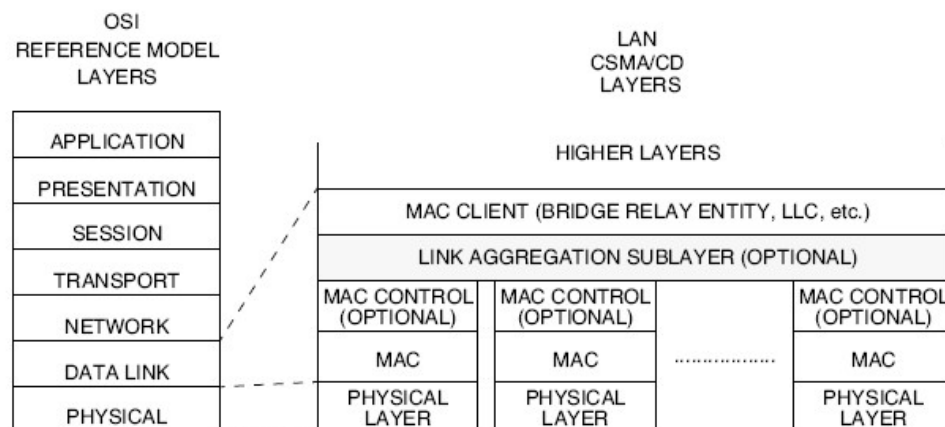
Other proprietary trunking protocols (megelőzték a 802.3ad-t):

- Cisco: **EtherChannel, Port Aggregation Protocol (PAgP)**
 - EtherChannel
 - FastEtherChannel
 - GigaEtherChannel
 - 10GigaEtherChannel (0.16TBit/s!!)
 - megelőzte
- Adaptec: Duralink trunking
- Nortel Multi-link Trunking (MLT) ...
- Általában csak ugyanazon gyártó eszközeivel, sőt esetenként csak ugyanazon gyártó egyes eszközeivel kompatibilisek

Transzparens hidak – Link Aggregation

A 802.3ad felépítése

- **Frame Collector/Distributor**
- **Aggregator**
- **Aggregation Control**



Transzparens hidak – Link Aggregation

Keret elosztás az összefogott linkek között

- **IEEE 802.3ad nem specifikálja**
- **Cisco:**
 - **L2: Forrás/Cél MAC cím szerint**
 - **L3: Forrás/Cél IP cím szerint**
 - **L4: Port szerint**
- **Problémát okozhatnak: pl. keret sorrend csere**

Transzparens hidak – Link Aggregation

Negotiation (egyeztetés):

- **IEEE: Link Aggregation Control Protocol (LACP) – 802.1ad**
- **Aktív:** küldözget LACP PDU-kat, a vonal másik végén a párja:
- **Passzív:** ha kap, akkor válaszol rá, de ő nem kezdeményez

Mode	Description
On	Forces the port to channel without LACP. With the on mode, a usable EtherChannel exists only when a port group in on mode is connected to another port group in on mode.
Off	Prevents the port from channeling.
Passive	Similar to the automode for PAgP, places a port into a passive negotiating state, in which the port responds to LACP packets it receives but does not initiate LACP packet negotiation. This is the default.
Active	Similar to the desirable mode for PAgP, places a port into an active negotiating state, in which the port initiates negotiation with other ports by sending LACP packets.

Transzparens hidak – Link Aggregation

Negotiation (egyeztetés):

- **Cisco: Port Aggregation Protocol (PAgP)**
 - A kapcsoló automatikusan felfedezi a másik oldal képességeit és kiépíti az optimális számú/típusú link csoportot

Mode or Keyword	Description
On	The mode that forces the port to channel without PAgP. With the on mode, a usable EtherChannel exists only when a port group in on mode is connected to another port group in on mode.
Off	The mode that prevents the port from channeling.
Auto	The mode that places a port into a passive negotiating state, in which the port responds to PAgP packets it receives but does not initiate PAgP packet negotiation. This is the default setting.
Desirable	The mode that places a port into an active negotiating state, in which the port initiates negotiations with other ports by sending PAgP packets.
silent	The keyword that is used with auto or desirable mode when no traffic is expected from the other device. This options prevents the link from being reported to the Spanning Tree Protocol as down, this is the default, secondary PAgP setting.
non-silent	The keyword that is used with auto or desirable mode when traffic is expected from the other device.

Transzparens hidak – Jellemzőik

- **Különböző MAC protokollú hálózatok összekötésére is alkalmas** (a gyakorlatban ha nem muszáj erre nem alkalmazzák, mert problémákat okoznak az eltérő keretformátumok – pl. az eltérő max. kerethosszak – de pl. a **802.11 WLAN Access Point** pont ezt csinálja)

Megoldás:

- **encapsulation bridging** \Rightarrow az egyik keretformátumba „becsomagolják” a másikat, majd kilépéskor, vagy a célállomásra érkezéskor „kicsomagolják” azt. Pl: **FDDI-Ethernet bridge** (az FDDI-be csomagolja be az Ethernetet)
- **Felsőbb protokollokra transzparens**
- **Korlátozottan képes forgalmat szeparálni** (a tanulás alatt eláraszta)
- **Alkalmas nagy távolság áthidalására**
 \Rightarrow nincs elvi korlát, csak gyakorlati pl.: max. késleltetés
- **A hálózat méretére, állomásszámára nincs elvi korlát** (akármekkora hálózat is építhető belőle), **de gyakorlati korlátok:** Broadcast Storm (Broadcast Domain), maximális Hash tábla méretek.

Forrás által forgalomirányított hidak

- **Source Routing Bridge** (pl. IBM Token Ring – napjainkban alig használják)
- **Feltételezi, hogy minden egyes állomás ismeri a célcímig terjedő teljes útvonalat és azt beleírja a továbbítandó keretbe (*Directed Frame*).**
 - (Pl. IBM Token Ring keret: **Routing Information Field (RIF)** - ilyenkor a Source MAC cím első bitje 1 (mint a multicast MAC), max. 15db útvonal bejegyzés)
- **A hidak eszerint a (RIF) lista szerint továbbítják a kereteket.**
- **Az útvonalak felderítése – forrás elárasztással:**
 - **Felfedező keretet (*Explorer Frame*) küld a célállomásnak.**
 - **ARE: all-routes explorer (mindenfelé) IBM TR, max. 15 hop**
 - **SRE: single-route explorer (spanning tree mentén) TR max. 15 hop**
 - **A továbbítás során a felfedező keretekbe a hidak bejegyzik, a saját azonosítójukat (Route Descriptor (Bridge ID + Ring ID) az Explorer Frame RIF-jébe).**
 - **Ha megérkezik a célba az első felderítő keret
⇒ tartalmazza az optimális útvonalat.**
 - **Ezt visszaküldi a forrásnak (*Directed Frame*) és mind a cél, mind a forrás bejegyzik egy táblába a forrás/célcímhez tartozó útvonalat.**

Forrás által forgalomirányított hidak – Jellemzőik

Előnyei:

- **Optimális!**
- **Többszörösen összefüggő topológián is működik!**

Hátrányai:

- **Nem transzparens, az állomásoknak pontosan ismerniük kell a topológiát (táblázatok kezelése).**
- **Nehézkes a sok táblázat kezelése az állomásokon.**
- **Lassan alkalmazkodik a topológia változásaihoz (újból felderítő keretek kellenek).**
- **A felderítő keretek elárasztása túl nagy forgalmat generálhat (pl. a rendszer indulása reggel egyszerre).**

Router - forgalomirányító (hálózati réteg)

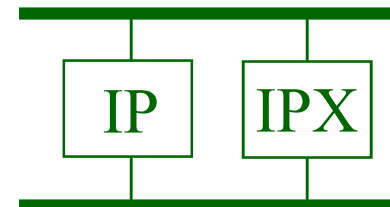
- Router - forgalomirányító - útvonal-irányító

Funkciója:

- Szeparált hálózatokat össze

Működése

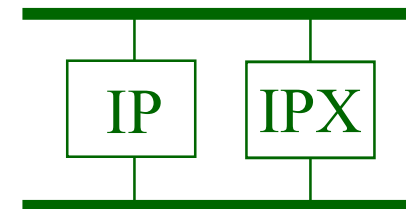
- Forgalomirányítás (csomagok forgalomirányítása) router táblázatok alapján.
- A hálózati rétegben működik, ezért:
hálózati-protokoll függő.



Routerek - Típusai

Lehetnek:

- **Egy protokollt kezelő router**
- **Multiprotocol router**
 - Több protokoll csomagformáját ismeri
 - Párhuzamosan köt össze különböző protokollok szerint
- **Brouter (bridge router)**
 - Ha felismerhető a protokoll \Rightarrow router
 - Ha nem felismerhető a protokoll \Rightarrow bridge-ként működik



Router - egyebek

Gond:

az olyan hosszúságú csomagok kezelése, amely meghaladja valamely köztes alhálózat maximális csomagméretét

- **Kezelése**

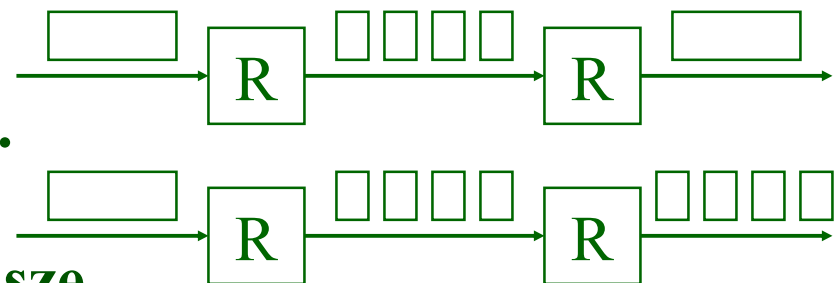
- a továbbítás megtagadása (és visszajelzés), vagy
- a csomag feldarabolása (fragmentation)

A feldarabolás lehet

- **Transzparens:**
a routerek össze is rakják.

- **Nem transzparens:**
csak a célállomás rakja össze.

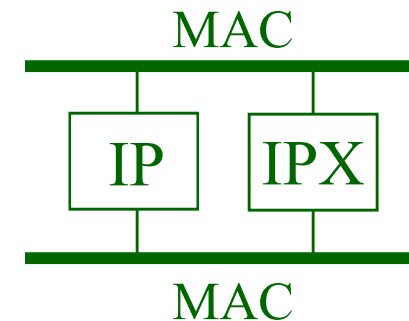
(A darabolást követően mindenki feldarabolva továbbítja.)



Routerek - Jellemzőik

Jellemzői :

- **Különböző MAC hálózatokat köthet össze.**
- **Protokollfüggő eszköz.**
- **Teljes forgalomszeparálásra képes.**
 - (Csak a forgalomirányításhoz szükséges protokoll jelent plusz forgalmat.)
- **Alkalmas nagy távolság áthidalására.**
- **A hálózat méretére, állomásszámára nincs elvi korlát.**



További funkciók lehetnek:

- **Adat-/hálózatvédelem – csomagszűrő tűzfal.**
- **Felhasználó menedzsment – hozzáférés engedélyezés/tiltás (pl. ISP behívó pont).**
- **Kapcsolat és útvonal menedzsment – kapcsolat engedélyezés/tiltás, útvonalak megválasztása, redundáns (tartalék) utak kezelése (megbízhatóság növelése).**

Routerek - Layer 3 Switch

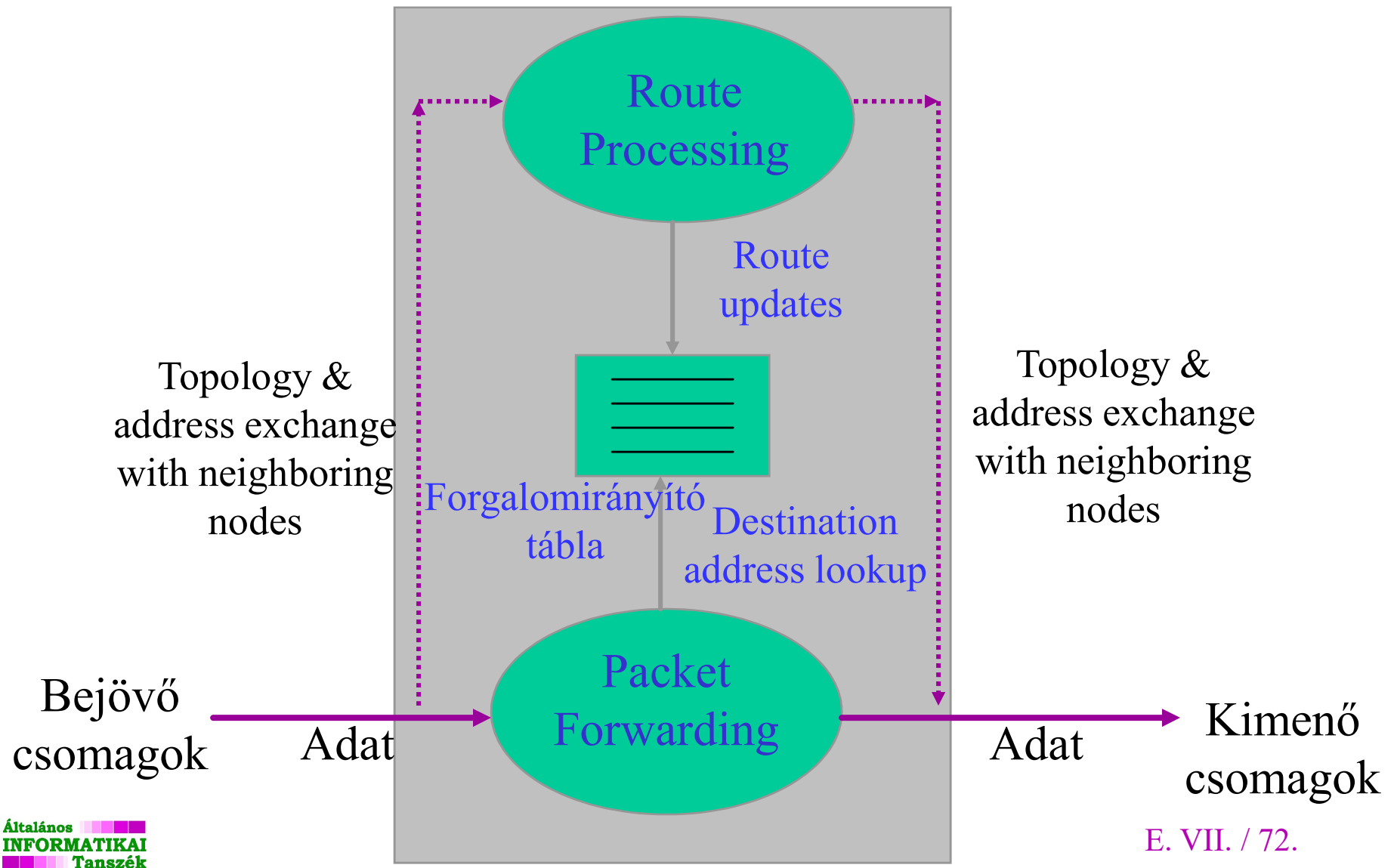
- Nagysebességű router
- Általában speciális cél-architektúra

Alapötlet:

- Valamely forrás-cél kapcsolat általában több csomagból áll és azokat hasonlóan kell kezelni.
- Miután az első csomagra elvégzi a forgalomirányítást, a kapott irányt a várható csomagsorozat jellemzőivel (3. fölötti réteg tartalom, funkciók) együtt táblázatba tölti.
- Ezen csomag-szekvencia további csomagjai már a táblázatban tárolt jellemzők („fingerprint”) alapján kerülnek irányításra (jóval gyorsabb), illetve változtatásra (ha kell, pl. TTL, CRC mezők újraszámítása).
(Ha nincs illeszkedés a táblázatra \Rightarrow teljes feldolgozás újból)

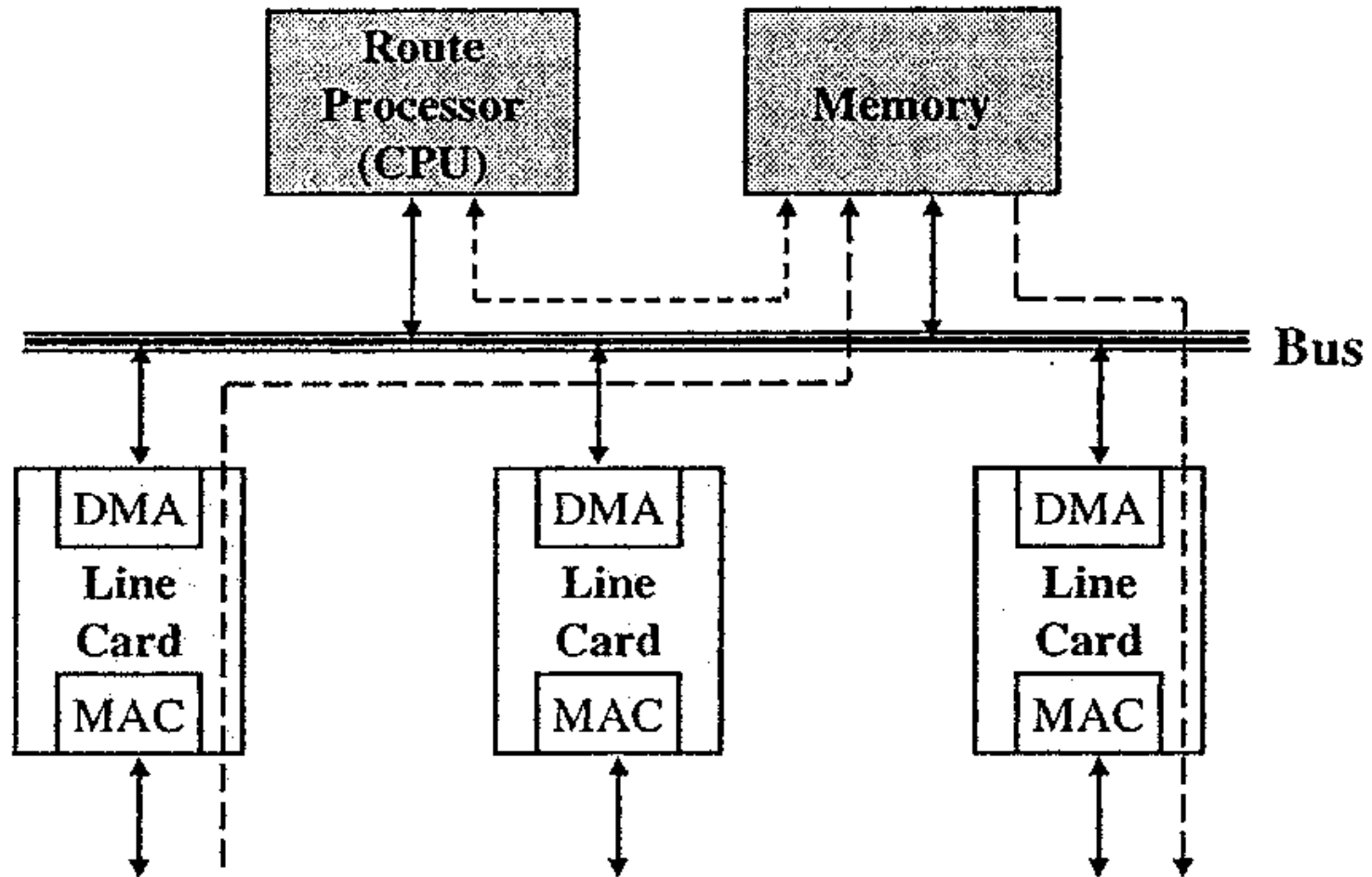
Routerek - Layer 3 Switch

- **Forgalomirányító, főbb komponensek**



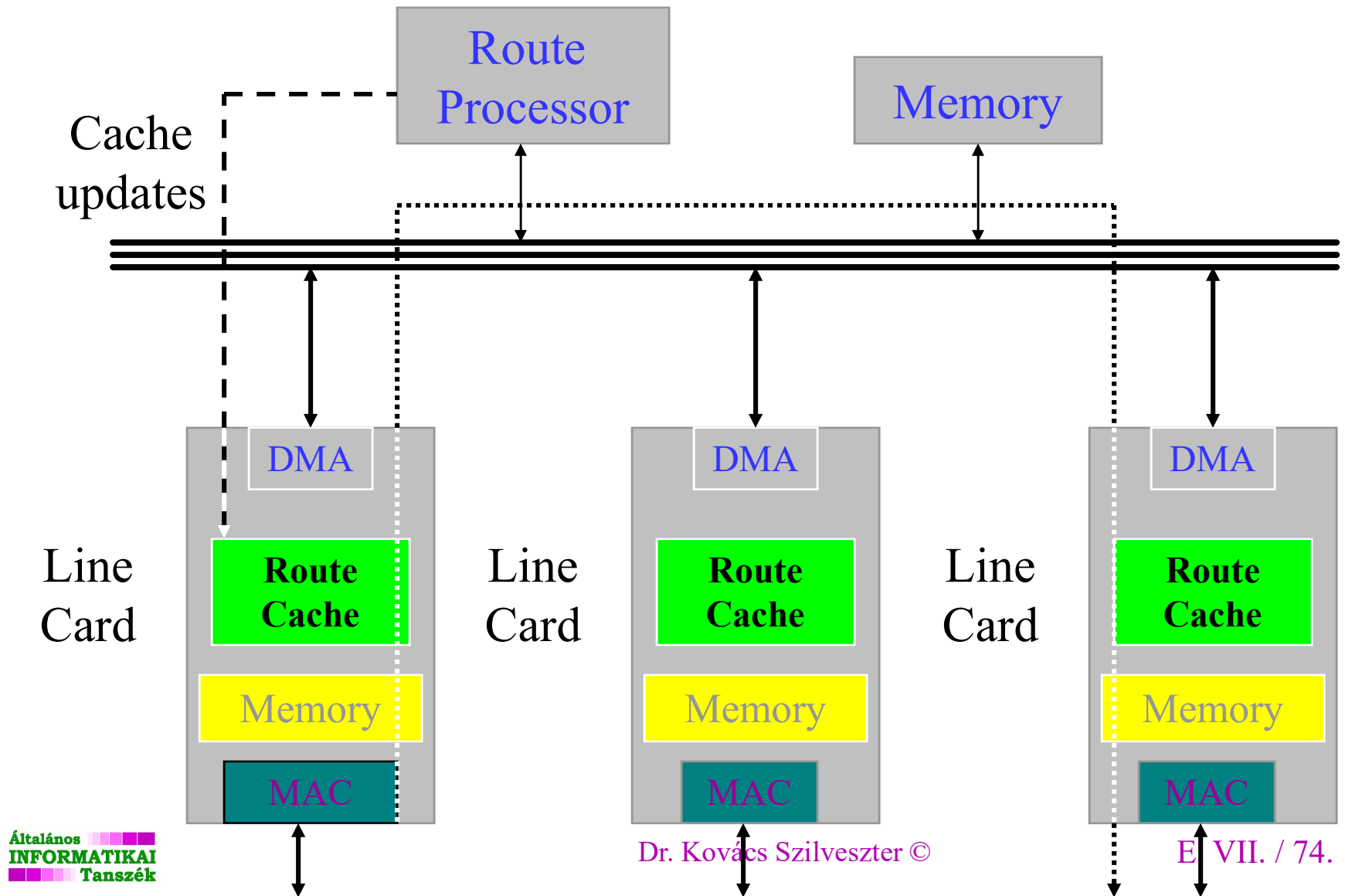
Routerek - Layer 3 Switch

- Klasszikus architektúra



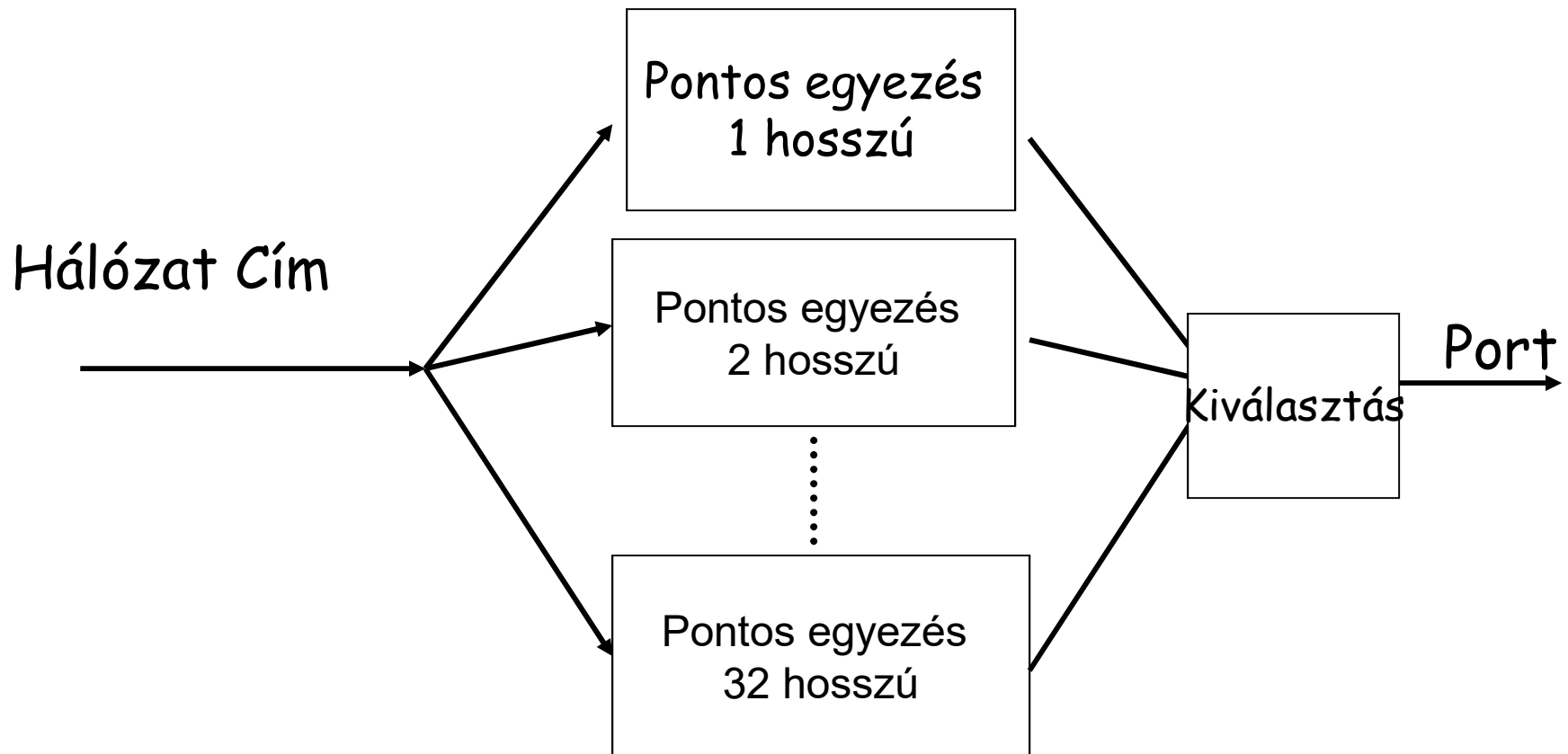
Routerek - Layer 3 Switch

- Útvonal gyorstár



Routerek - Layer 3 Switch

- A „leg hosszabb egyezés” (VLSM) párhuzamos feldolgozása



Nem route-olható protokollok

- Azok a protokollok, melyeknek nincs „valódi” hálózati rétegük – hierarchikus címzésük (pl. a MAC réteg globális címeit használják „hálózati” rétegbeli címekként), **nem route-olhatók!**
 - Pl. a DEC Lat, NetBIOS, NetBEUI, stb.
- A nem route-olható protokollokat híddal, vagy ismétlővel lehet csak továbbítani.

Bridge – Router

- **Egyes alkalmazásokban mindkettő egyaránt alkalmas lehet hálózatok összekapcsolásra.**
(Pl. valami egyéb okból nincs feltétlenül szükség router alkalmazására.)
- Gyakorlatilag valamennyi manapság kapható router **Brouter (bridge router).**
- **Azonban a Bridge-ek (Layer 2 Swith-ek) ugyanazon teljesítményű kivitelben lényegesen olcsóbbak.**
- **Mikor elégséges hát Bridge-et telepíteni?**

Bridge – Előnyök

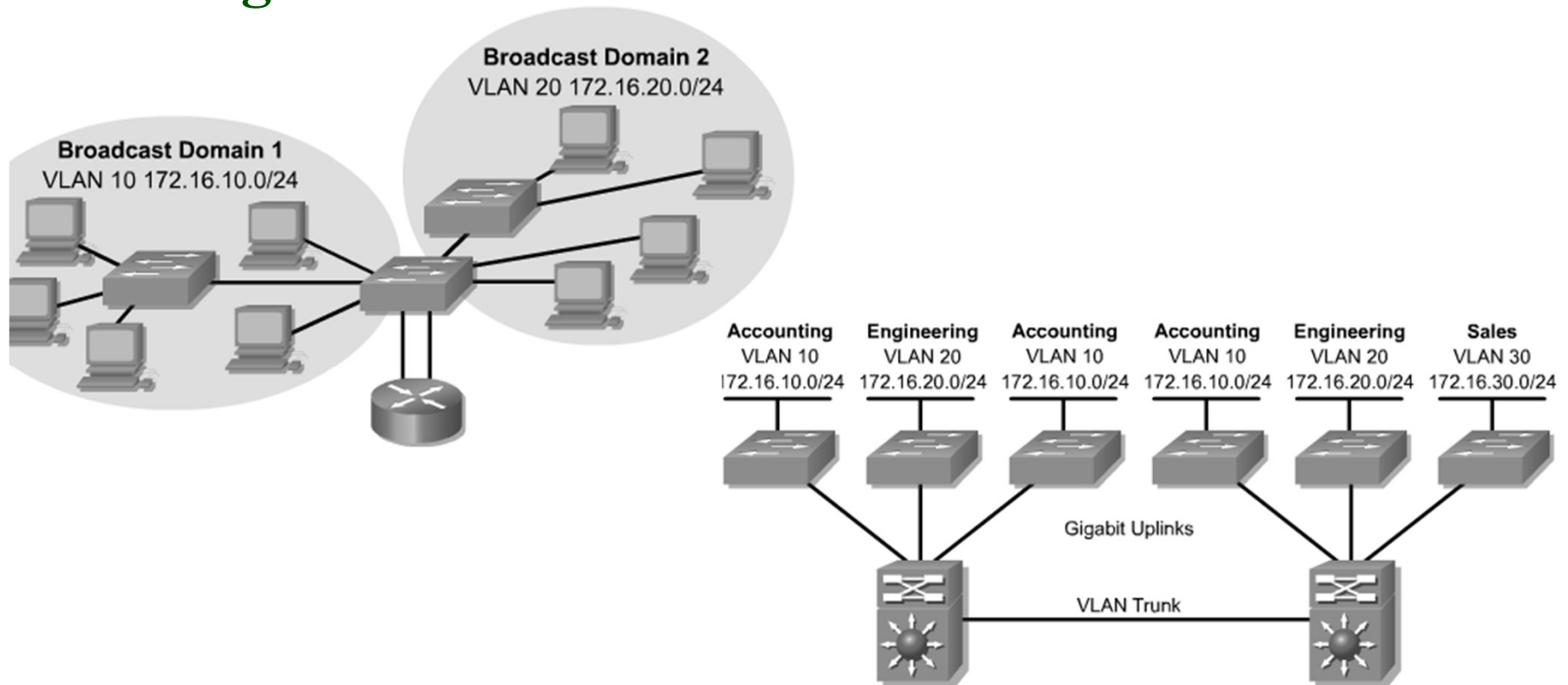
- **Egyszerű installálhatóság** (plug and pay/pray/play).
(esetleg port, VLAN, menedzsment konfiguráció)
- **Transzparens**, bárhova tehető, ahol korábban nem volt semmi, vagy repeater volt.
- **Hálózati protokoll független:**
 - Ha a hálózati protokoll nem route-olható, csak hidakkal/ismétlőkkel lehet összekötni hálózatokat.
 - Új, korábban nem ismert protokoll is bevezethető a kommunikációs infrastruktúra változtatása nélkül.
- A pusztán hidakkal/ismétlőkkel összekötött hálózat **egy logikai hálózatnak tűnik (egy „broadcast domain”)**:
 - Valamely állomás a hálózati címének megváltoztatása nélkül áthelyezhető.
- **Jó ár/teljesítmény viszony.**

Bridge – Hátrányok

- **Nem képesek terhelésmegosztásra a redundáns utak között – spanning tree** (hidak egyes esetekben képesek híd párok közti párhuzamos kapcsolatok terhelésmegosztására (**Ethernet channel**)).
- **Bizonyos helyzetekben nagy forgalomtorlódást okozhatnak: ismeretlen MAC cím: broadcast \Rightarrow nagy hálózat esetén: broadcast storm** $p_{\text{üres}} = (1 - p_{\text{broadcast}})^n$, n állomás esetén $n \rightarrow \infty$ $p_{\text{üres}} \rightarrow 0$
Hidakból épített nagy hálózat esetén a „fool-proof” alkalmazások (pl. a nem route-olható NetBEUI) eláraszthatják a rendszert („broadcast storm control” – egy szint fölött eldobál).
- **Az egyes hálózati részek forgalma részben keveredik, nehéz a forgalmat kézben tartani, hibát (támadást) keresni.**
- **A hálózat forgalmának bármely része lehallgatható** (táblák elárasztása (sok hamis forráscím) \rightarrow broadcast, bár ez részben implementációs hiba és orvosolható (egy portról lefoglalható terület limitálása)).

Bridge – Router

- A VLAN-ok között csak **Router** (vagy **Gateway**) biztosíthat átjárást
- Üzenetszórás tartomány (**Broadcast Domain**) szegmentálás



Router – Előnyök

- **Teljes forgalom szeparáció.**
⇒ **Igazán nagy távolsági hálózat csak router-ekből építhető.**
- **Alternatív utak közötti terhelésmegosztás.**
- **Rugalmas konfigurációs lehetőségek,
forgalomirányítási szabályok**
⇒ **„csomagszűrő” tűzfal.**

Router – Hátrányok

- **Konfigurálni kell.**
- **Protokollfüggő.**
- **Valamivel lassabb a Bridge-nél**
(még a Layer 3 Switch is a Layer 2 Switch-nél).
- **Nem route-olható protokoll esetén ő is csak bridge-ként működik.**

Bridge – Router

Mikor elégséges hát Bridge-et telepíteni?

- „Kis” hálózatokban szinte mindig.
- Ha szükség van a WAN kapcsolat miatt egy routerre, akkor általában arra a célra elég egy „kisebb”-fajta router, ami még ki bírja terhelni a WAN linket.
(Esetleg ez egyben tűzfal, illetve NAT is lehet.)

Mikor kell mégis a Router?

- Ha muszáj.
- Ott ahol az alkalmazott protokoll route-olható és van értelme „gerinchálózatról” beszélni.
- WAN hálózatokban.

Felhasznált irodalom

- **STP:**
<http://www.cisco.com/warp/public/473/5.html>
- **RSTP:**
<http://www.cisco.com/warp/public/473/146.html>
- **MSTP:**
<http://www.cisco.com/warp/public/473/147.html>
- **STP Timers:**
<http://www.cisco.com/warp/public/473/122.html>