Hálózatok építése és üzemeltetése

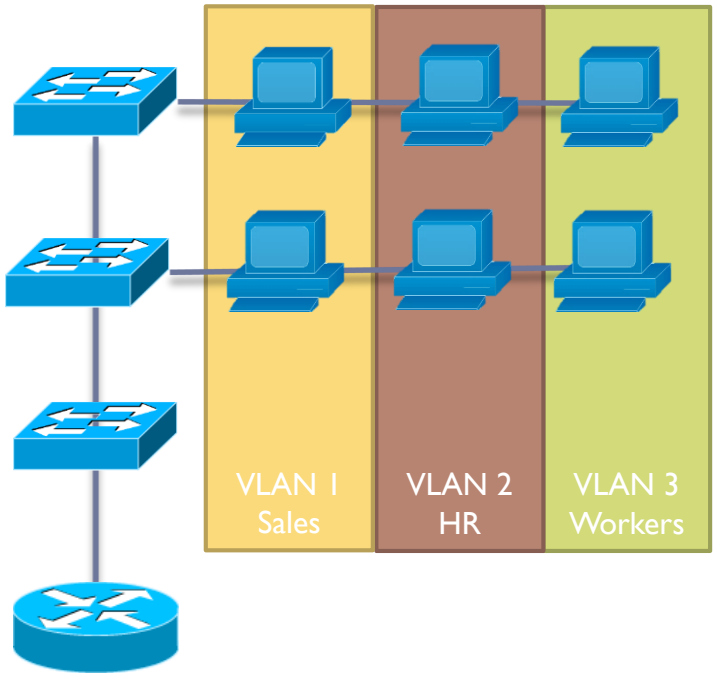
Hálózatbiztonság 2.

Hálózatok biztonságos darabolása és összekötése

Virtuális helyi hálózatok

Virtuális helyi hálózat - VLAN

- Nagy hálózatok szétdarabolása
  - Kisebb hálózat, jobb hálózati teljesítmény
  - Szétdarabolás kapcsolókkal (switch), a forgalomirányító (router) nem erre való
- Célok szerint a szétválasztjuk a helyi hálózatot
  - Menedzsment forgalom, felhasználói forgalom és vendég forgalom
  - VoIP forgalom és adatforgalom
- Virtuális hálózatok - VLAN



VLAN előnyök

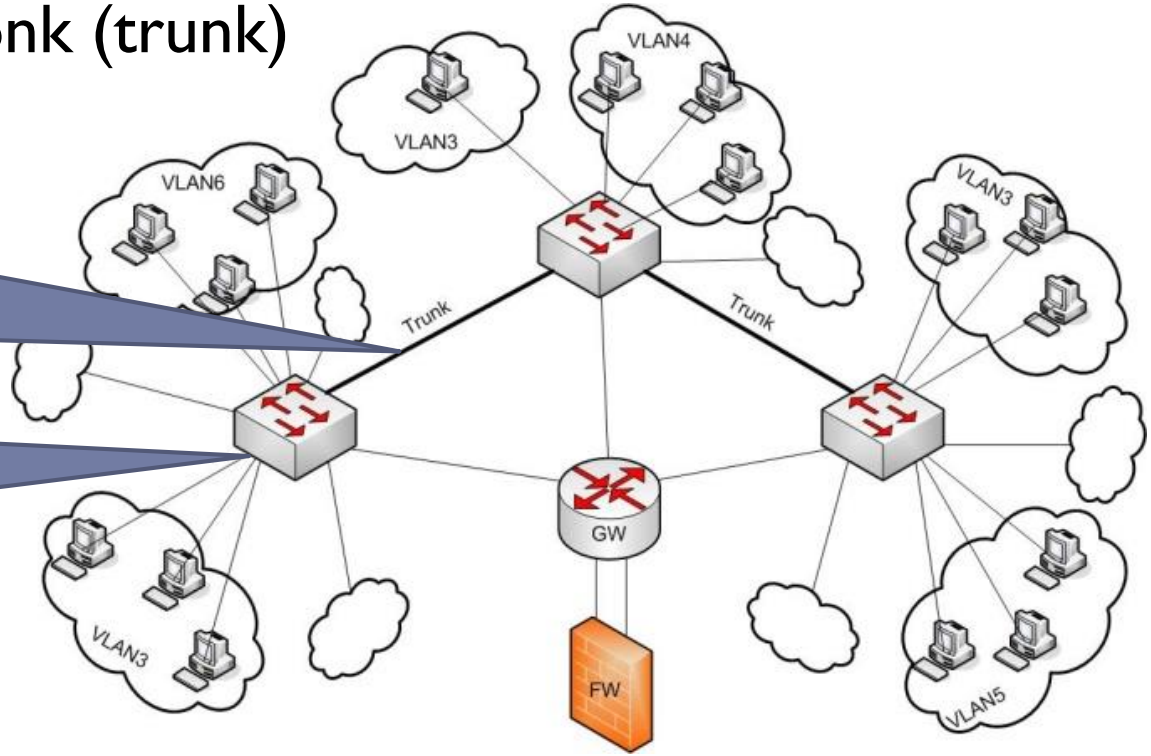
- Biztonság
  - A szenzitív adatok el vannak választva a többi adattól
- Költség
  - Olcsóbb eszközök, jobb kihasználtság
- Broadcast tartományok csökkenése
  - Hatékonyabb hállózat
- Egyszerűbb menedzsment
  - Felhasználók azonos felhasználói profillal
  - Egyszerűbb konfiguráció (VLAN nevek alapján)

VLAN technikai megvalósítás

- VLAN port és trönk (trunk)

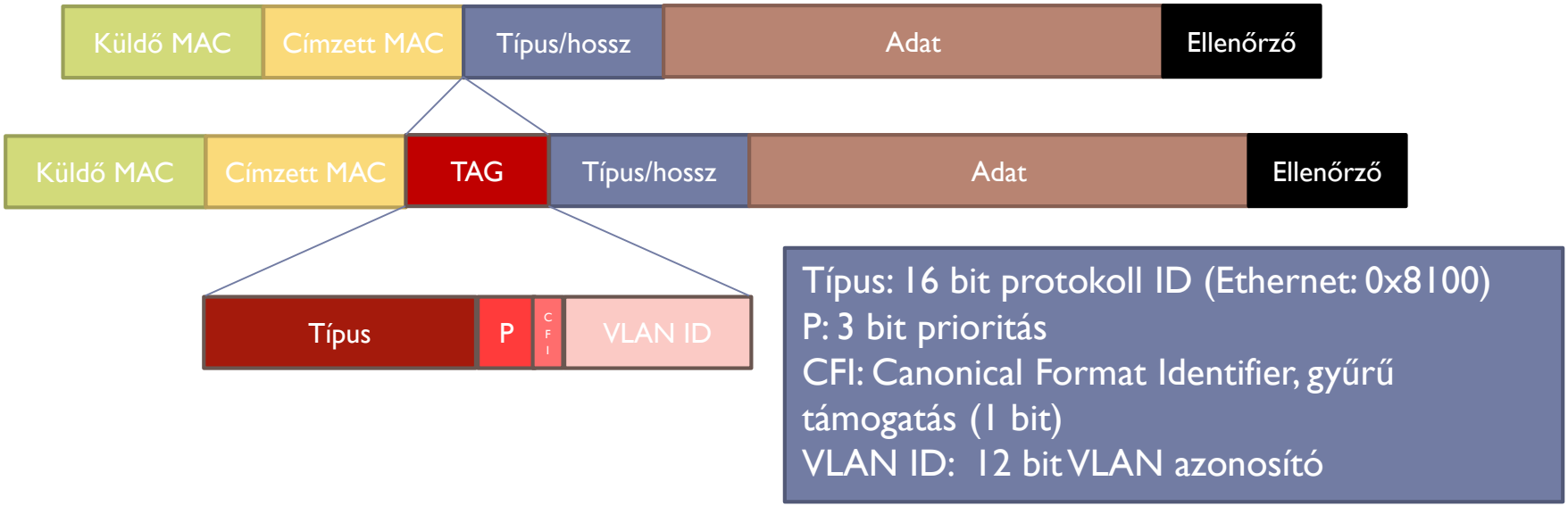
VLAN trönk: több VLAN forgalmának szállítása

VLAN port: Egyetlen VLAN hálózat adatai



VLAN technikai megvalósítás 2.

- IEEE 802.1Q - Bridged Networks (1998/2005/2011/2014)
- VLAN Tag



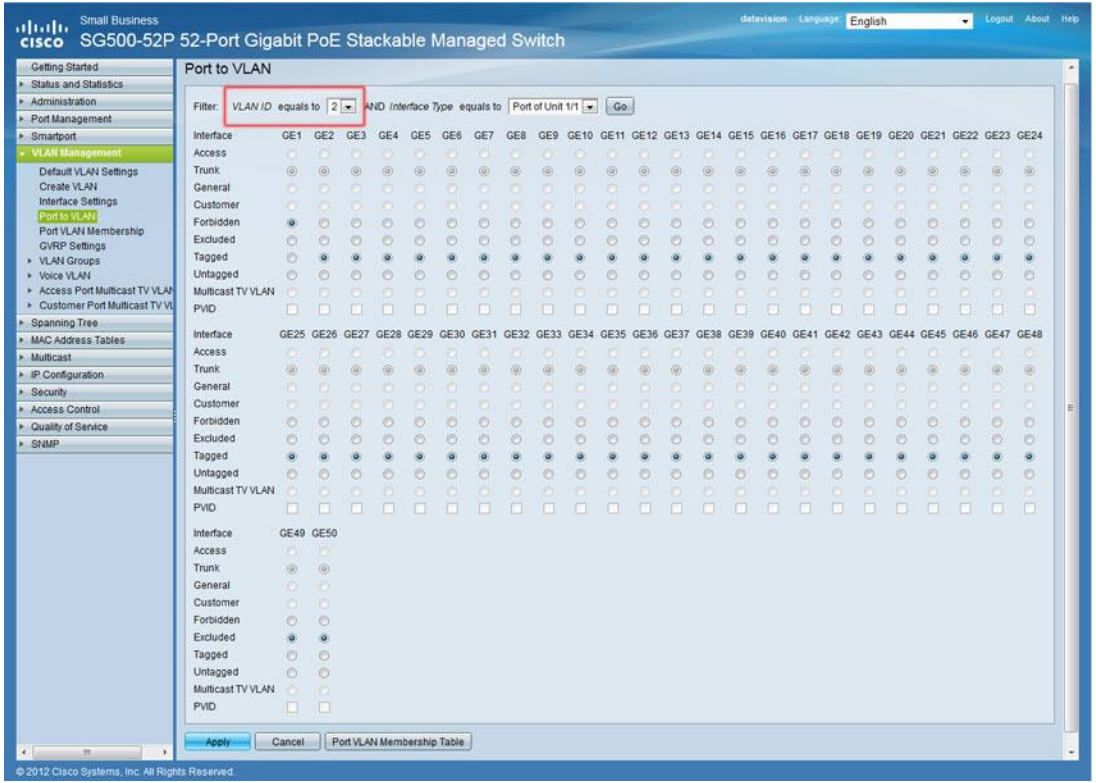
Típus: 16 bit protokoll ID (Ethernet: 0x8100)
P: 3 bit prioritás
CFI: Canonical Format Identifier, gyűrű támogatás (1 bit)
VLAN ID: 12 bit VLAN azonosító

VLAN technikai megvalósítás 3.

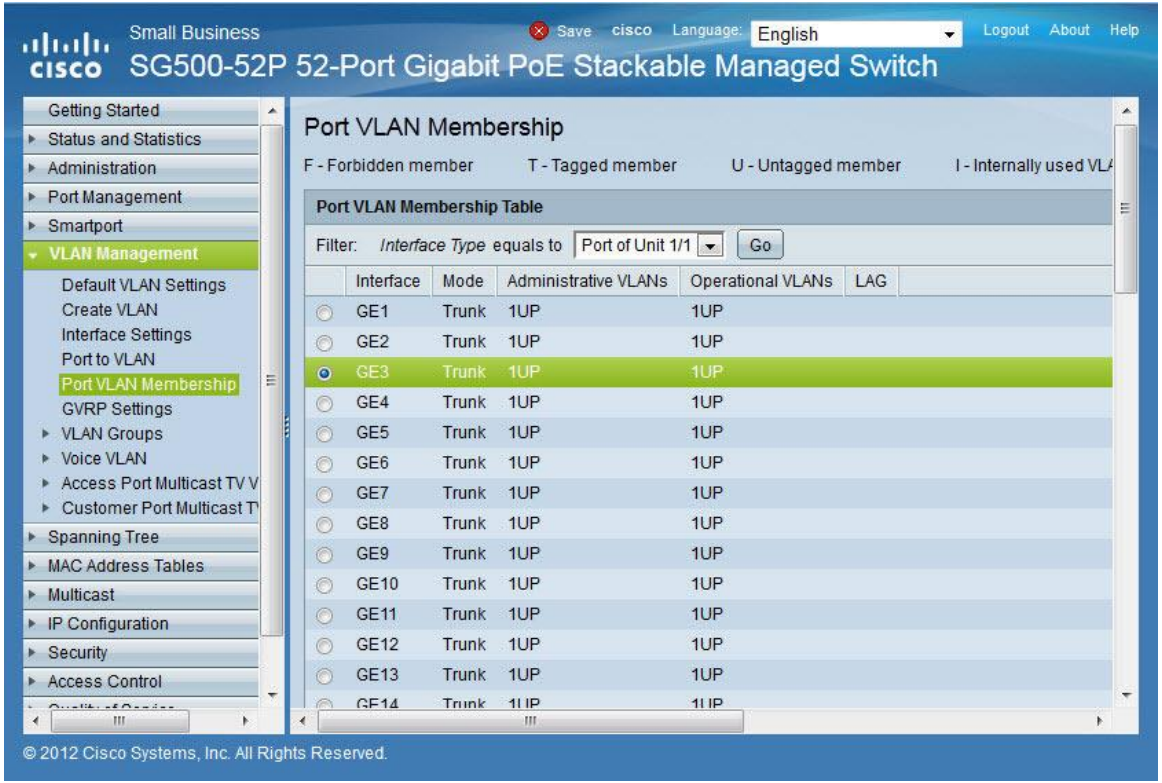
- Native VLAN
  - Az a VLAN hálózat, ami nincsen megjelölve a hálózatban
  - Minden trönk viszi a Native VLAN forgalmat is
  - Van hozzárendelt VLAN ID (Cisco: VLAN 1)

  - A Native VLAN porton nem szabad címkézett forgalmat küldeni
    - A Native VLAN-nak címkézett keret a Native VLAN porton eldobható
  - Minden címke nélküli forgalom a Native VLAN-ba tartozik

VLAN konfiguráció



VLAN konfiguráció 2.



DTP - Dynamic Trunking Protocol

- Cisco specifikus trönk kezelés két összekötött porton
  - Port beállítások
    - access, dynamic auto, dynamic desirable, trunk, nonegotiate
  - DTP letiltása: nonegotiate
  - Alap beállítások
    - Dynamic auto
    - Dynamic desirable
  - Végeredmény
    - Trunk vagy Access

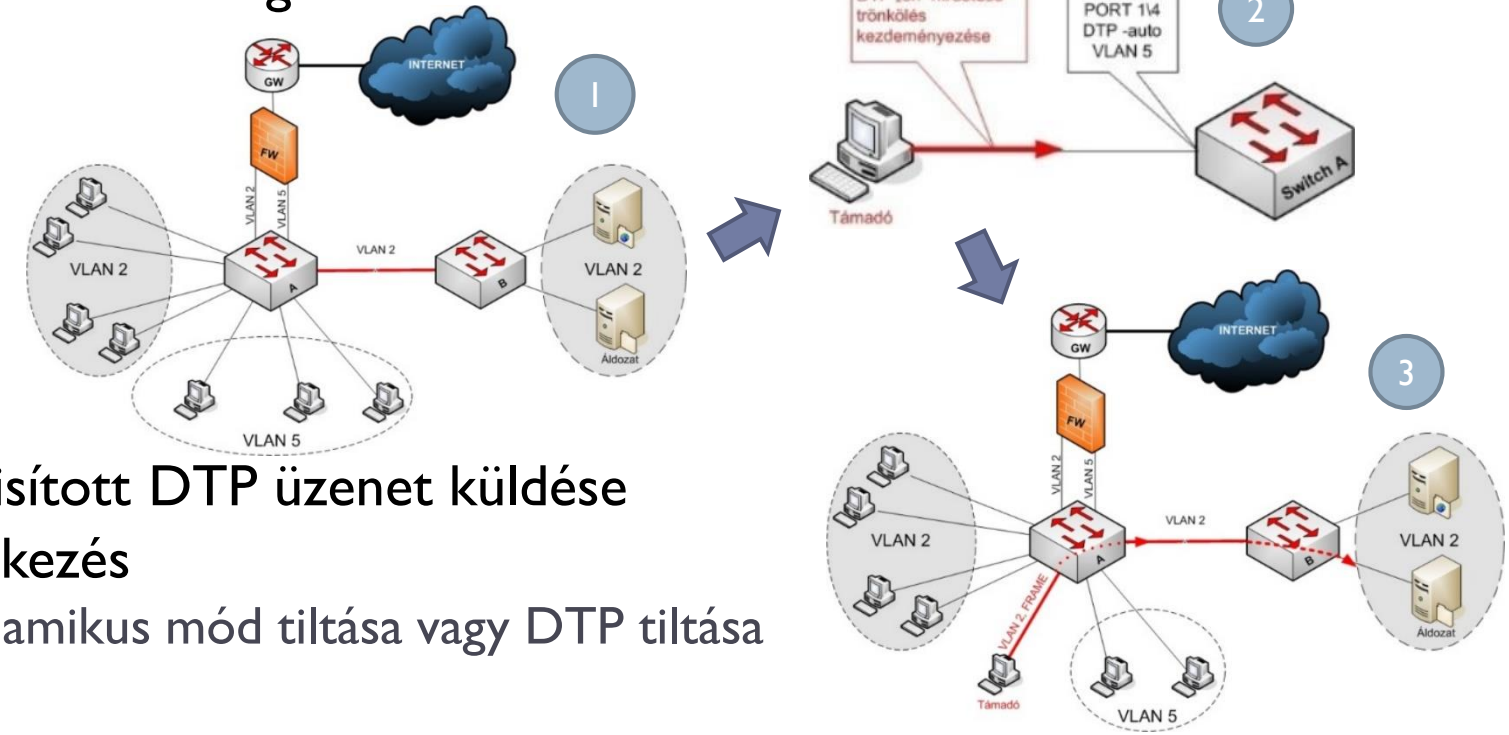
	Dynamic Auto	**Dynamic Desirable**	**Trunk**	**Access**
Dynamic Auto	Access	Trunk	Trunk	Access
Dynamic Desirable	Trunk	Trunk	Trunk	Access
Trunk	Trunk	Trunk	Trunk	Limited connectivity
Access	Access	Access	Limited connectivity	Access

VLAN biztonság

- VLAN hopping
  - Más VLAN forgalmának elérése (Switch spoofing)
  - A forgalom áthelyezése másik VLAN hálózatba

VLAN hopping 1.

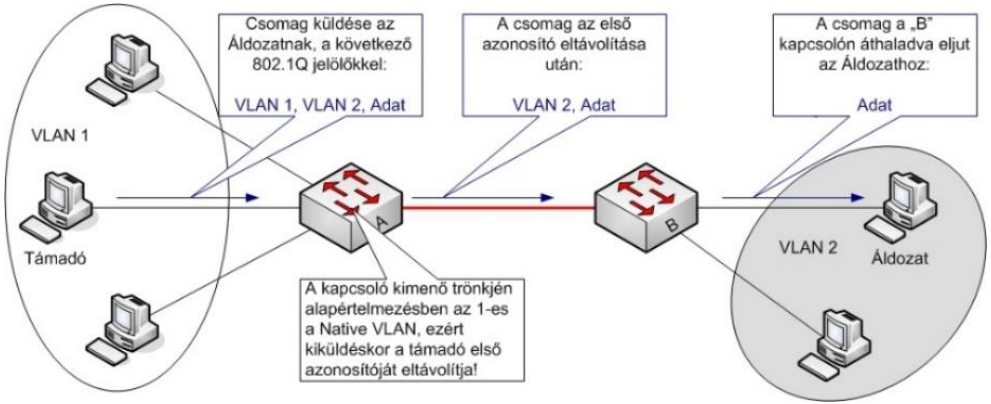
- Más VLAN lehallgatása



- Hamisított DTP üzenet küldése
- Védekezés
  - dinamikus mód tiltása vagy DTP tiltása

VLAN hopping 2.

- Double-Encapsulated 802.1Q
  - Native VLAN támogatás a (802.3) kompatibilitás miatt
- Támadó a Native VLAN tartományban
- Speciális (dupla) címke készítése
- Csak forgalom beszúrás
- Védekezés
  - A Native VLAN-t nem használjuk



Feszítőfák

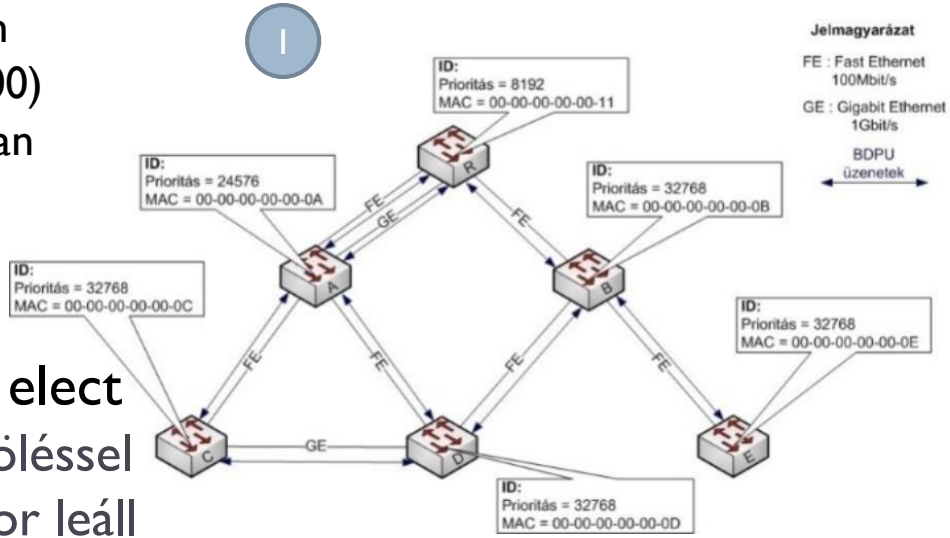
Feszítőfa - Spanning tree

- Feszítőfa készítése: IEEE 802.1D protokoll
  - Gyökér megválasztása
  - Gyökér portok megválasztása
    - sw -> root minimális költséggel
  - *Designated* port megválasztása
    - root -> lan minimális költséggel
  - Más portok letiltása

- CST (Common ST) és PVST (Per VLAN ST)

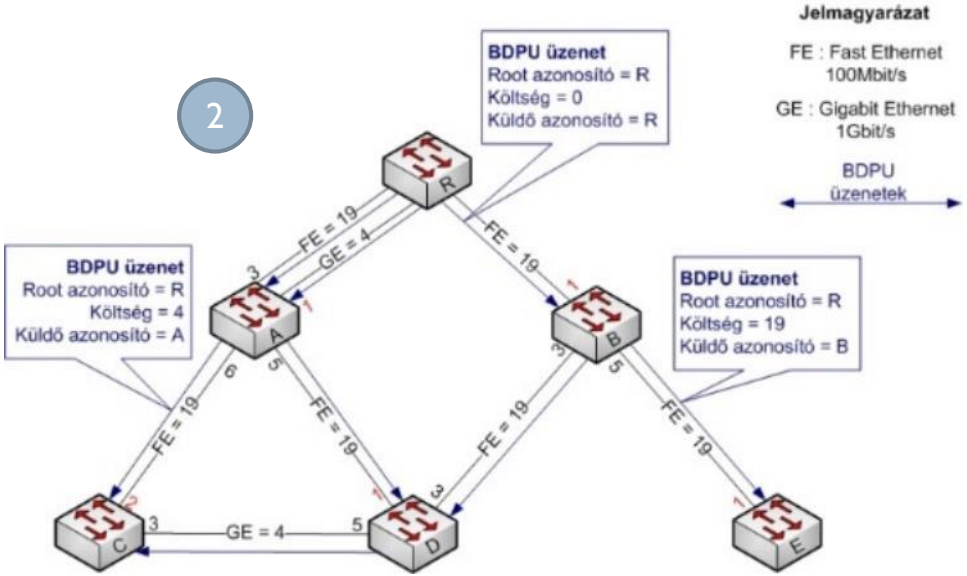
Feszítőfa készítés 1.

- BPDU – Bridge Protocol Data Unit
  - Hurkos felderítése
    - Küldés minden 2. másodpercben
    - Multicast cím (01-80-c2-00-00-00)
    - Ha visszaérkezik, akkor hurok van
  - Egyben prioritás is a feszítőfa kialakításához
- Gyökér megválasztása – root elect
  - Üzenetküldés saját gyökér jelöléssel
  - Ha nagyobb prioritás van, akkor leáll a küldés



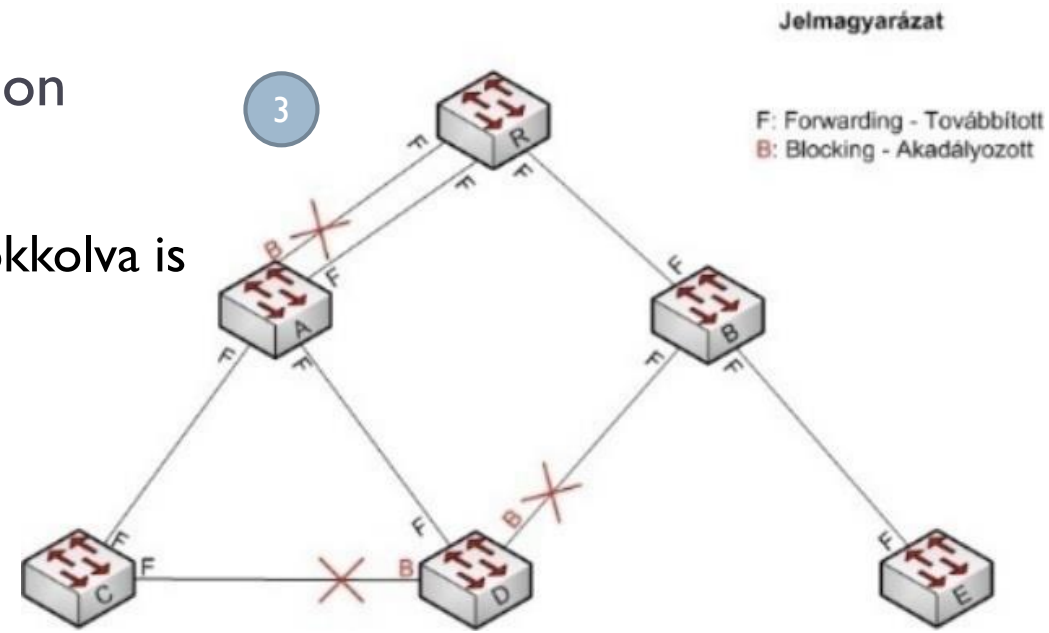
Feszítőfa készítés 2.

- Gyökér (root bridge)
  - Legkisebb ID
- Gyökér port (root port)
  - Minden kapcsolón egyetlen
  - A legrövidebb út a gyökérig
- Kijelölt továbbító (designated) portok megválasztása
  - BPDU küldése a gyökértől
  - Ismételt BPDU érkezés esetén a nagyobb költséget le kell tiltani



Feszítőfa készítés 3.

- Kijelölt port
  - Továbbítja a forgalmat
  - Kijelölés prioritás alapon
  - Minden linknek van
    - A másik oldal lehet blokkolva is



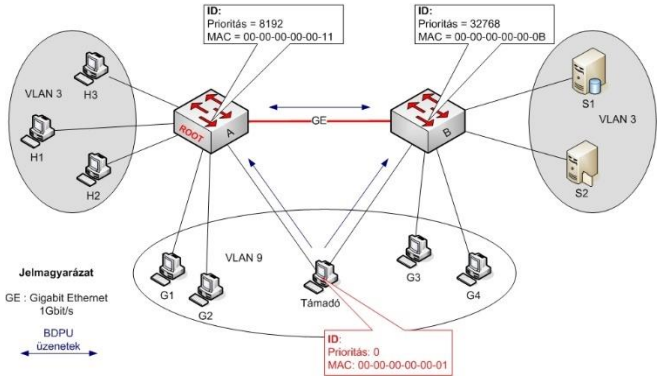
STP támadások

- Meghamisított gyökér (root bridge)
  - Forgalom elterelése
- BPDU forgalommal elárasztás
  - Ismételt gyökér választások
    - STP kiiktatása
  - Hálózat elárasztása a hurkok miatt

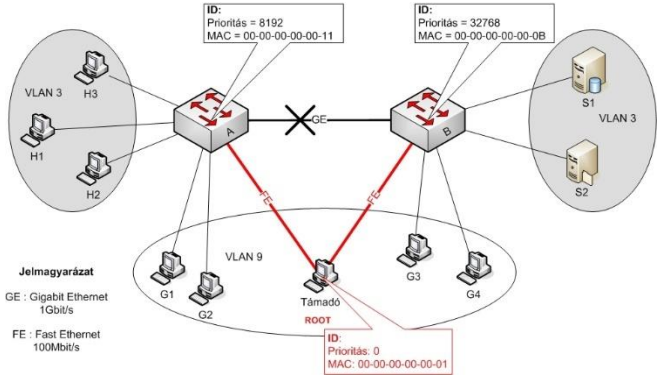
STP dual-homed root

- Hamis BPDU üzenetek új gyökér választáshoz
  - Forgalom elterelése
- Védekezés
  - BPDU guard
    - BPDU forgalom letiltása az adott porton
  - Root guard
    - Lehetetlen gyökérnek lenni egy adott porton

1

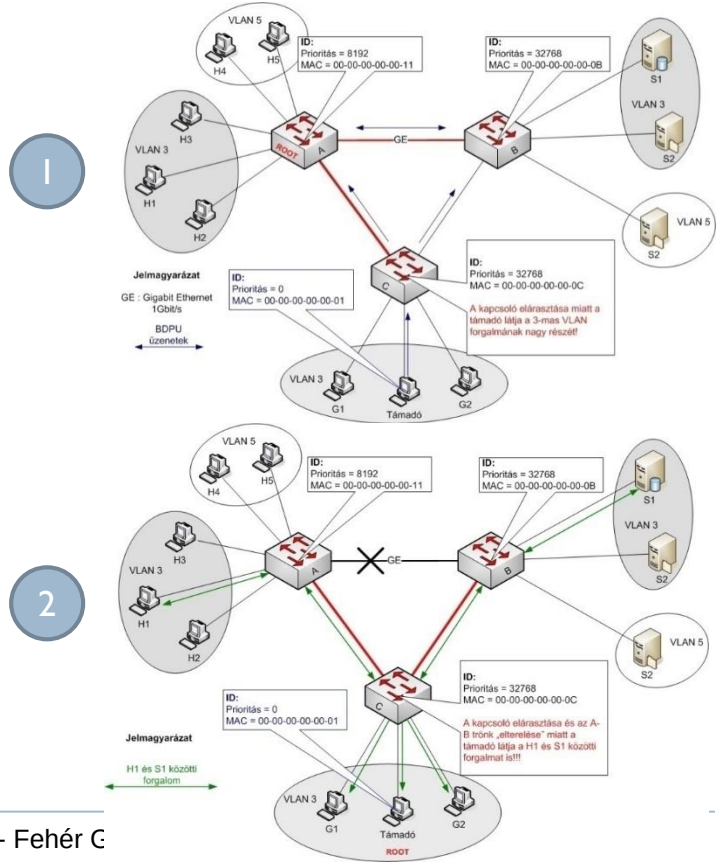


2



STP single-homed root

- Hamis BPDU üzenetek
  - Forgalom elterelése
- Védekezés:
  - BPDU guard
  - Root guard



STP forgalom elárasztás

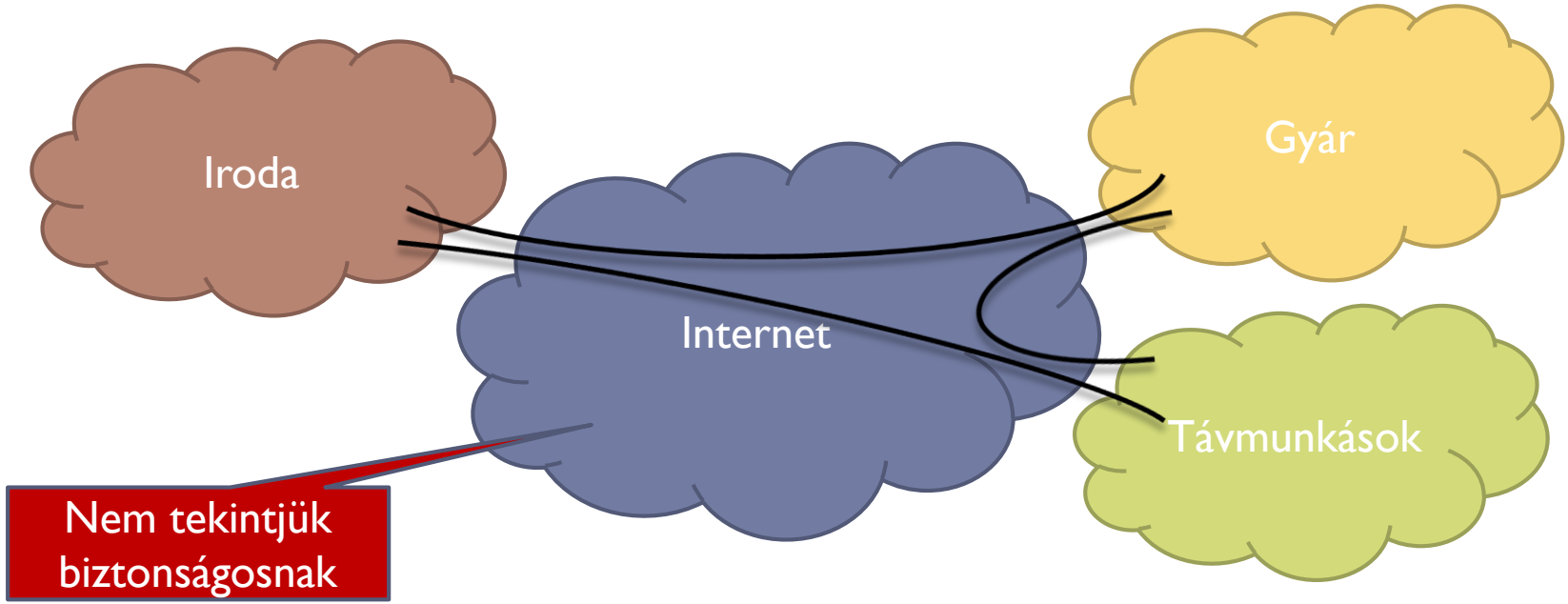
- BPDU üzenet új gyökér választáshoz
  - Legmagasabb prioritás (legkisebb ID)
  - A választás időszakában csend, majd ismételt választás
  - STP feszítőfa nem jön létre

- BPDU üzenettel elárasztás
  - 10000 üzenet másofpercenként
  - Elviselhetetlen terhelés a kapcsolókon
  - STP feszítőfa nem használható

Alagutak

Hálózatok összekapcsolása - tunneling

- Virtuális magánhálózatok / Virtual Private Network (VPN)



Magánhálózat kialakítás

- Hálózat fizikai elkülönítése
  - Elkülönítésre alkalmas hálózati technológia alkalmazása
    - Bérelt vonal
    - Optikai kábel esetén különböző hullámhossz
- Adatcsomagok elkülönített irányítása
  - IP hálózatokban, adott szolgáltatón belül
    - Multiprotocol Label Switching – MPLS
      - A forgalom meg van címkézve, amint beér a hálózatba
      - A címkék rögzített útvonalon közlekednek
      - Opcionálisan erőforrás-foglalás is (Minőségi garancia)
- Elkülönítés titkosítással
  - IP szintű titkosítás
  - Adatkapcsolat szintű alagutak

Virtuális!

Gyakorlatban a legnagyobb biztonság

Elkülönítés titkosítással

- A magánhálózat adata a többi forgalommal együtt halad
- A titkosítás biztosítja, hogy illetéktelen személy nem férhet hozzá
  - Nem tudhatja meg tartalmát
  - Nem módosíthatja
  - Nem hozhat létre új (valós) csomagokat
  - De törölheti (rombolás)
- Nincsen prioritásos kezelés, nincs minőségi garancia
  - Best effort Internet
  - Más protokollokkal kiegészíthető
- Független a hordozó hálózat biztonságától

IPSec

- IPSec
  - Szabványos protokoll az Internetes adatforgalom biztonságára

- IPSec tulajdonságai
  - Hozzáférés védelem
    - Mások nem láthatják az adatforgalmat
  - Integritásvédelem
    - Az adatforgalmat nem lehet megváltoztatni
  - Hitelesítés
    - Bizonyosság, hogy valóban a küldő fél küldte az adatokat
    - A kapcsolatban lévő felek ismerik egymást
  - Védelem a visszajátszások ellen
    - Az adatforgalmat nem lehet ugyanazokkal az IP csomagokkal megismételni később

Security Association

- SA – Security Association
  - Logikai kapcsolat két kommunikáló pont között
  - Leírja a kapcsolat biztonsági szolgáltatásait
    - Üzemmód
    - Algoritmusok
    - Kulcsok
  - Egy SA: egyetlen kapcsolat
    - Duplex esetben két SA szükséges
    - Kombinált üzemmódok esetén szintén több SA

SAD – SA adatbázis

- Az aktív SA-k tárolása
  - Külső IP cím, protokoll, Paraméter index (SPI)
  - Paraméterek
    - Hitelesítési algoritmus és kulcs, Titkosító algoritmus és kulcs, élettartam, protokoll üzemmód, visszajátszás elleni sorszámok, biztonsági házirend hivatkozás

SPD – Biztonsági házirend adatbázis

- Minden egyes csomagra megvizsgálj a házirendet (szabályok)
- Csomag és házirend azonosítása
  - Cél IP cím, forrás IP cím, név (falhasználó vagy rendszernév), transzport protokoll, forrás és cél portok.

- Házirend
  - Csomag eldobás, átengedés, IPSec alkalmazás
  - IPSec esetén
    - Biztonsági protokoll és üzemmód
    - Engedélyezett műveletek (visszajátszás ellen, hitelesítés, titkosítás)
    - Algoritmusok
  - Hivatkozás az SAD-re

IPSec és kulcsok

- Az IPSec protokollok működéséhez szükséges a megfelelő kulcsok ismerete a végpontokon
  - Manuális kulcselosztás
    - Félrekonfigurálási hibák, tipikusan gyenge kulcsok, nem jól skálázható
  - Automatikus kulcsmenedzsment
    - Erős kulcsok, dinamikusan új kulcsok, nincs emberi hiba, skálázható

- Internet Key Exchange (IKE)
  - Működés
    - Titkos csatorna kialakítása
    - Végpontok hitelesítése
      - Jelszó, aláírás (RSA, DSA), tanúsítvány
    - Paraméteregyeztetés
  - Kulcscsere
    - Diffie-Hellman kulcscsere
    - Kerberos (Windows)

IPSec protokollok

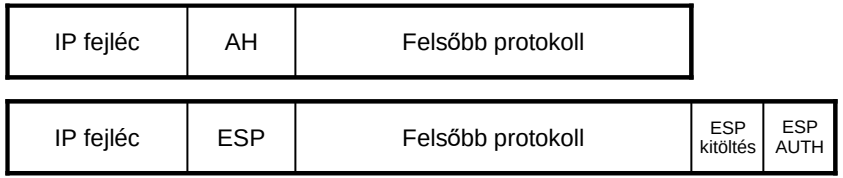
- Hitelesítés – Authentication Header (AH)
  - Az adat (IP fejléc és magasabb rétegek) eredetének hitelesítése
    - Hash függvény segítségével a továbbítás közben nem változó mezők tartalma
  - Integritás védelem
  - Védelem a visszajátszás ellen
  - Nincs titkosítás

- Titkosítás – Encapsulating Security Payload (ESP)
  - Az adatok titkossága
  - Plusz hitelesítés és integritásvédelem
    - De csak ESP adatok + tartalom,
      IP fejléc nem hitelesített
  - Visszajátszás elleni védelem

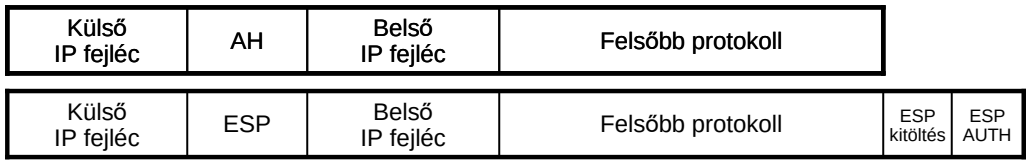
- Titkosítás és hitelesítés AH + ESP
  - Titkosított tartalom és a hitelesítés kiterjed az IP fejlécekre is

IPSec üzemmódok

- Szállítási (Transport) üzemmód
  - Védelem az IP feletti protokolloknak



- Alagút (Tunnel) üzemmód
  - Az egész IP csomag védelme



VPN típusok

- Remote access VPN (Road Warrior)
  - Cél a mobil felhasználóknak távoli elérés nyújtása
- Intranet VPN
  - Telephelyek összekötése
- Extranet VPN
  - Üzleti partner bekapcsolása

Adatkapcsolati szintű titkosítás

- IPSec:
  - IP protokoll feletti protokollok biztonságos átvitele
  - Tűzfal és NAT gondot jelenthet a kommunikációban
    - Bele kell látni a csomagokba
    - Nem változhat az IP fejléc
  - Implementációk
    - Linux (Freeswan, openswan), Windows (mmc snapin), Átjárók
- Sokszor kell, hogy ne csak IP feletti protokollok legyenek
  - Pl.: Telephelyek összekötése egyetlen (L2) Ethernet hálózatba
  - Alagút kiépítése az IP hálózatban. Az alagútban IP csomagba ágyazott Ethernet keretek
    - PPTP és OpenVPN