BMEVIHIMA00 Hálózati technológiák integrációja

Hálózati szolgáltatások folytonossága

Hálózati szolgáltatások hibatűrése és rendelkezésreállása

Jakab Tivadar

jakab@hit.bme.hu

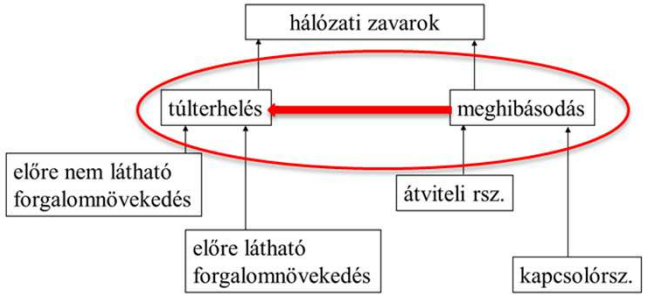
Budapest,
2021.04.21.

TARTALOM

- Szolgáltatások minősége
- Motivációk
- Védelmi alapsémák
- Többrétegű védelem
- Mire, hogyan használjuk?
- Modellezés, számítás

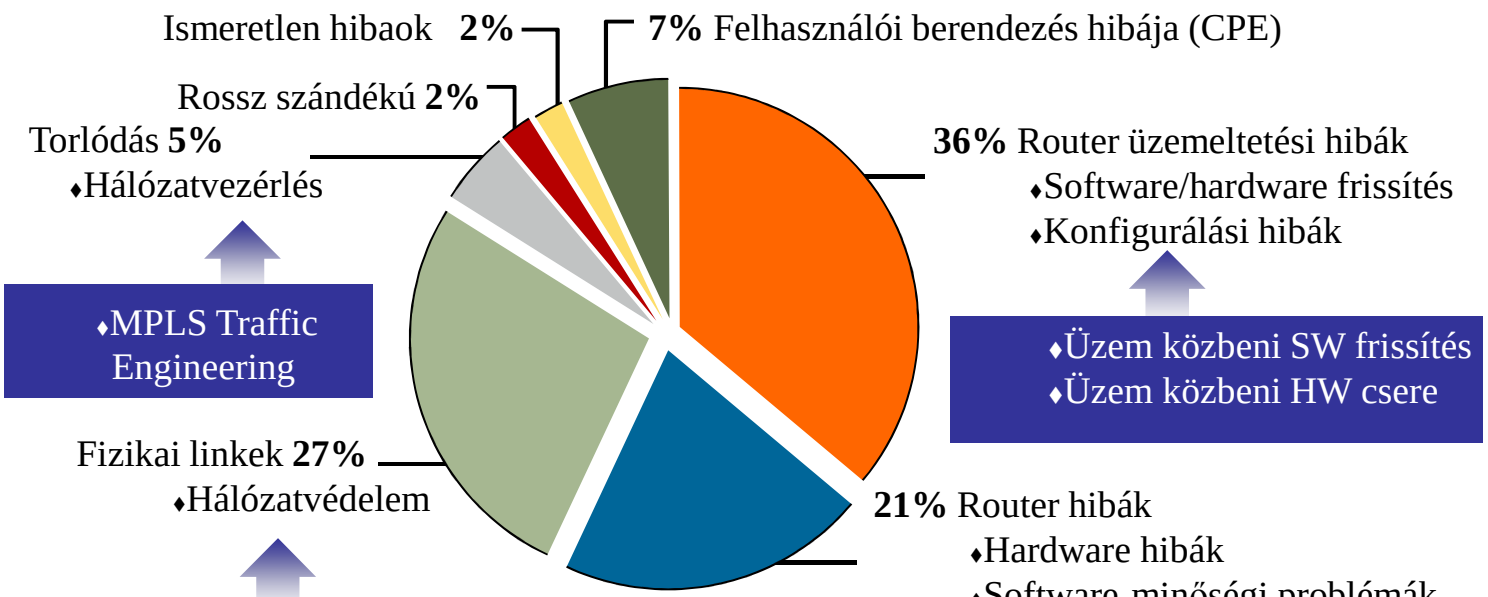
HÁLÓZATI SZOLGÁLTATÁSOK FOLYTONOSSÁGA: ÁTTEKINTŐ KÉP 2/1

- Szolgáltatás, követelmények (SLA)
  - Adott időpillanatban megállapítható, hogy teljesül-e (igen/nem – kétállapotú!)
  - Hogyan állapítható meg ? – Szolgáltatástól (technológiától) függő – az üzemeltetéstámogatás funkciói alapján (monitorozás, mérések, stb. -> hálózatmenedzsment)
  - Példák: IP, connectivity, ping (de …!), WDM, optikai csatorna, vevő oldali jelszint (de …!)
- Miért nem teljesül?
  - Forgalmi túlterhelés/*erőforráshiba* -> nincs elegendő erőforrás (az aktuálisan kiszolgálandó forgalomhoz képest)
- Mi hibásodhat meg? (Murphy ☺, ☹)
- Mire van szükség a szolgáltatás fenntartásához, hibáik?
  - HW (aktív, passzív), SW, tápáram-ellátás, …
  - Példák: aktív hálózati eszközök (pl. elektronikus komponensek öregedése), aktív eszközökön futó szoftverkomponensek (pl. memóriaszivárgás), passzív hálózatelemek (pl. kábel véletlen átvágása), áramkimaradás
  - Egy nagykiterjedésű nyilvános szolgáltatói hálózatban vajon mi a domináns (legtöbb gondot okozó)?
- Hogyan jellemezhetők a meghibásodások?
  - Véletlen folyamat (de …! rosszindulatú támadó – más eset, sebezhetőség)
  - Statisztikus eloszlások: exponenciális (de …! kopó alkatrészek Weibull), időparaméterek
  - Várható értékek: állapotváltozásig eltelt idő (pl. nem javított rendszer MTTF), állapotban eltöltött idő (pl. javított rendszer MUT, MDT)
  - Rendelkezésreállás



- Szolgáltatói minőségű eszközök (alacsony meghibásodási valószínűség, de sok eszköz)
- Hibafelügyelet (szolgáltatói minőségű hálózatban felügyelet – a felügyeleti rendszer többnyire a felhasználói panaszok megjelenése előtt érzékeli a hibát)
- Javított rendszer (gyors hibadetektálás, egyszerű javítás – elemcsere)
- Automatikus és manuális beavatkozások a hibahatás gyors ellensúlyozására, kiküszöbölésére (automatikus, vagy manuálisan konfigurált módosítása)
- Redundanciák szükségesek (hw felépítése, hálózat topológiája, erőforrásai)
  - kritikus hw elemek duplikálása (pl. vezérlő, hűtés, táp)
  - többszörös összefüggőségű hálózati topológia
  - függetlenül meghibásodó összeköttetések, utak

HIBAOKOK MEGOSZLÁSA AZ IP HÁLÓZATBAN



Forrás: University of Michigan
(Régi statisztika, csak illusztráció)

HÁLÓZATI SZOLGÁLTATÁSOK FOLYTONOSSÁGA: ÁTTEKINTŐ KÉP 2/2

- Jó minőségű eszközök (alacsony meghibásodási valószínűség, de sok eszköz) Hogyan növelhető a folytonossági jellemző?
- Redundanciamentes rendszer
  - Minden hiba katasztrofális – szolgáltatáskiesést eredményez
- Redundáns rendszer
  - Legyen beépítve a meghibásodott erőforrást pótolni képes tartalék (+ gyors átkapcsolás)
  - Hány tartalék? (Logaritmikusan növeli a folytonossági jellemzőt)
- Javított rendszer (gyors hibadetektálás, egyszerű javítás – elemcsere)
  - Szolgáltatáskiesés a javítás idejére
- Kombináljuk a kettőt
  - Legyen beépítve a meghibásodott erőforrást pótolni képes tartalék (+ gyors átkapcsolás)
  - Kritikus HW komponensek duplikálása (pl. vezérlő, hűtés, táp)
  - Az erőforrás redundancia mellett strukturális redunadancia is szükséges lehet (pl. hálózat – többszörösen összefüggő topológia)
  - Hibafelügyelet (szolgáltatói minőségű hálózatban felügyelet – a felügyeleti rendszer többnyire a felhasználói panaszok megjelenése előtt érzékeli a hibát)
  - Javítsuk a meghibásodott elemet

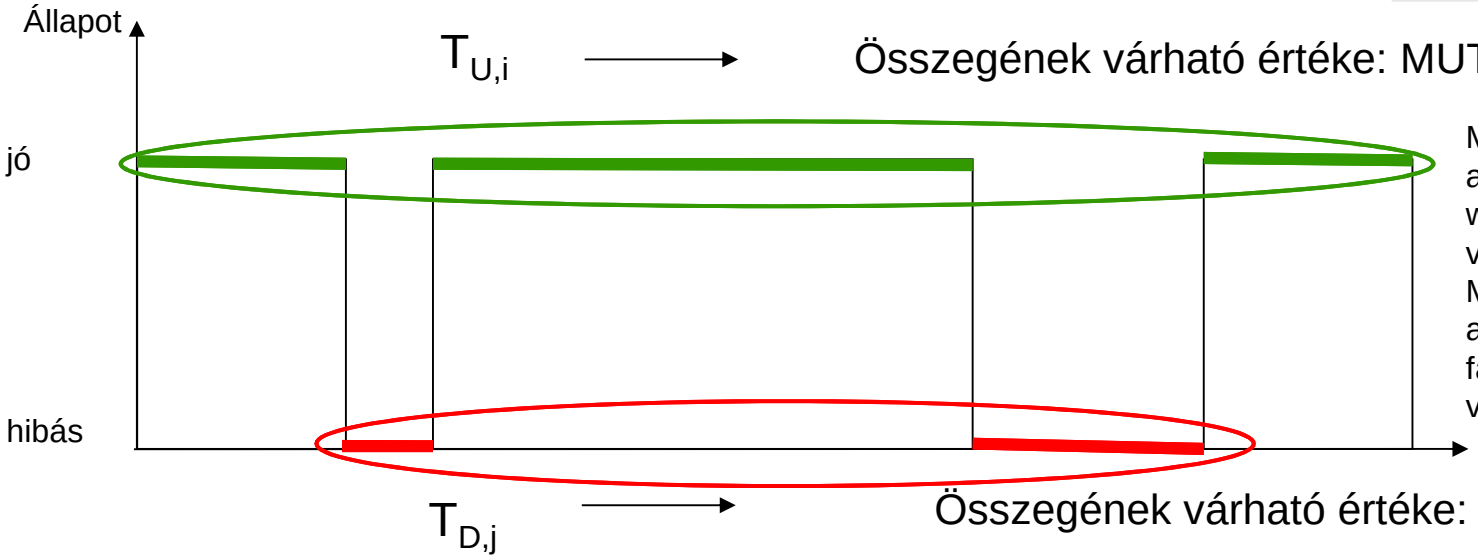
Hálózat, hálózati szolgáltatások

- Szolgáltatói minőségű eszközök (alacsony meghibásodási valószínűség, de sok eszköz)
- Hibafelügyelet (szolgáltatói minőségű hálózatban felügyelet – a felügyeleti rendszer többnyire a felhasználói panaszok megjelenése előtt érzékeli a hibát)
- Javított rendszer (gyors hibadetektálás, egyszerű javítás – komponens cseréje)
- Automatikus és manuális beavatkozások a hibahatás gyors ellensúlyozására, kiküszöbölésére (automatikus, vagy manuális változtatások)
- Redundanciák szükségesek (hw felépítése, hálózat topológiája, erőforrásai)
  - kritikus hw elemek duplikálása (pl. vezérlő, hűtés, táp)
  - többszörös összefüggőségű hálózati topológia
  - függetlenül meghibásodó összeköttetések, utak

ÉLETCIKLUS, RENDELKEZÉSREÁLLÁS

- Modellezési feltételezések
  - Kétállapotú komponensek
  - Javított rendszer
  - Független meghibásodások, javítások

A [%]	kiesés [óra]	Kiesés [perc]
99%	87,6	
99,9%	8,76	
99,99%	0,876	52,56
99,999%	0,0876	5,256



MUT – Mean Up Time: accumulated time spent in working state (expected value)
MDT – Mean Down Time: accumulated time spent in failore state (expected value)

$$A = MUT/(MUT+MDT) = 1-DTR$$

A – Availability, DTR – Down Time Ratio,

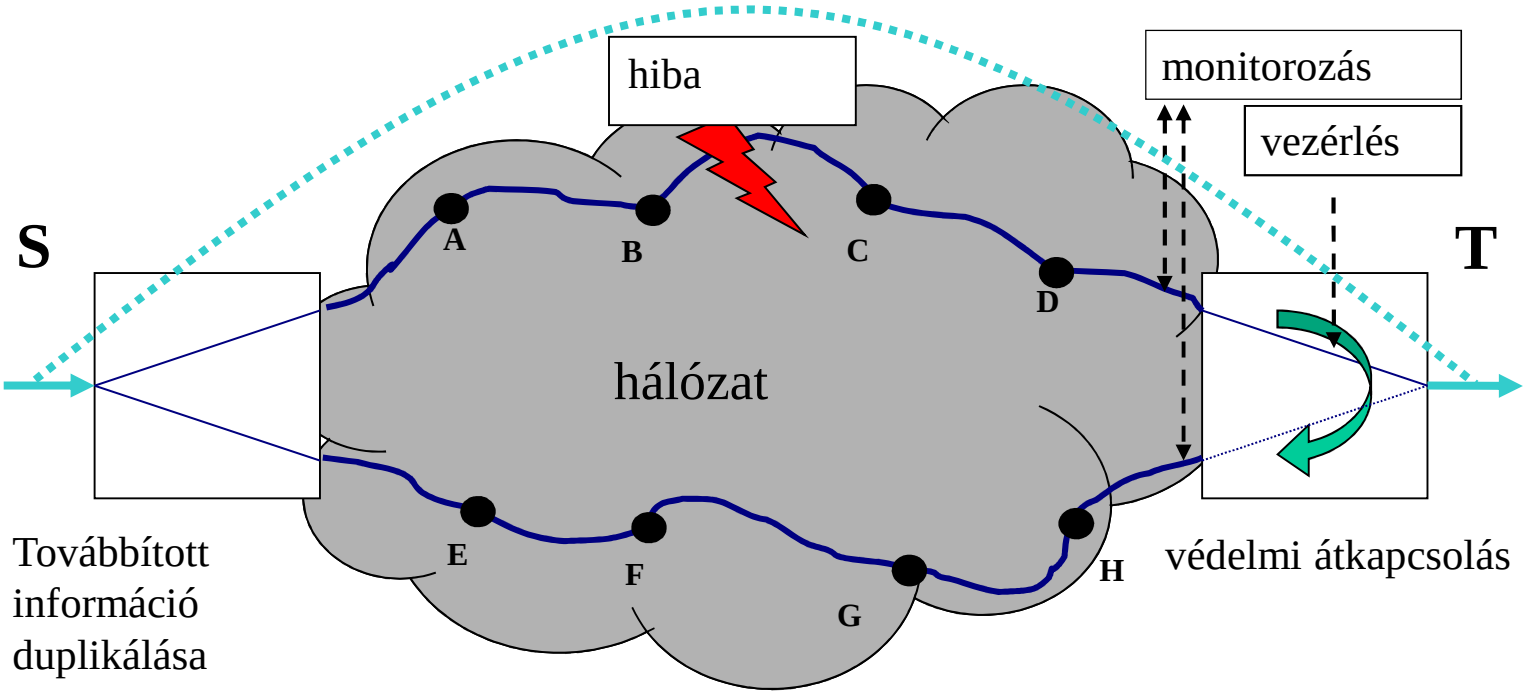
Időarányok (de …! Markovi modell, ergodikus folyamat, időarány – állapotban tartózkodás valószínűsége)

A [%] e.g. 99,99%, ,

HÁLÓZATVÉDELEM

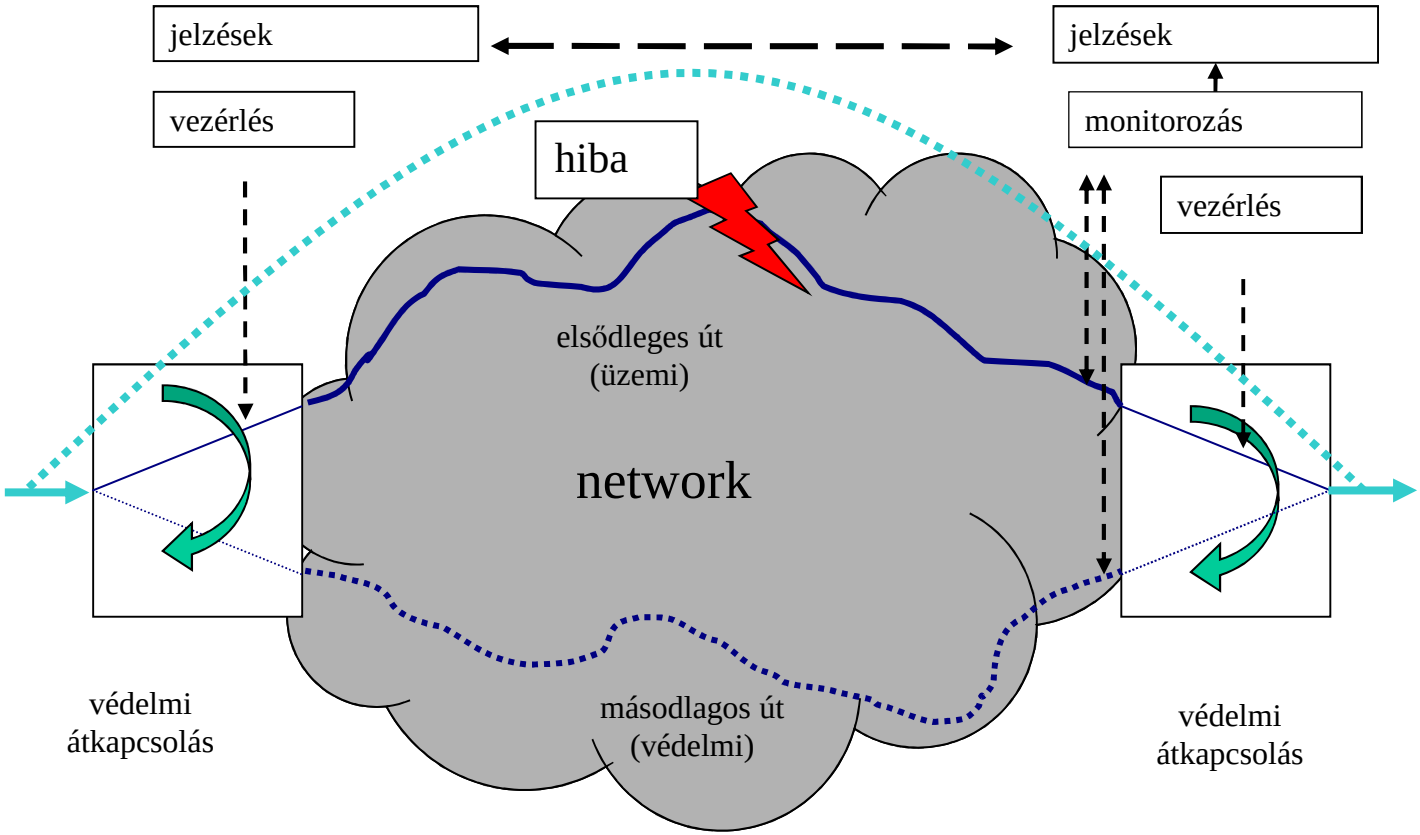
- Hibák hatása elleni védelem, hibatűrés, rugalmasság (resilience) növelése
- Szolgáltatások rendelkezésreállását javító általános megoldási sémák
- Pont-pont relációban (szolgáltatás,vagy – rétegelt szemléletben egy kliens link)
- Tipikusan egy időben egy hibát feltételezve (gyakorlatias megfontolás: megoldás költéshatékonysága, komplexitása, üzemetetési tapasztalatok)

1+1 VÉDELMI SÉMA

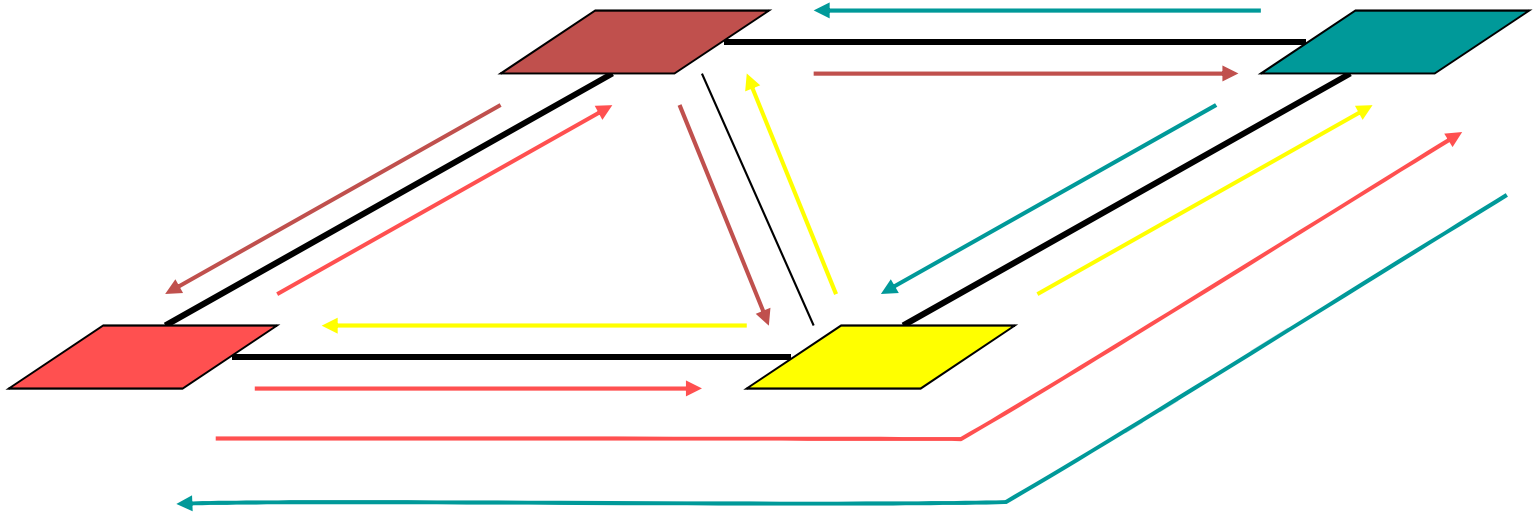


Példa: tipikusan „áramkörkapcsolt” jellegű esetekben – DF vagy WDM optikai csatorna (csomag alapú platformon konfliktusba kerülhet a megbízható transzporttal)

1:1 VÉDELMI SÉMA

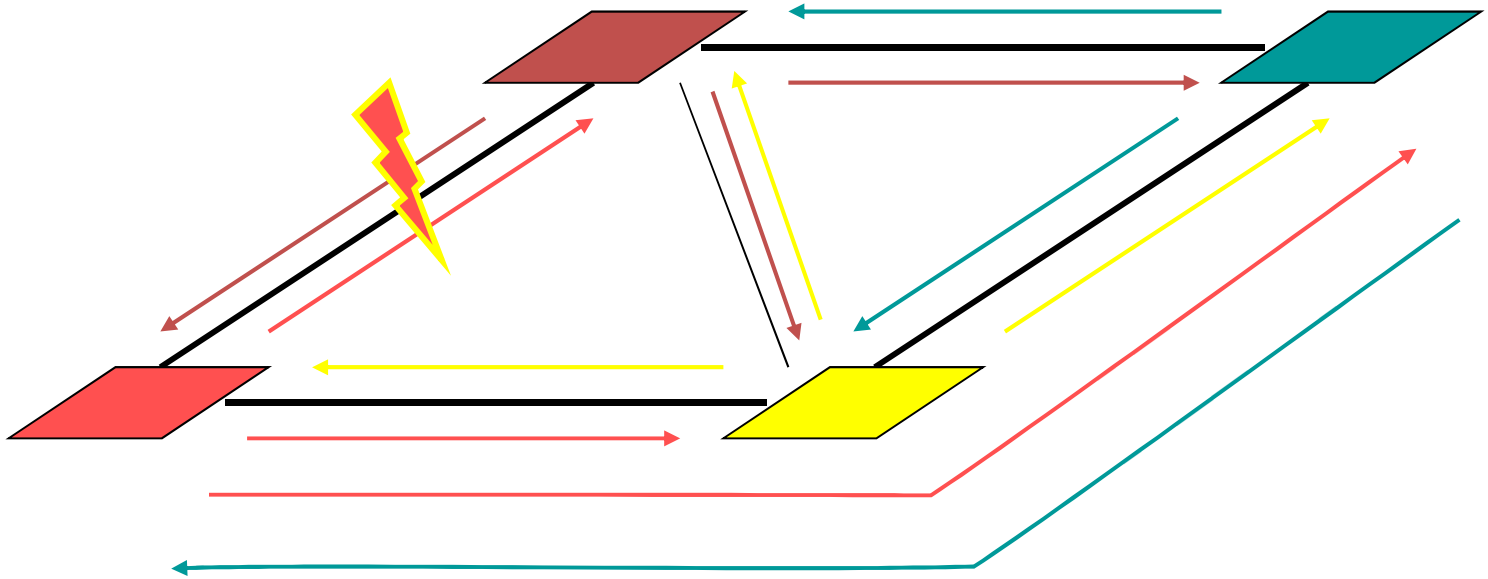


ADATPTÁCIÓS SÉMA 1/3



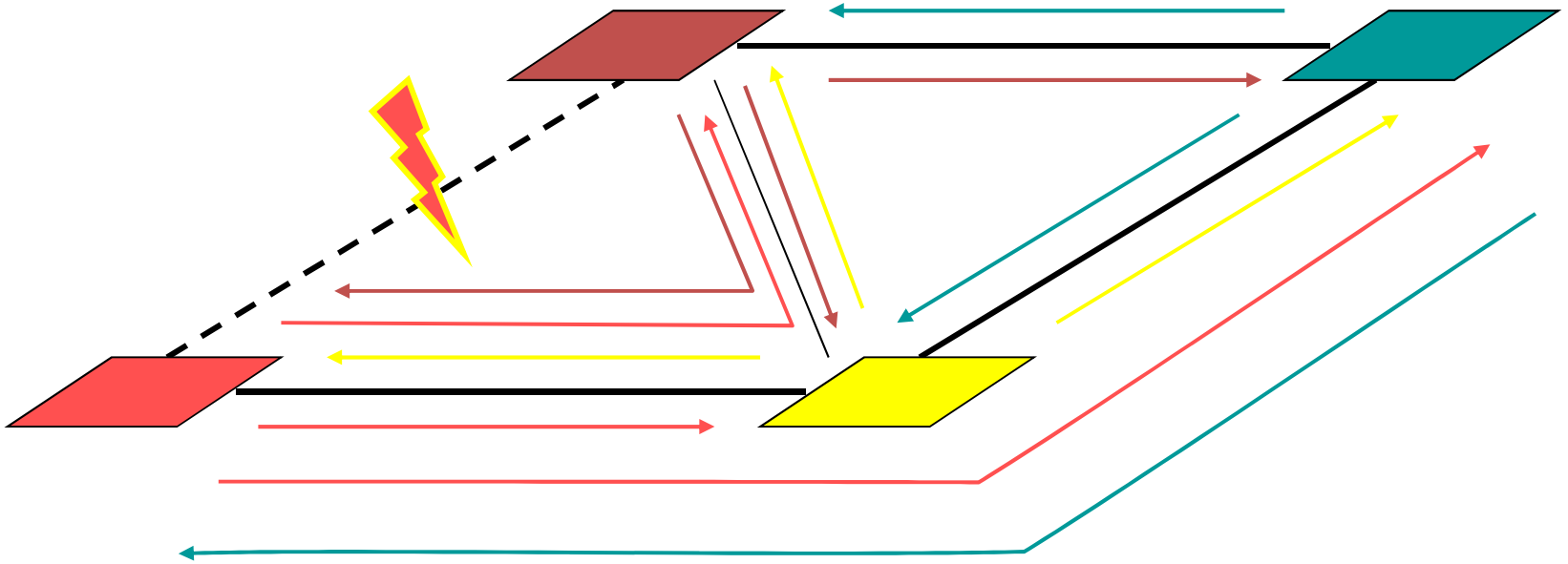
- Központi vagy elosztott (pl. linkállapot alapú IGP: OSPF) vezérlés alapján létrehozott utak

ADATPTÁCIÓS SÉMA 2/3



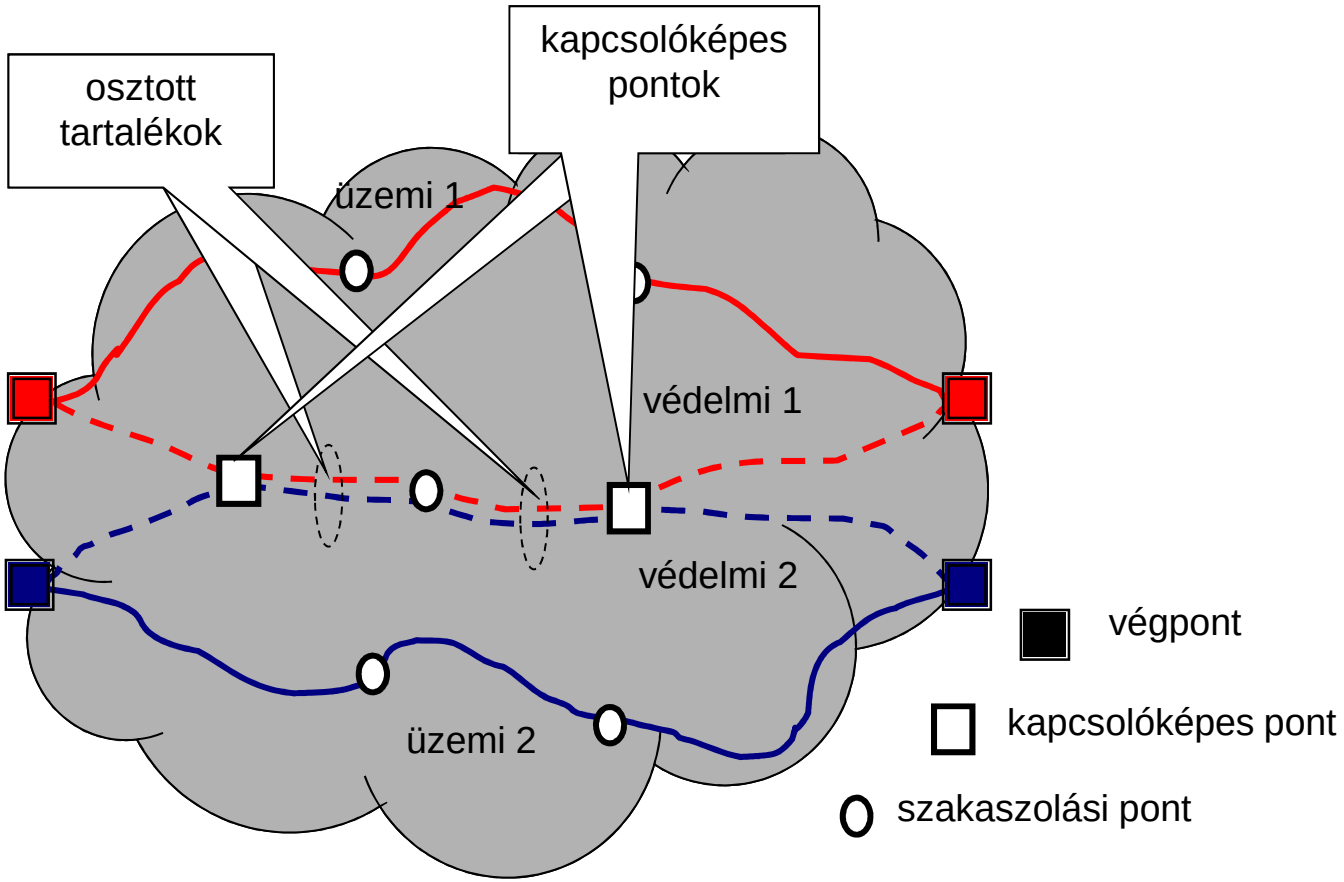
- Egy (link)hiba utak megszakadását okozza

ADATPTÁCIÓS SÉMA 3/3

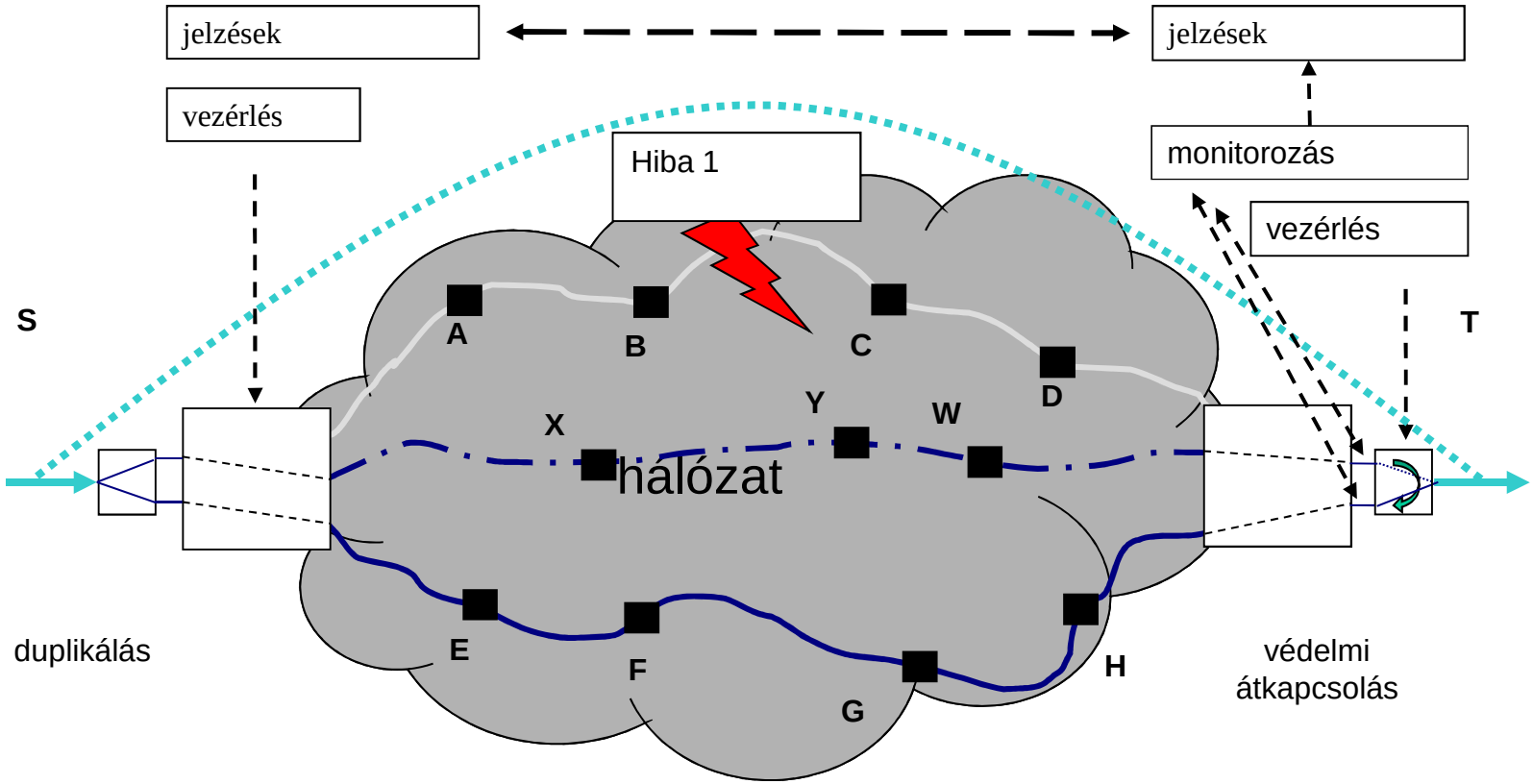


- A megszakadt utak újraszámolása az aktuális linktopológián (a meghibásodott linket figyelmen kívül hagyva)

OSZTOTT ÚTVÉDELEM

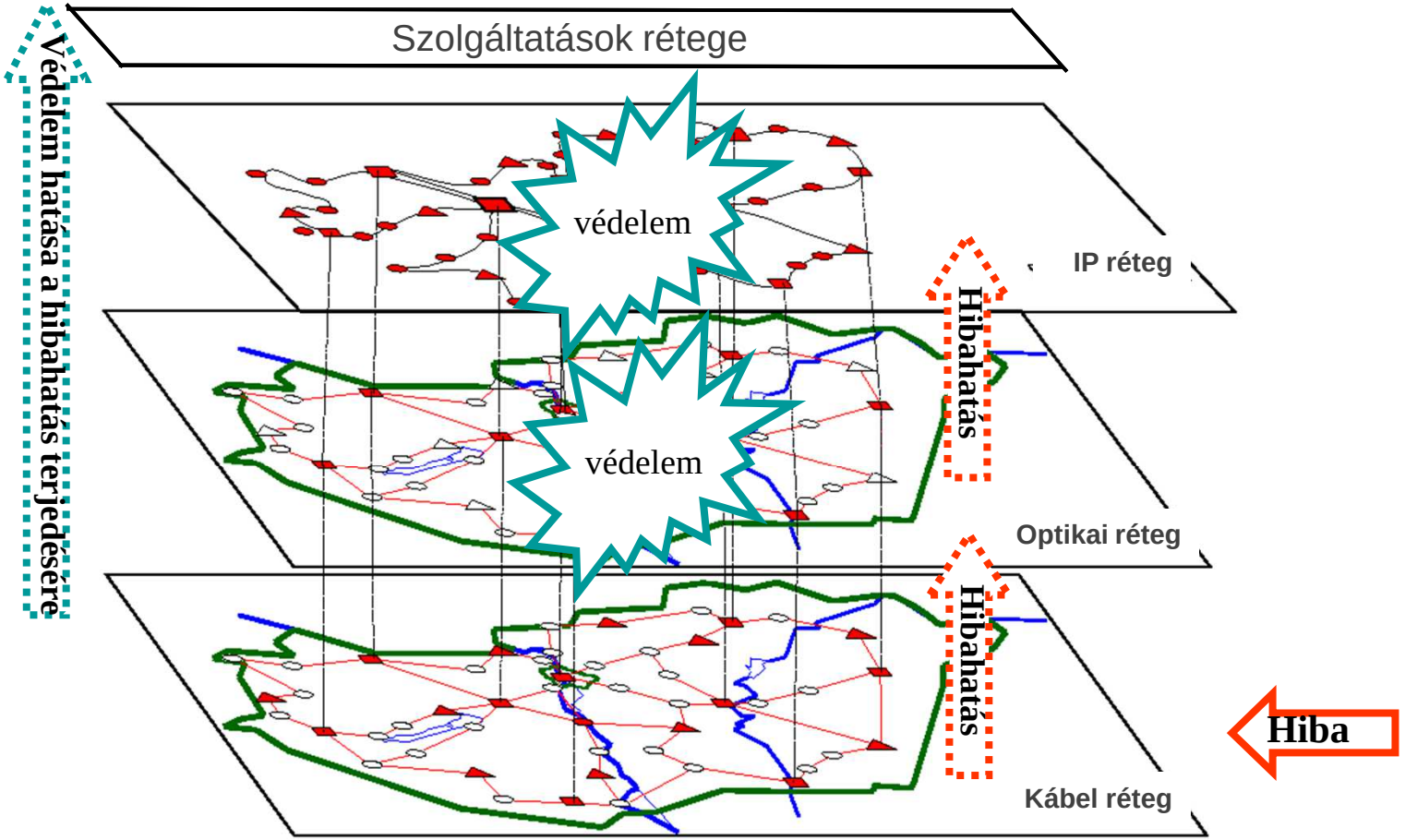


KITERJESZTETT 1+1 VÉDELMI SÉMA

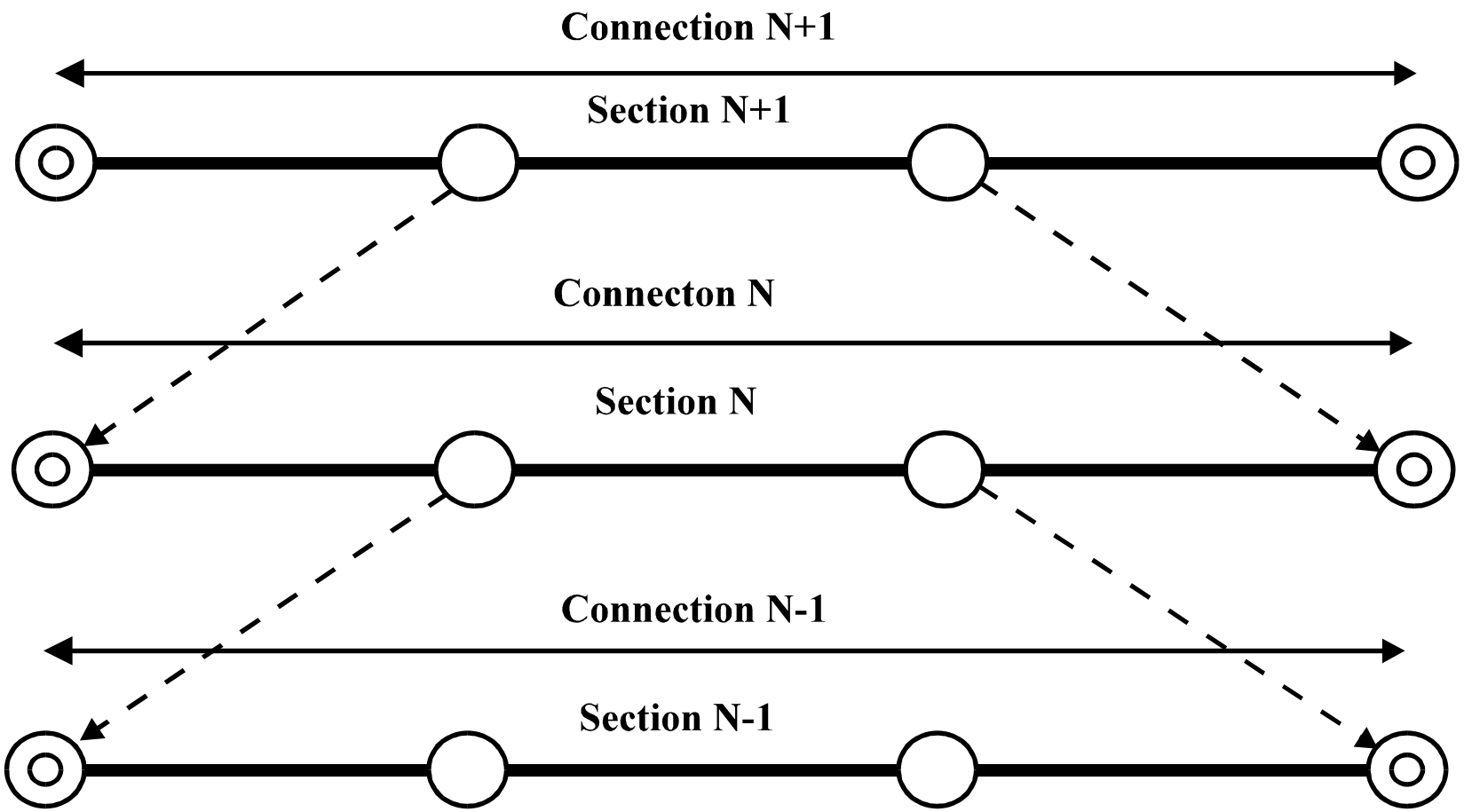


Második hibára felkészülve: a bekövetkezett hiba után is legyen egy előre konfigurált védelmi út (ennek konfigurálása csak a bekövetkezett hiba hatására

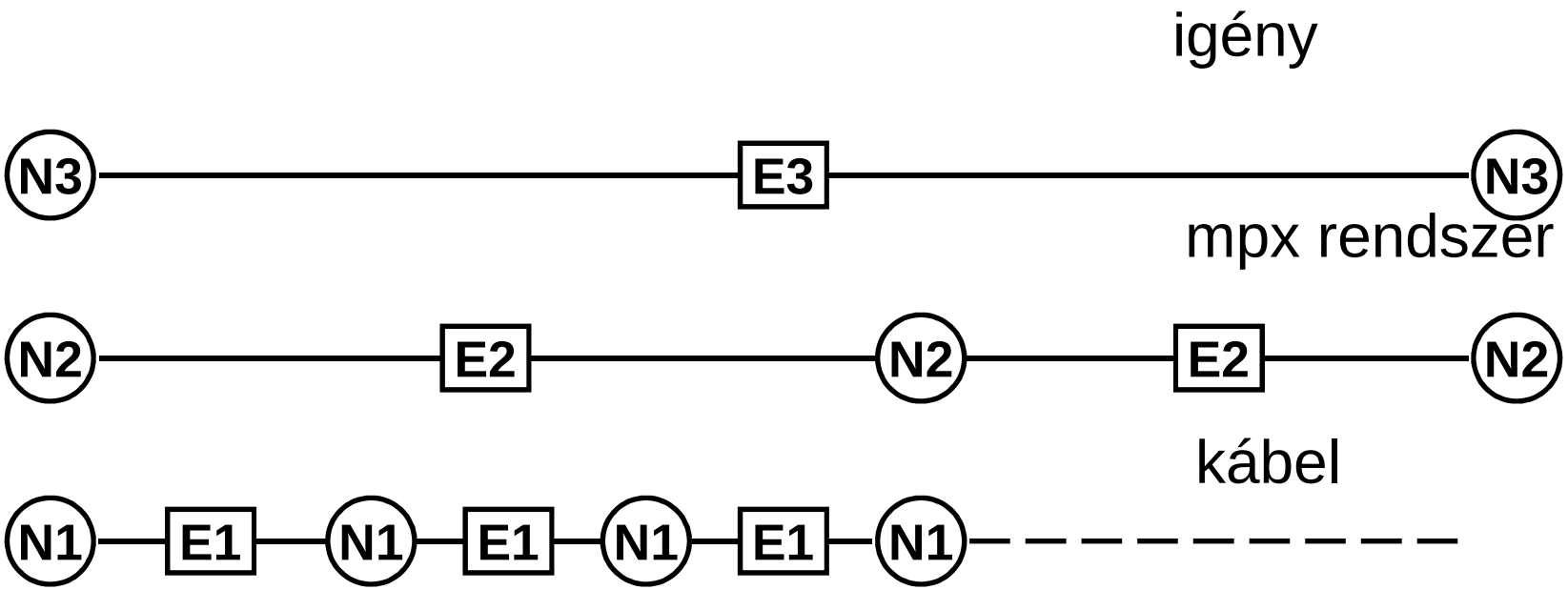
TÖBB VÉDELMI KÉPESSÉGŰ RÉTEG IS LEHET A HÁLÓZATBAN



TÖBBRÉTEGŰ HÁLÓZATMODELL

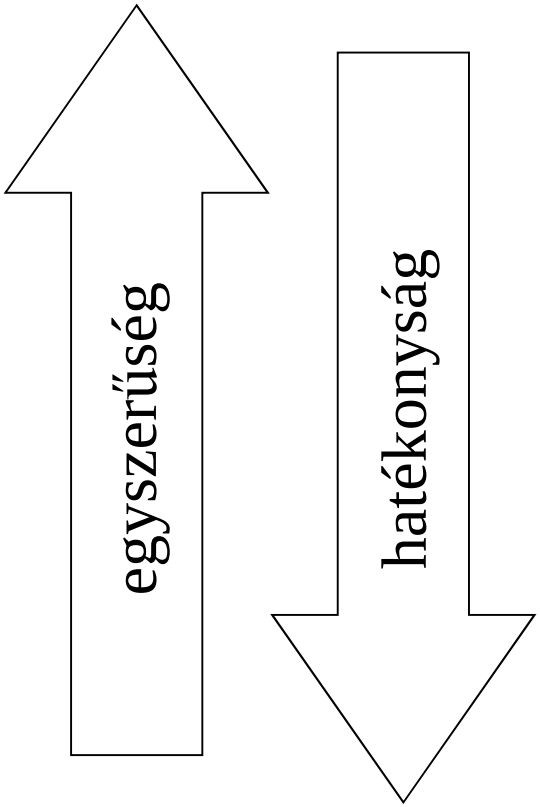


TÖBBRÉTEGŰ MEGBÍZHATÓSÁGI MODELL (HÁROMRÉTEGŰ PÉLDA)

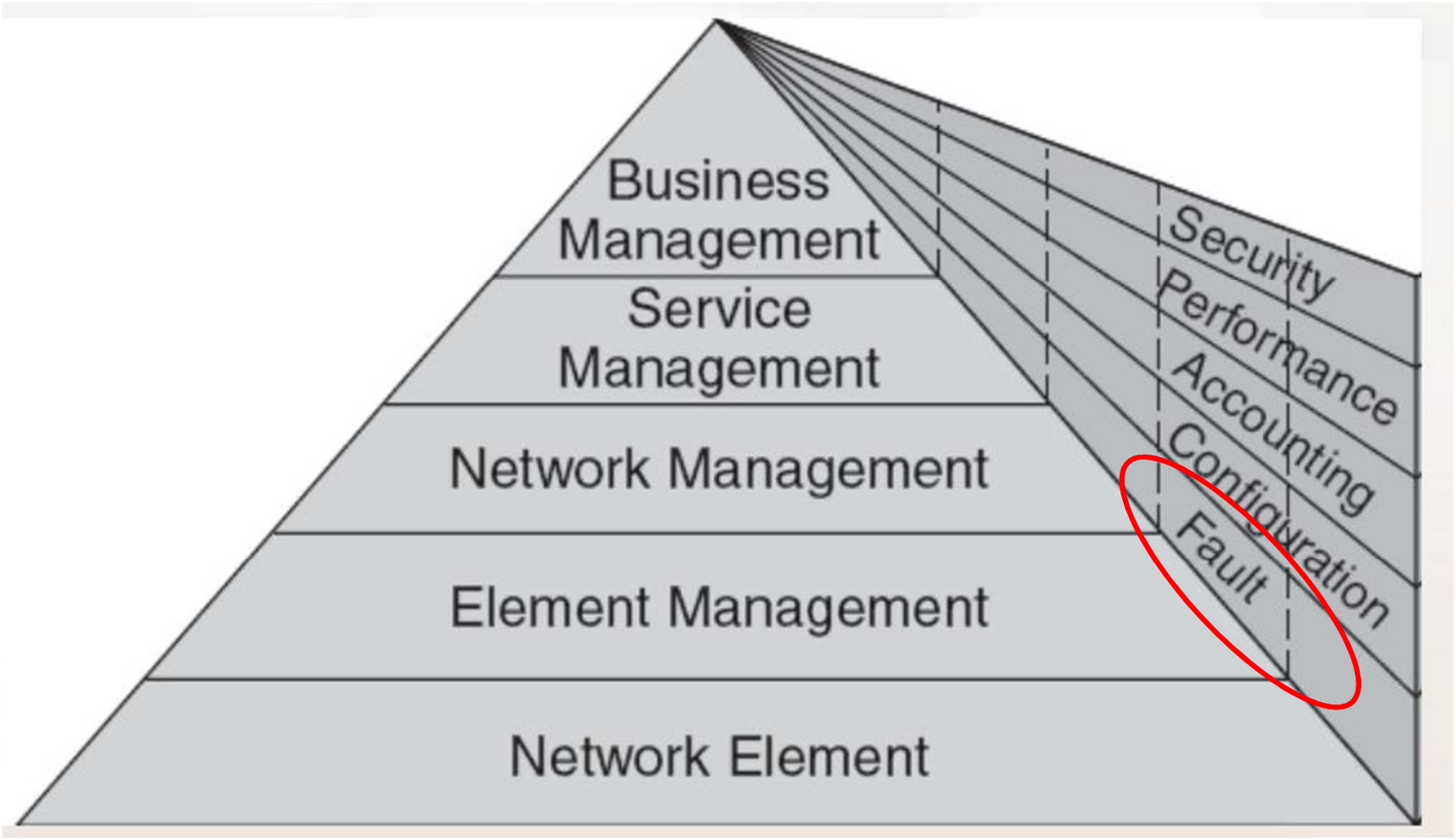


EGYÜTTMŰKÖDÉS TÖBBRÉTEGŰ VÉDELEM ESETÉN

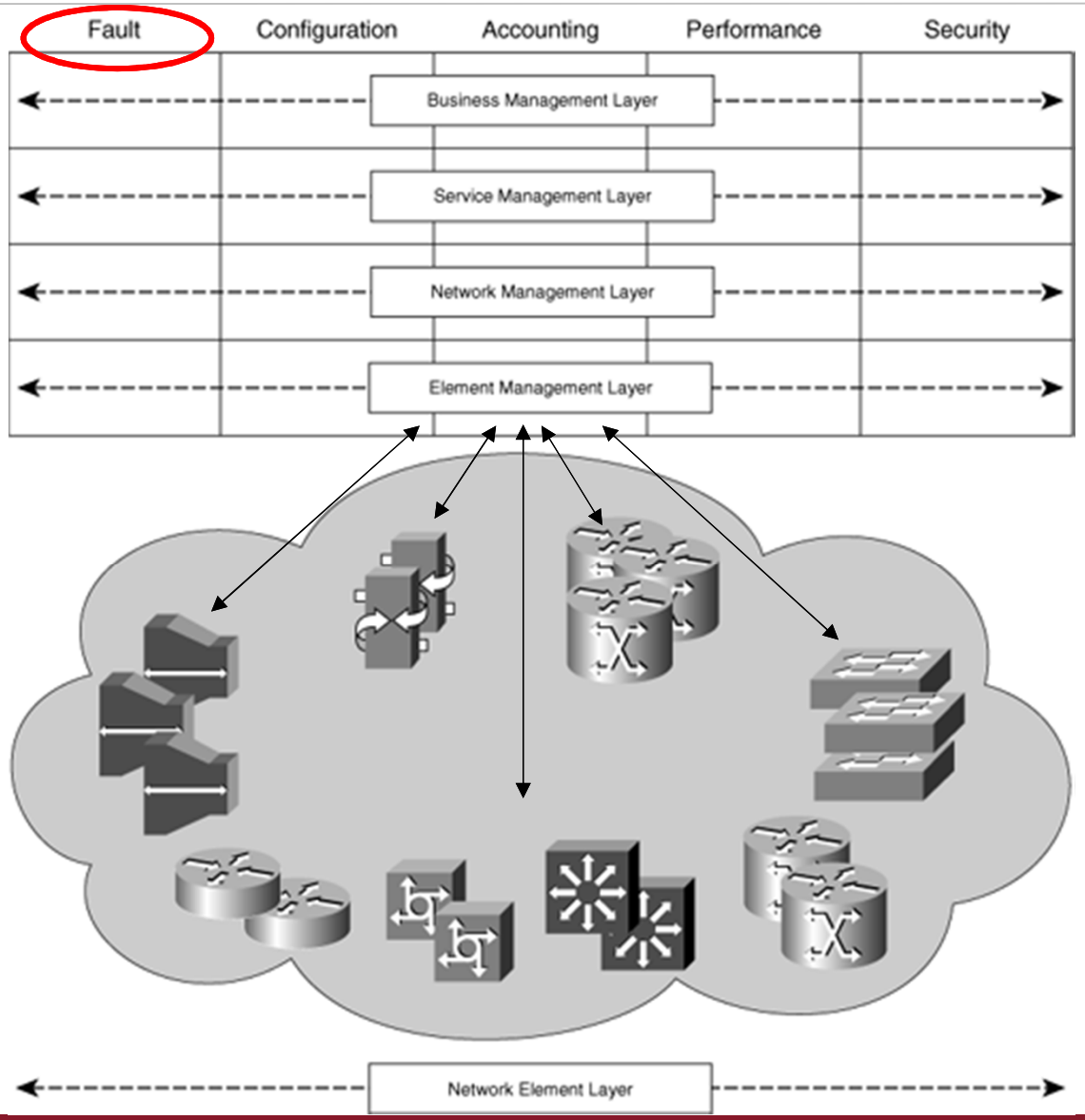
- Az együttműködés mértéke:
  - nincs - *független működés* -> instabilitás veszélye
  - információcsere nélkül, konfigurálási alapon – *időzítés* -> az elérhetőnél lassabb reagálás
  - minimális információcsere – *token* -> rétegenként független tartalékok
  - szoros együttműködés – *integrált menedzsment* -> eltérő alapon működő technológiai rétegek együttes menedzselése ?!



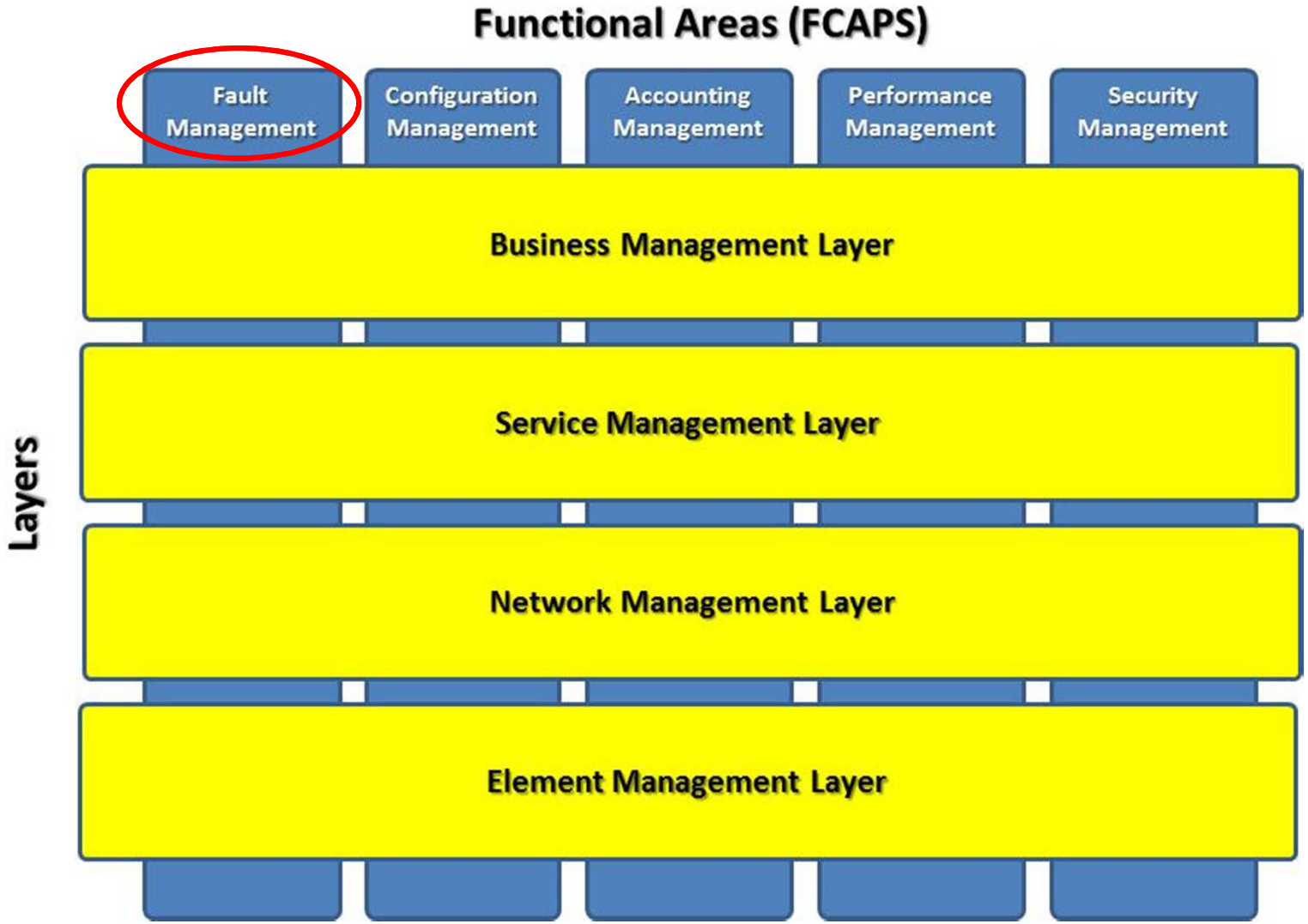
HÁLÓZATMENEDZSMENT: HIBAMENEDZSMENT FUNKCIÓK



HÁLÓZATMENEDZSMENT: TMN MODELL



HÁLÓZATMENEDZSMENT: FCAPS MODELL



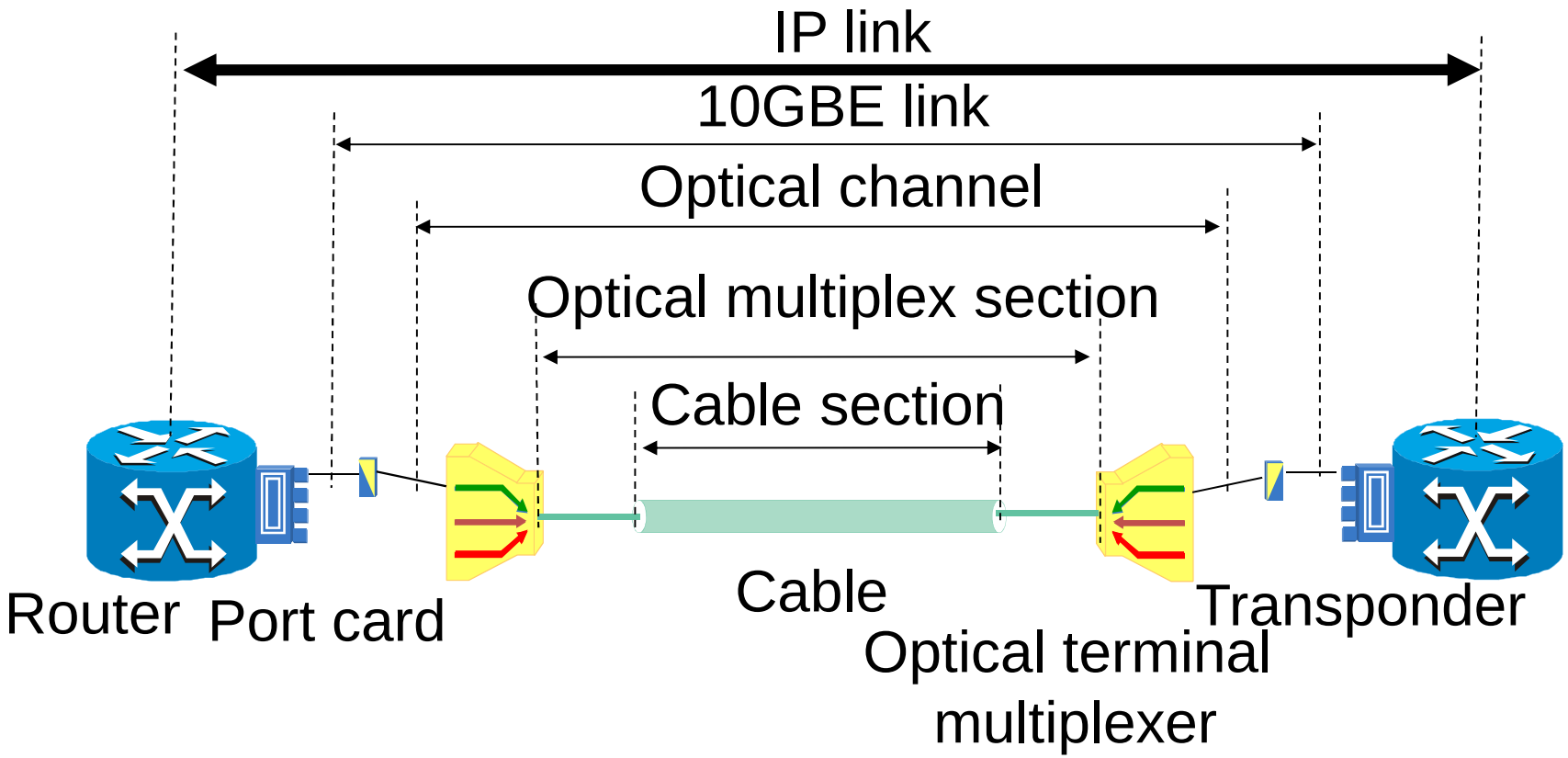
Rendelkezésreállási elemzés

EGY ILLUSZTRATÍV PÉLDA I.

Hungarian Telekom IP-optical backbone 2007

Element category	Number of elements	Typical order of DTR
Router	**119**	**10^{-4} ..10^{-5}**
Router port card	**286**	**10^{-5}**
Optical channel	**32**	**10^{-5}**
Optical multiplex section	**36**	**10^{-4}**
Optical amplifier section	**56**	**10^{-5}**
Cable link	**437**	**10^{-4} ..10^{-6}**
Network node (e.g. common functions like power supply)	**33**	**10^{-7}**

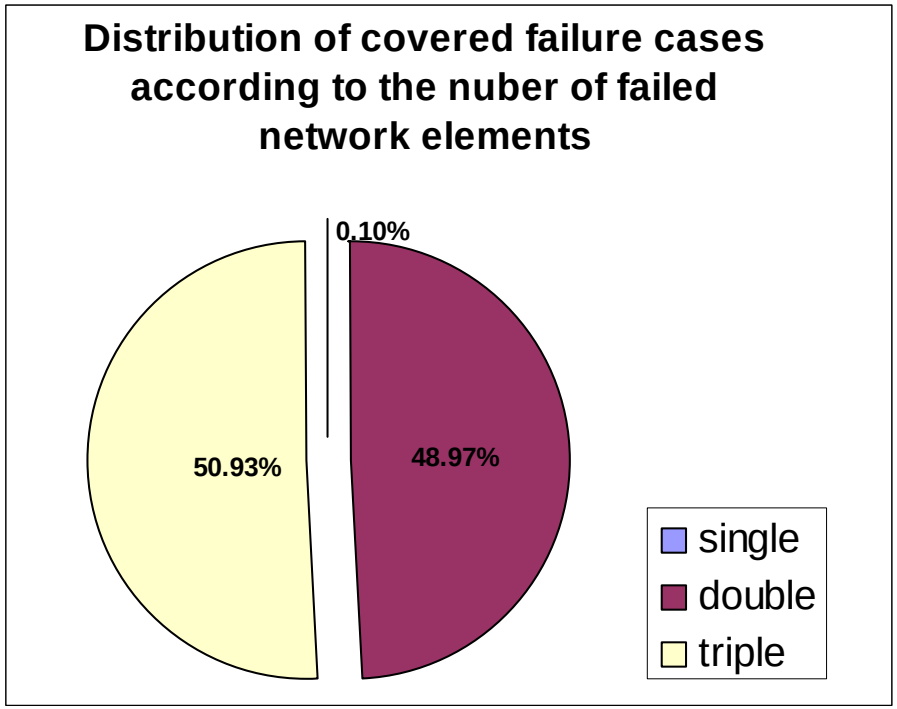
PÉLDA: HÁLÓZATI RÉTEGARCHITKTÚRA

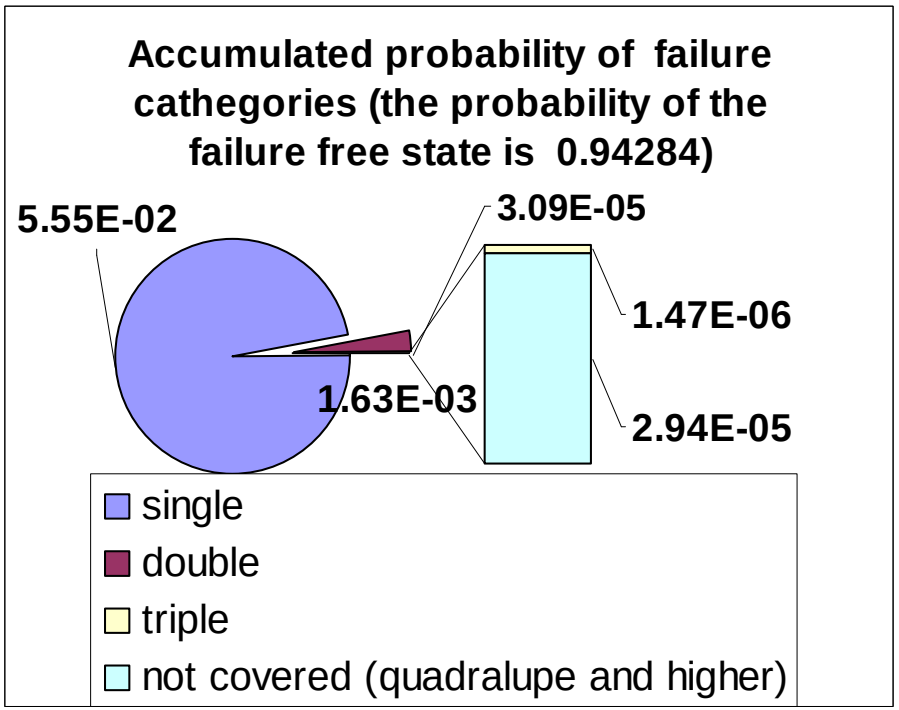


- A simple serial reliability structure
- The failure of any element interrupts the IP link

Rendelkezésreállási elemzés

EGY ILLUSZTRATÍV PÉLDA II.





- 999 model elements,
- 1 000 000 failure configurations

Rendelkezésreállási elemzés

EGY ILLUSZTRATÍV PÉLDA III.

- Li-Silvester deterministic estimation
  - The accumulated probability of the analyzed 1 000 000 failure cases: 0.9999706
  - The 1 000 000 failure cases imply 445874 different Layer 3 configurations

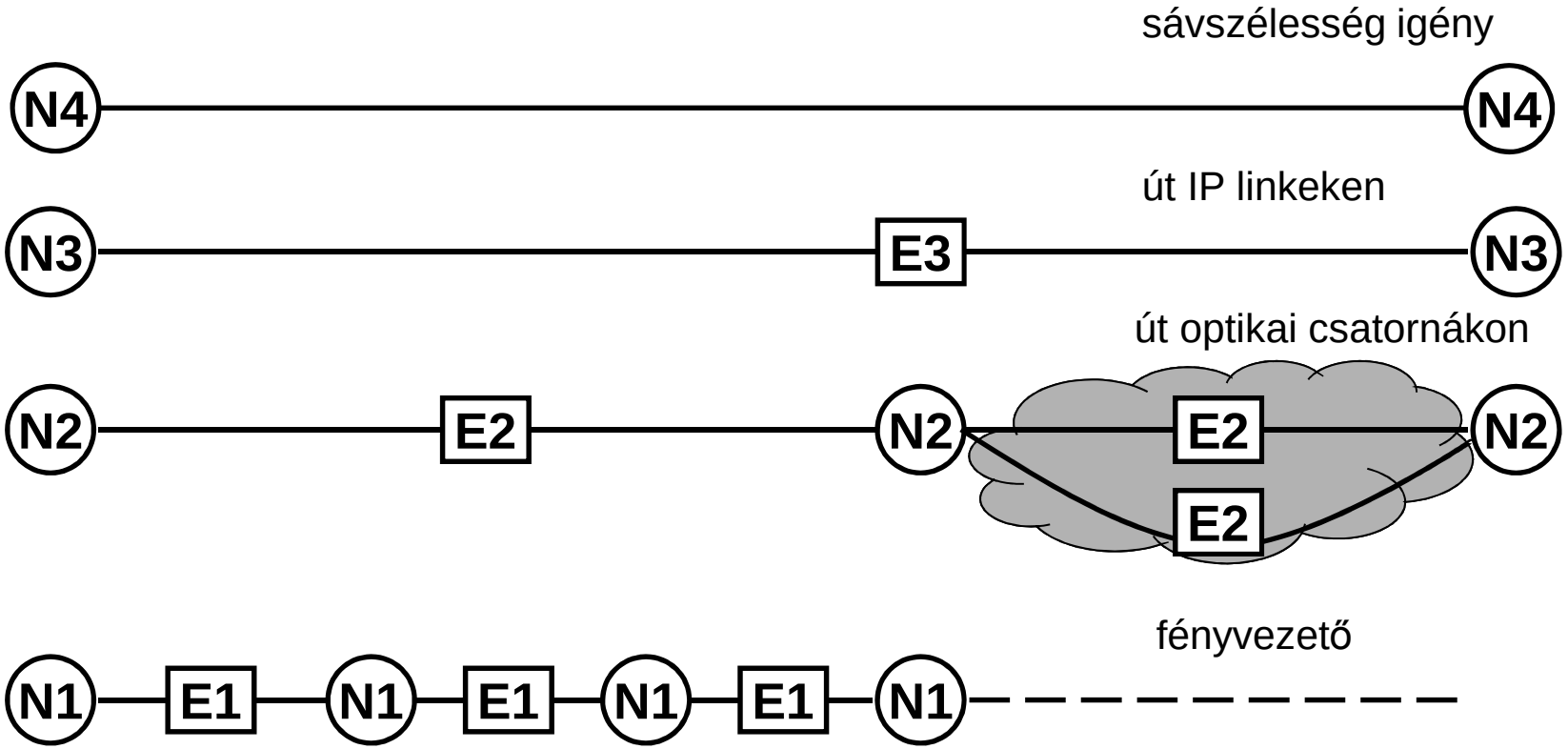
DEPARTMENT OF
NETWORKED SYSTEMS
AND SERVICES

Hálózatvédelmi megoldások

MIRE HASZNÁLJUK?
HOGYAN VALÓSÍTJUK MEG?

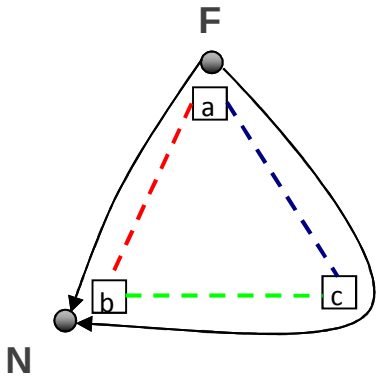
Hálózatvédelmi sémák
MIRE HASZNÁLJUK?

- Pont-pont (unicast jellegű) szolgáltatás hibák elleni védelme
- Útvédelem / szakaszvédelem – nézőpont kérdése
  - IP linket hordozó optikai csatorna védelme – az optikai csatorna útjának védelem
  - ugyanez az IP linket útjában tartalmazó IP sávszélesség szolgáltatás szempontjából szakaszvédelem



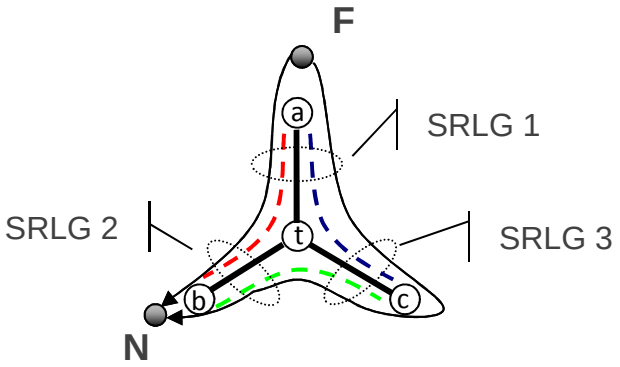
Hálózatvédelmi sémák
MIRE HASZNÁLJUK?

- Pont-pont (unicast jellegű) szolgáltatás hibák elleni védelme
- Út függetlensége (csomópont/szakasz)– nézőpont kérdése
  - pl. a közvetlen szolgáltató rétegben független, de a hálózat egészét (a közvetlen szolgáltaó réteget hordozó réteg(ek)et is tekintve nem független
  - Shared Risk Ling Group – SRLG: azonos (alsóbb rétegbeli) fizikai erőforrás szolgáltatását igénybe vevő összeköttetések csoportja (az SRLG-ktipikusan nem diszjunkt halmazok)



IP linkek topológiája

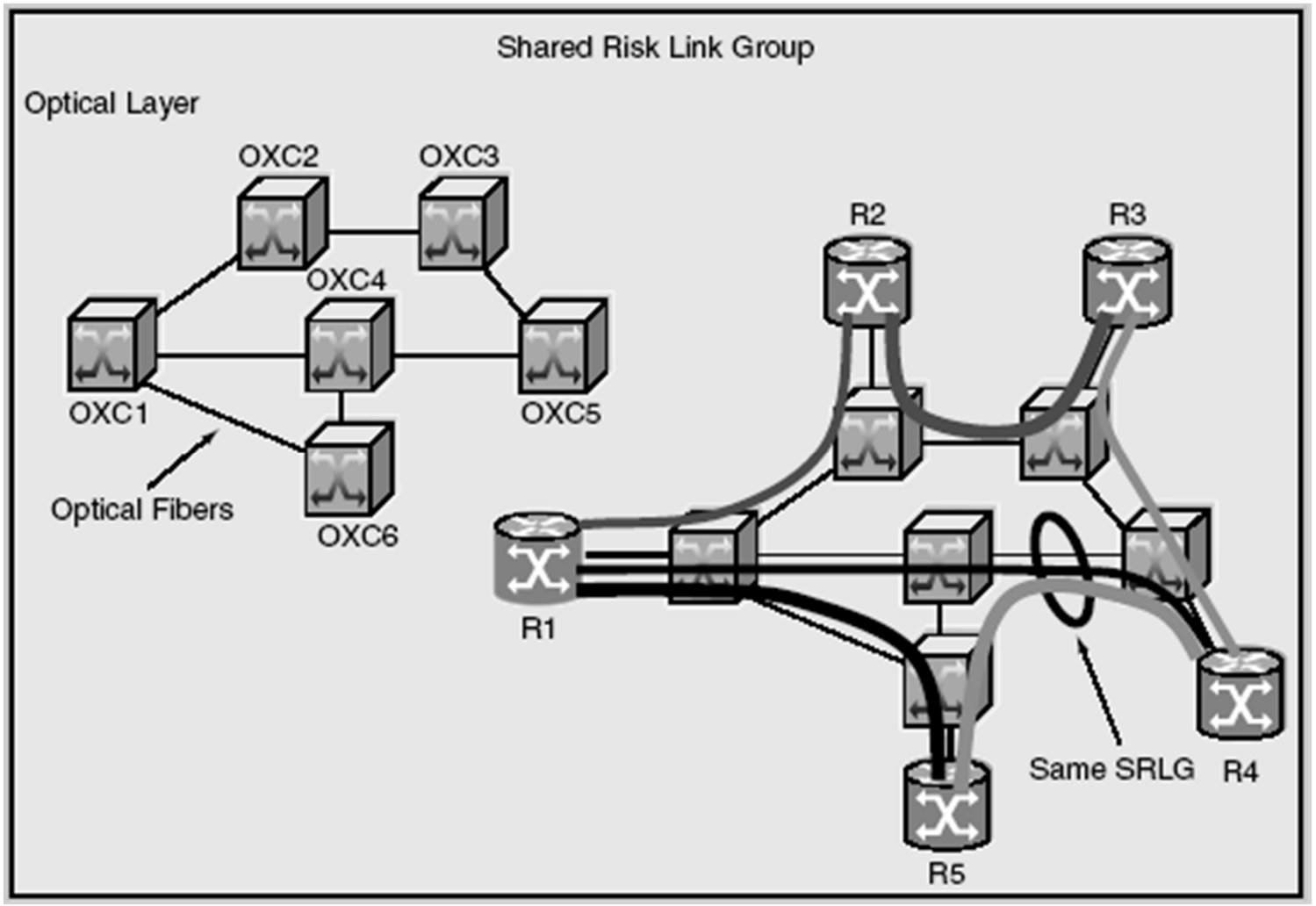
van F->N két csomópont-független független út az IP link topológián



fényvezető szakaszok topológiája

nincs F->N két csomópont-független független út az IP-optikai hálózaton

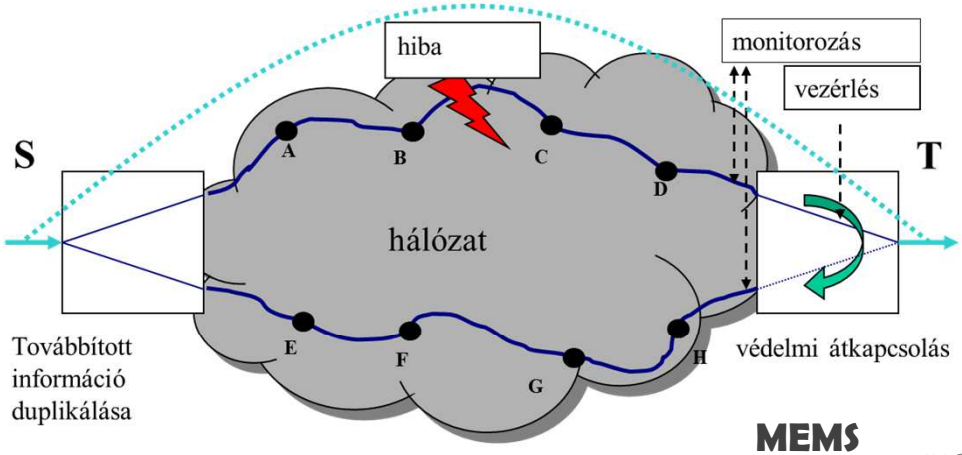
SRLG

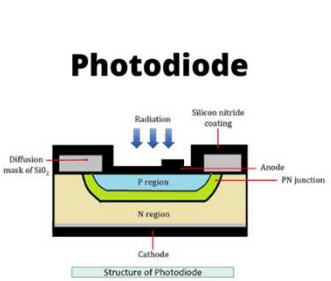

Shared Risk Link Group
Optical Layer
OXC2
OXC3
OXC4
OXC1
OXC5
OXC6
Optical Fibers
R2
R3
R1
R4
R5
Same SRLG

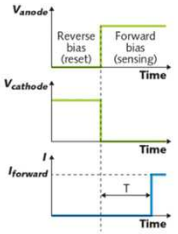
Hálózatvédelmi sémák

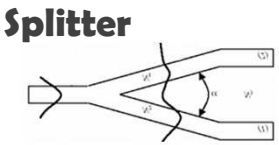
MEGVALÓSÍTÁS: OCH ÚTVÉDELEM

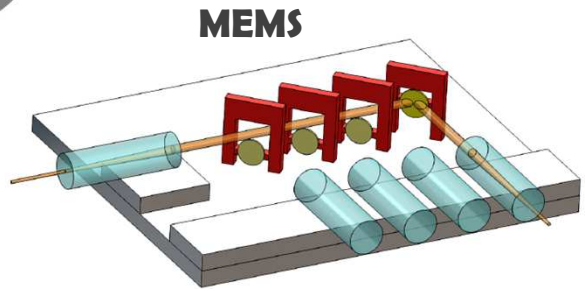
- Pl. pont-pont optikai csatorna 1+1 útvédelme
- Egyszerű funkcionális modell
  - Adó oldal: jelduplikálás passzív osztóval (teljesítményfelezés)
  - Vevő oldal: monitorozás vett jel teljesítménye alapján, kapcsoló: 1x2 MEMS







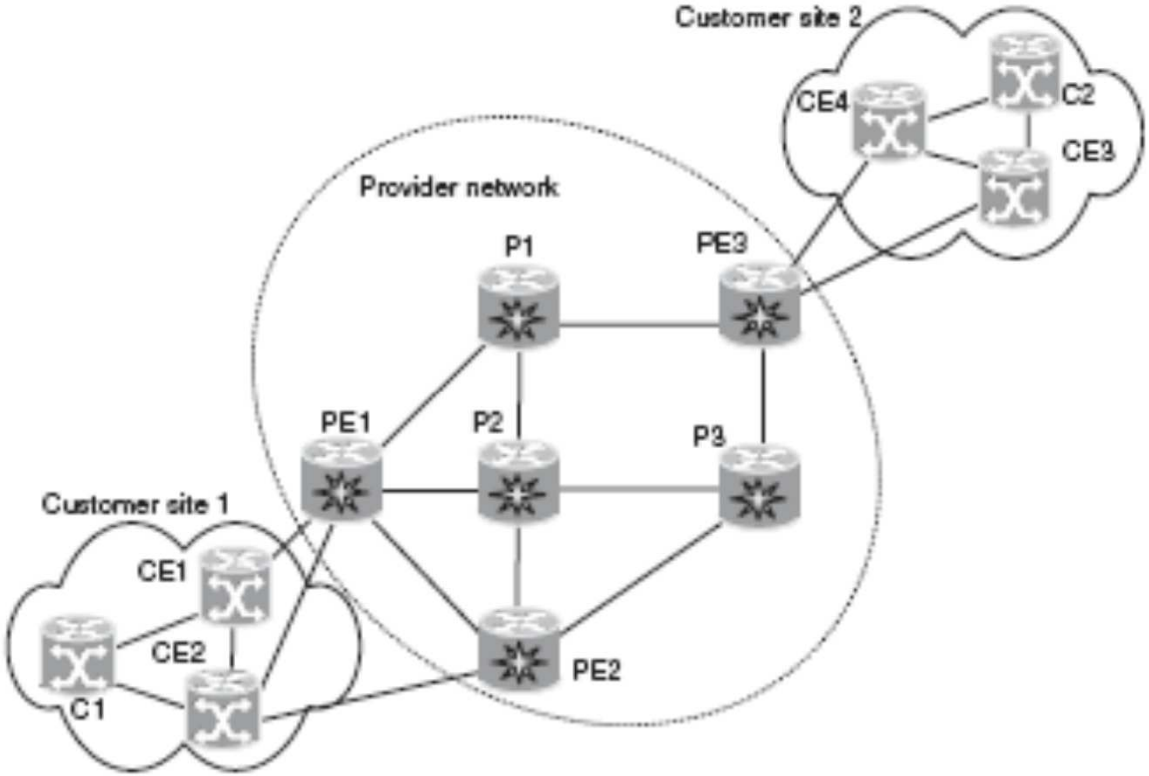




MEGVALÓSÍTÁS: IP/MPLS TE

- Különböző IP/MPLS TE útvédelmek
- Egyszerű funkcionális modell
  - PE és P routerek
  - Útszámítás (független meghibásodások constraint based routing)
  - Állapotok, vezérlés (jelzésfunkciók, jelzésprotokoll)
- IP/MPLS TE
  - tipikusan maghálózati (IP core) technológia (nagy aggregáltságú forgalom továbbítására, de szolgáltatási képességei miatt kijjebb is)
  - a hálózat építőeleme Label Switch Router (LSR)
  - a továbbítás (forwarding) lokális érvényességű címkék alapján történik (push, pop, swap, label stacking)
  - ER- LSP (Explicitly Routed LSP)
    - a forrás csomópont dönti el az útvonalat
    - az ingress és egress csomópont között felépül egy LSP (Label Switched Path)
    - a út felépítésében résztvevő LSR-ek forwarding táblázatai ennek megfelelően módosulnak (jelzésprotokoll LDP)
  - belépés: az MPLS domain határán lévő ingress LSR (LER) „megcímkézi” a csomagokat
  - minden további LSR címkecserét hajt végre a rajta átmenő csomagokon
  - kilépés: az MPLS domain határán lévő egress LSR leveszi a címkéket a csomagokból
  - Hibadetektálás, hibajelzés
    - LOS (Loss of Signal) – kapcsolatos elvesztése (pl. Ethernet-link hiba, vagy OCh hiba) – downstream csp. érzékeli
    - LMP (Link Management Protocol) – kétirányú, sávon kívüli jelzéscsatornán upstream irányú hibajelzés
    - hello, keep alive
    - notify (ingress vagy recovery csp-nek)
    - crank-back – bővebb információ a hibáról
  - Védelmi átkapcsolás (Protection Switching)
  - Gyors útvonal-módosítás (Fast Rerout)

IP/MPLS HÁLÓZAT

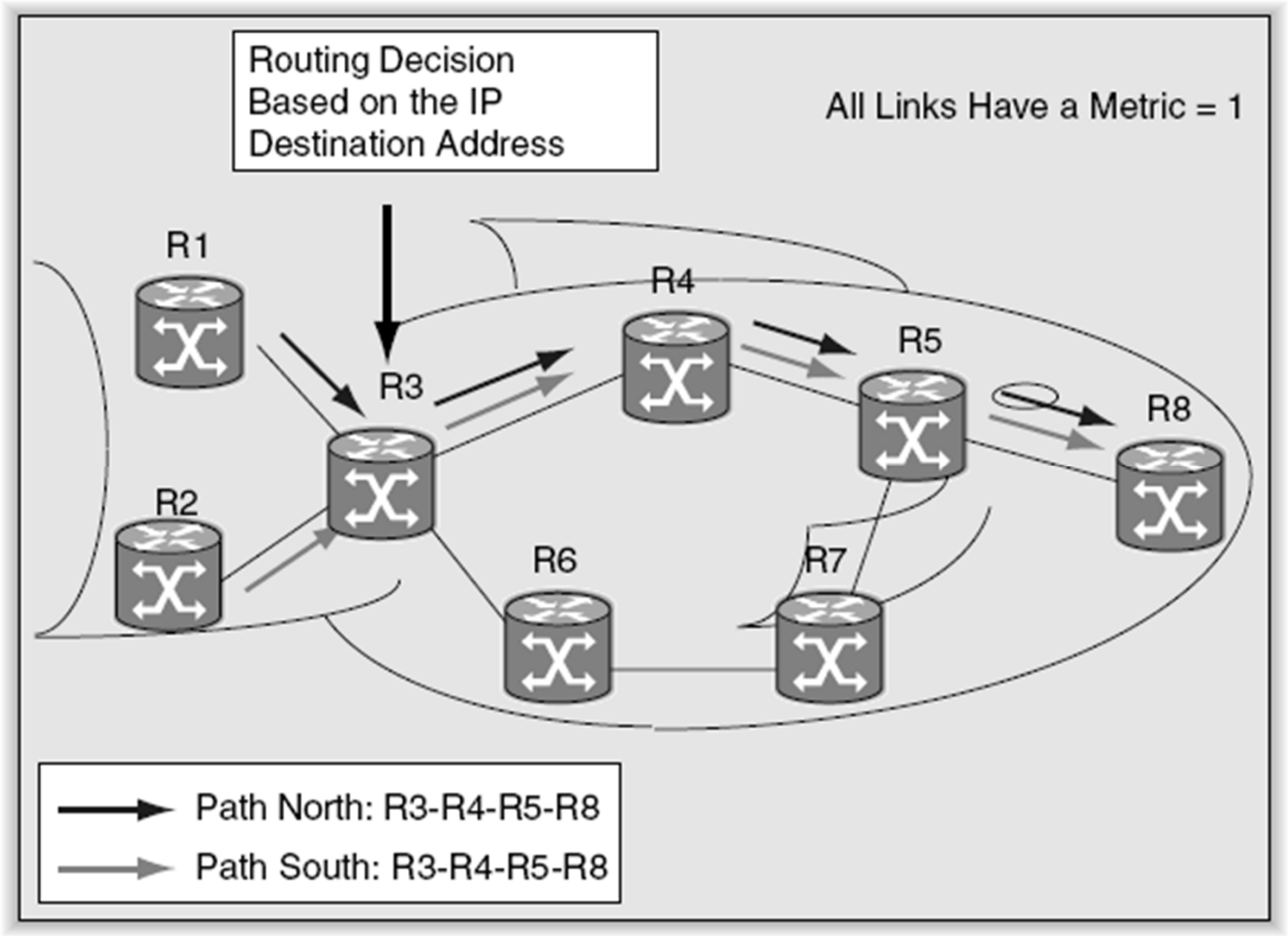


- PE – Provider Edge router (LER – Label Edge Router)
  - az MPLS hálózat határán
  - forgalom beillesztése az MPLS továbbításba (hol lép ki, mi legyen vele)
  - forgalom kicsomagolása, továbbítása (adott interfészre, vagy IP routing alapján meghatározott next hopra)
- P – Provider router (LSR – Label Switch Router)
  - forgalom továbbítása a címke alapján

MPLS MOTIVÁCIÓK ÉS CÉLKITŰZÉSEK

- ~25 éves hálózati technológia
- az IP térhódításával kapcsolatos várakozásokhoz kötődik
  - skálázhatósági problémák
    - növekvő forgalom
    - dinamikusan bővülő aktív címtér
    - routerek növekvő erőforrás-igénye
  - hatékonysági probléma
    - nincs forgalomvezérlés, torlódás és alig használt linkek egyi dőben vannak jelen a hálózatban
    - a „hal” (fish) probléma
  - szolgáltatási megfontolások
    - VPN
    - egységes szolgáltatási platform
- kell egy olyan gerinchálózati technológia, ami a nagymennyiségű forgalmat a rengeteg célcím felé hatékonyan továbbítja, és hatékonyan támogat L3, L2 (és akár L1) szolgáltatásokat is

MINIMÁLUTAK „HÚZÓHATÁSA” A HAL PROBLÉMA (FISH PROBLEM)



MŰKÖDÉSI KOMPONENSEK

- Gerinchálózat, aggregált forgalom
- Továbbítási komponens
  - Forwarding Information Base (FIB) alapján címkealapú továbbítás
- Kontroll komponens
  - FIB felépítése, karbantartása
- Forwarding Equivalent Class (FEC)
  - azonos elbánást igénylő forgalmak csomagjai
  - a hálózat határán történik meg a forgalom -> FEC összerendelés
    - Hol fog kilépni az MPLS hálózatból?
    - Mit kell vele csinálni kilépéskor?

A CÍMKEALAPÚ TOVÁBBÍTÁS

- a hálózat határán (ingress PE) felcímkézett MPLS keretek továbbítása a hálózaton át (egress PE)
- a címke (és az input interfész) alapján döntés az output interfészről (next hop)
- lokális hatókörű címkék
  - az LSR-ek minden továbbítási lépésben lecserélik a címkét

CÍMKEALAPÚ TOVÁBBÍTÁS

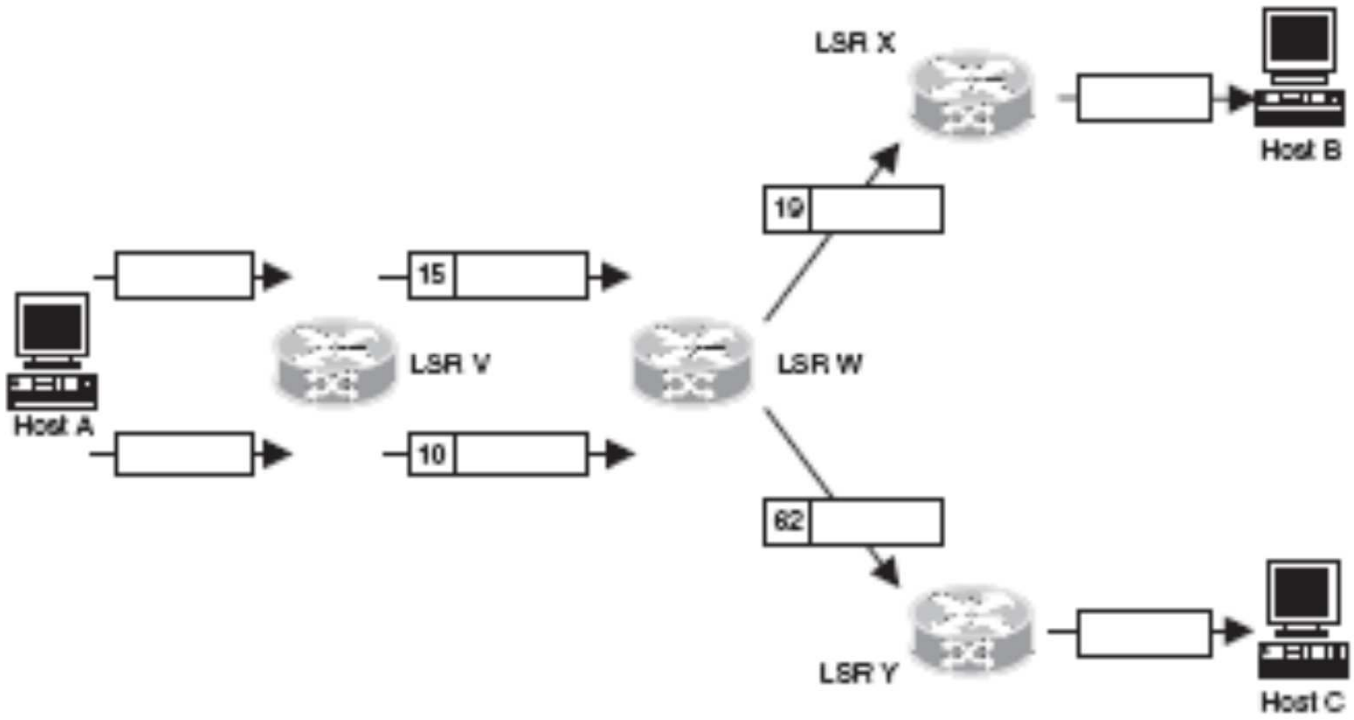
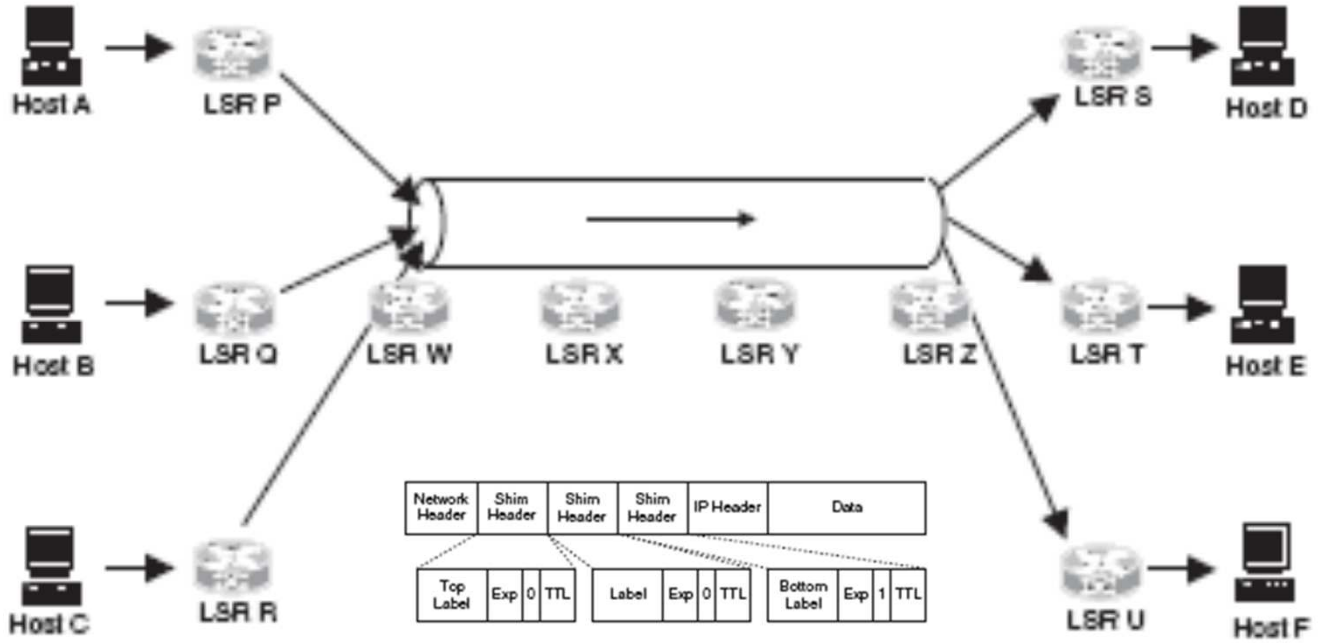


Table 2.1 The LFIB at LSR W.

Incoming Interface	Incoming Label	Outgoing Interface	Outgoing Label
From LSR V	15	To LSR X	19
From LSR V	10	To LSR Y	62

HIERARCHIKUS CÍMKÉZÉS



- Hierarchikus címkék alagutak kialakításához
  - Közös továbbítási szakaszon közös – felső - címke
  - Eltérő kezelés pontján az eltérő – alsó – címke vezérli a továbbítást

TOVÁBBÍTÁS HIERARCHIKUS CÍMKÉK ALAPJÁN

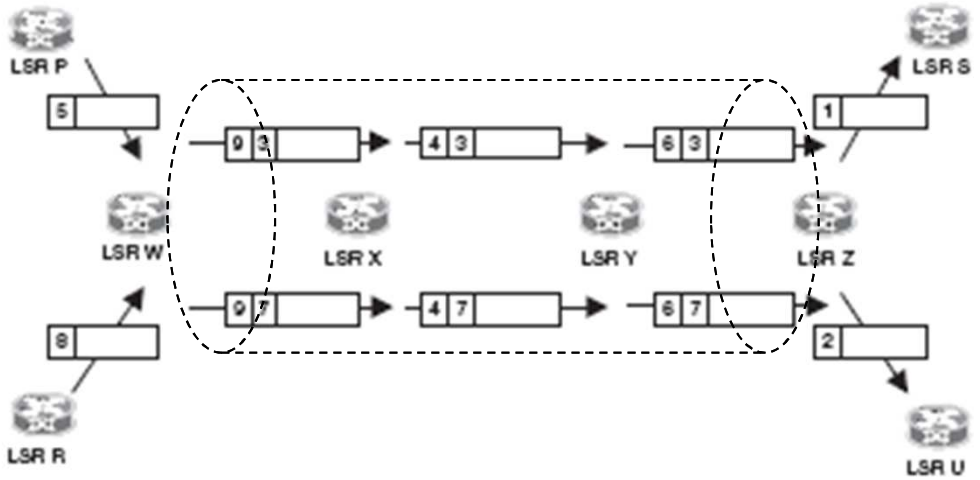


Table 2.2 LFIBs at LSR W, LSR X and LSR Z for LSP Tunnels.

Incoming Interface	Incoming Label	Action	Outgoing Interface	Outgoing Labels
LSR W				
From LSR P	5	Swap and Push	To LSR X	9, 3
From LSR R	8	Swap and Push	To LSR X	9, 7
LSR X				
From LSR W	9	Swap	To LSR Y	4
LSR Z				
From LSR Y	6	Pop	N/A	N/A
From Tunnel	3	Swap	To LSR S	1
From Tunnel	7	Swap	To LSR U	2

EGYSZERŰSÍTETT FELDOLGOZÁS A KILÉPŐ OLDALON

- Az egress PE-ben a „felső címke” miatt kétkörös keresés
- Egyszerűsíthető, ha az utolsó előtti MPLS-link elején lekerül a felső címke Penultimate Hop Popping (PHP)
- Csökkenti az egress PE feldolgozási terhelését, gyorsítja a továbbítást (de azért vannak kellemetlen következményei is menedzsment és forgalomi statisztikák szempontjából)

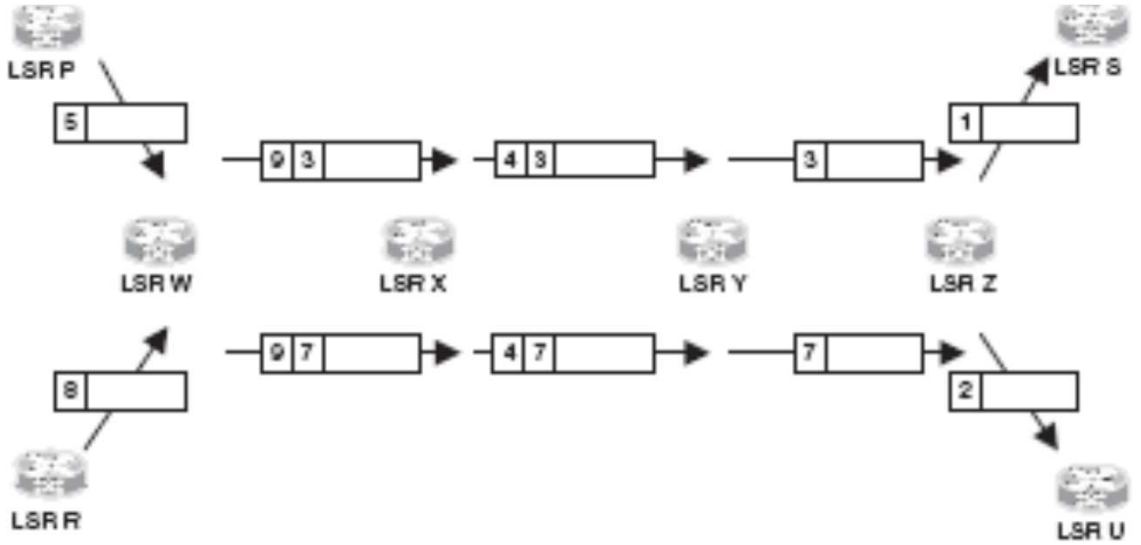


Table 2.3 LFIBs at LSR Y and LSR Z for Previous Hop Popping.

Incoming Interface	Incoming Label	Action	Outgoing Interface	Outgoing Label
LSR Y				
From LSR X	4	Pop	To LSR Z	N/A
LSR Z				
From LSR Y	3	Swap	To LSR S	1
From LSR Y	7	Swap	To LSR U	2

CÍMKEALAPÚ TOVÁBBÍTÁS ÖSSZEFOGLALÁSA

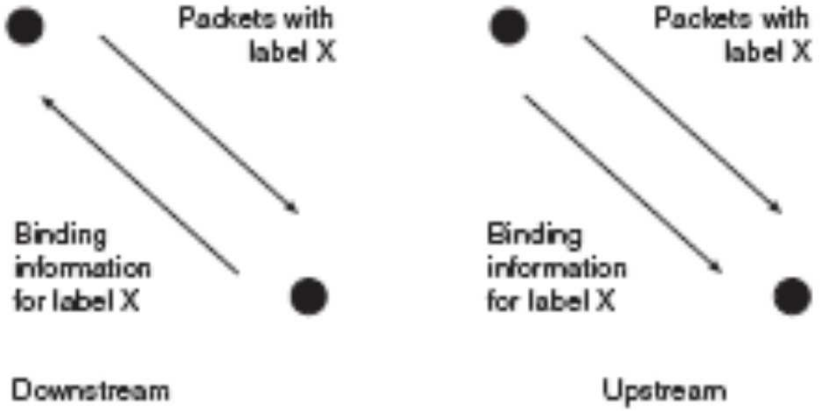
- MPLS továbbítási komponens
- Egyetlen továbbítási algoritmus a címkecserére alapozva
- A címke egy rövid, fix hosszúságú strukturálatlan információ, aminek továbbítási (és erőforrás lefoglalási) jelentése van
- A továbbítási komponens nem korlátozza a továbbítás címkéhez köthető felbontását (granularitását)
- A továbbítási komponens különböző hálózati réteg és link réteg protokollt támogat

A VEZÉRLÉSI KOMPONENS

- Címke:
  - Hová kell továbbítani a forgalmat az MPLS hálózatban?
  - Mit kell csinálni a kilépő forgalommal?
- IGP és EGP (OSPF, BGP, PIM)
  - FEC – next hop összerendelés
- Címkék és FEC-ek összerendelése
  - FEC – címkék összerendelés
- A címkeinformációk terjesztése
- A FIB karbantartása

CÍMKEKIOSZTÁS

- Lokális: a router válaszja meg a címkét
- Távoli: a router egy másik router által meghatározott címkét használ
- Előre irányú (upstream) címkeosztás
- Visszirányú (dowstream) címkeosztás
- Címketartomány – FIB szervezésétől függően
  - routerhez rendelt
  - interfészhez rendelt
- Osztás/visszavonás



CÍMKEINFORMÁCIÓK TERJESZTÉSE

- a routing protokoll információihoz kapcsoltan
  - elkerülhetőek a versenyhelyzetek (eltérő időbeli lefolyások)
  - mind a címke – FEC, mind a címke – next hop információ egy időben rendelkezésre áll
  - egyszerűsíti a működést, mert nem kell külön címkeinformációt terjesztő protokoll
  - Ugyanakkor a meglévő protokollok ilyen kiterjesztése számos problémát vet fel (információ formátuma, visszamenőleges kompatibilitás a meglévő eszközökkel)
- Címkeinformációt terjesztése külön protokollal
  - nehezebben elkerülhetőek e versenyhelyzetek
  - még egy protokoll – nagyobb rendszerkomplexitás
- A pragmatikus megoldás
  - mindkettő együttes alkalmazása célorientáltan

MI TÖRTÉNIK A HÁLÓZAT HATÁRÁN?

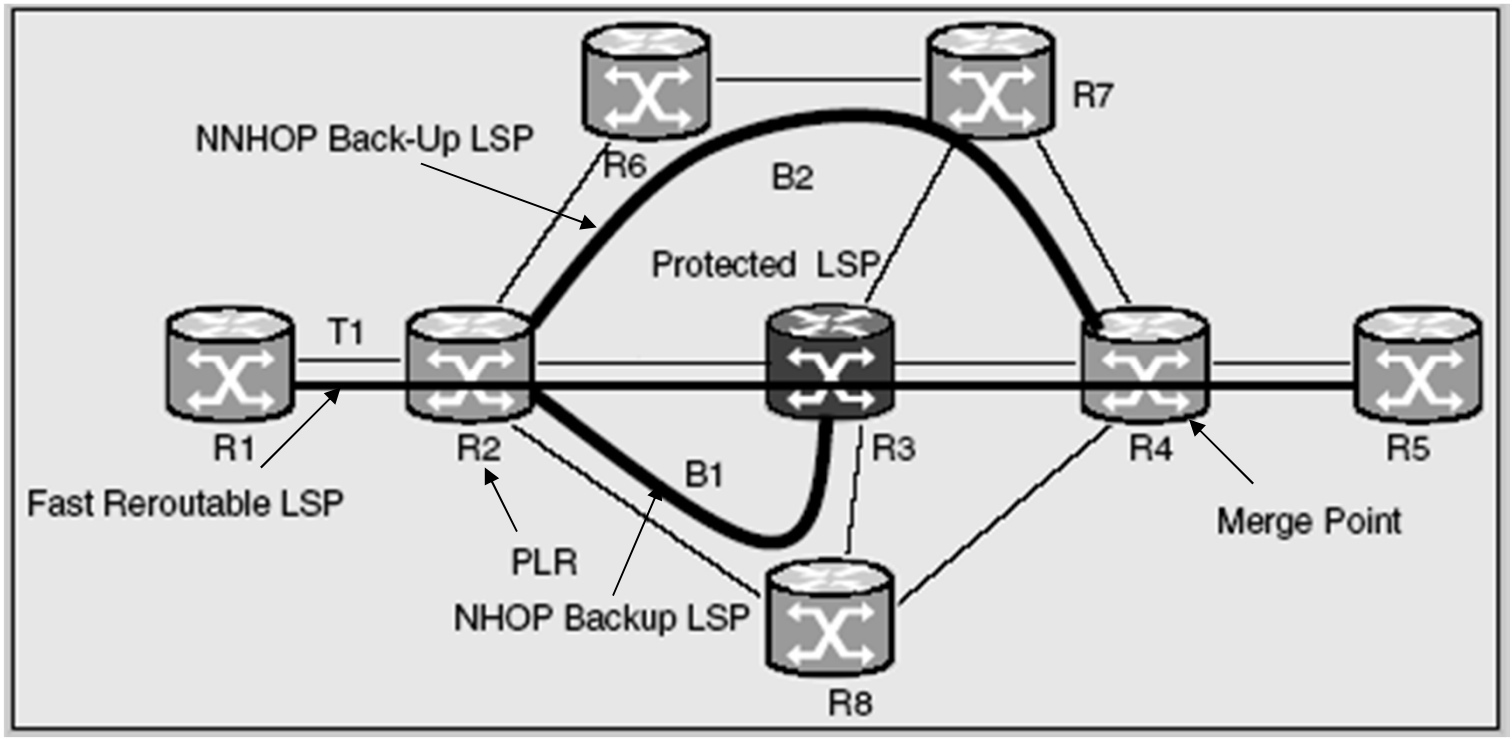
- Belépők címkézése, kilépők címkétlenítése a hálózat határán
- Next hop meghatározása
  - ha LSR, akkor címkézés, továbbítás
  - ha nem LSR, akkor címkétlenítés és továbbítás logikai vagy fizikai interfészre

- Gyakorlatban a PE és P funkció logikai, és méretgazdaságossági megfontolásokból egyetlen eszközben integrálódhat

MPLS – MELYIK RÉTEG?

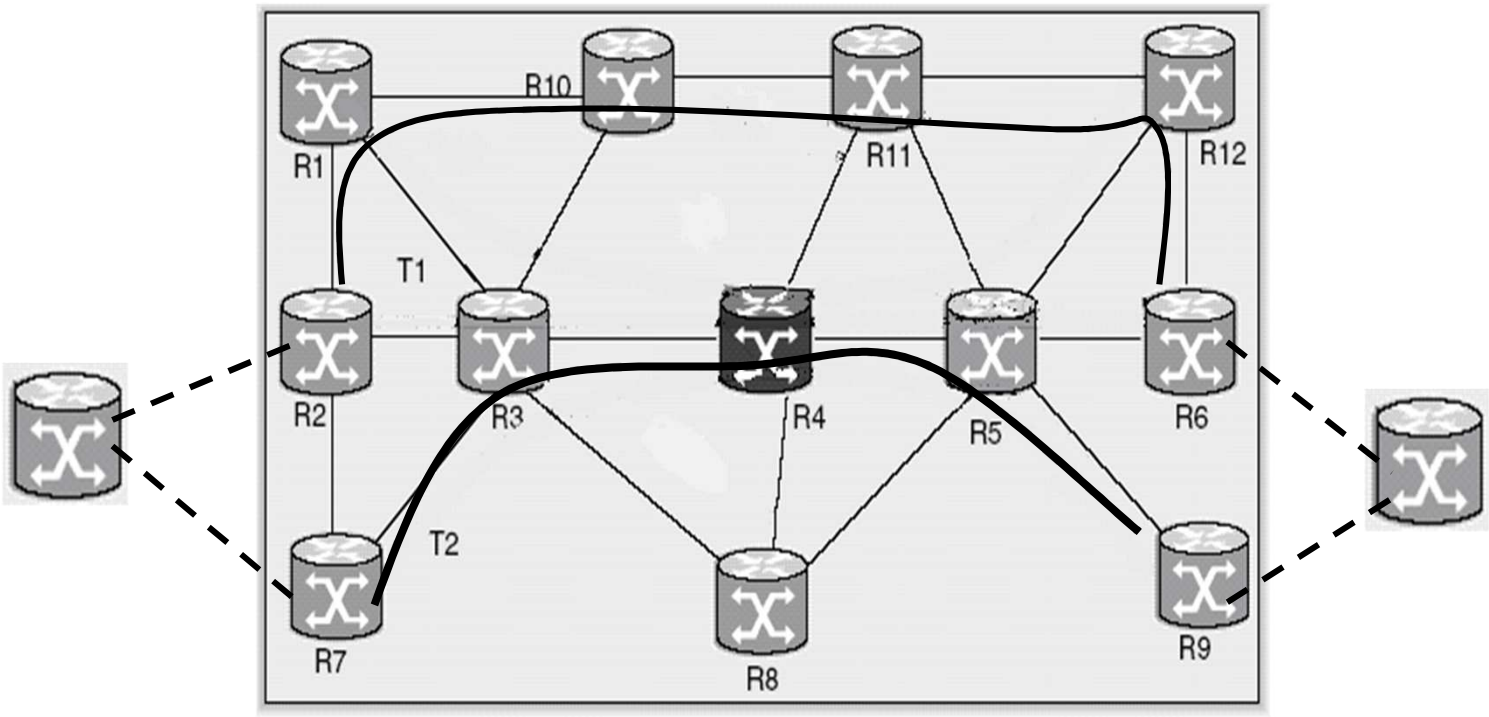
- ISO OSI 7 réteg
- Nem Layer 2 – mert független a Layer 2 technológiáktól (alkalmazható pl. ATM, Ethernet vagy P2P link felett)
- Nem Layer 3 – nincs saját routing és címzés
- Nem illeszkedik a modellbe, de komoly gyakorlati jelentősége van
- Praktikusan Layer 2.5-nek szokták nevezni

IP/MPLS TE ÚTVÉDELEM ALAPFOGALAMAK

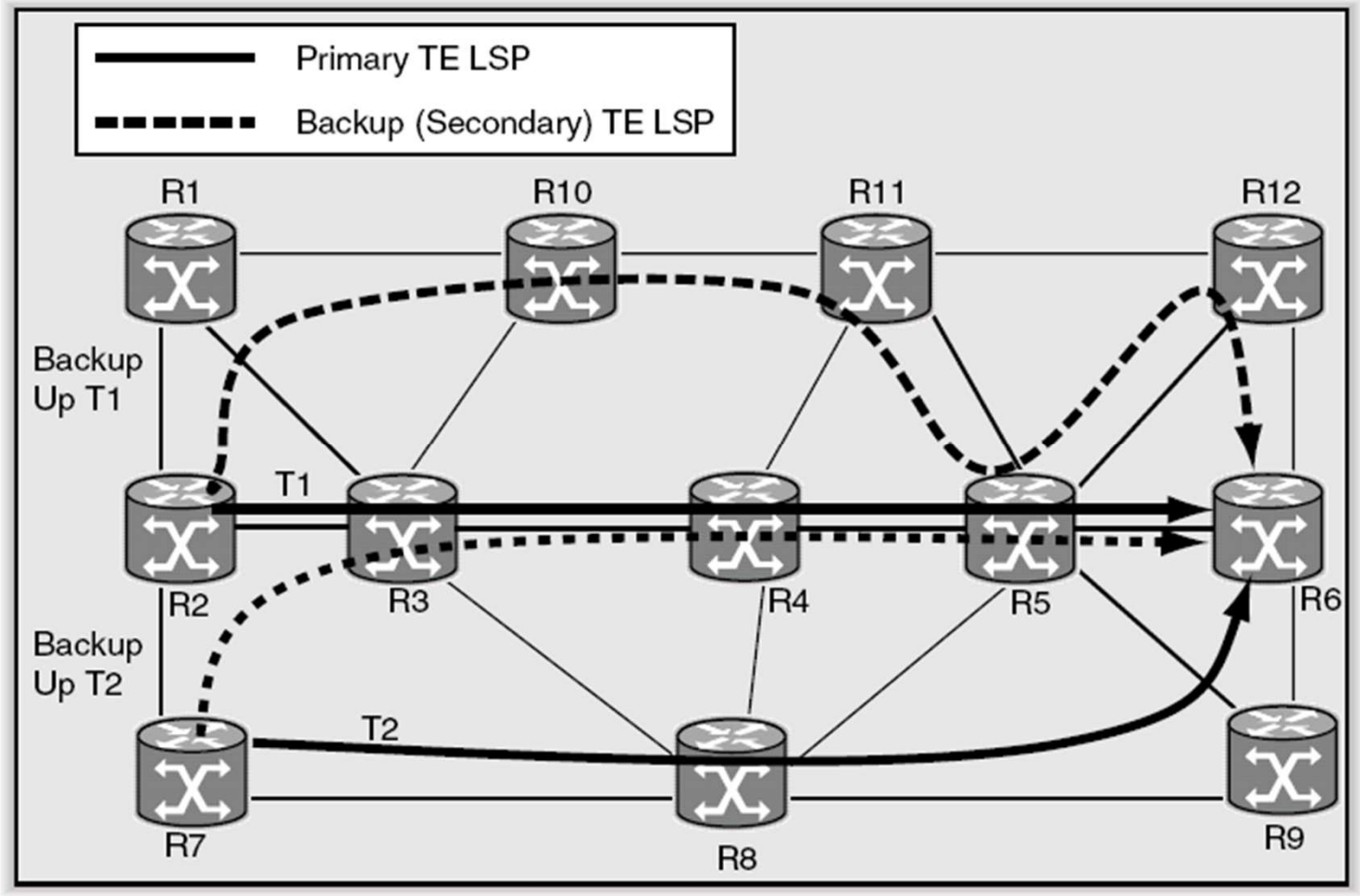


- PLR – Point of Local Recovery
- NHOP Recovery LSP – Next Hop Recovery LSP (végződés PLR-hez képest), pl. R2-R3 linkhiba esetén
- NNHOP Recovery LSP – Non Next Hop Recovery LSP (végződés PLR-hez képest), pl. R3 routerhiba esetén

SRLG-FÜGGETLEN LSP ÚTPÁR

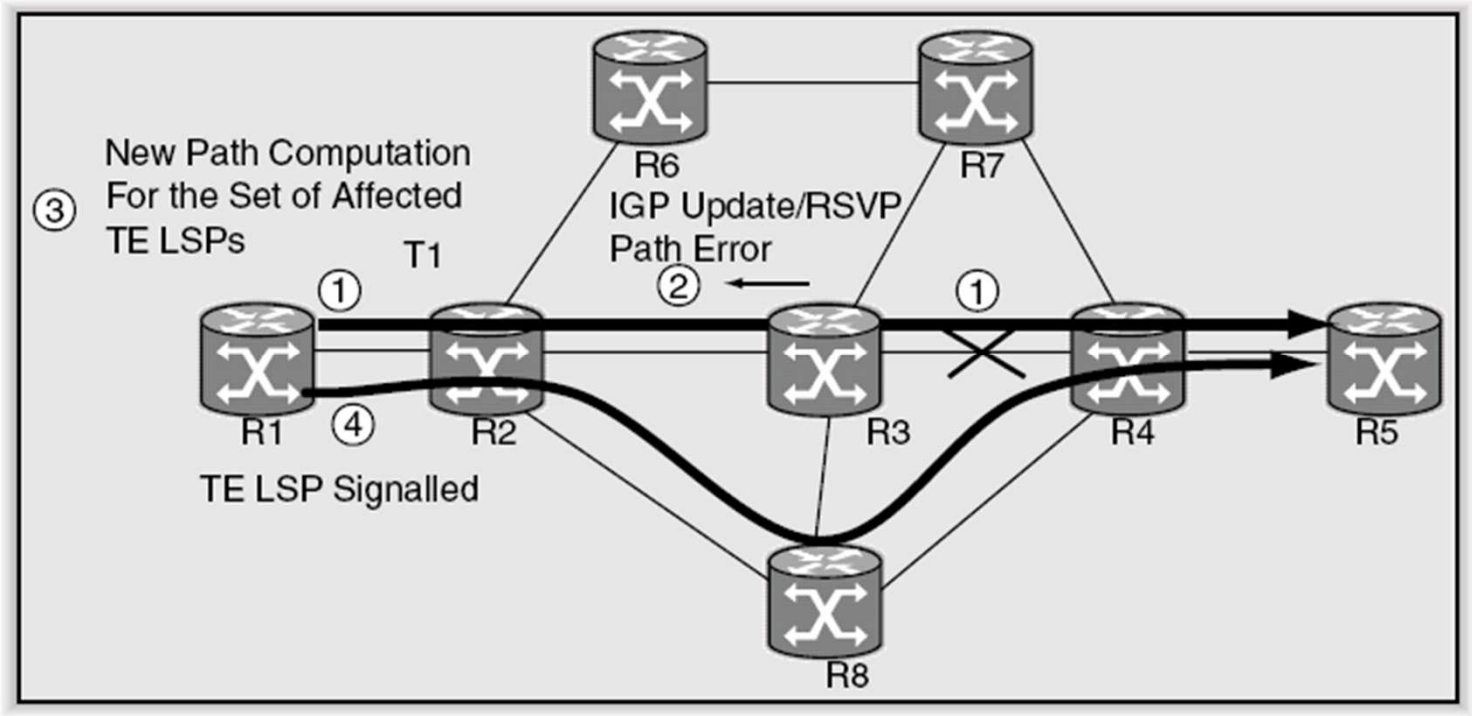


GLOBAL PATH PROTECTION

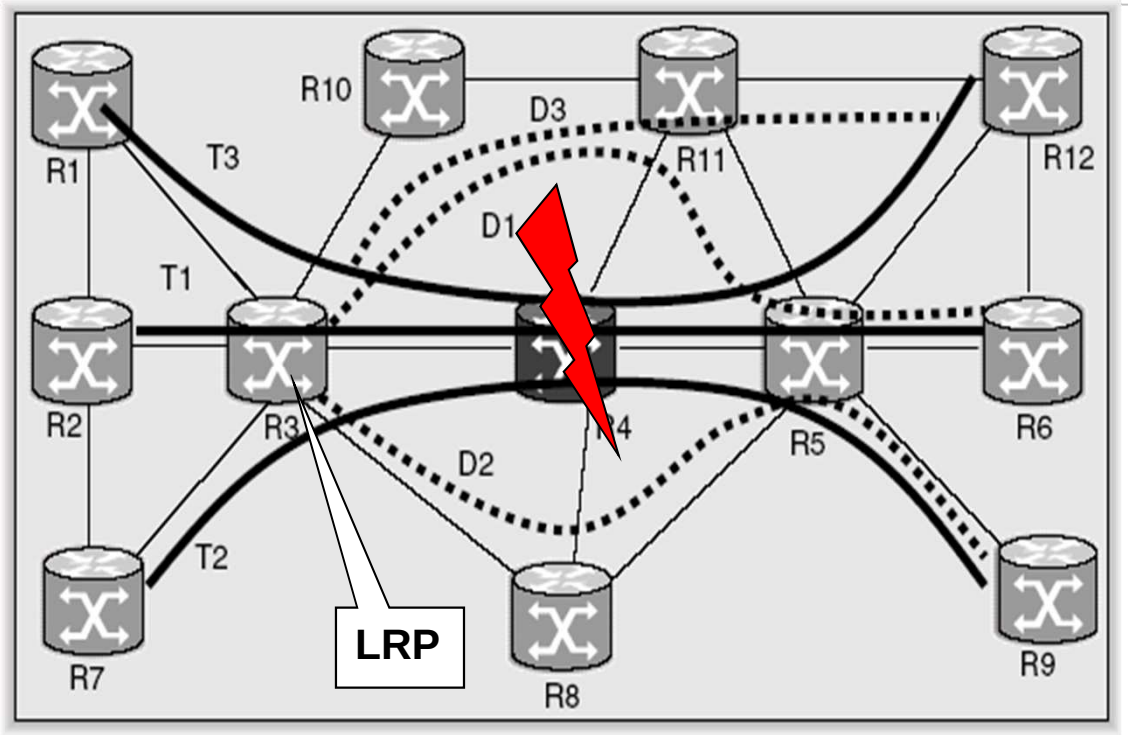


- 1:1 jellegű
- Ingress oldalon kell átkapcsolás (primary -> backup)
- folyamatosan monitorozni kell az utat (ingress-egress üzenetváltások az úton!)

GLOBAL DEFAULT RESTORATION

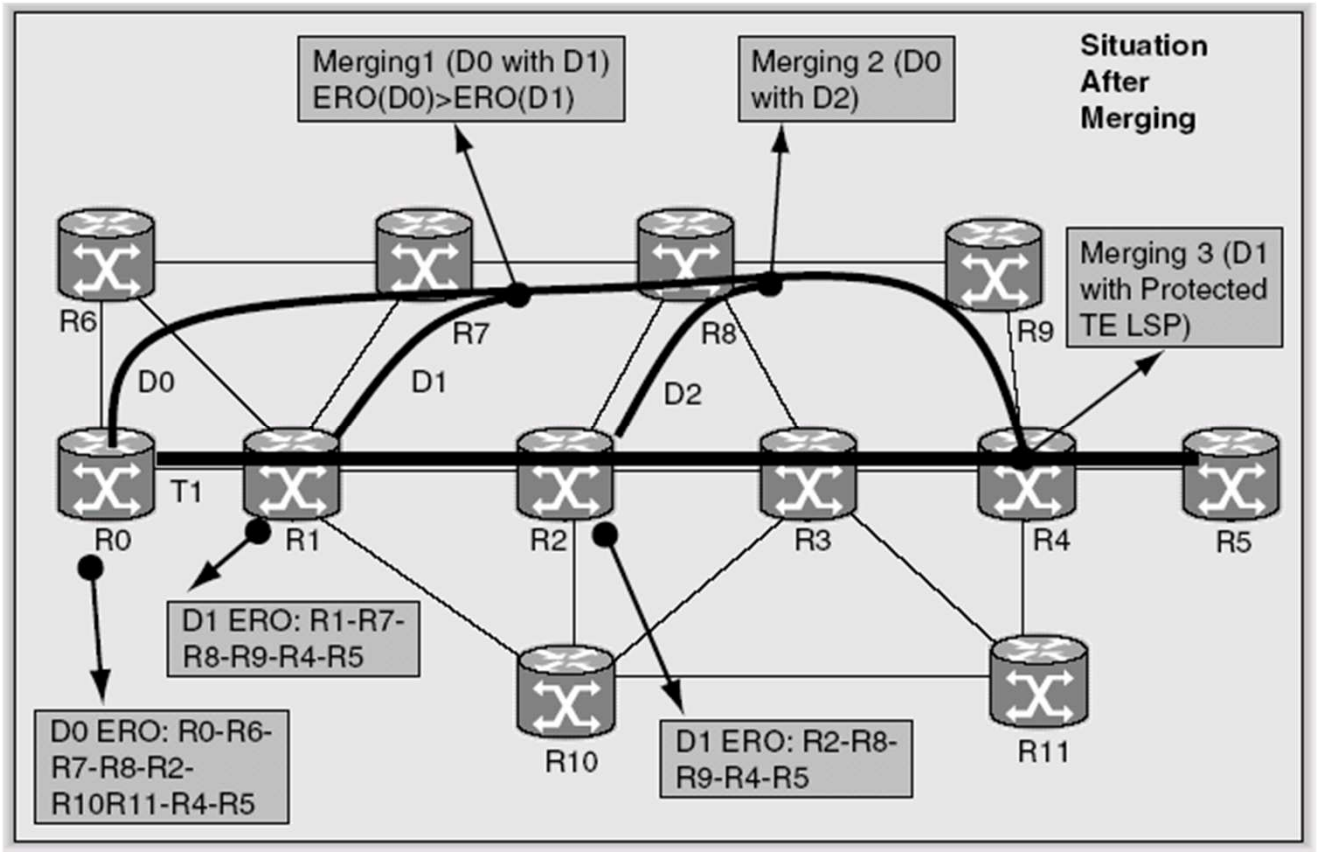


FAST REROUTE ONE-TO-ONE BACKUP



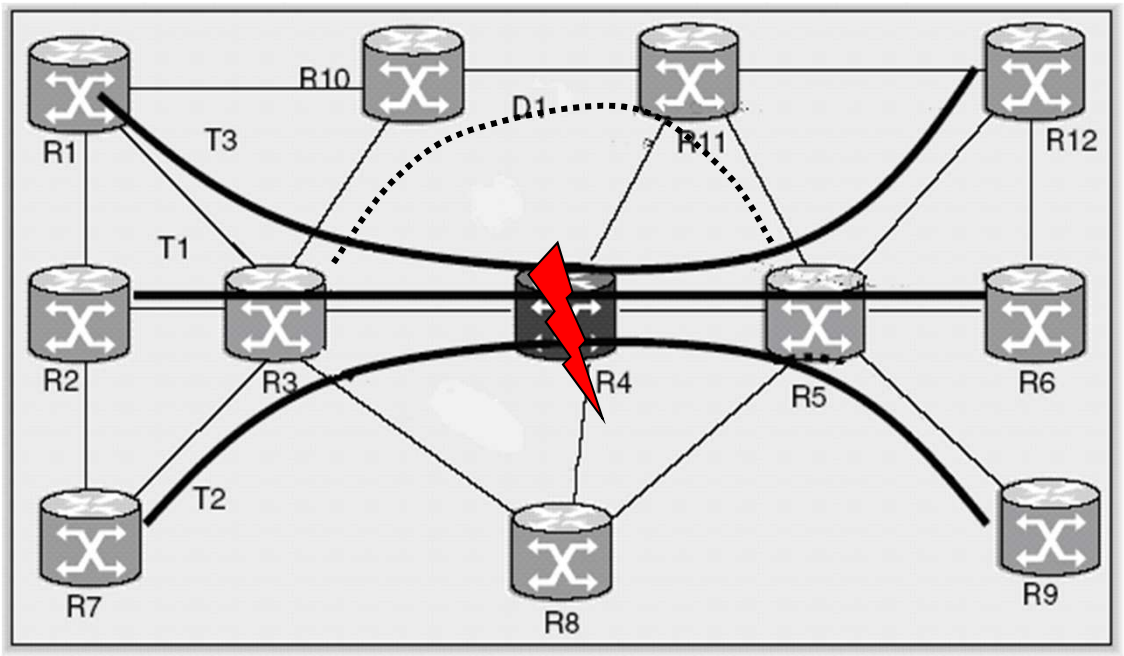
Út alapú – pontosabban útszakasz alapú – védelem:
• minden védett úthoz külön-külön tartalékutak előre konfigurálva (címkekiosztás)
• a helyreállítási pont és a végpont közti útszakaszra (egy-egy úthoz több LRP és tartalékút is megadható
LRP – Local Restoration Point – a védelmi átkapcsolás helye:
• ide kell eljuttatni a hibajelzést, és
• itt történik meg a forgalom tartalékútra terelése

FAST REROUTE ONE-TO-ONE BACKUP LSP MERGING



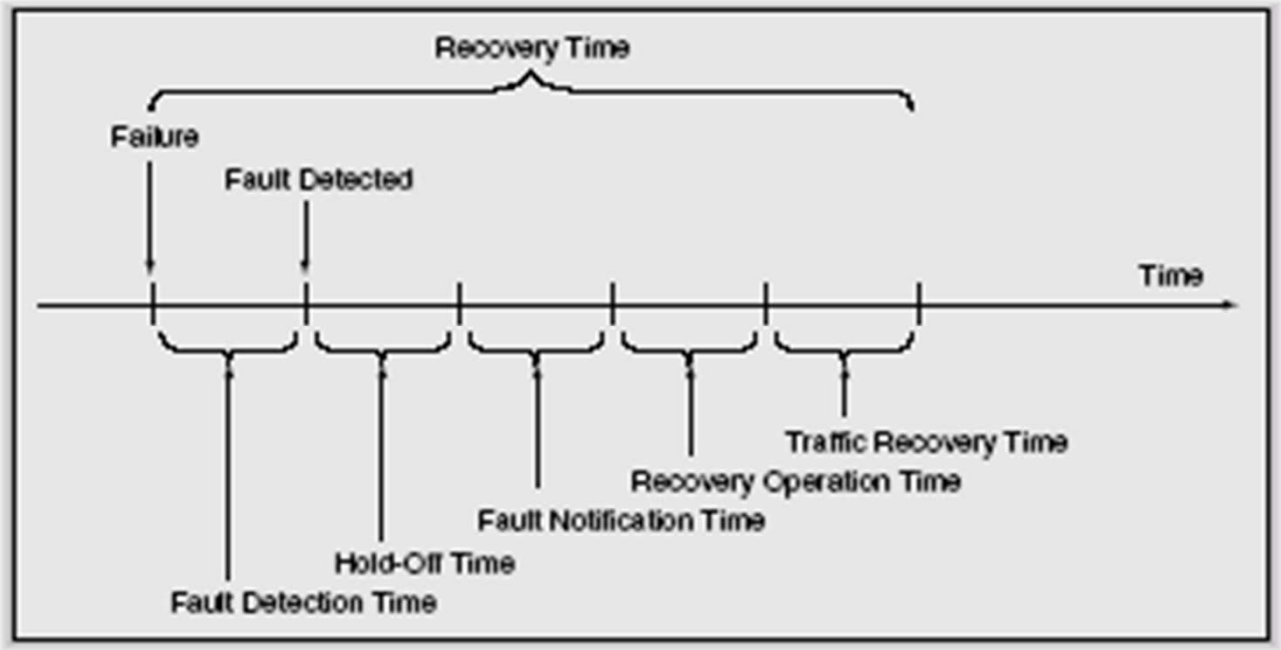
Azonos kiszolgálást igénylő és nyomvonalszakaszú utak összefogása hierarchikus címkéket alkalmazva, üzemeltetési megfontolás (kevesebb címke, kevesebb bejegyzés az úttáblában, kevesebb menedzselt állapot)

FAST REROUTE FACILITY BACKUP



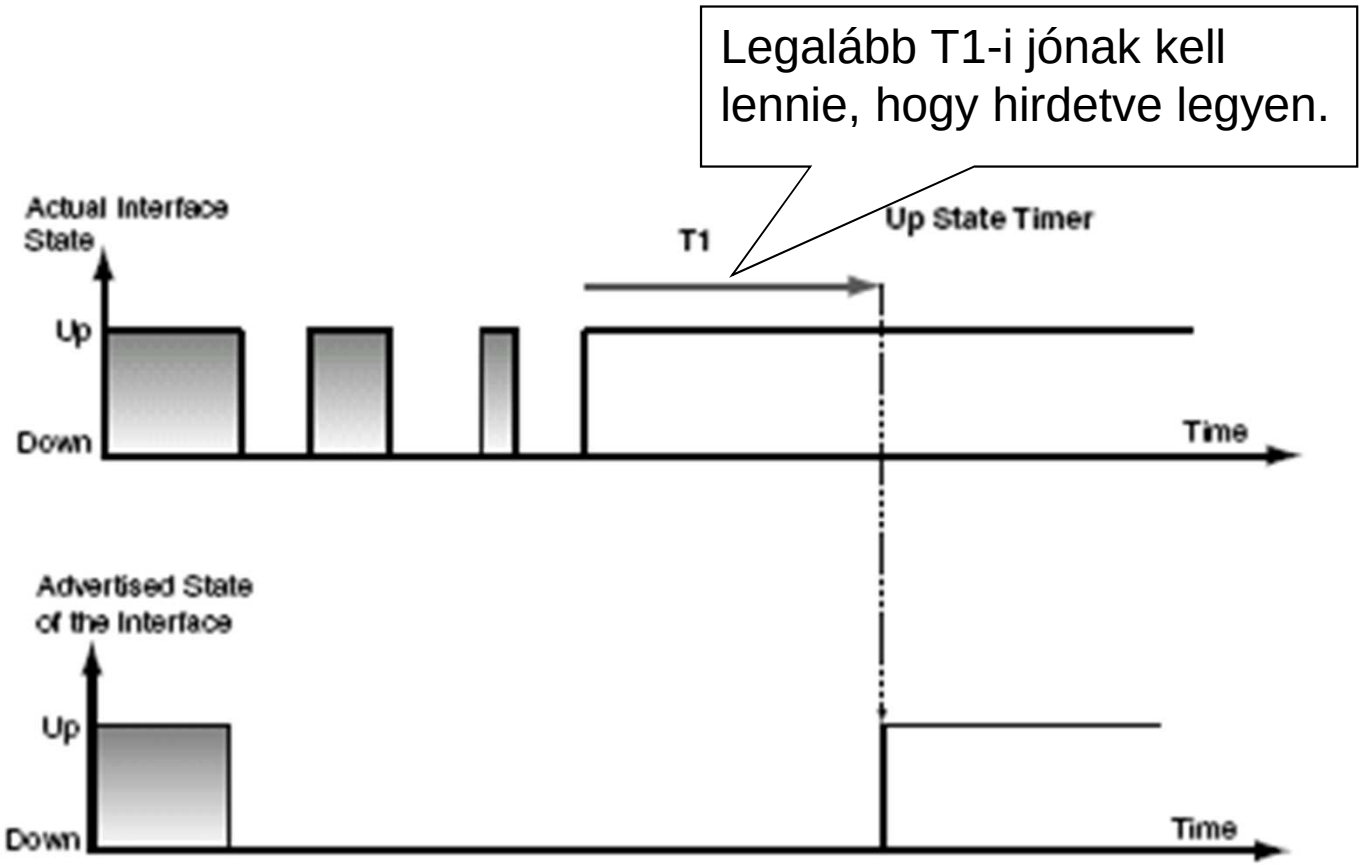
szakasz alapú védelem, közös tartalékszakasz a meghibásodás miatt megszakadt útszakasz kerülésére (több út közös szakaszára egy közös kerülő)
gyakorlatilag egy alagút a hibát határoló LSR-ek között hierarchikus címkéket alkalmazva
R3 a beavatkozó pont, R5 transzparensen továbbít (a kerülőúton érkező forgalom továbbítás is bekonfigurálva)

IDŐZÍTÉSEK



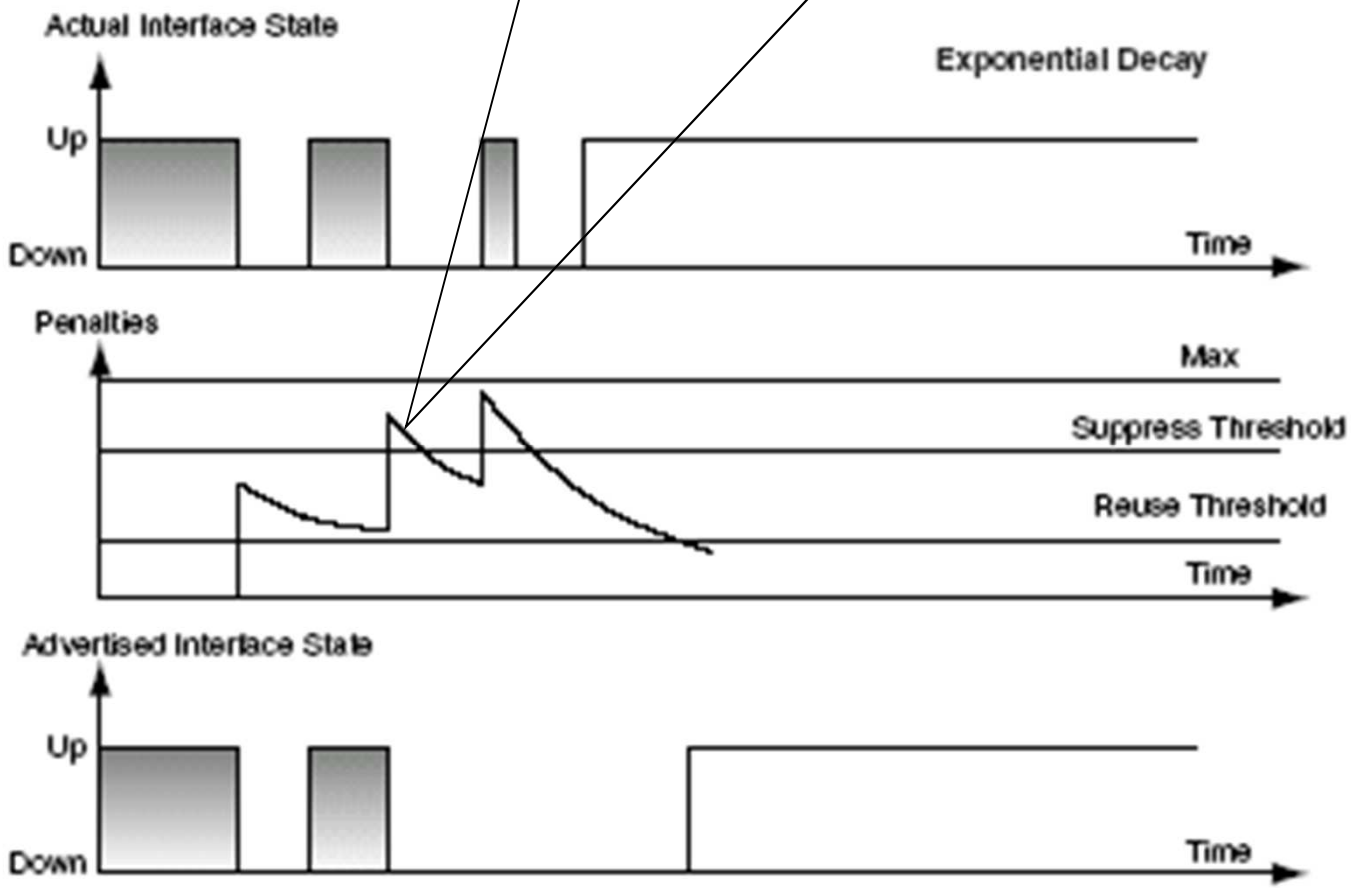
Fault Detection Time – a hiba érzékelésig eltelő idő
Hold-Off Time – várakozási idő a reagálás megkezdéséig (≥ 0) – pl. többrétegű védelem
Fault Notification Time – értesítések, riasztások kiküldése
Recovery Operation Time – védelmi mechanizmusok működése
Traffic Recovery Time – a transzportszolgáltatás helyreáll

UP STATE TIMER

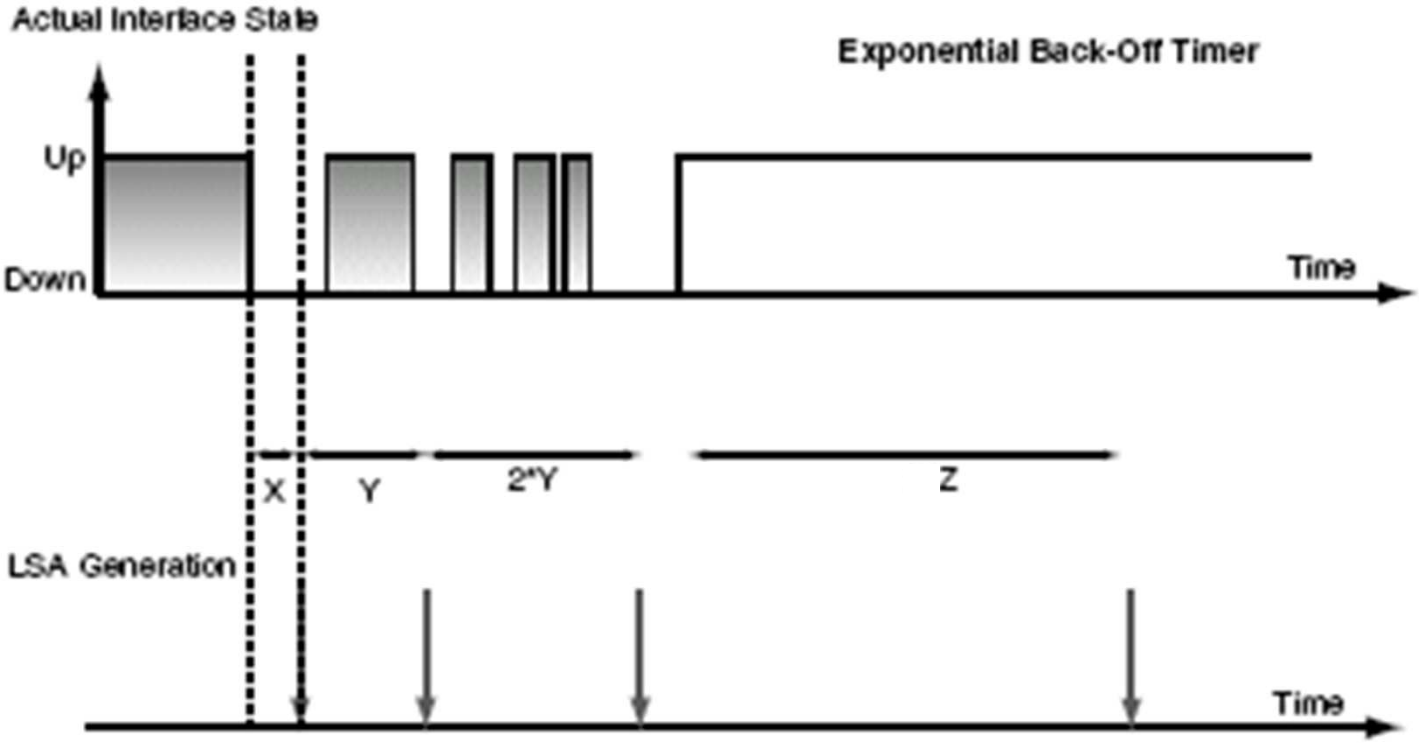


EXPONENTIAL DECAY

A gyors állapotváltozások növelik a büntetést, ha stabil állapot csökkenti. Amíg a büntetés egy adott küszöb alá nem csökken, nincs hirdetve a jó állapot.



EXPONENTIAL BACK-OFF



X: az első állapotváltozás ennyi várakozás után hirdethető
Y: a második után ennyit várunk
A további – n-edik - változások esetén $2^{(n-2)}Y$ amig Z-t el nem éri
Ha 2Z ideig nincs állapotváltozás az alapállapot áll vissza

DEPARTMENT OF
NETWORKED SYSTEMS
AND SERVICES

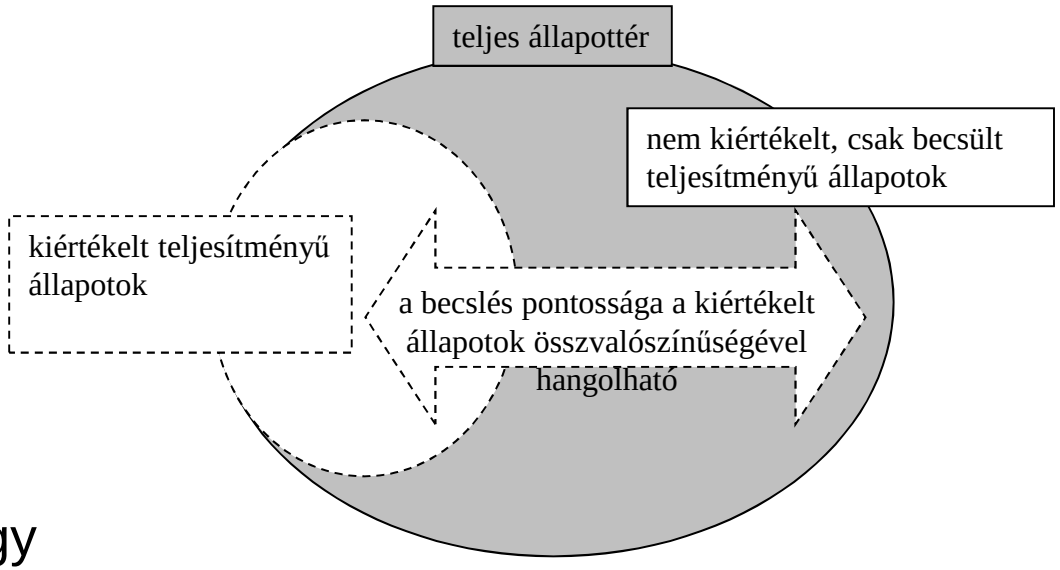
MODELLEZÉS, SZÁMÍTÁS 1
HÁLÓZATI SZOLGÁLTATÁSOK RENDELKEZÉSREÁLLÁSA

SZÁMÍTÁSI MÓDSZEREK

- Klasszikus megközelítés: Markov-modell
- Hálózatos sajátosság: az állapotok kiértékelése komplex (pl. routing adaptáció) lehet
- Gyakorlati esetekben nem skálázódó hálózati állapottér
- Becslések, korlátok
- Determinisztikus becslés: Li-Silvester módszer
- Statisztikus becslések:
  - Monte-Carlo módszer: kiértékelendő állapotok „vak” sorsolása, konvergencia?
  - Stratified Sampling: a hálózatról rendelkezésre álló tudás felhasználásával állapotcsoportokat (hibarétegeket) alakítunk ki, és ezekből sorsolunk kiértékelendő állapotokat, állapotcsoportok száma, mérete, csoportosítási kritérium? konvergencia! (MC-hez képest)

RENDELKEZÉSREÁLLÁS SZÁMÍTÁSA
Lee-Silvester becsléssel

- Nagy állapottér (~1000 kétállapotú, függetlenül meghibásodó hálózatelem)
- Becslés, aminek pontossága a ki nem értékelt állapotok összvalószínűségével arányos
- Védett hálózatokban (egy hiba elleni védelem) legalább a kéthibás állapotokat ki kell értékelni



DETERMINISZTIKUS KORLÁTOK (LI - SILVESTER MEGKÖZELÍTÉS)

$$\mathbf{E}g(\mathbf{y})_{\max} =$$

$$= \sum_{y \in Y_0} g(\mathbf{y}) \Pr(\mathbf{y}) + \sum_{y \in Y_c} g_{\max}(\mathbf{y}) \Pr(\mathbf{y}) =$$

$$= \mathbf{E}g(\mathbf{y})_{\min} + \sum_{y \in Y_c} \Pr(\mathbf{y})$$

- ***y*** : állapotvektor (kétállapotú hálózatelemek jó/rossz)
- Y_0: kiértékelt állapotok, Y_c: nem kiértékelt (csak becsült teljesítményű) állapotok,
- g(***y***): állapotvalószínűség
- Pr(***y***): teljesítmény az adott állapotban (pl. IP connectivity van út/nincs út), egyszerű becsült értékei min: nincs út-0, max: van út-1
- Pl. IP connectivity kiértékelés: az adott hálózati állapotban működőképes IP linkek felett routing adaptálása, eredménye alapján van út/nincs út

LI-SILVESTER BECSLÉS

Li-Silvester alsó és felső korlátok előállítása:

$$NPI_{min} = \frac{\sum_{\mathbf{y}\in\mathbf{Y_0}} Perf(\mathbf{y})\ p(\mathbf{y})}{Perf_{nom}} + \frac{\sum_{\mathbf{y}\in\mathbf{Y_c}} Perf_{min}\ p(\mathbf{y})}{Perf_{nom}}$$

$$NPI_{max} = \frac{\sum_{\mathbf{y}\in\mathbf{Y_0}} Perf(\mathbf{y})\ p(\mathbf{y})}{Perf_{nom}} + \frac{\sum_{\mathbf{y}\in\mathbf{Y_c}} Perf_{max}\ p(\mathbf{y})}{Perf_{nom}}$$

Egy egyszerű eset a veszteség meghatározása, amikor $Perf_{nom} = 1 = Perf_{max}$ és $Perf_{min} = 0$, ekkor:

$$NPI_{max} - NPI_{min} = \sum_{\mathbf{y}\in\mathbf{Y_c}} p(\mathbf{y})$$

STRATIFIED SAMPLING

- A hálózati komponenseket osztályokba soroljuk, ezek meghibásodását vizsgálva az állapottér hibavektorai is L db diszjunkt réteget alkotnak.
- Meghatározzuk az egyes rétegekben tartózkodás valószínűségét.
- Adott N össz mintaszám mellett definiáljuk az egyes rétegekből venni kívánt minták számát.
- Rétegenként a Monte Carlo módszert alkalmazva kisorsoljuk a megfelelő számú mintát, és ezek alapján megbecsüljük a feltételes várható értékeket.
- A rétegvalószínűségek és a rétegenkénti feltételes várható értékekre vonatkozó becslések alapján kiszámítjuk a teljes hálózatra vonatkozó becslést.

DEPARTMENT OF
NETWORKED SYSTEMS
AND SERVICES

BERENDEZÉSEK HIBATŰRÉSE

MIRŐL VOLT SZÓ EDDIG?

- szolgáltatások életciklusa
- rendelkezésreállási alapfogalmak, követelmények
- védelmi alapsémák (pont-pont relációkra), példák technológiai megvalósításokra
- hálózati szintű vonatkozások (több technológiai réteg, működési, együttműködési elvek)
- rendelkezésreállás modellezési, számítási módszerek

- ennek során a berendezéseket egy-két jellemzővel (meghibásodás, javítás, rendelkezésreállás, kiesési időarány) leírható alapegységnek tekintettük

Honnan, hogyan származtathatók a berendezések alapjellemzői?

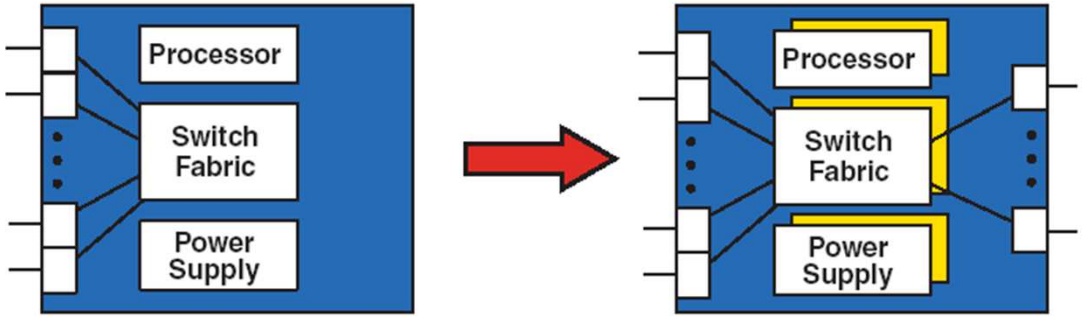
BERENDEZÉSEK HIBATŰRÉS

- hw és sw komponensek, meghibásodásuk berendezés szintű (minden támogatott szolgáltatást érintő) vagy részleges (csak egy/néhány szolgáltatást érintő)
- a hibatűrés javításának gyártástechnológiai, architekturális és üzemeltetési vonatkozásai is vannak
- architekturális: a kritikus komponensek (pl. vezérlés, tápegység, hűtés) legyenek redundánsak
- két példa: switch, router
- berendezések hibatűrő összekapcsolása:
  - port duplication (1:1 séma):
  - link aggregation - Cisco: EtherChannel (túlméretezés, független hordozó komponensek):
- hálózatrészek hibatűrő összekapcsolása
  - IP subnet csatlakoztatása redundáns uplinkekkel (dual homing, HSRP)

SZOLGÁLTATÓI KATEGÓRIÁJÚ L2 SWITCH

Redundáns kapcsolóarchitektúra

- HW redundancy:
  - Power
  - switch fabric
  - Fans
  - …etc.
- SW-based resilience technologies:
  - VRRP
  - HPS/HPR
  - Link Layer Resilience
  - Path Protections
  - …etc.

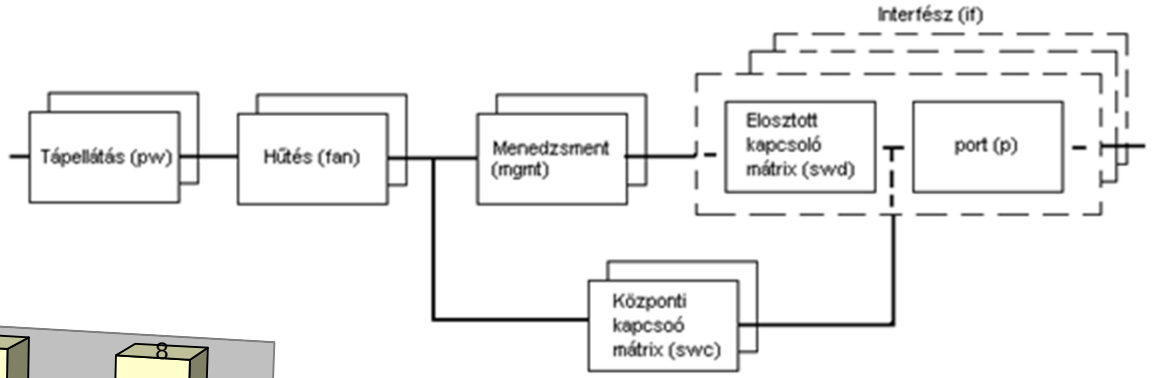


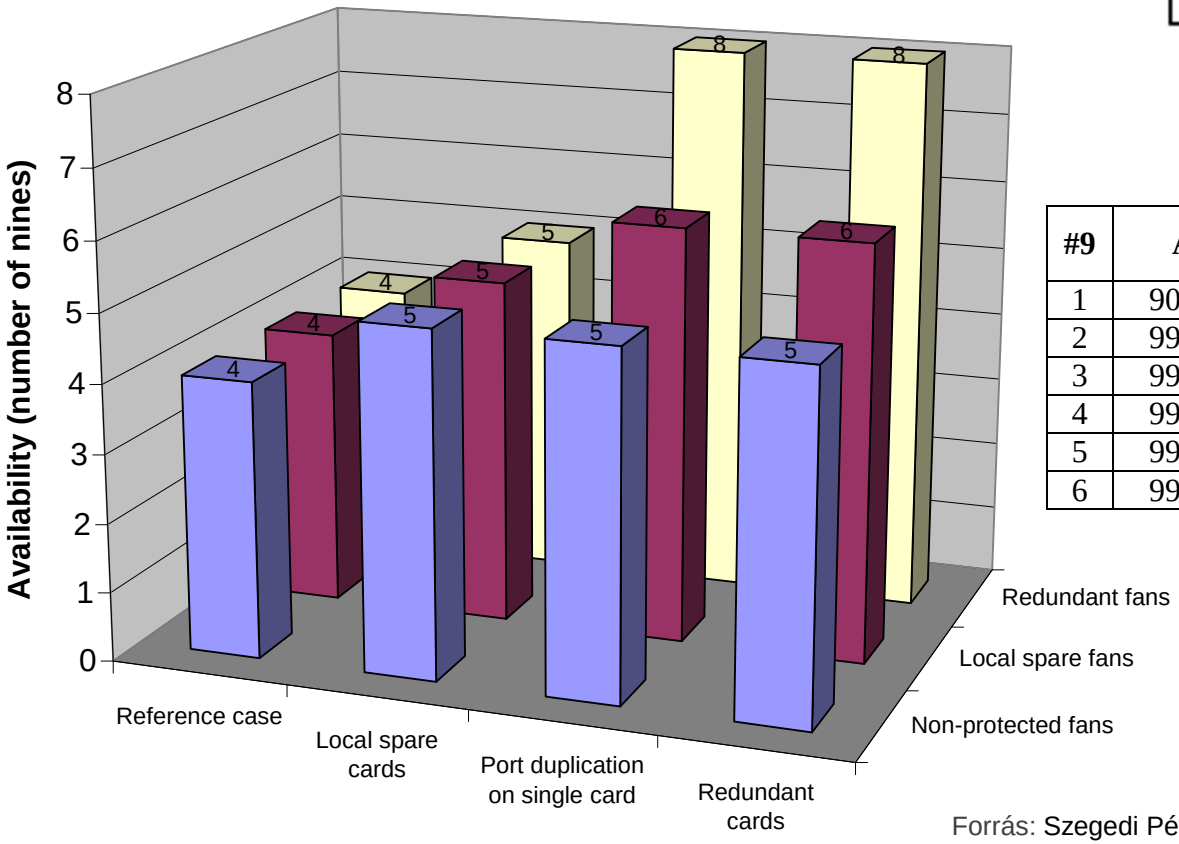
Enterprise Ethernet | Carrier-Class Ethernet

Resilience Technology	Typical Restoration Time
Software Resilience	
Virtual Router Redundancy Protocol	5 to 10 seconds
Hitless Protection System	5 to 10 seconds
Hitless Protocol Restart	3 to 5 seconds
Link-layer Resilience	
Rapid Spanning Tree	2 to 3 seconds
Rapid Ring Spanning Tree	0.5 to 1 second
Path Protection	
MPLS fast failover LSPs	< 50 milliseconds
MPLS RSVP-TE Fast Reroute	< 50 milliseconds
Spatial Replacement Protocol/RPR	< 50 milliseconds
Hardware Redundancy	
Power, switch fabrics, fans, CMs	< 50 milliseconds

Forrás: Szegedi Péter: Ethernet kapcsolók megbízhatósága, HIT kézirat, 2005

CARRIER ETHERNET L2 KAPCSOLÓ RENDELKEZÉSREÁLLÁSA

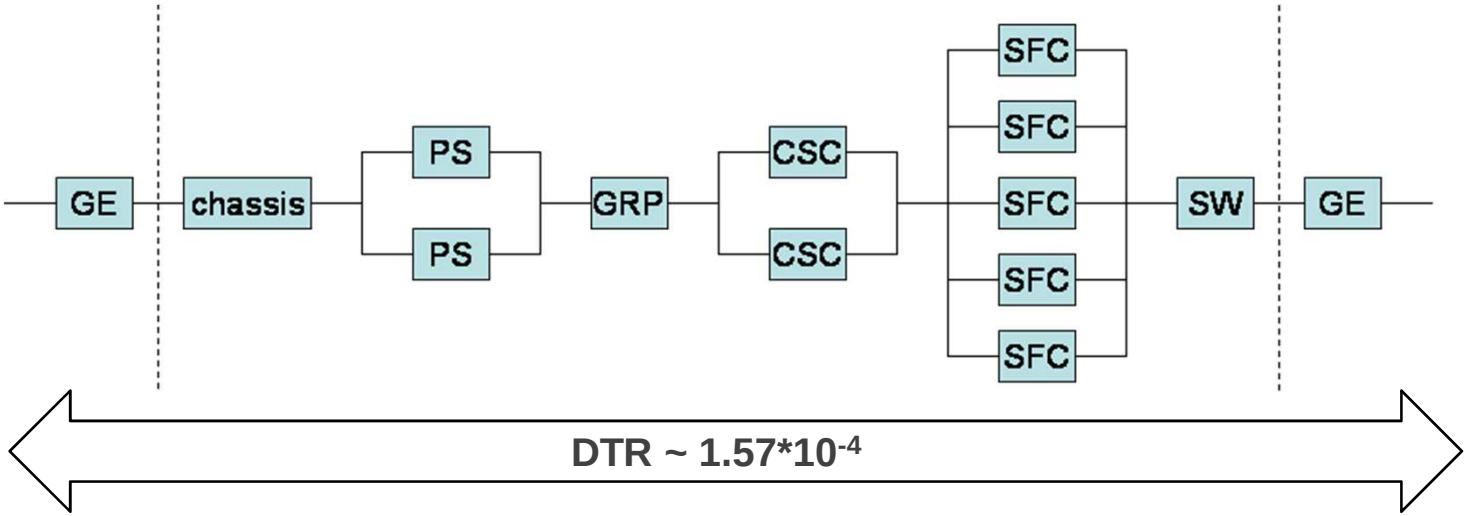




#9	A (%)	Éves szintű várható kiesés	Megjegyzés
1	90.0000%	36 nap 12 óra	-
2	99.0000%	87 óra 36 perc	Kommersz eszközök
3	99.9000%	8 óra 46 perc	Nem kritikus alkalmazások
4	99.9900%	52 perc 33 mp	Adatközpontok
5	99.9990%	5 perc 15 mpc	Megbízható rendszerek
6	99.9999%	31,5 mp	Kiemelten megbízható rsz.

Forrás: Szegedi Péter: Ethernet kapcsolók megbízhatósága, HIT kézirat, 2005

ROUTER RENDELKEZÉSREÁLLÁSA



.	DTR
chassis	$1.5 * 10^{-5}$
GRP	$2.9 * 10^{-9}$
PS	$1.4 * 10^{-5}$
CSC	$2.3 * 10^{-5}$
SFC	$1.2 * 10^{-5}$
GE	$4.1 * 10^{-5}$
SW	$6.0 * 10^{-5}$

- ház (**chassis**): MTBF=398788h,
- route processzor (**GRP**): duplázott redundáns elem, MTBF=188768h processzoronként, amelyből a route processzor párra MTBF≈283152 (exponenciális viselkedést feltételezve), valamint MTTR=3s, ha feltételezzük, hogy a meghibásodást követő $MTTR_s$ időn belül nem következik be újabb hiba (ennek valószínűsége elhanyagolható), és a rendszer automatikusan átkapcsol a rendelkezésre álló tartalék processzorra,
- tápegység (**PS**): duplázott, redundáns elem, MTBF=414931h,
- clock scheduler kártya (**CSC**): a kapcsolómátrix komponense, duplázott, redundáns elem, MTBF=256470h,
- switch fabric kártya (**SFC**): a kapcsolómátrix komponense, ötszörözött, redundáns elem, MTBF=492917h,
- GE modul (**GE**): interfész kártya, nem redundáns, MTBF=147248h,
- operációs rendszer (**SW**): alapján az MTBF=100000h becslés adható meg.

Forrás: Pándi Zsolt: IP routerek megbízhatósági modellezése, HIT kézirat, 2005

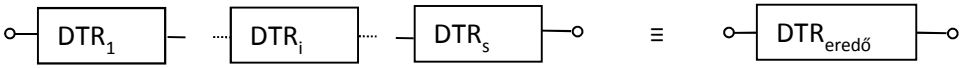
DEPARTMENT OF
NETWORKED SYSTEMS
AND SERVICES

MODELLEZÉS, SZÁMÍTÁS 2: SOROS-PÁRHUZAMOS SZERKEZETŰ RENDSZEREK RENDELKEZÉSREÁLLÁSA

MODELLEZÉS, SZÁMOLÁS

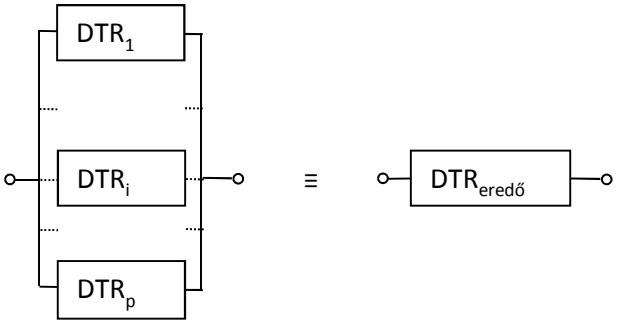
- egyszerű alapmodellek (soros, párhuzamos), elemi kiértékelési lépések és összefüggések
- korlátozott alkalmazhatóság (rendszerkomplexitás, skálázódás, hatékony algoritmizálás), de pl. „követelmény-szétosztás”-ra (komplex funkcionális komponensek soros modellje) egyszerűen használható

Soros rendszer A_{soros}=1-DTR_{soros}: $DTR_{soros} = 1 - \prod_{i=1}^{s}(1 - DTR_i)$

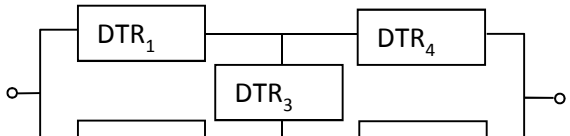


Párhuzamos rendszer

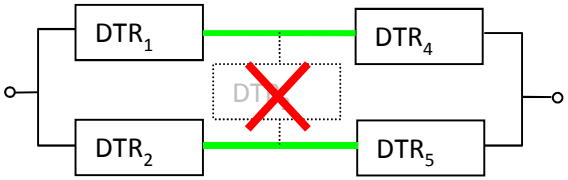
$A_{parhuzamos}$=1-$DTR_{parhuzamos}$: $DTR_{parhuzamos} = \prod_{i=1}^{p} DTR_i$



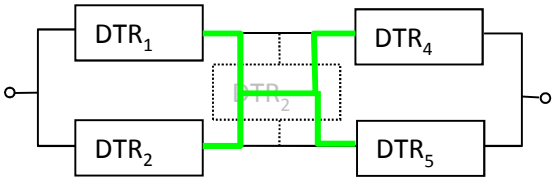
Soros-párhuzamos részekre közvetlenül nem bontható összetett rendszer



DTR3 — Dekompozíció teljes valószínűség alapján — 1-DTR3

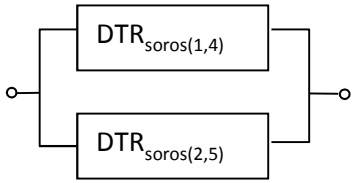


≡

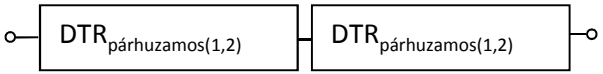


≡

DTR3



1-DTR3



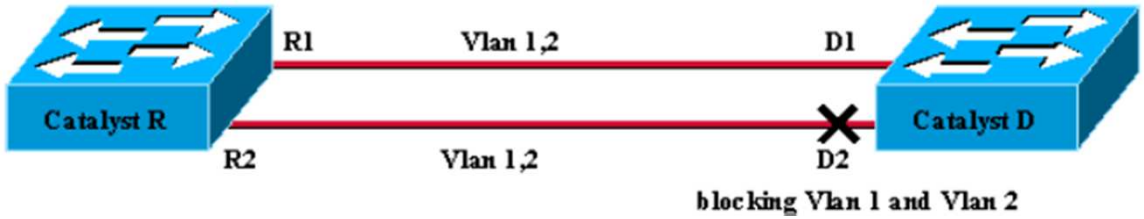
Soros-párhuzamos részekre közvetlenül nem bontható összetett rendszer:

$DTR_{eredő} = DTR_3 * [1-(1-DTR_1)*(1-DTR_4)] * [1-(1-DTR_2)*(1-DTR_5)] + (1-DTR_3) * [1-(1-DTR_1 * DTR_2)*(1-DTR_4 * DTR_5)]$

DEPARTMENT OF
NETWORKED SYSTEMS
AND SERVICES

BERENDEZÉSEK, HÁLÓZATRÉSZEK ÖSSZEKAPCSOLÁSA

BERENDEZÉSEK ÖSSZEKAPCSOLÁSA

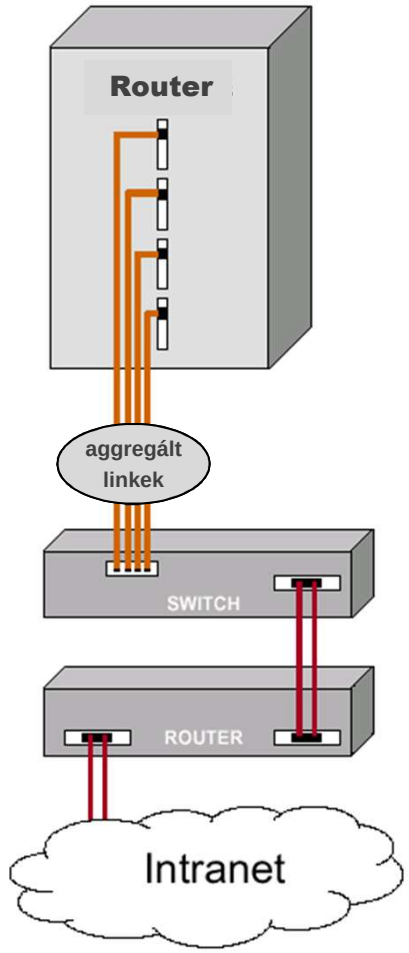


Port duplikálás

- Kapcsolók közötti linkek redundanciája.
- Meghibásodás esetén egyszerű átkapcsolás

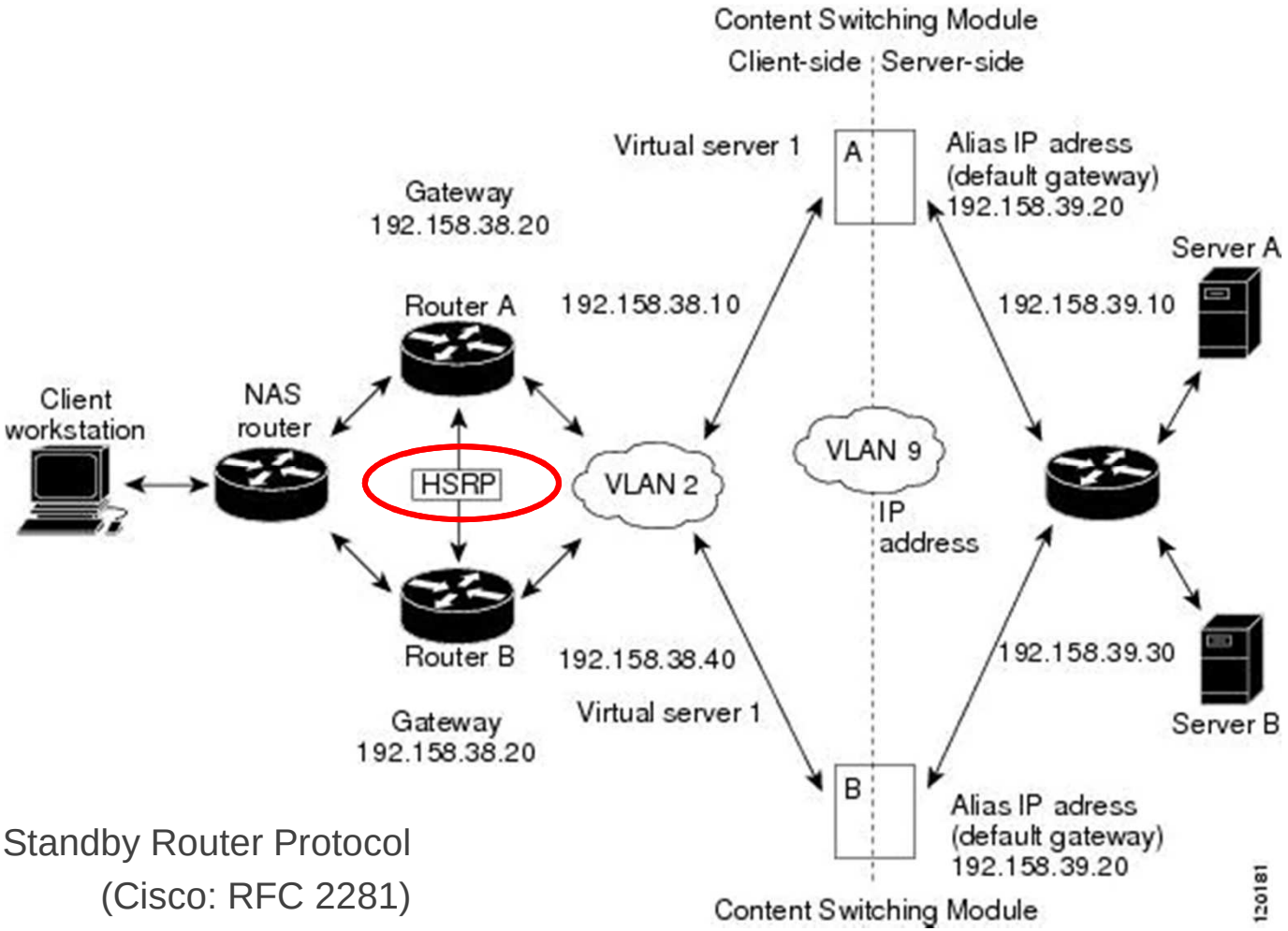
Link aggregálás

- 802.1ab Link Aggregation Control Protocol (LACP)
- Finomabb skálázás
- Hibatűrő képesség növelése
- De: szolgáltatási képesség korlátok (hasonlóan, mint IP ECMP esetén: flow és nem datagram szintű forgalomszétosztás)



Ha a két (vagy több) link szállítása (opt. csat., kábelnyomvonal) függetlenül meghibásodó, akkor alacsonyabb szintű hibák ellen is védelmet nyújt)

IP ALHÁLÓZAT REDUNDÁNS CSATLAKOZTATÁSA



HSRP: Hot Standby Router Protocol
(Cisco: RFC 2281)

Forrás: https://www.cisco.com/c/en/us/td/docs/interfaces_modules/services_modules/csms/1-1-1/configuration/guide/redun.html#wp1002608

DEPARTMENT OF
NETWORKED SYSTEMS
AND SERVICES

ÖSSZEFOGLALÁS

ÖSSZEFOGLALÁS: HÁLÓZATI HIBÁK HATÁSA A SZOLGÁLTATÁSI KÉPESSÉGEKRE

- a szolgáltatási követelmények alkalmazásfüggőek
- valós hálózatelemek, véges meghibásodási valószínűséggel
- meghibásodások hatása: csökkenő erőforrás-mennyiség -> változatlan forgalommennyiség mellett degradációt eredményezhet
- hibahatások mérséklése, kiküszöbölése: a javítás mellett redundanciák szükségesek is (szerkezeti, kapacitás)
- hibatűrő alapsémák, eltérő hatékonyságú technológiai megvalósíthatóság
- üzemeltetési vonatkozások (tartalékeszközök, gyors javítás, hibamenedzsment)

- különböző modellezési módszerek, számítási modellek
- az alapinformációk (részegységek, berendezések jellemzői) műszakilag és tapasztalatilag megalapozott *becslések*
- modellezési eredmények gyakorlati alkalmazhatósága (elsősorban megoldások összehasonlíthatósága, és nem abszolút jellemző)
- gyakorlati mérnöki megközelítés: mit feltételezhetünk/tudhatunk, mire használható, *tudatos* worst case szemlélet

AJÁNLOTT OLVASNIVALÓK

- Jereb László, Telek Miklós: Megbízhatóság modellezés, BME HIT jegyzet, 1998, tárolt változat
- ***Farkas György, Gondolatok a megbízhatóság megbízhatóságáról, Elemző tanulmány, BME HIT kézirat, 2006. június,*** *tárolt változat*
- L Jereb, T Jakab, F Unghváry, Availability Analysis of Multi-Layer Optical Networks, JOURNAL OF OPTICAL NETWORKING 3: pp. 84-95. (2002), tárolt változat
- Tivadar Jakab, Gábor Horváth, Éva Csákány, Mrs László Konkoly, Availability and QoS Performance Evaluation of Public Service IP Networks, In: Proceedings of 2007 International Symposium on Performance Evaluation of Computer and Telecommunication Systems. , San Diego, US, 2007.07.16-2007.07.18., pp. 1-10. (Proceedings of 2007 International Symposium on Performance Evaluation of Computer and Telecommunication Systems) , tárolt változat
- Szegedi Péter: Ethernet kapcsolók megbízhatósága, BME HIT kézirat, 2005
- Pándi Zsolt: IP routerek megbízhatósági modellezése, BME HIT kézirat, 2005
- Pándi Zsolt, Mitterer Ádám Ákos, Bencsik Gergely: Hálózat-megbízhatósági adatok statisztikai elemzése, BME HIT kézirat, 2005

FOLYTATÁS

- Hálózatmenedzsment
- Hálózatvirtualizáció
- 5G architektúra
- alkalmazási esettanulmányok (5G verticals és backhaul, V2x bakhaul)
- WiFi 6 (802.11ax) – ha befér

- javasolt vizsgaidőpontok
  - hétfő, 2021. május 31. 10-12
  - hétfő, 2021. június 7. 10-12
  - hétfő, 2021. június 14. 10-12
  - hétfő, 2021. június 21. 10-12
- szóbeli vizsga (MS Teams), választott témakör, saját prezentáció alapján, egyeztetett témakör és időpont
- a Neptunban meghirdetett időpontok a jegybeíráshoz