Balla Attila, vezető technikai tanácsadó

SYNERGON

Ethernet hálózatok tervezése

SYNERGON GROUP

SPAN SAO infinity FibeX SYNERGON

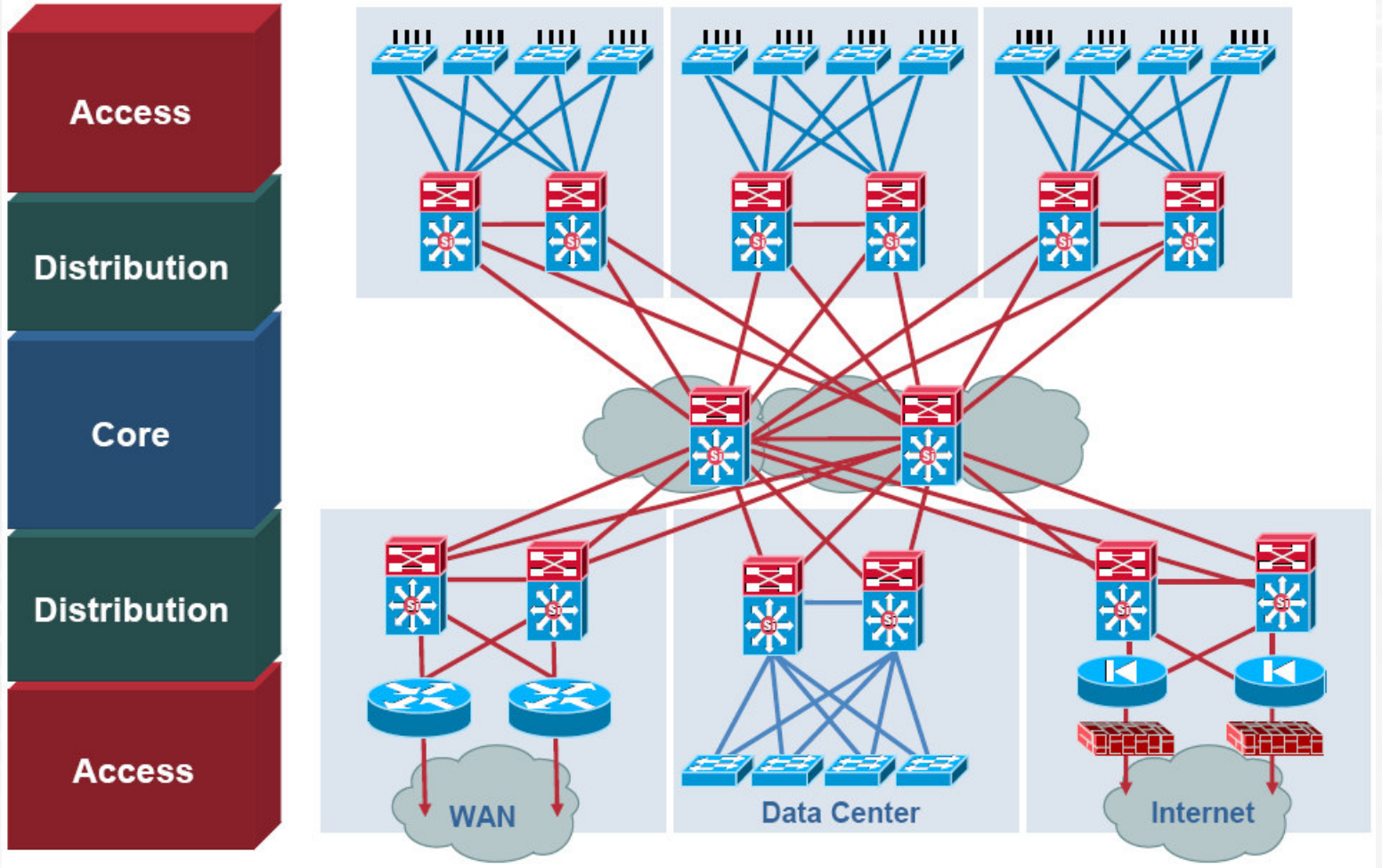
Bevezető

- Ethernet hálózatok
  - 1973-80, Bob Metcalfe és David Boggs
  - 10Mbps → 10Gbps
    - 100Gbps, 2006. november
  - Coax, UTP, Optika
- Ma kikerülhetetlen
  - Nemcsak LAN környezetben

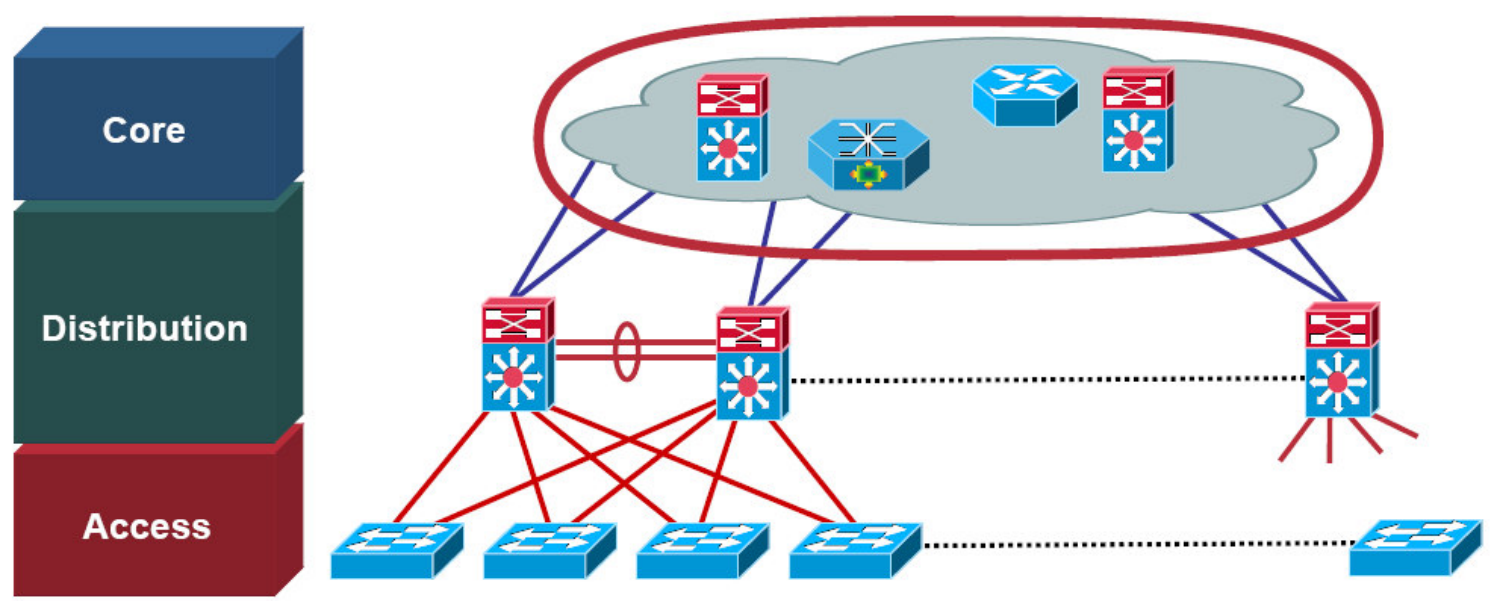
Tartalom

- Hierarchikus Hálózat Design
- STP optimalizálás
- CISF
- FHRP
- Esettanulmány

Klasszikus felépítés

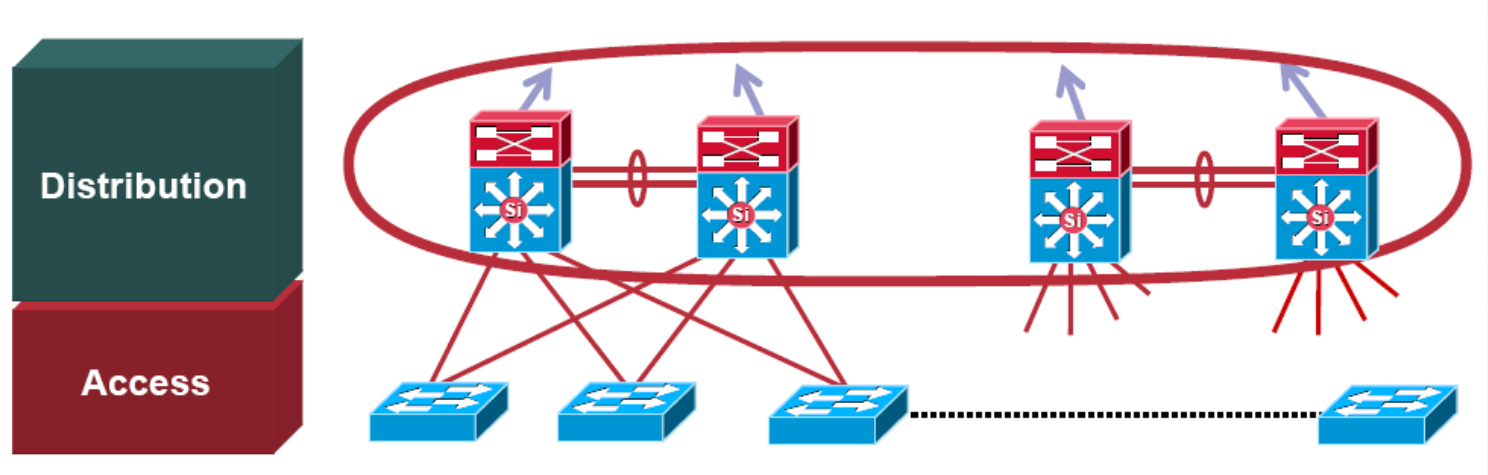


Core Réteg



- Gerinchálózat – hálózati részeket köt össze
- Teljesítmény és stabilitás
  - Összetettség nem előny
- Skálázhatóbb
- Technológiailag független legyen

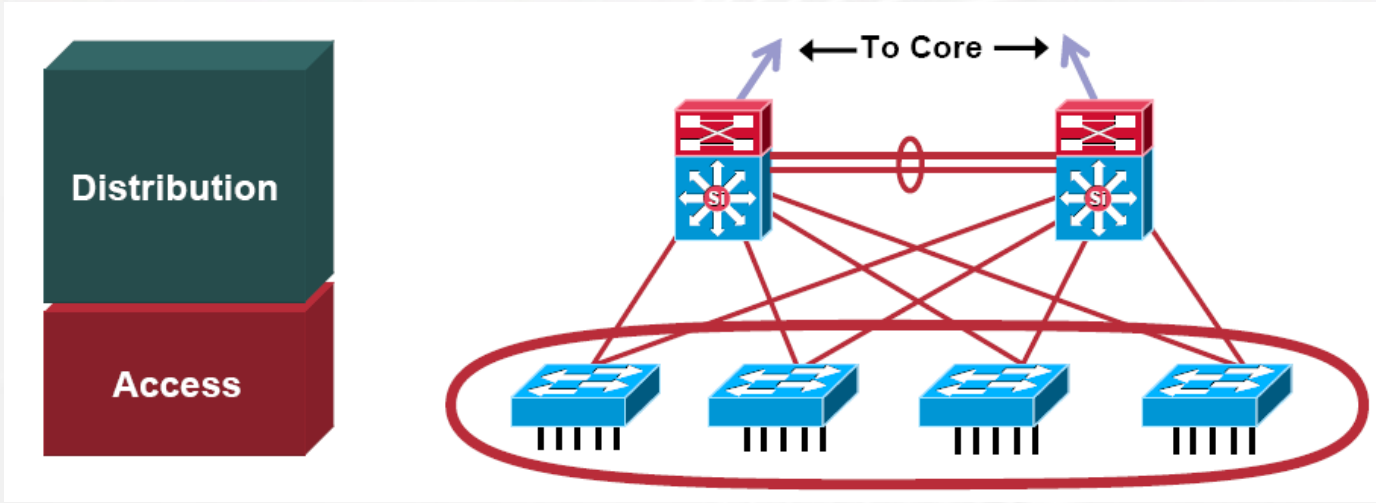
Distribution Réteg



- Rendelkezésre állás
- Terhelés elosztás
- Védi a Core Réteget az Access Rétegbeli problémáktól és a sok peer-től

- STP, csak ha muszáj
- Route summary, konvergencia
- FHRP
  - VRRP, HSRP, GLBP

Access Réteg



- Hálózati végpontok aggregálása
- Layer2 szolgáltatások
  - STP, RSTP, MST
  - Multicast
  - Védelmi eszközök
- QoS

- Layer3 szolgáltatások
  - Routing
  - Multicast
- Integrated Security eszközök
  - Port-Security, DHCP snooping, DAI, IP Source Guard, 802.1x,...

Tartalom

- Hierarchikus Hálózat Design
- STP optimalizálás
- CISF
- FHRP
- Esettanulmányok

Spanning Tree Protocol és Társai

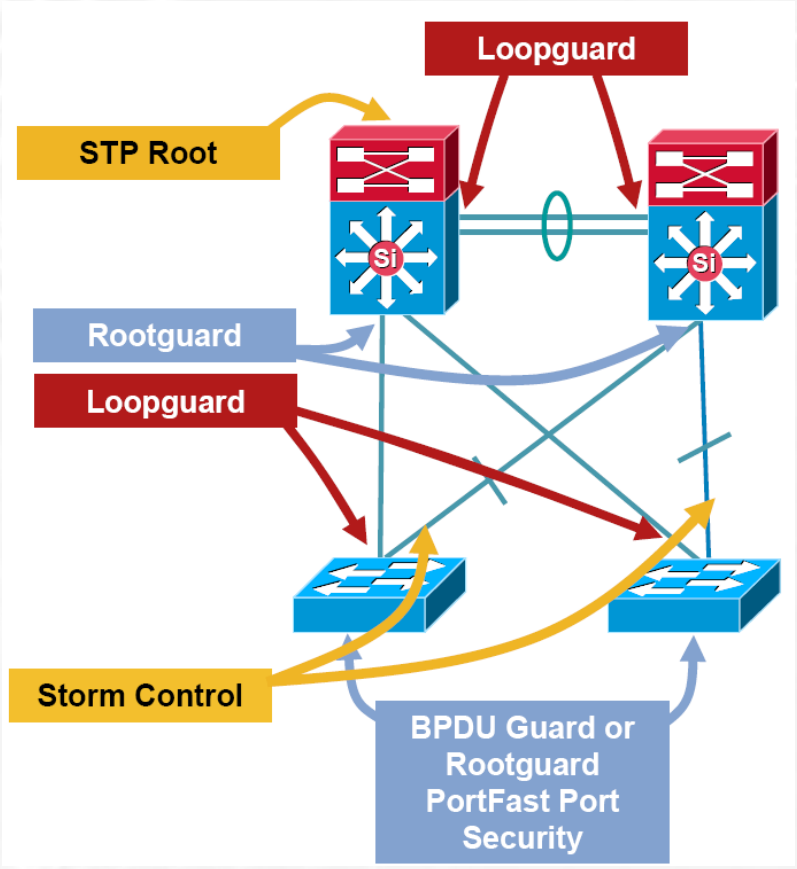
- PVST+: STP (802.1d) per VLAN
  - Portfast, Uplinkfast, BackboneFast, BPDUGuard, BPDUFilter, RootGuard, és LoopGuard
- Rapid PVST+: RSTP (802.1w) per VLAN
  - Portfast, BPDUGuard, BPDUFilter, RootGuard, és LoopGuard
- MST (802.1s):
  - Nem per VLAN, hanem per instance, 16 lehet
  - Minden instance-hoz több VLAN-t lehet rendelni
  - Portfast, BPDUGuard, BPDUFilter, RootGuard, and LoopGuard

STP Konfiguráció

- Csak ha szükséges!
- Adatparkokban tipikus
- Access rétegben átnyúló VLAN-ok
- Erős védelem szükséges

Layer2 Access Védelem

- Root bridge
  - Loopguard
  - Rootguard
  - UDLD
- Access port
  - BPDU guard
  - PortFast
  - Port-security
- Backup link
  - Storm control



Csomagvesztés

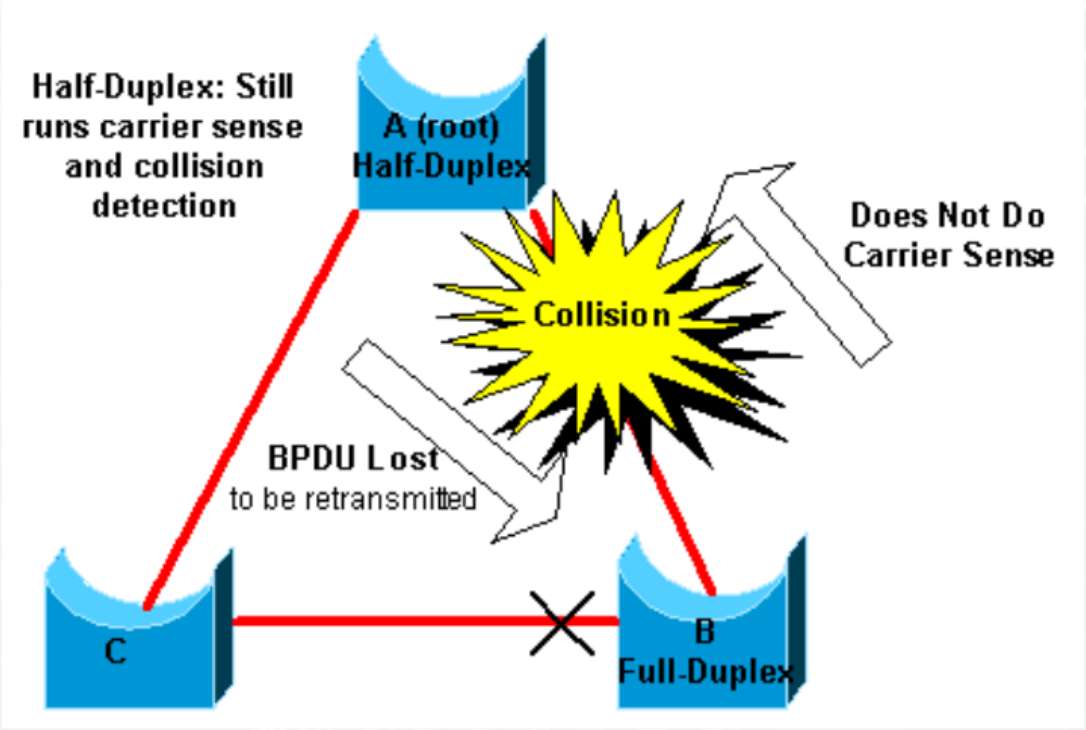
- Magas csomagvesztés egy fizikai összeköttetésen
  - Elveszhetnek a BPDU-k
- 50s -> blocking portból forwarding-ba
- Hurok
- Lehetséges okok:
  - Rossz kábel
  - Duplexitás
  - Kábelhossz

`show interfaces`

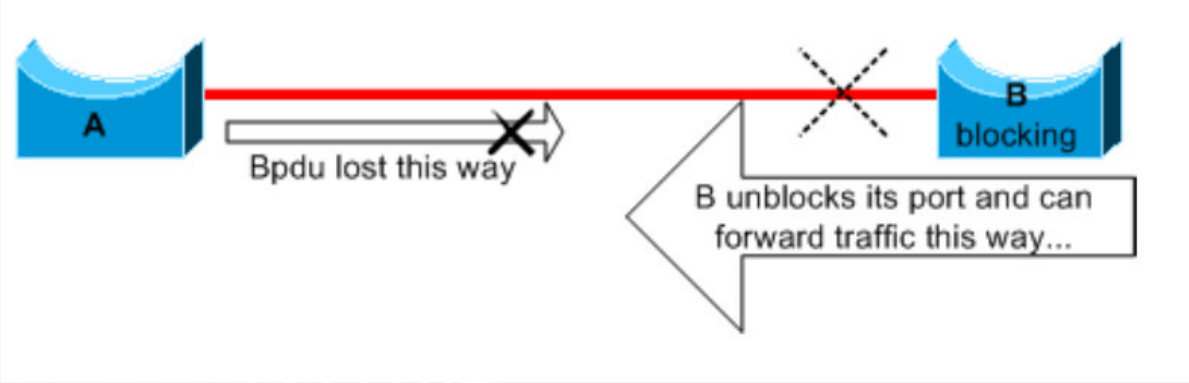
runts, giants, no buffer, CRC, frame, overrun, ignored

Duplexitás

1. „B” küldi a frame-ket
2. „A” használja a linket
3. „A” észreveszi az ütközést, backoff
4. „B” nem kap BPDU-t
5. Hurok... ;-(



UDLD



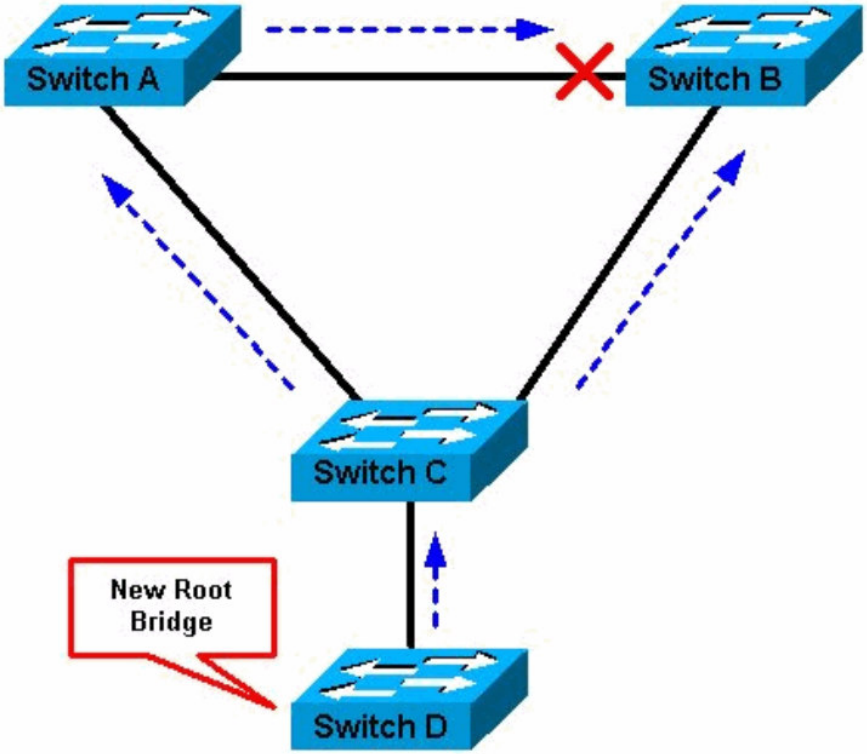
1. B blocking
2. A->B rossz
3. B->A jó
4. A-tól jövő BPDU-k elvesznek
5. B nem maradhat blocking állapotban
6. Hurok...
7. Megoldás: UDLD
   - Aggressive mode: errdisable állapot

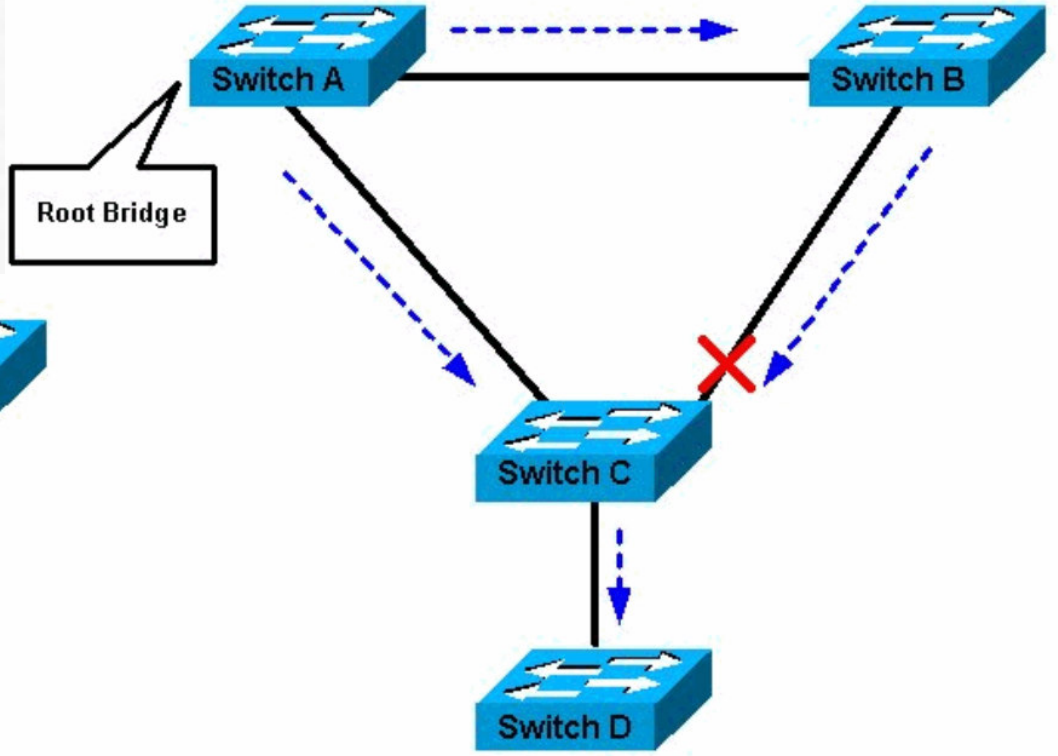
UDLD

- Cisco proprietary
  - Optika, UTP
  - unidirectional link detektálás
- Layer2 protokoll
  - Echo
  - Mindkét oldalon kell
- Normal
  - 15s
- Aggressive
  - Port stuck
  - Egyik oldalon up/másik oldalon down

Root Guard

- Bridge Priority kevés
  - Alacsonyabb MAC-address





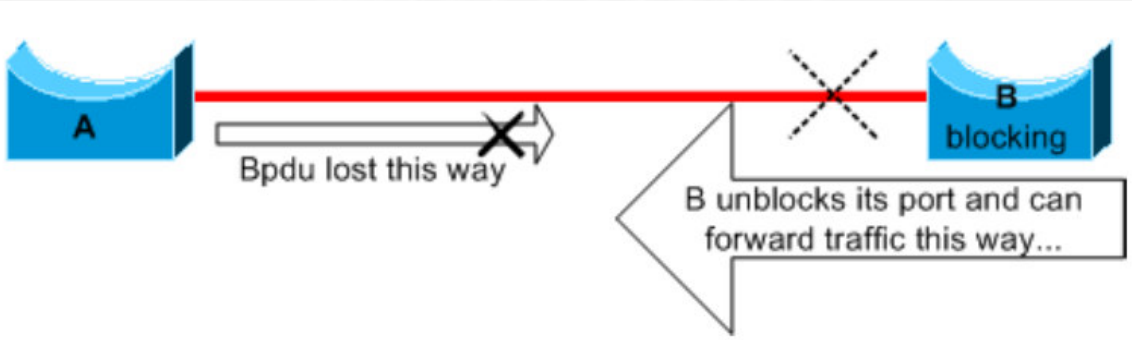
- root-inconsistent state
  - ~ listening, nincs forwarding
- Automatikus visszaállás

```
spanning-tree guard root
```

Loop Guard

- Ugyanaz, mint UDLD esetén
- DE: új port státusz
  - loop–inconsistent blocking
- Ha kap BPDU-t, akkor kerül ki
  - Automatikus
- Port alapú feature
  - De a porton konfigurált Vlan-okra külön működik
- Milyen portokon szükséges?
  - Blocking
  - Root
  - Alternate

```
spanning-tree guard loop
```



Loop Guard

- Loop Guard vs UDLD
  - Port alapú konfiguráció
  - Vlan vs Port működés
  - Automatikus visszaállás
  - Egyirányú link ellen jó
  - Software hibákra Loop Guard
  - Kábelezési hibákra UDLD
- Root Guard
  - Kölcsönösen kizárják egymást
- PortFast
  - Kölcsönösen kizárják egymást
- Osztott link
  - Nem lehet
- MST
  - Együttműködik

PortFast

- Nincs listening és learning fázis
  - Azonnal forwarding állapot
  - STP része a port -> támadási felület
    - Root Bridge
- BPDU Guard
  - Errdisable állapotba kerül a port BPDU esetén

```
spanning-tree portfast bpduguard
errdisable recovery cause bpduguard
errdisable recovery interval 400
```

Trunk

- Általában az Access és a Distribution réteg között
- Csak a szükséges VLAN-okat kell átengedni
- Native VLAN változtatás

- Bevésni az enkapszulációt és a nonegotiate-t
  - DTP kikapcsolása

```
switchport trunk encapsulation dot1q
switchport trunk native vlan <>
switchport trunk allowed vlan <>,<>,<>
switchport mode trunk
switchport nonegotiate
```

VLAN Trunking Protocol

SYNERGON

- Központosított VLAN menedzsment
- VTP szerver switch hirdeti a VLAN táblát
- Csak trunk-n fut
- Négy lehetőség:
  - Server
  - Client
  - Transparent
  - Off
- Ha muszáj, akkor VTPv3
  - Extended VLAN
  - Private VLAN
  - Authentikáció
  - VTPv1 és v2-vel együttműködik
  - Per-port alapú
  - CatOS ;-(

STP Skálázhatóság

- Logikai interface-k és a BPDU-k határozzák meg
  - Csak a szükséges Vlan-k legyenek minden trunk-ön
  - Általában az RPVST+ elegendő

	MST	RPVST+	PVST+
Total Active STP Logical Interfaces	50,000 total 30,000 total with Release 12.2(17b)SXA	10,000 total	13,000 total
Total Virtual Ports per LineCard	6,000 per switching module	1,800 per switching module	1,800 per switching module

CLI

- show spantree summary total
  - ➢STP Active
- show vlan virtual-port slot <mod>

- Számolás
  - ➢∑ (trunk-ökön levő Vlan-ok) + Access portok

Tartalom

- Hierarchikus Hálózat Design
- STP optimalizálás
- CISF
- FHRP
- Esettanulmányok

Cisco Integrated Security Features

- Port Security
  - CAM tábla védelem
- DHCP Snooping
  - DHCP server védelem
- Dynamic ARP Inspection
  - ARP védelem
- IP Source Guard
  - IP/MAC spoofing

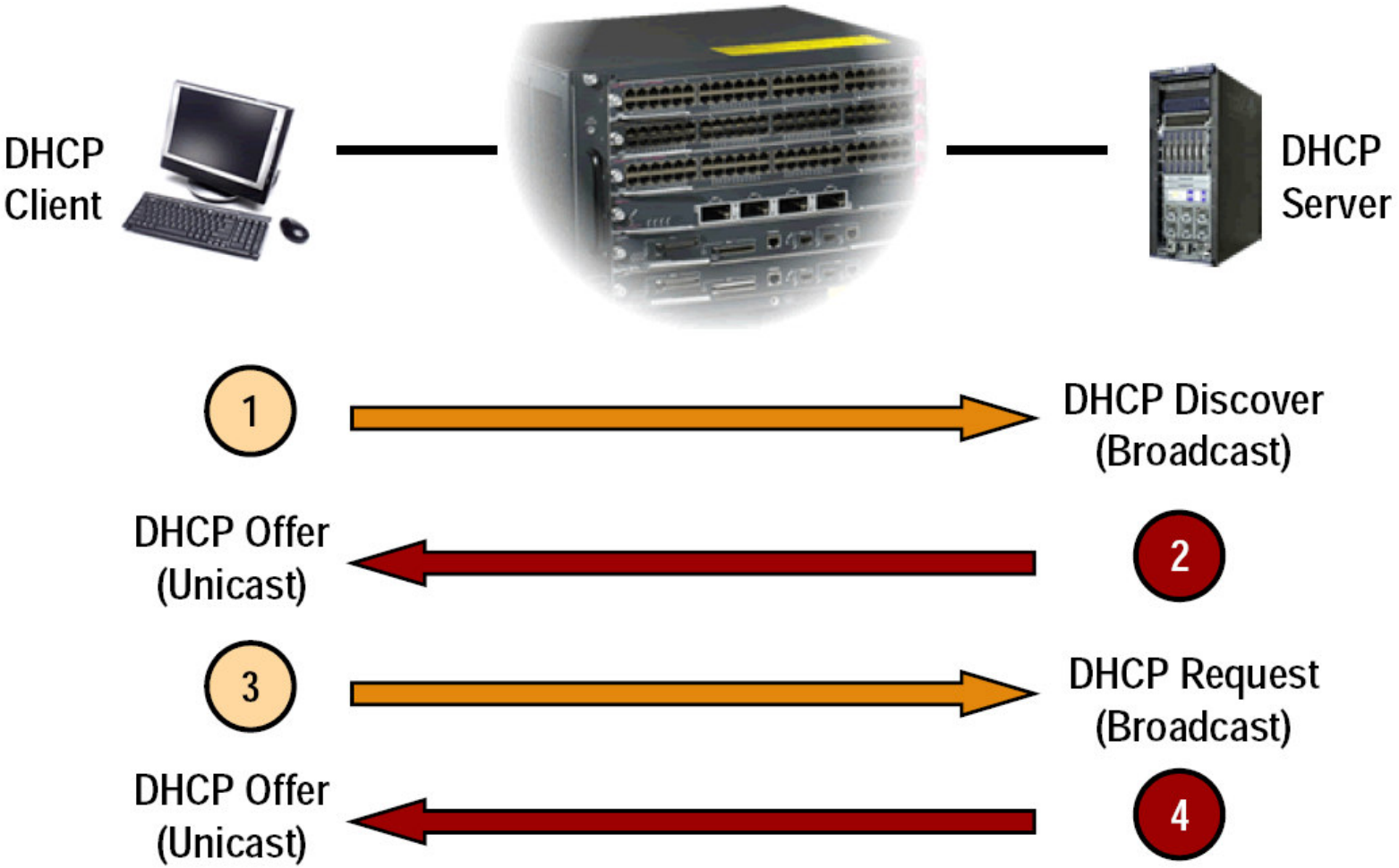
Port Security

- Csak bizonyos MAC-address-ek használhatják a portot

- Módszerek
  - Protect
  - Restrict
  - Shutdown

```
6500(config-if)# switchport port-security ?
  aging          Port-security aging commands
  mac-address    Secure mac address
  maximum        Max secure addresses
  violation      Security violation mode
```

DHCP – RFC2131



DHCP Snooping

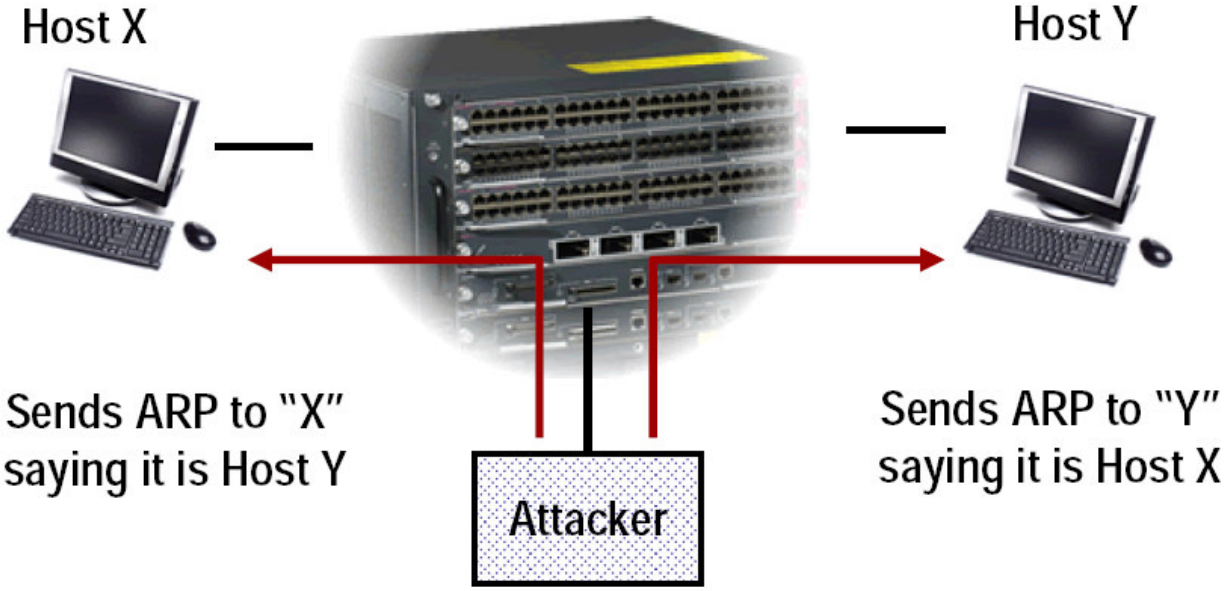
- Csak a megbízható portokról jöhet DHCP offer
- Adatbázis, 8000 összekapcsolás
  - MAC cím
  - IP cím
  - Lease Time
  - Binding Type
  - VLAN
- DAI ezt az adatbázist használja

```
ip dhcp snooping
ip dhcp snooping vlan <>

ip dhcp snooping trust

ip dhcp snooping database
   tftp://...
```

Dynamic ARP Inspection



- Man in the Middle Attack
- Nem valós IP/MAC bejegyzés a Host-okon
- A Támadó képes monitorozni X és Y közötti forgalmat

DAI

- Ellenőrzi az ARP csomagokat
  - DHCP Snooping adatbázisa alapján
  - Inkonzisztens ARP csomagokat eldobja
  - Trust port-n nem ellenőriz

```
ip arp inspection vlan <>
interface type number
  ip arp inspection trust

errdisable recovery cause arp-inspection
```

IP Source Guard

- Ugyanúgy működik, mint a DAI
  - Összes csomagot ellenőriz
  - DHCP snooping adatbázis alapján
  - Nemcsak ARP csomagokat

```
ip dhcp snooping
ip dhcp snooping vlan 10
interface X/Y
 switchport mode access
 switchport access vlan 10
 no ip dhcp snooping trust
 ip verify source vlan dhcp-snooping
```

Egyéb lehetőségek

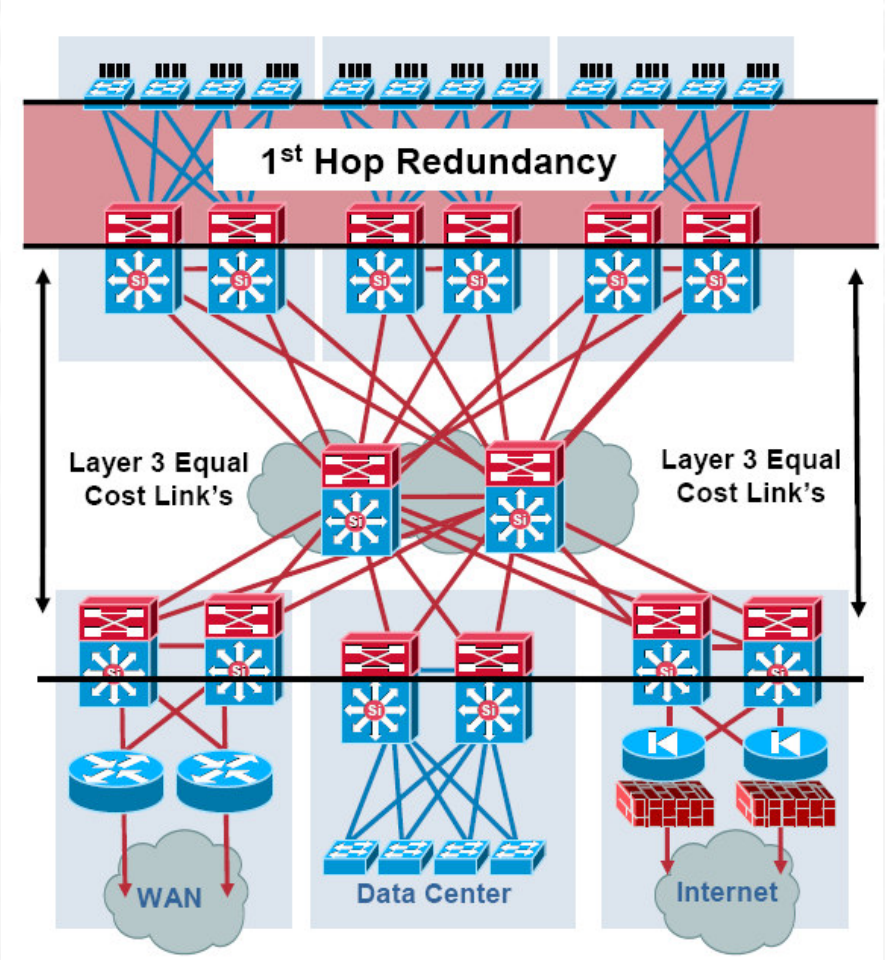
- Network Admission Control
- IEEE 802.1x authentikáció
- Web alapú authentikáció

Tartalom

- Hierarchikus Hálózat Design
- STP optimalizálás
- CISF
- FHRP
- Esettanulmányok

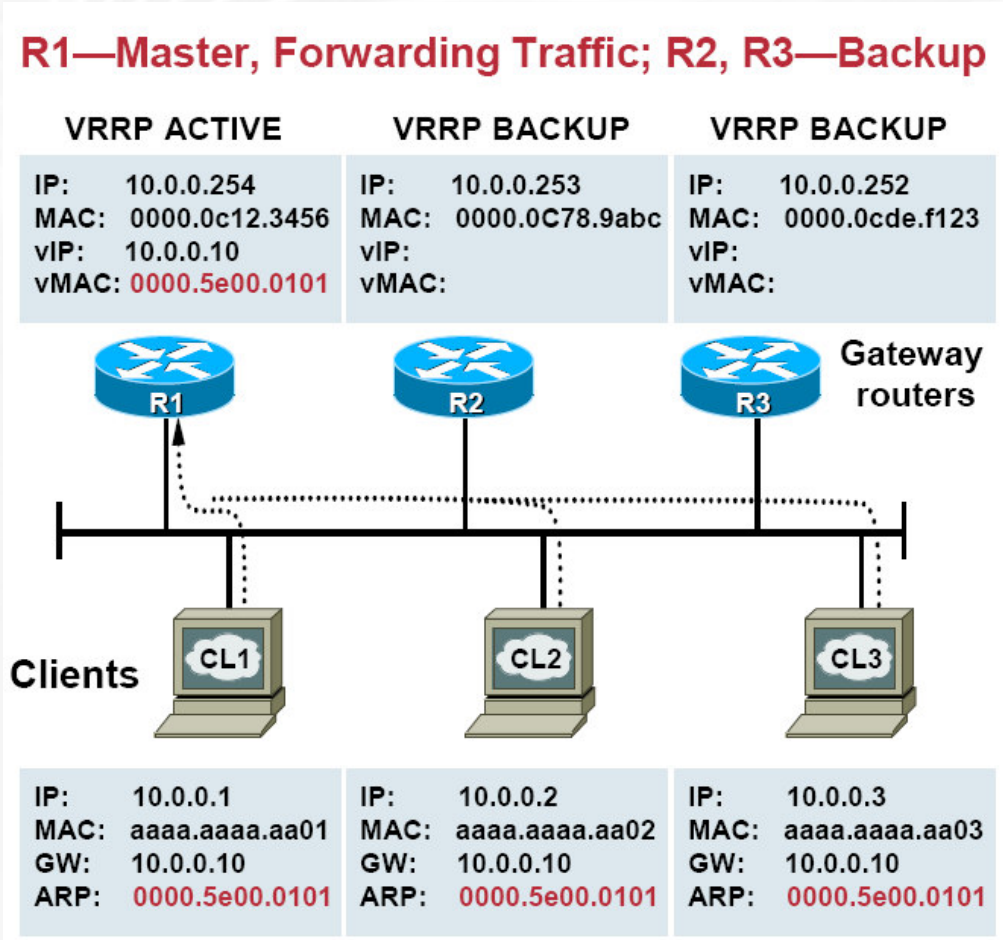
FHRP

- First Hop Redundancy Protocol
- Redundáns default-gw a végberendezéseknek
- HSRP, VRRP, GLBP lehetőségek
  - Másodpercen belüli konvergencia
- VRRP-t más gyártók is implementálták
- GLBP uplink terhelés elosztás



VRRP – RFC2338

- Virtual Router Redundancy Protocol
- Egy virtuális router
  - Egy VIP
  - Egy VMAC
- Csak a „master” router végez adattovábbítást
- Backup router-ek



VRRP előnyei

- Redundancia
  - Több router 1 GW
- Terhelés elosztás
  - Csoportosítás
- Több virtuális router
  - Max. 255
  - 00-00-5E-00-01-{VRID}
- Több IP cím
  - Egy interface több csoport cím
  - Secondary címek
- Preempív mód
  - Kijelölt aktív router
- Authentikáció
  - védelem
- Dedikált multicast cím
  - 224.0.0.18
- Object tracking
  - Komplex
  - Prioritást csökkenthet
  - 12.3(2)T, 12.2(25)S

VRRP konfigurálás

```
interface type number
 ip address ip-address mask
  vrrp group description text
  vrrp group priority level
  vrrp group preempt [delay minimum seconds]
  vrrp group timers advertise [msec] interval
  vrrp group timers learn
  vrrp group ip ip-address [secondary]

track object-number interface type number {line-
   protocol | ip routing}

vrrp group track object-number [decrement priority]
```

HSRP – RFC2281

- Hot Standby Routing Protocol
- Ugyanaz, mint a VRRP
- Nem szabványos
- Virtuális címek
  - 0000.0C07.AC{VRID}
  - 224.0.0.2

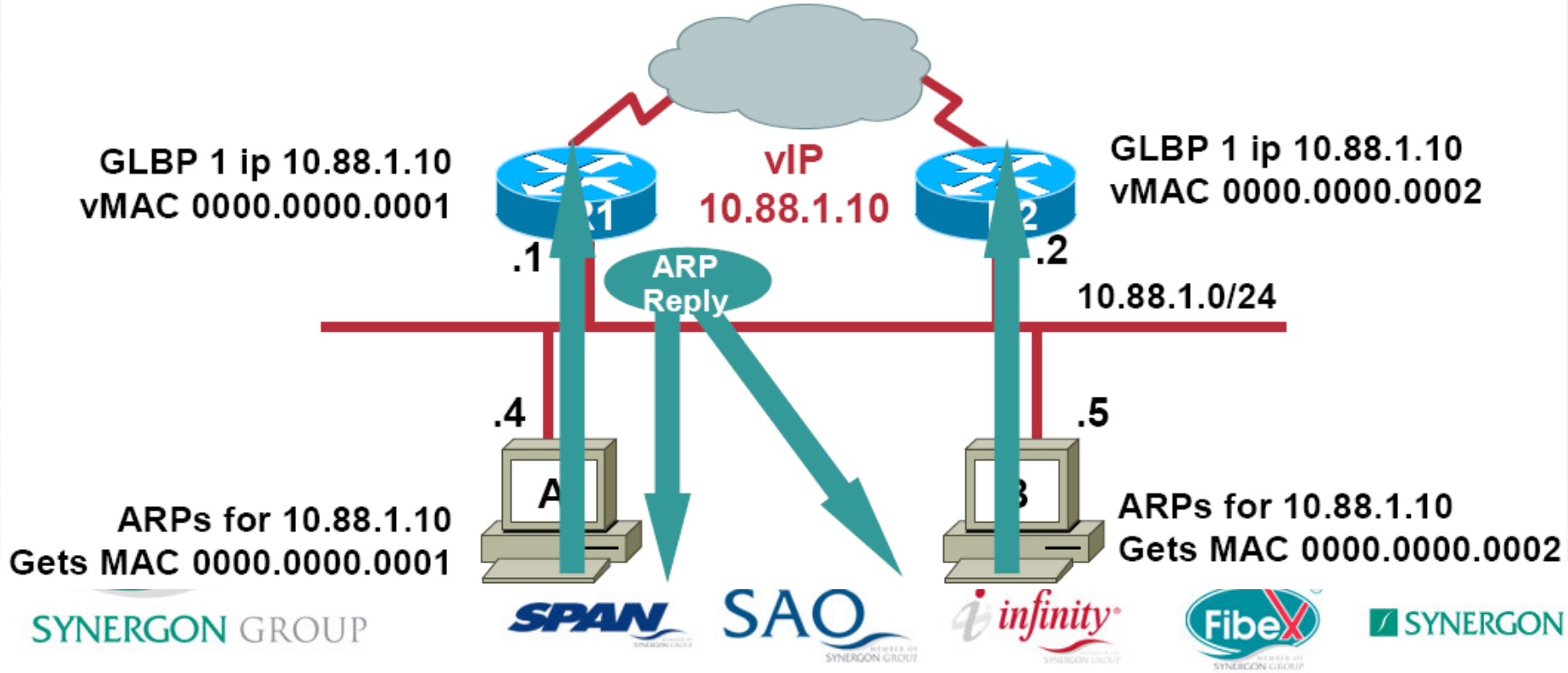
```
interface type number
  ip address ip-address mask
  standby delay minimum min-delay reload min-delay
  standby [group-number] ip [ip-address [secondary]]
  standby [group-number] priority priority
  standby [group-number] preempt [delay {minimum delay |
                                  reload delay | sync delay}

  standby [group-number] track object-number
                              [decrement priority-decrement]
```

GLBP

- Gateway Load Balancing Protocol
- Egy VIP-hez több VMAC
- DefGW-re különböző ARP-t kap

- Kommunikáció
  - 224.0.0.102:3222
  - 3s



GLBP

- Active Virtual Gateway – AVG választás
  - A többi backup
- AVG generálja az összes VMAC-t
  - Ez alapján történik a továbbítás
  - Active Virtual Forwarders – AVF
- Skálázhatóság
  - 1024/interface
  - 4 AVF/csoport

GLBP Konfigurálás

SYNERGON

```
interface type number
 ip address ip-address mask [secondary]
 glbp group timers [msec] hellotime [msec] holdtime
 glbp group timers redirect redirect timeout
 glbp group load-balancing [host-dependent|round-robin|weighted]
 glbp group priority level
 glbp group preempt [delay minimum seconds]
 glbp group name redundancy-name

 glbp group weighting maximum [lower lower] [upper upper]
 glbp group weighting track object-number [decrement value]
```

Melyiket válasszuk?

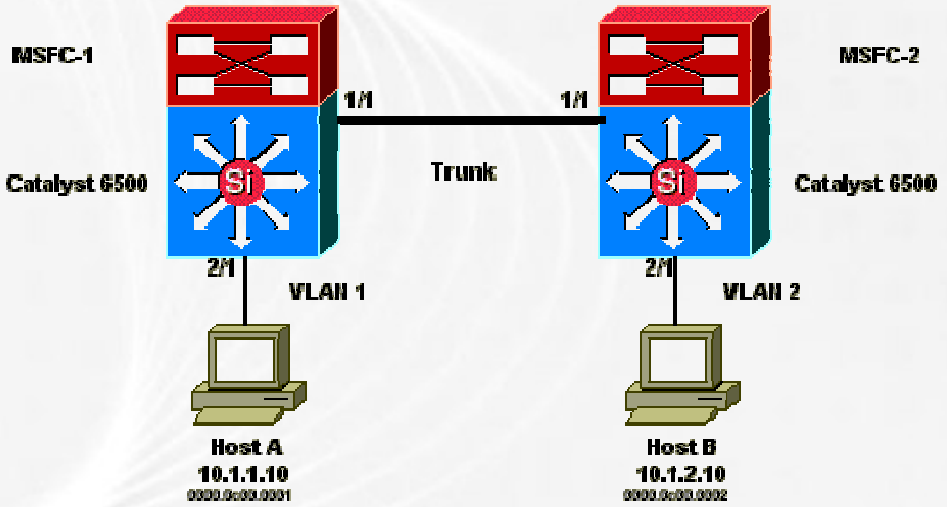
- VRRP-nek már van subsecond időzítője
  - szabványos
- HSRP/VRRP egy router-en megy át az összes flow
- GLBP esetén csak a flow-k felét érinti a hiba

Esettanulmány

- Aszimmetrikus routing HSRP esetén
  - Unicast Flood – Sniffer
  - Nincs MLS bejegyzés
  - Csomageldobás a kapcsolódó host-okon
- Időzítők
  - ARP = 1440s
  - CAM = 300s
- MSFC-k
  - MSFC-1 Active HSRP Vlan1-ben
    - Host A DefGW
  - MSFC-2 Active HSRP Vlan2-ben
    - Host B DefGW

- Switch-1-ből kiöregszik „B” MAC címe
- Switch-2-ből kiöregszik „A” MAC címe

```
mac-address-table aging-time 1440
```



Balla Attila, vezető technikai tanácsadó

SYNERGON

Köszönöm a figyelmüket!

SYNERGON GROUP

SPAN SAO infinity FibeX SYNERGON