Tartalomjegyzék

Bevezetés

Diplomamunkám témája első hallásra talán túl elcsépeltnek tűnhet, ezért szeretném már az elején tisztázni, a célom az, hogy szigorúan a jelenhez kapcsolódva elemezzem, és mutassam be az új követelményeket a megjelenő új technológiákat és a szolgáltatók és az ügyfelek közti megváltozott viszonyt. Miben változtak meg az ügyfelek követelményei? Röviden, és frappánsan összefoglalva: nem sokban. Ahogy eddig, a továbbiakban is évről évre elvárják az olcsó, biztonságos, megbízható és az ügyfél specifikus igényeihez igazodó, kevés leállással járó szolgáltatást. Így a szolgáltatók szempontjából egy hálózat fenntarthatósága és fejlesztése abban rejlik, hogyan lehet évről évre - jobb esetben az ügyfelek számának növekedése mellett - folyamatos minőségjavulást elérni. Ilyen tendenciák mellett a régi távközlési technológiák fokozatosan kiszorulóban vannak, és a helyükre a városokban és nagyobb régiókban manapság már alapszolgáltatásként elvárt nagy sebességű optikai (SONET/SDH, OTN) és Ethernet technológiák kerülnek fejlesztésre és kiépítésre.

A szolgáltatók számára az optikai és Ethernet vonalak előnye, hogy nagy teljesítményükkel, megbízhatóságukkal és üzemeltetési egyszerűségükkel képessé teszik a szolgáltatókat arra, hogy megfeleljenek az ügyfelek jövőbeni sávszélességbeli elvárásainak. Olyan hálózatra van szükség, mely a jövőben is képes lesz az ügyfelek növekvő forgalmát stabilan kezelni, elfogadható átviteli sebességet nyújtani, az ügyfél alkalmazásainak egyre kevésbé hibatűrő forgalmának egyre több különböző forgalomi prioritást rendelni. De az ügyfelek szempontjából jelenlegi nagy hátrányuk, hogy egy 400Gbit/s-os forgalmú interfészen nagyobb kárt tud okozni egy egyperces leállás, mint egy E3-as vonalon egy 5 perces, így a szolgáltatás megbízhatósága a sávszélesség növekedése mellett csökken, így kézenfekvő, hogy javítani kell a ma használt hibakeresési, detektálási, és megoldási folyamatokat.

A szolgáltatók szempontjából sürgető probléma, hogy miként lehet a hibakeresést a megjelenő új technológiákkal folyamatosan hatékonyan végezni, és idővel továbbfejleszteni? Ha a teljesítmény romlásakor kezdik el mérni a teljesítményt, akkor már túl nagy lehetőséget adnak a hiba bekövetkezésének valószínűségére. Így egy esetleges kiesés bekövetkeztekor a felkészületlenség

miatt túl nagy terhelés nehezedhet a szakemberekre, fel nem osztható konfliktus alakulhat ki, és gyakran egymásra mutogatva, nem egyenes vonalon halad előre a hiba megoldása. Ezért célszerű felosztani a teljesítménymutatókat, és munkafázisokat az egyes csoportok között, és ezek szerint kialakítani a munkahatásköröket.

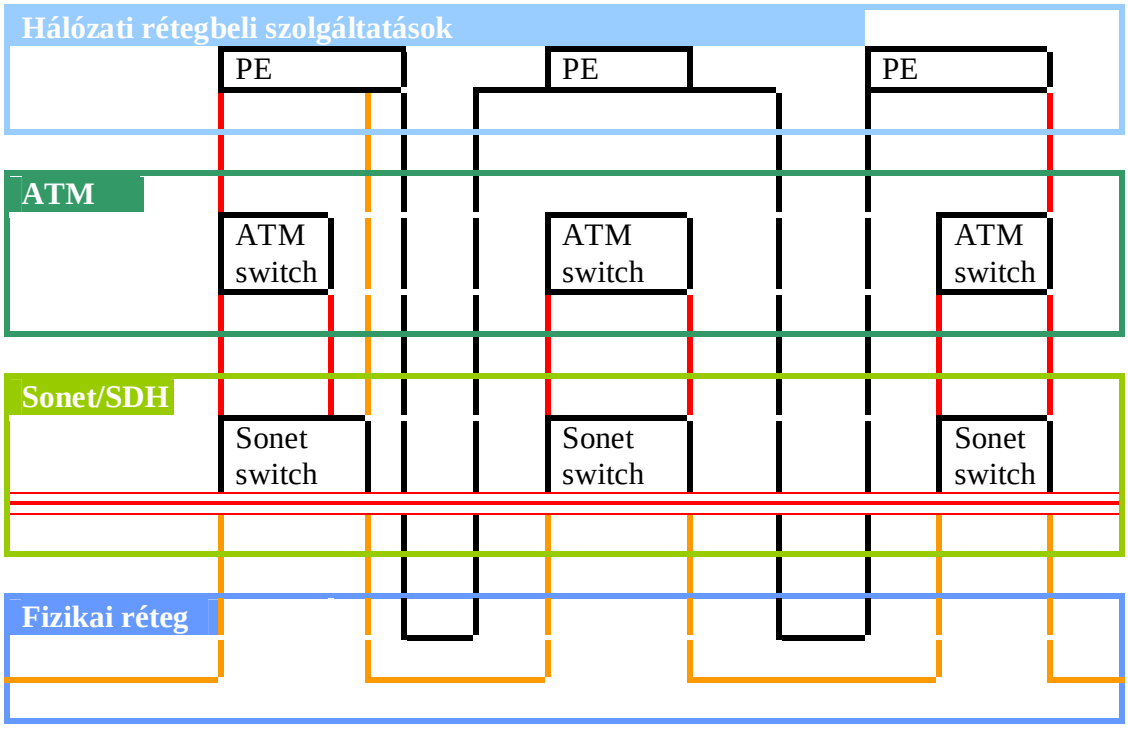
A szolgáltatóknak azt a célt kell kitűzniük, hogy proaktív szemléletmód mellett valós idejű teljesítménymonitorozást valósítsanak meg, és már a probléma bekövetkezésekor meglévő teljesítménymutatókból tudjanak hibát elemezni, csökkentve ezzel a nem a hiba konkrét megoldásával töltött időt. További cél: ha teljesítményszint egy még elfogadható küszöb értékre süllyed, akkor időben értesüljenek róla, hogy meg tudják oldani még mielőtt az elfogadható szint alá süllyedne, elkerülve így a szolgáltatás kiesését. Ehhez az eddigi teljesítménymutatók mellett figyelembe kell venni az új ügyfél alkalmazások megjelenésével az egyre specifikusabb és kevésbé hibatűrő forgalom megjelenését, így a velük együtt megjelenő új teljesítménymutatók implementálását a teljesítményfigyelő rendszerekbe.

Dolgozatomban szeretném bemutatni a Mutiprotocol Label Switching – Transport Profile-t (MPLS-TP) és a vele együtt megjelenő protokollokat és szabványokat. Részletesen kitérek a jövőbeli hálózatok követelményeire, valamint arra, hogy ezekre a követelményekre a szolgáltatók hogyan készíthetnek megoldásokat. Ezt a problémakört nyolc részre tagoltan kívánom bemutatni. Az első részben összefoglalom a csomagkapcsolt hálózatok fejlődését az MPLS és az MPLS-TP megjelenéséig. A második részben az MPLS-TP-ről szeretnék átfogó leírást adni. A további részekben kifejtem a Traffic Engineering-et, a Generalized Multiprotocol Label Switching-et, a Resource Reservation Protocol Traffic Engineering-et, az MPLS-TP hálózati referencia modelljét, majd egy részletes Operations, Administration, and Maintenance eszközgyüjteményt mutatok be. A dolgozatom befejezésében szeretném összegezni, és egy statisztikai felméréssel igazolni az MPLS-TP és az újgenerációs hálózatok irányvonalának létjogosultságát.

1 Multiprotocol Label Switching – Transport Profile

1.1 Csomagkapcsolt hálózatok

A csomagkapcsolt hálózatok történeti áttekintésében először szeretném megemlíteni az Mutiprotocol Label Switching-et megelőző két legelterjedtebb szolgáltatást, az ATM[1]-et és az SONET/SDH[2]-t, melyeknek, annak ellenére, hogy már kiszorulóban vannak, a mai hálózatok kialakulásában jelentős szerepük és hatásuk volt. Ezek különböző technológiák, ezért különböző szaktudást igényel az üzemeltetésük, így a kiszorulásukkal együtt az üzemeltetési költségük is egyre magasabb.



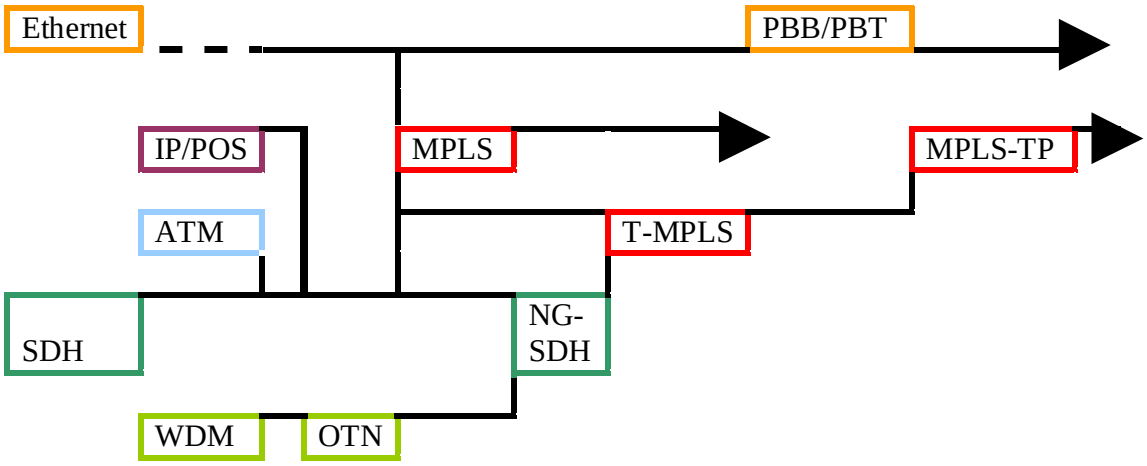
1. Rétegezett csomagkapcsolt hálózati modell

[1] Asynchronous Transfer Mode: egy cellakapcsolt hálózati technológia
[2] A Synchronous Optical Networking (SONET) és a Synchronous Digital Hierarchy (SDH) együtt multiplexelési szabványokat megvalósító protokollok, melyek leírják, hogy több kommunikációs csatorn hogyan haladhat egyetlen egy optikai szálon.

Mivel a rétegezett csomagkapcsolt hálózatok a múltban kerültek kidolgozásra és kiépítésre, így nem az MPLS hálózatoktól jelenleg elvárt csomagkapcsolásra lettek eredetileg tervezve. Ahogy az 1-es ábra is szemlélteti, a szolgáltatók hálózataiban a múltban kialakult és megjelent ATM és SDH architektúrák erősen rétegezett hierarchiája és elavultsága nagyon megnehezíti a hibakeresést, és körülményessé teszi a megoldását.

1.2 Az MPLS-TP megjelenése

A szolgáltatóknak olyan csomagkapcsolt hálózati protokollt kell választaniuk, amely az MPLS technológiához hasonlóan robosztus és skálázható, és rendelkezik olyan az MPLS-ből hiányzó megoldásokkal, amelyek képessé tennék arra, hogy szolgáltatói hálózatokban fontos szerepet játsszon. Fontos szempont a migrálhatóság, vagyis, hogy a már meglévő hálózatokat sikeresen lehessen beépíteni ebbe a csomagkapcsolt hálózatba, valamint szükséges a végpontok közötti vezérlés megvalósítása, amelynek segítségével a hálózati útvonalakat a hálózati erőforrások figyelembevételével hatékonyan és megbízhatóan tudja kiépíteni.



2. Csomagkapcsolt hálózati töréneti fejlődési ábra

A 2. Csomagkapcsolt hálózati történeti fejlődési ábrán látható, hogy mely protokollok voltak eredetileg elterjedtek, majd a követelményekkel lépést tartva, majd azok továbbfejlődésével mely

irányba haladtak tovább. Az MPLS megjelenése után az MPLS-TP előfutáraként jött létre a T-MPLS, majd 2008 februárjában az ITU-T és az IETF megegyeztek, hogy közösen dolgozzák ki az MPLS-TP szabványt. A jelenleg meglévő dokumentumok közül az RFC5654-es dokumentum tartalmazza a követelmények konkrét kidolgozását, és az RFC5921-es pedig az MPLS-TP keretrendszer leírását.

Az MPLS-TP technológia az MPLS egyszerűsített, kibővített verziója, mellyel a jövőbeni felhasználói igényeknek próbálnak hatékony hibakereséssel, szolgáltatási szintméréssel (QoS[3]), és a korábbi hálózati protokollokban alkalmazott széles körű OAM funkciókkal megfelelni.

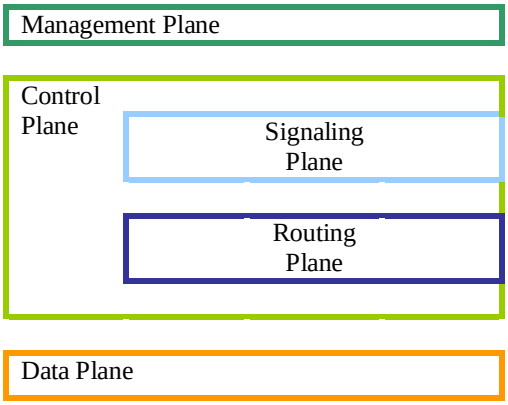
1.3 Traffic Engineering (TE)

A szolgáltatók saját hálózatával szemben támasztott jelenlegi és jövőbeni fontos követelmény, hogy a hálózatukon belül ne legyenek, és ne alakulhassanak ki túlságosan leterhelt vagy kihasználatlan vonalak és csomópontok. Összességében a hálózat 100%-os kihasználtságára kell törekedni, ebben segítenek a forgalomszabályozást (Traffic Engineering) támogató protokollok. Nyílván csak elméletileg lehet egy vonalat teljesen kihasználni, gyakorlatilag ez lehetetlen, de egy optimális kihasználtság eléréséhez egy jól kiépített, és következetesen átgondolt hálózati architektúrán felül elengedhetetlen a hálózat forgalmának manipulálása és szabályozása.

1.4 Generalized Multiprotocol Label Switching (GMPLS)

A 3-as ábrán látható a GMPLS hálózati architektúrája, melyben A Signaling Plane-hez fognak tartozni az olyan protokollok, melyek dinamikusan hozzák létre a Data Plane-beli kapcsolatokat. A Routing Plane fogja tartalmazni a dinamikus útválasztó protokollokat, melyek megosztják egymással az útvonalakat, és a Traffic Engineering beállításokat.

[3] QoS Quality of Service, egy szolgáltatás minőségét jelenti



3. GMPLS

A Signaling Plane és a Routing Plane együttese alkotja a Control Plane-t. A Management Plane lesz felelős a diagnosztikáért, a konfiguráció lekérésért, és a statisztika gyűjtésért. A Data Plane feladata pedig a csomagok továbbítása a Control Plane által meghatározott útvonalakon.

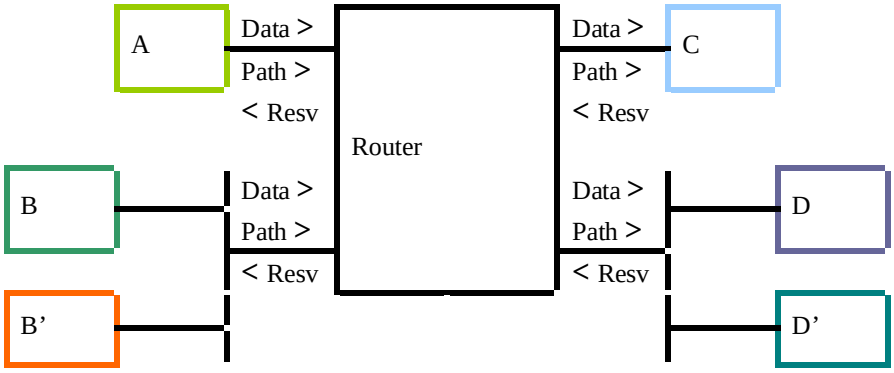
Az GMPLS Control Plane a forgalomirányítási adatbázis, és az MPLS címkék megosztásával oldja meg az MPLS-TP útvonalainak (Label Switched Path és Pseudo Wire[4]) kiépítésért, megszüntetéséért és az útvonalának átirányításáért.

Az MPLS-TP nagy előnye, amely a telekommunikációs cégeket a már meglévő IP/MPLS hálózatába integrálására készteti, hogy a Control Plane opcionális, vagyis így megvalósítható a Hálózati rétegbeli funkciók elhagyásával, hogy csupán a Szállítási rétegre támaszkodva működjön a hálózat. GMPLS többféle típus (Time-division multiplexing[5], lambda[6], és optikai) alapján támogatja a címkekapcsolást. Ezáltal nő a teljesítmény, csökken reakcióidő, és felgyorsul az átviteli sebesség.

[4] Ezek MPLS útvonal meghatározások.
[5] Több csatorna egy csatornába való multiplexelése úgy, hogy a fő csatornát felosztja több idő intervallumokra, és a csatornákhoz időintervallumokat rendel, és azokban továbbítja.
[6] Egy optikai kábelen a fény több hullámtartomány van amiket lambdának neveznek, és lehetőség van, hogy egy optikai kábelen a különböző lambdákat különböző különválasztva más irányba továbbítsuk.

1.5 Resource Reservation Protocol Traffic Engineering (RSVP-TE)

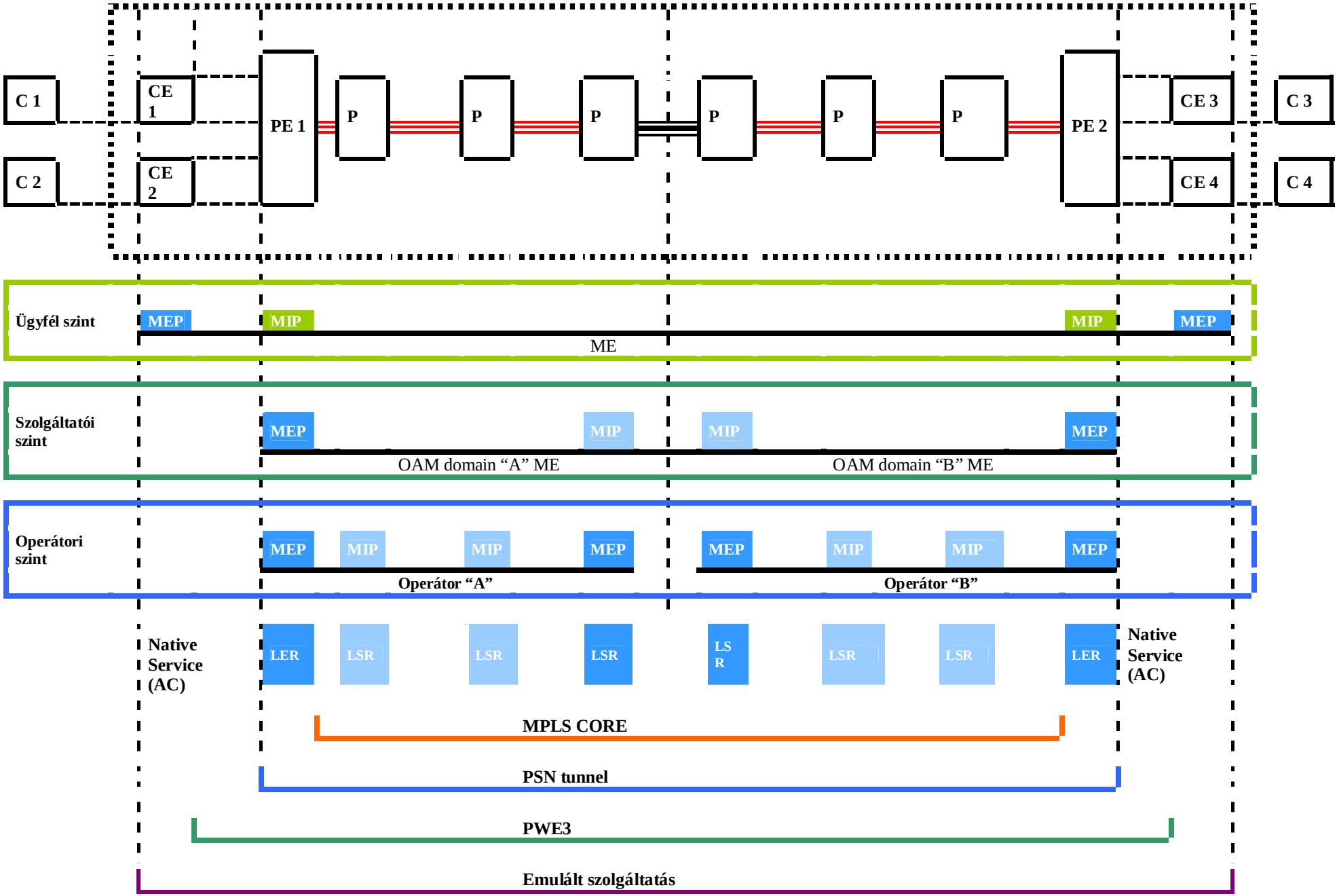
Resource Reservation Protocol felelős egy útvonalon az erőforrások lefoglalásáért és biztosításáért. Ez nem egy forgalom irányító protokoll, így csakis szigorúan egy már működő, tőle független protokollal együtt tudja ellátni ezt a feladatot. A forgalomirányító protokoll megállapítja a hálózat két pontja közötti útvonalat, majd az előállt a konzisztens forgalomirányító adatbázisból az RSVP meghatározza az útvonalat alkotó eszközöket, és vezérlő üzenetekkel lefoglalja rajtuk az erőforrásokat.



4. RSVP-TE működési példa

Egyik ilyen üzenet a RSVP Resv, vagyis a „reservation request”, melyel az adatforgalom fogadója üzeni a küldőjének, hogy erőforrást szeretne lefoglalni. Fontos említeni, hogy ugyanazon az útvonalon visszafelé haladva foglalja le az erőforrásokat, mint ahol az aktuális adatforgalom halad, és minden egyes köztes eszközön beállítja a „reservation state”-et, vagyis a lefoglalási állapotot. Másik üzenet az RSVP Path, melyet az adatforgalom küldője küld a köztes eszközöknek, hogy beállítson egy ’Path State”-et, vagyis egy útvonal állapotot, ami tartalmazza az előző ugrás IP címét. Ez azért fontos, mert így áll elő egy esközöket láncoló hivatkozás, ami mentén a „Resv” üzenetek majd visszafele tudnak haladni.

1.6 Hálózati Referencia modell



1.6.1 Pseudo Wire End to End [7](PWE3)

A Pseudo Wire (PW) segítségével egy hálózati szolgáltatást (E/1, Frame Relay, Ethernet, Sonet [8]stb.) lehet emulálni egy csomag kapcsolt hálózaton (IP, MPLS) keresztül. Ennek a részletes kidolgozását, és működésének megoldását tartalmazza az RFC3985 dokumentum. Az ügyfél telephelyén használt hálózati szolgáltatásainak (Native service) megfelelő adat forgalmi egységeket (biteket, csomagokat, cellákat) a PE útválasztók egy Pseudo Wire PDU-ba csomagolják be, majd azt a szolgáltató csomagkapcsolt hálózatán keresztül az ügyfél cél telephelye felé továbbítják, ahol a PE útválasztó kicsomagolja az adat egységet, majd továbbítja a cél CE útválasztónak.

1.6.2 MPLS modell

Az MPLS-TP az MPLS-ez hasonló architektúrát és címkekapcsolást használ. Az MPLS-TP hálózati referencia modell kiegészül a több szolgáltatón áthaladó Pseudo Wire fogalmával, és az így megjelenő új eszközökkel, és logikai egységekkel.

MPLS-TP Label Switched Path (LSP)
Az ügyfél számára biztosított MPLS-TP útvonal, amin a csomag végig halad. A csomagnak rendelkezni kell egy egyedi címkével ami alapján a szolgáltató eszközei a megfelelő irányba tudják kapcsolni.

Native Service (AC)
Az ügyfél által használt hálózati technológia, vagy szolgáltatás, melyet a Pseudo Wire-ek fognak majd összekapcsolni.

[7] Végponttól-végpontig
[8] Kommunkiációs szabványok.

Customer Edge

A szolgáltató vagy az ügyfél saját eszköze, melyek egy PE útválasztókhoz kapcsolódnak.

MPLS-TP Provider Router

A szolgáltató eszközei, amelyeken keresztül kiépülnek a LSP-k. Miután kiépültek az útvonalak, a Provider routerek a csomagokat címkéjük szerint a megfelelő interfészükön továbbítják.

MPLS-TP Provider Edge Router

A szolgáltató eszközei, amelyen keresztül kapcsolódik az ügyfél a szolgáltatóhoz. A bejövő csomagokat az LSP-nek megfelelően felcímkézi, a kimenőkről pedig eltávolítja a címkét.

MPLS-TP Label Switching Router (LSR)

Az LSR egy PE vagy egy P router lehet. A címkének megfelelő irányba továbbítja a csomagot, vagyis a kiépített LSP-n tovább.

Label Edge Router (LER)

Olyan LSR, amely a az LSP végpontján helyezkedik el és az ügyfél csomagjait címkézi meg az LSP egyedi címkéjével.

Pseudo Wire Switching Provider Edge Router (S-PE)

Egy olyan PE, mely egy szolgáltató csomagkapcsolt hálózat alagút két végén helyezkedik el, és Pseudo Wire-okat kapcsol más szolgáltatók csomagkapcsolt hálózatához.

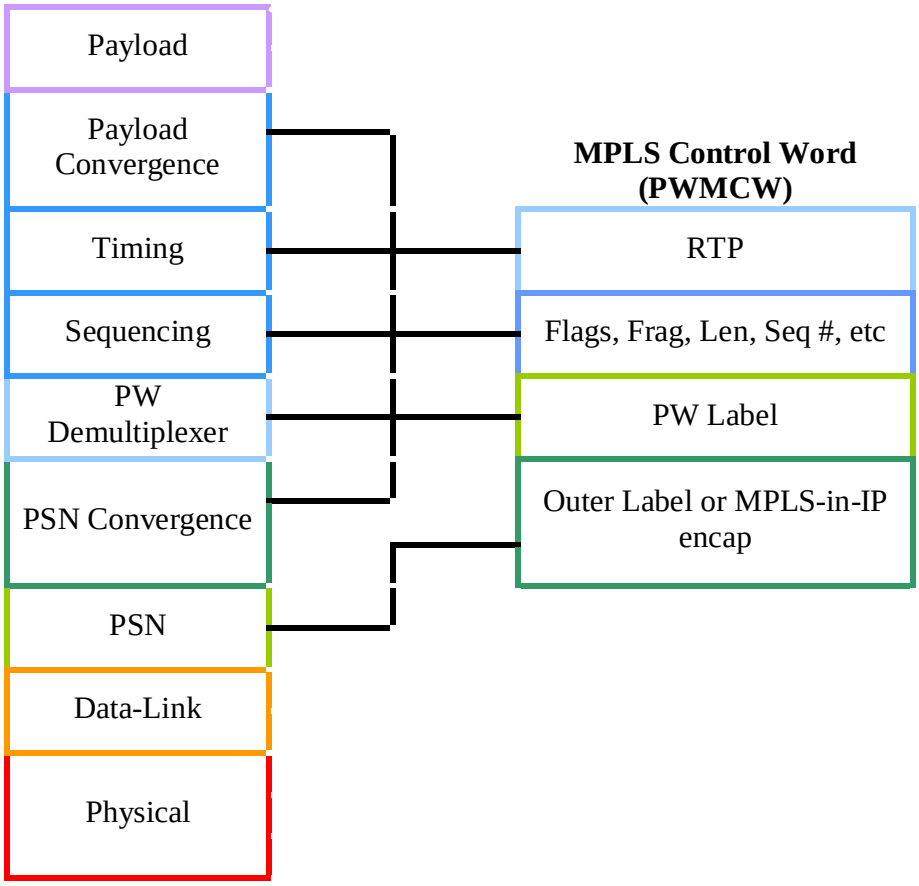
Pseudo Wire Terminating Provider Edge (T-PE) Router

Olyan PE mely a Pseudo Wire két végén helyezkedik el, és az AC-hez kapcsolódik.

1.6.3 MPLS-TP mint csomagkapcsolt hálózat (PSN)

Ebben a hálózati referencia modellben a csomagkapcsolt hálózat szerepét az MPLS-TP tölti be, tehát az MPLS-hez hasonlóan címkekapcsolást végez két PE útválasztó között egy LSP

útvonalon. Az útvonalakat a LSR-ek fogják alkotni. Tehát értelemszerűen szükség van a Pseudo Wire-ek és a LSP-k közötti megfeleltetésre. Ezt egy Control Word segítségével fogja megvalósítani, ami tartalmazza a PWE3 „Encapsulation” és a PSN „Convergence” réteg közti megfeleltetéshez szükséges információkat. A következő 4-es ábrán látható a baloldali PW3E MPLS architektúra, és a jobboldali Control Word közötti logikai megfeleltetés.



5. PW3E MPLS architektúra és MPLS Control Word

Az ábrán lévő rövidítések és elnevezések jelentései:

Payload

A szolgáltatás specifikus adategységet fogja jelenteni, adatkapcsolati és fizikai rétegbeli információkkal.

Payload Convergence

A Payload Convergence réteg feladata, hogy a beérkező szolgáltatás specifikus adat egységet egy Pseudo Wire PDU[9]-ba csomagolja, mégpedig úgy, hogy megbízható vezérlő csatornát szolgáltasson, és a csatornákhoz DSCP [10]értékek alapján Prioritás értékeket rendeljen.

PW Demultiplexer

Ahogy bizonyos hálózati szolgáltatások képesek egyszerre több vonalat, például ATM esetében több VC-t [11]egy VP[12]-n, Ethernet esetében több VLAN-t [13]egy kábelen, több DS0-t [14]egy E1-en keresztül trönkölni egy vezetéken. A PW Demultiplexer lehetővé teszi, hogy egyetlen alagúton keresztül egyszerre több, akár különböző hálózati szolgáltatást tartalmazó Pseudo Wire kommunikációja haladhasson.

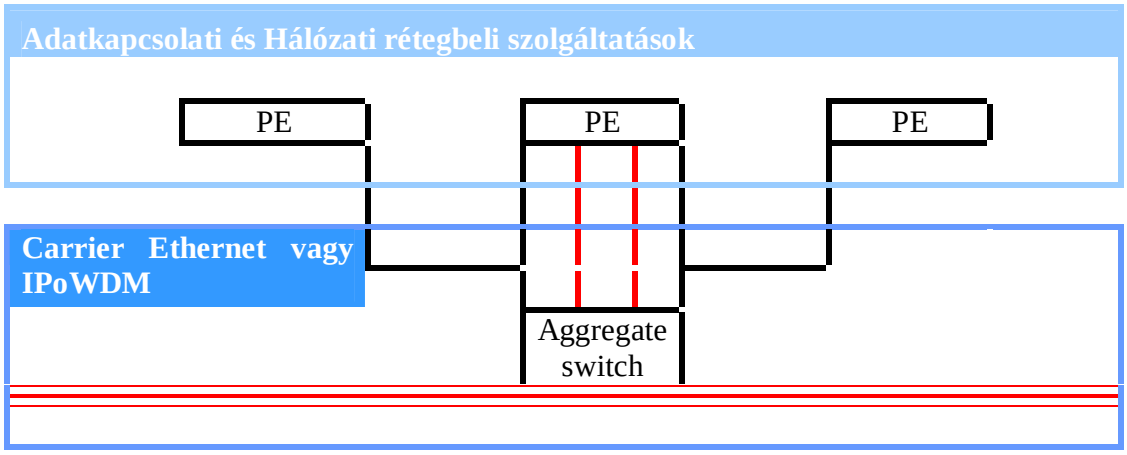
1.6.4 Fizikai réteg

A fizikai réteget az ügyfél igényeihez mérten optikai, illetve Ethernet alapokon kell megvalósítani. A ma használt sokszínű (E1, T1, E3, T3, ATM stb.) technológiák miatt csak nehezen átlátható hierarchiák, és körülményesen összekapcsolható hálózati topológiák alakultak ki. Egy példán keresztül szemléltetve: már korábban látható volt az 1-es ábrán, hogy a hálózati rétegbeli PE útválasztókat az ATM és az SDH kapcsolatok szövevényes rendszere kapcsolja össze. Célszerű lenne ezeket az architektúrákat egyszerűsíteni, ezáltal csökkenteni az üzemeltetési költségeket és a hibakeresést is egyszerűsíteni. Ahogy azt a 6-os ábra is szemléltette ezt, a jövőben a minimális rétegszámú hálózati hierarchiák kiépítésre kell törekedni.

[9] Protocol Data Unit, egy protokol vezérlő és egyéb információit tartalmazó adat egysége.
[10] Differentiated Services Code Point, a forgalom prioritását jelzi egy IP csomagon belül.
[11] Virtual Channels, ATM esetében ezek a virtuális csatornák
[12] Virtual Paths, ATM esetében ezek ezek a virtuális útvonalak.
[13] Virtuális helyi hálózat, logikailag összetartozó hálózati eszközök alkotják.
[14] A Digital Signal 0, egy 64 kbit/s-os csatorna.

1.6.4.1 Carrier Ethernet, és Ethernet Virtual Connection (EVC)

A hálózati hierarchiák egyszerűsítésére, és a régi technológiák felváltására dolgozták ki a Carrier Ethernetet. Az Ethernet technológia olcsósága miatt hamar elterjedt, és az Ethernet OAM kidolgozása után széles körben elfogadottak lettek. A Metro Ethernet Forum (MEF) szabványügyi szervezet foglalkozik a Carrier Ethernet és az Ethernet Virtual Connection (EVC) továbbfejlesztésével. Feladatának öt fő területe a szolgáltatások, a skálázhatóság, a megbízhatóság, a QoS és a service management szabványosítása.

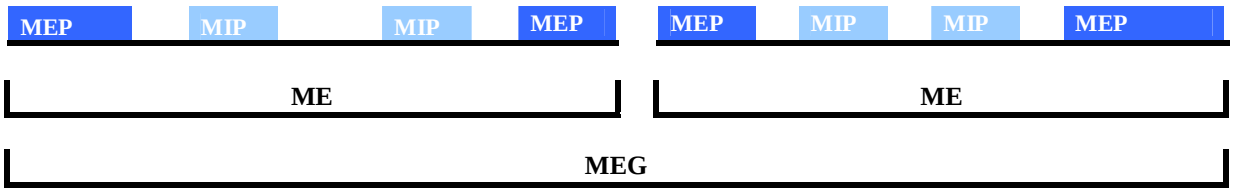


6. Rétegezett újgenerációs csomagkapcsolt hálózati modell

Az IEEE a 802.1Qay dokumentumban fogalmazta meg a Carrier ethernet továbbfejlesztett változatát, a Provider Backbone Bridge Traffic Engineering-et (PBB-TE). Ebben a dokumentumban sok új elnevezést és definíció került bevezetésre, de mivel túlságosan előremutató technológia, ezért megkérdőjelezhető volt a befektetett tőke és tudás rövid időn belüli megtérülése. Idővel olyan több nagy piaci résztvevő, mint a BT is elpártolt a technológia azonnali megvalósításától és bevezetésétől.

Carrier Ethernet OAM hálózati referencia modell

Szeretném kifejteni a Carrier Ethernet által definiált eszközöket, és logikai szerepköröket, melyekre alapozva a hibakeresés során a szolgáltatók felépíthetik a tesztelést, és a hiba detektálásának a folyamatát.



7. Carrier Ethernet OAM hálózati referencia modell

Az ábrán lévő rövidítések és elnevezések jelentései:

OAM domain

Egy kapcsolat megfigyelésében résztvevő eszközök összessége.

Maintenance Entity (ME)

Az útvonal azon két csomópontja közötti rész, amelyet meg kell figyelni.

Maintenance Entity Group (MEG)

Egy OAM domainben egy adott útvonalat megfigyelő egy vagy több ME eszközök csoportja. Rendelkezik saját egyedi MEG azonosítóval.

MEP (MEG end point)

MEG végpontok, melyek képesek küldeni és fogadni hibakeresési és teljesítmény megfigyelési OAM üzeneteket. Rendelkeznie kell az őt tartalmazó MEG azosoítójával, egy saját egyedi MEP azonosítóval, és a MEG-en belül található összes MEP listájával.

MIP (MEG intermediate point)

Fogadja a neki küldött OAM üzeneteket, és válaszolhat is rájuk, de másoktól függetlenül nem küld, vagy kezdeményezhet további üzeneteket.

1.7 Operations, Administration, and Maintenance (OAM)

Az OAM egy olyan általános protokoll gyűjtemény, mely segítségével tudjuk észlelni és jelenteni egy adott kapcsolat hibáit, valamint minősíteni azt teljesítménybeli mérőszámokkal. Szeretném ebben a részben bemutatni azokat az eszközöket amik együttesen egy új generációs hálózatban a hibakeresést végző szakemberek segítségére lehetnek, valamint támpontot és irányelveket adhatnak a hiba behatárolására és megoldására. Ehhez szeretném kifejteni a jelenleg fejlesztés alatt álló OAM protokollokat, majd felépíteni egy MPLS-TP OAM referencia modellt, amelyen keresztül értelmezni lehet ezeket a hálózati protokollokat.

- ICMP[15] Echo request
- LSP Ping[16] pont-multipont MPLS
- Virtual Circuit Connectivity Check (VCCV)
- Bidirectional Forwarding Detection (BFD)
- IP Performance Metrics (IPPM)
- OAM Ethernet alapú hálózatok számára (ITU-T Y.1731)
- ITU-T által definiált OAM MPLS LSP-knek (ITU-T Y.1711)
- OAM követelmények MPLS TP számára

1.7.1 Bidirectional Forwarding Detection (BFD)

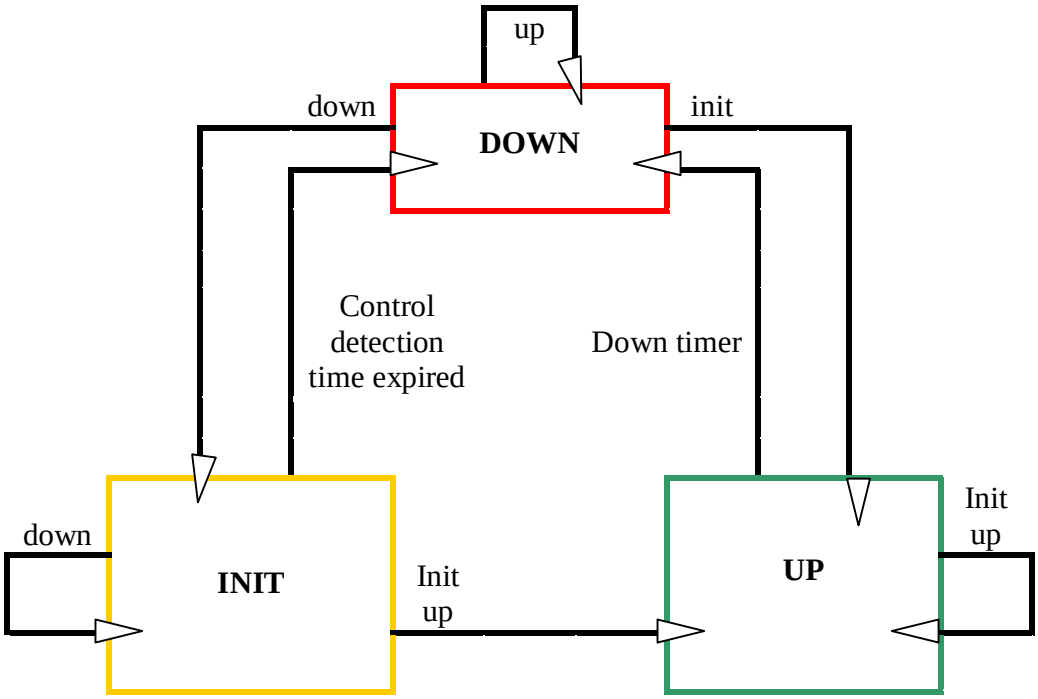
Ahhoz hogy egy kapcsolatot WAN közegként használhassanak, elsősorban a vonalkapcsolt SONET, E1/T1, E3/T3, és az ATM hálózatokban használt technológiáktól már régóta elvárt hibaészlelési és hibajelzési megoldásokat kellett megvalósítani. Erre a célra hozta létre az RFC 5580-ban az IETF a Bidirectional Forwarding Detection (BFD) protokollt. Lényege: az eddig már sok más protokollban előre beépített „hello” protokollhoz hasonlóan, hogy más protokollal együttműködve, bármely hálózati közegben és hálózati rétegben, két különálló rendszer között

[15] Az Internet Control Message Protocol lehetővé teszi eszközök számára, hogy üzeneteket osszanak meg egymással.
[16] Hálózati eszköz, mely segítségével ellenőrizhető hogy egy eszköz elérjető-e.

nyújtson lehetőséget arra, hogy azok rendkívül gyorsan tudjanak reagálni vonalhibákra, és kapcsolati megszakadásokra. Ezáltal felgyorsul a konvergálási idő, hamarabb előáll az alternatív útvonal a célhoz. Használatának nagy előnye, hogy töredékére csökken az az adatmennyiség, ami az inkonzisztens hálózat miatt elvész.

1.7.1.1 BFD Működési módok

Aszinkron módban a két rendszer periodikusan vezérlő BFD üzeneteket küld egymásnak. Ha egy előre rögzített üzenetre nem érkezik válasz, akkor a kapcsolatot megszakadtnak („DOWN”) ítélik.



8. BFD Állapot gráf

A „Demand” módban a két rendszer feltételezi, hogy van egy másik, független módja annak, hogy ellenőrizni tudják a másik fél elérhetőségét. Miután kiépítették a BFD viszonyt vezérlő üzeneteket már csak akkor váltanak egymással, ha a hálózati körülmények megváltozásával

ellenőrizni akarják a másik fél elérhetőségét. Nagy előnye, hogy kevesebb többletterhelést jelent a vonal számára.

A fenti két módhoz beállíthatunk egy kiegészítő „Echo” módot, melynek lényege, hogy az egyik fél üzeneteket küld a másik félnek, mely azokat egyszerűen visszaküldi a forrásnak. Ezt a módot a másik féltől függetlenül használhatják, ezáltal lehetőség nyílik a távoli fél továbbító útvonalának ellenőrzésére. Ha egy előre rögzített számú „Echo” üzenet nem ér vissza, akkor a kapcsolatot megszakadtnak („DOWN”) ítélik.

Miután a kapcsolat megszakadt és „DOWN” állapotban van, lehetőség van arra, hogy a BFD a szolgáltató által használt forgalomirányító protokollt is értesítse a kapcsolat megszakadásról, és a saját „hold down”[17] időzítőjének lejárta előtt a szomszédját elérhetetlennek ítélje, ezáltal gyorsabban reagál a hálózat a kapcsolat megszakadásaira, hamarabb előáll egy alternatív útvonal, és kevesebb idő kell a hálózat konvergálásához.

1.7.1.2 Általános BFD vezérlő üzenet formátuma

Ez az üzenet szolgál a BFD viszonyok kiépítésére és fenntartására. A BFD csomagnak kötelezően kell tartalmaznia az alábbi mezőket:

Version	Diagnostic	State	P	F	C	A	D	M	Detect Mult	Length
My Discriminator										
Your Discriminator										
Desired Min TX Interval										
Required Min RX Interval										
Required Min Echo RX Interval										

A keretformátumban lévő mező nevek értelmezése és fő funkciói.

Version (Vers)

A BFD protokoll verziószáma. Jelenleg az 1-es verzió van használatban.

[17] Egy visszaszámláló időzítő, mely ideig a rendszer vár míg a szomszédját elérhetetlennek nyílvánítja.

Diagnostic (Diag)

Ebből a mezőből megállapítható a megszakadás oka, azaz, hogy a lokális rendszer előző viszonya miért szakadt meg a másik féllel. Ennek a mezőnek a jelentései.

0 – Nincs diagnosztika

1 – Vezérlés észlelési idő lejár.

2 -- Sikertelen „Echo” mód.

3 – A szomszéd a viszony bontását jelzi.

4 -- Forwarding Plane Reset.

5 – Elérhetetlen útvonal.

6 -- Elérhetetlen útvonal láncolat.

7 – Adminisztratívan elérhetetlen útvonal.

8 – Fordított elérhetetlen útvonal láncolat.

9-31 – Jövőbeni használatra fenntartott.

State (Sta)

A jelenlegi BFD viszony állapota, ahogy azt a csomagot előállító rendszer látja. Ennek a mezőnek a jelentései a következők lehetnek.

0 – AdminDown – Letíltott állapot

1 – Down – Megszakadt állapot

2 – Init – Kezdeti kiépülő állapot

3 – Up – Kiépített állapot

Poll (P)

Ezzel jelzi a küldő rendszer a másik félnek, hogy megerősítést kér a kapcsolat állapotáról, ez általában a kapcsolatban bekövetkezett változás után történik.

Final (F)

A küldő ezzel az opcióval tud válaszolni egy Poll kérésre, és jelzi a távoli félnek a kapcsolat állapotát.

Control Plane Independent (C)

Alkalmazástól függő opció. Lehetőség van beállítani, és jelezni, hogy a BFD a Control Plane-től függetlenül a Data Plane-ben lett implementálva.

Authentication Present (A)

A kapcsolat hitelesítéséhez szükséges opció, és ez jelzi, hogy a viszonyt authentikálni kell.

Demand (D)

A demand mód beállításához szükséges opció, a küldője utasítja a távoli rendszert, hogy az ne küldjön BFD vezérlő csomagokat.

Multipoint (M)

Jövőbeni BFD point-to-multipoint[18] kiegészítéseknek fenntartott mező.

Detect Mult

Az egyeztetett üzenet küldési intervallum szorzója aszinkron módban, mely alatt, ha nem kap választ akkor megszakadtnak ítéli a kapcsolatot.

Length

Maga a BFD vezérlő üzenet hossza byte-okban.

My Discriminator

Egyedi, nem nulla diszkriminátor érték, melyet a küldő rendszer generál, hogy meg lehessen különböztetni a két rendszeren futó BFD viszonyokat.

[18] Pont-multipont kapcsolat

Your Discriminator

Ez egy másik féltől kapott diszkriminátor, mely a My Discriminator értékét tükrözi vissza.

Desired Min TX Interval

Ez a legkisebb idő intervallum mikro szekundumban, amelyet a küldő fél szeretne várni a vezérlő üzenetek küldése között. Ennek az értéke nagyban függ az alkalmazott hálózati közegtől, egy olyan intervallumot kell választani, ami nagy kihasználtság alatt is optimálisan tartható.

Required Min RX Interval

Ez a legkisebb idő intervallum mikro szekundumban, a fogadott vezérlő üzenetek között, amelyet a rendszer még támogatni tud.

Required Min Echo RX Interval

A fogadott „Echo” üzenetek között ez a legkisebb idő intervallum mikro szekundumban, amelyet a rendszer még támogatni tud.

1.7.1.3 BFD Authentikáció

Lehetőséget nyújt arra, hogy a BFD vezérlő üzenetek titkosítva, biztonságosan továbbítódjanak a hálózaton, így kizárható egy harmadik féltől származó támadás. Csak akkor működik hitelesített módban, ha az A bit használatban van. A hitelesítés keretformátuma és a mezőinek fő funkciói az alábbiak.

0 1 2 3
0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1

Auth Type	Auth Len	Auth Key ID	Password
Sequence number			
Auth Key/Hash			

Auth Type

Ez a mező jelzi az adott BFD viszony által használt hitelesítési módokat, melyek az alábbiak lehetnek.

0- Fenntartott

1– Egyszerű jelszó

2- MD5[19]

3- Meticulous Keyed MD5

4- Keyed SHA1[20]

5- Meticulous Keyed SHA1

6--255 – Jövőbeni használatra fenntartott

Auth Len

Az authentikációs rész hossza. Egyszerű jelszó esetén ez a jelszó hossza, MD5 esetében ez 24, SHA1 esetében 28 bit

Auth Key ID

Authentikációs kulcsazonosító, melyet a BFD csomagban használnak. Ez lehetővé teszi, hogy egyszerre több kulcsot is használjon.

Password

Egyszerű jelszó a titkosításhoz.

Sequence Number

A csomag sorszáma, keyed MD5 vagy SHA1 esetében értéke csak néha növekedik, Meticulous Keyed MD5 vagy SHA1 esetében minden csomag után növekszik.

Auth Key/Digest

Ez a mező tartalmazza a kiszámolt 16 bájtos MD5, vagy a 20 bájtos SHA1 értéket

[19] Message-Digest algorithm 5, egy 128 bites egyirányú kódolási algoritmus.
[20] SHA-1 egy kriptográfiai hash függvény.

1.7.1.4 A BFD beállítása

A BFD-t először egy adott interfészre vonatozóan kell beállítani. Ennek Cisco IOS utasításainak lépései:

1. enable
2. configure terminal
3. interface *típus*
4. bfd interval *miliszekundumok* **min_rx** *miliszekundumok* **multiplier** *idő_intervallum_szorzó*
5. end

Majd a használt forgalomirányító protokollhoz kell rendelni a megfelelő interfészt. Ennek Cisco IOS utasításonkénti lépései, BGP forgalomirányító protokoll esetén:

1. enable
2. configure terminal
3. router bgp *as_azonosító*
4. neighbor *ip-cím* **fall-over bfd**
5. end

1.7.2 Az LSP Ping

Az IETF az MPLS hálózatok hibakeresésére létrehozta a draft-ietf-mpls-p2mp-lsp-ping vázlatot. Ebben az LSP-k hibakeresésére alkalmaz egy LSP ping funkciót, mely az ICMP ping analógiájára támaszkodva két működési módot tartalmaz:

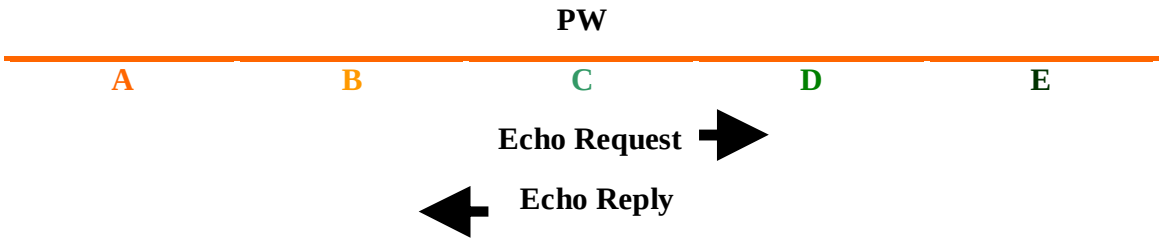
- "Ping" mód: ebben a módban két LSR közötti kapcsolatot ellenőrizhetjük
- "Traceroute" mód: ebben a módban a kapcsolatot alkotó ugrásokat ellenőrizhetjük, és lokalizálhatjuk a hibát.

Az „Echo”[21] üzenetben szereplő TTL, vagyis az ugrások számát egy könnyebben felhasználható Type Length Value (TLV) keretben rögzíti, melynek mezőinek formátuma:

0 1 2 3
0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1

type	Length = 8
value	

Vegyük például az adott Pseudo Wire-t, ekkor, ha B-ből akarunk küldeni D-nek egy LSP-Ping requestet, vagyis, hogy TTL a D-nél járjon le, akkor a TTL-TLV-nek a kettő értéket kell választanunk.



9. LSP ping működés közben

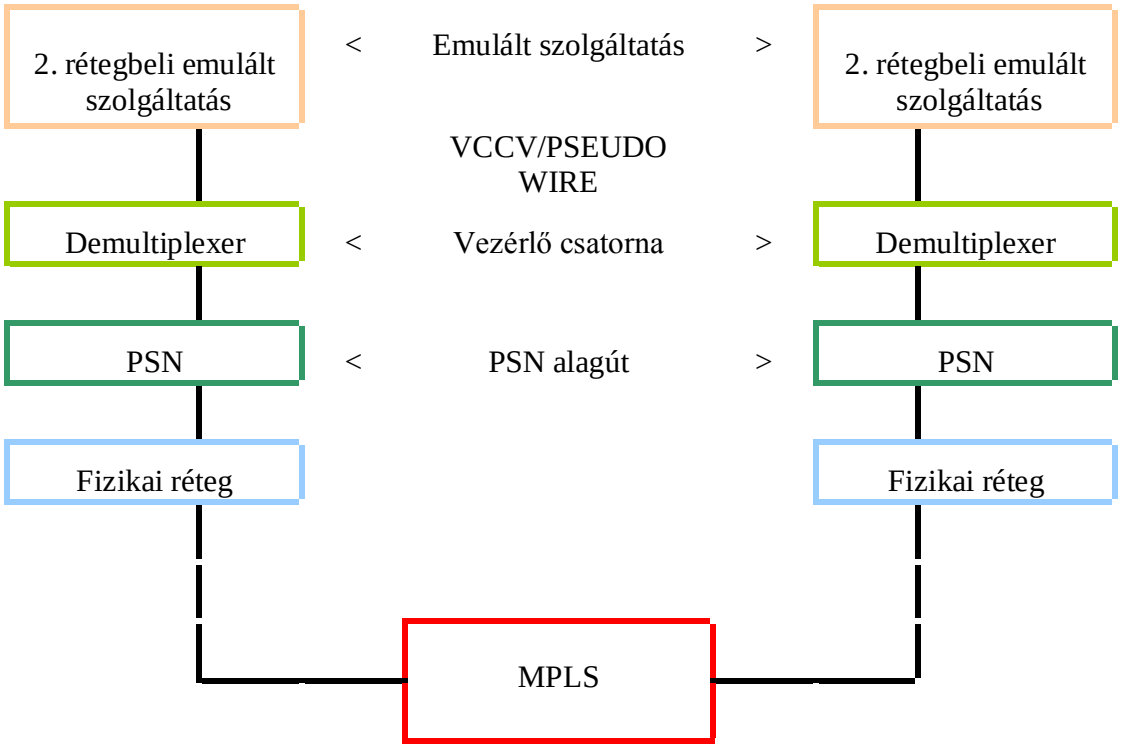
LSP Ping támogatja mind az aszinkron és mind az igény szerinti „on-demand” aktiválást. Mindemellett a „point-to-multipoint” LSP és MPLS útvonalakat is támogatja.

1.7.3 Virtual Circuit Connectivity Verification (VCCV)

Az IETF kidolgozta az RFC-5085-ben a VCCV szabványt. Ez a szabvány rögzíti a Pseudo Wire vezetékek kapcsolatainak, és az adatforgalmat lebonyolító Data Plane-nek az ellenőrzését és felügyeletét. Így amikor a Pseudo Wire kiépül két PE útválasztó között, a VCCV információkat tartalmazó LDP[22] protokollt fogják használni. A PE útválasztók ezekből az információkból tudják

[21] Egy eszköz az ICMP-ben definiált Echo request, segítségével kérhet egy másik eszköztől válasz üzenetet.
[22] Label Distributuon Protocol az MPLS hálózaton belül a cimkék megosztásának egyik módja.

majd megállapítani, hogy milyen Control Chanel (CC) és Connectivity Verification (CV) típusokat képesek kezelni. Csak akkor kezdődik el a tényleges forgalom továbbítása a két PE között, miután a Pseudo Wire kiépült. Ekkor kezdődik VCCV kommunikáció is, mely olyan csomagolást használ, amelyet a Data Plane nem tud megkülönböztetni a közönséges forgalomtól. A VCCV minden demultiplexer típushoz definiál egy CC CV típust.



10. Példa aVCCV kommunikációra, két pont között.

1.7.3.1 VCCV Control Channel (CC)

PW Associated Channel (PWAC)

Ez nem egy csatorna típus, hanem egy olyan csatorna, melyet a Pseudo Wire vezetékbe multiplexelve a csomagkapcsolt hálózatban az ügyfél forgalmának útvonalát követi. Ennek egy keretformátuma, és a mezőinek jelentése:

0 1 2 3
0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1

Type	Version	Reserved	Channel Type

Type

Magának a vezérlő csatornának a típusát fogja ez jelenteni, melynek a típusonkénti értéke lehet:

Bit 0 (0x01) - Type 1: PW3 Control Word 0001b PW-ACH

Bit 1 (0x02) - Type 2: MPLS Router Alert címke

Bit 2 (0x04) - Type 3: MPLS PSEUDO WIRE címke TTL = 1

Bit 3 (0x08) Bit 4 (0x10) Bit 5 (0x20) Bit 6 (0x40) Bit 7 (0x80) – Fentartott

Channel Type

A csatorna típusa, ennek az értéke 0x0021 IPv4 esetén vagy 0x0057 Ipv6 esetén.

Type 1 In-band

Ebben a módban a vezérlő üzenetek az adatforgalom részeként kerülnek továbbításra. Ha Control Word van használatban, akkor egy Pseudo Wire Associated Channel Header (PW-ACH) formátumot használ. Ennek egy keretformátuma és mezőinek jelentése.

0 1 2 3
0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1

0001	Version	Reserved	Channel Type

Type 2 Out-band

Lehetőség van arra, hogy Router Alert labelt használva hozzuk létre a control channelt. Ez a megközelítés sajnos nem támogatott az MPL-TP-ben, mivel így Equal Cost Multi-Path (ECMP) lép fel, és a VCCV control channel forgalma az ügyfél forgalmának útvonalától eltérően is mehet.

1.7.3.2 VCCV Connectivity Verification (CV)

Magához a kapcsolat ellenőrzéséhez nyújt eszközöket. Idővel több új és továbbfejlesztett eszköz kerülhet használatra. Ezeknek az eszközöknek megfelelő értékek:

Bit 0 (0x01) - ICMP Ping
Bit 1 (0x02) - LSP Ping
Bit 2 (0x04) Bit 3 (0x08) Bit 4 (0x10) Bit 5 (0x20) Bit 6 (0x40) Bit 7 (0x80) – Fenntartott

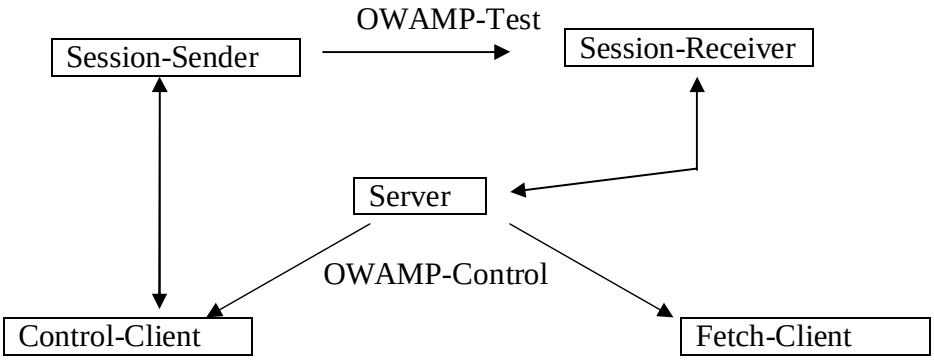
1.7.4 IP Performance Metrics (IPPM)

Ezt az eszközt az IETF állította össze, segítségével lehetővé válik az IP forgalom teljesítményének, csomagveszteségének, és késleltetésének a mérése. Ezekre a tényezőkre metrikákat, és a mérések kivitelezésére a One-Way Active Measurement (OWAMP) és a Two-Way Active Measurement (TWAMP) protokollokat definiál. Mindkét protokollt felosztja két belső protokollra: a Control plane, és a Test plane protokollra. A Control plane feladata, hogy kezdeményezze, elindítsa és befejezze a teszteket, míg a Test protokoll felel a teszt forgalmáért, csomagformátumáért, az ütemezésért, és a statisztikáért.

1.7.4.1 One-Way Active Measurement (OWAMP)

Az OWAMP Logikai modellje

Szertném a következő részben bemutatni azt az eszközt, melyet egy vonal egyirányú tesztjeihez lehet alkalmazni. Ebben a tesztben résztvevő eszközök több logikai módban is működhetnek. A kliens eszközhöz köthető módok a Control-Client, a Fetch-Client és a Session-Sender. A szerverhez pedig a Server és a Session-Receiver módok köthetőek.



11. OWAMP működési modell, és a szerepkörök közti kommunikáció iránya

A tesztelésben résztvevő szerepek:

Session-Sender	A tesztküldő végpontja.
Session-Receiver	A tesztfogadó végpontja.
Server	Egy végrendszer, amely egy vagy több tesztviszonyt menedzsel.
Control-Client	Egy végrendszer, mely tesztviszonyokat indít vagy fejez be
Fetch-Client	Olyan végrendszer, mely a lefutott teszteredményeket kérdezi le.

1.7.4.1.1 Kommunikáció felépülése

Mielőtt a Fetch-Client vagy a Control-Client vezérlő utasításokat adhatna a Servernek, első lépésként a TCP protokoll 861-es portján az eszközök között ki kell épülnie a kapcsolatnak. A feleknek még az OWAMP teszt elindulása előtt OWAMP-Controll üzeneteket kell küldeniük egymásnak, mert teszt futása közben már csak a leállításra van mód a Stop-session utasítással. Minden üzenet típusa megtalálható az első 16 oktetben.

Miután kiépül a TCP kapcsolat a kliens és a szerver között, első lépésként a szerver egy üdvözlő üzenetet küld.

0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
Unused (12 octets)
Modes
Challenge (16 octets)
Salt (16 octets)
Count (4 octets)
MBZ (12 octets)

A fenti keretformátumban lévő mezőnevek értelmezése és fő funkciói.

Modes

Ha a mód értéke 0, akkor a szerver nem kíván kommunikálni a klienssel és lezárja a kapcsolatot. Valamint a kliens lezárhatja a kapcsolatot, ha a szerver nem támogatja az általa kívánt módot. Három mód lehetséges:

“1”	Nem hitelesített
“2”	Hitelesített
“4”	Titkosított

Challenge

A szerver által véletlen generált oktet, egy megosztott titok, amivel a kliens tudja bizonyítani hitelességét.

Salt and Count

Olyan paraméterek, amelyekkel egy kulcs származtatható a megosztott titokból.

Második lépésként az üdvözlő üzenetre a kliens a következő kerettel válaszol.

0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
Mode
KeyID (80 octets)
Token (64 octets)
Client-IV (16 octets)

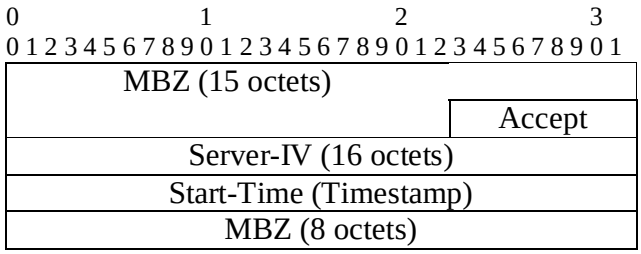
KeyID

Egy 80 oktet hosszúságú UTF-8 kódolású sztring, amely a szervernek mondja meg, hogy az authentikáláshoz melyik megosztott titkot használja.

Token

AES titkosítással van tárolva. Egy 16 oktetes Challange-ből, egy 16 oktetes AES Session kulcsból, és egy 32 oktetes HMAC-SHA1 Session kulcsból áll.
Nem authentikált módban a KeyID, Token és a Client-IV nem használtak.

Harmadik lépésként a szerver kötelezően küld egy szerver-start üzenetet.



A fenti keretformátumban lévő mezőnevek értelmezése és fő funkciói.

MBZ (MUST be zero)

Jövőbeni fejlesztésre szabadon hagyva.

Accept

Ez jelzi, hogy a szerver elfogadja-e a kommunikációt. Ennek a mezőnek a jelentései:

0	OK.
1	Meg nem határozott általános hiba.
2	Belső hiba.
3	A kérés nem támogatott.
4 - 5	Kevés erőforrás a kérés végrehajtásához.

Server-IV

Szerver által véletlenszerűen generált mező.

Start-Time

Egy időbélyeg, mely azt jelzi, hogy mikor kezdődött el az aktuális szerver folyamat.

1.7.4.1.2 Integrity Protection (HMAC)

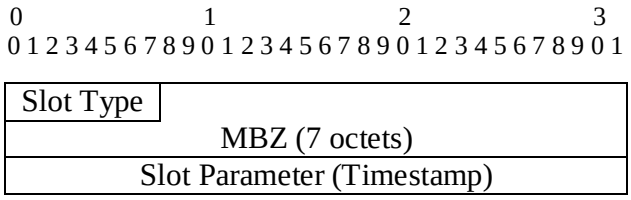
Fontos kérdés a viszonyok és a tesztek hitelesítése, így minden egyes OWAMP-controll üzenet egy HMAC mező hozzáadásával lesz hitelesítve. Az authentikálásnak még az üzenet titkosítása előtt meg kell történnie, majd kiolvasáskor a dekódolás után a fogadó eldönti, hogy helyes-e az üzenet.

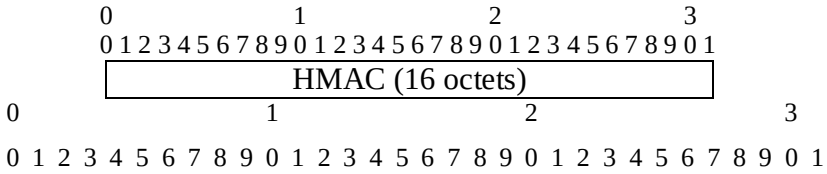
1.7.4.1.3 OWAMP-Control Commands

Ebben a részben szeretném bemutatni a teszt során az eszközök által használt vezérlés módját és a használt öt vezérlő üzenetet. Ezek együttesen fognak alkotni egy előre rögzített egységes tesztelő felületet.

1.7.4.1.3.1 Request-Session command

Egy OWAMP kliens egy Request-Session üzenettel kér a szervertől tesztet. Ezt az üzenetet három kisebb üzenet alkotja. Mezőinek, értékeinek és jelentéseinek értelmezése az alábbi.





0 1 2 3

0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1

1	MBZ	IPVN	Conf-Sender	Conf-Receiver
Number of Schedule Slots				
Number of Packets				
Sender Port			Receiver Port	
Sender Address				
Sender Address (cont.) or MBZ (12 octets)				
Receiver Address				
Receiver Address (cont.) or MBZ (12 octets)				
SID (16 octets)				
Padding Length				
Start Time				
Timeout, (8 octets)				
Type-P Descriptor				
MBZ (8 octets)				
HMAC (16 octets)				

1

Ez az érték jelzi, hogy ez egy Request-Session üzenet.

IPVN

A küldő és a fogadó által használt IP protokoll verziószáma. Ennek megfelelően értelmezi a Sender Address és a Receiver Address mezőket.

Conf-Sender, Conf-Receiver

Ez adja meg a szervernek, hogy a küldőt vagy a fogadót kell-e konfigurálnia. Értéke 0 vagy 1.

Number of Schedule Slots

Ez adja meg, hogy két HMAC mező között hány slot rekord kerül küldésre.

Number of Packets

A teszt alatt elküldött csomagok száma.

SID

Session azonosító. Itt még nem értelmezett, majd a szerver adja meg.

Padding Length

Egy teszt csomaghoz fűzött oktetek száma.

Start Time

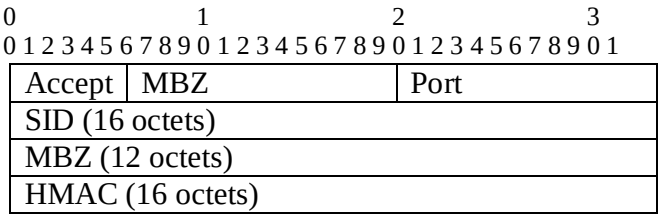
A Session indulásának kezdete.

Timeout

Az az idő, amely után ha a csomag nem érkezik meg, elveszettnek tekintik.

1.7.4.1.3.2 Accept-session message

A szerver a Request-Session üzenetre az alábbi Accept-Session üzenettel válaszol.



SID

A szerver itt adja meg a session azonosítót, úgy hogy veszi a saját négy oktetes IP címét, hozzáfűz egy nyolc oktetes időbélyeget, majd egy négy oktetes véletlen értéket.

Send Schedules

A küldőnek és a fogadónak egy közös ütemtervet kell követnie, hogy számon tudják tartani azt, hogy mikor kell vagy kellett volna egy tesztcsomagot megkapnia vagy elküldenie. Így ha bizonyos ideig nem érkezik meg, vagy késik a csomag, a fogadó fel tudja ismerni a hibát. Maga a teszt csomagok ismételt sorozatából áll, így az ütemezés úgy oldható meg, hogy fel kell osztani a

csomagsorozatot adott számú Slot-okra. Egy Slotnak van típusa és paramétere. Két típus támogatott: exponenciális eloszlású pszeudo-véletlenszám mennyiség (type 0) és egy rögzített mennyiség (type 1). A paramétert időbélyegben fejezzük ki, és egy időintervallumot ad meg. Exponenciális eloszlás esetén ez az érték az átlag, vagyis ha az exponenciális eloszlás sűrűségfüggvényét $\lambda*exp^{-\lambda*x}$-nek vesszük, akkor a várható értéke $1/\lambda$ lesz. Type 1 esetén ez az idő intervallum maga a késleltetés lesz.

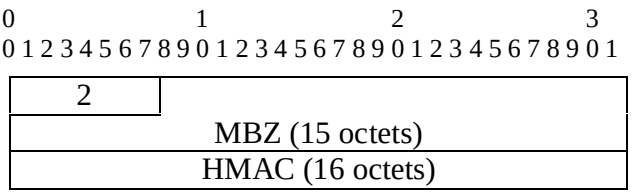
A küldő az ütemterv kezdetekor elkezdi végrehajtani a Slotokban lévő utasításokat. Tpye 0 esetén egy exponenciális eloszlás várható értékéig, Type 1 esetében egy előre megadott késleltetésig, vár, majd elküldi a teszt csomagot, és továbblép a következő Slotra. Ha elfogynak a Slotok, akkor az első Slottal kezdi újra a végrehajtást.
A típusokat kombinálva adhatunk meg tesztelési módokat:

Poisson sor: csak 0 típus
Periodikus Sor: csak 1 típus

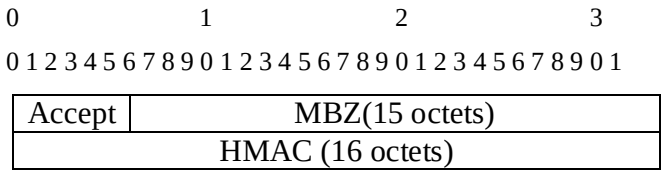
Egymást követő Poisson sor csomagpárok: két Slot, egyikben egy 0 típussal és egy nem nulla paraméterrel, másikban egy 1-es típussal és egy 1-es paraméterrel.

1.7.4.1.3.3 Test Session

Az OWAMP kliens, miután Accept-session megerősítést kap, egy Start–session üzenettel válaszol a szervernek, ami az alábbi üzenetek sorozata.



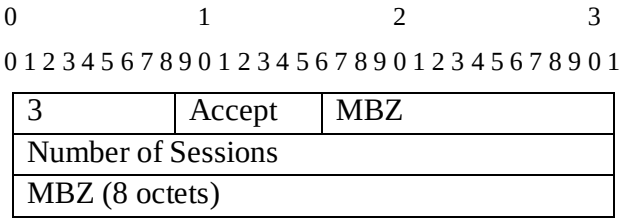
Erre a Server egy Start-Ack üzenettel válaszol.



Ezek után a küldő megkezdheti a tesztcsomagok küldését a fogadónak.

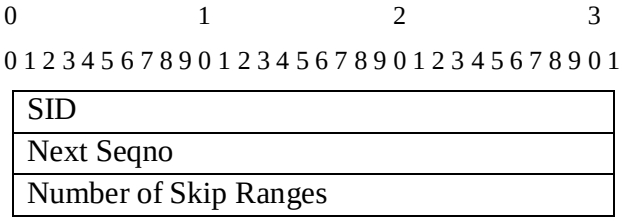
1.7.4.1.3.4 Stop-Sessions

A teszt leállításához szükséges üzenetet (Stop-Session) a server és a Kliens is küldhet.

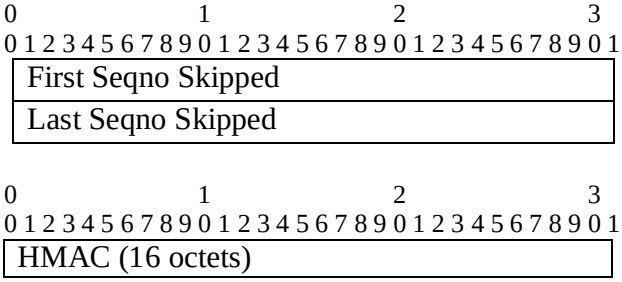


Number of Sessions

Session leíró rekordok száma, amelyek ezt az üzenetet majd követik.

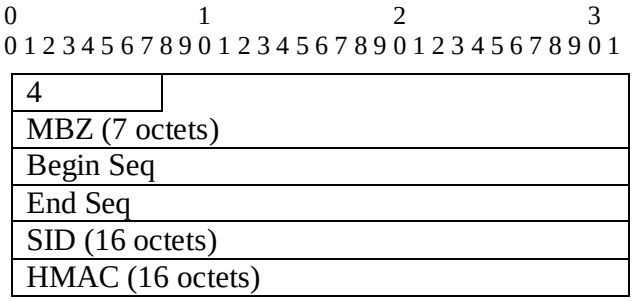


Ezt követi a Number of Skip Ranges számának megfelelő Skip range description:



1.7.4.1.3.5 Fetch-Session

Tipukusan klienshez köthető lekérdező üzenet.

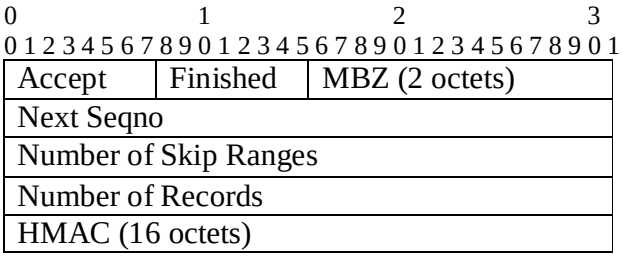


A keret mezőinek, értékeinek és jelentéseinek értelmezése:

Begin Seq: Az első csomag

End Seq: Az utolsó csomag

Erre a szerver egy Fetch-Ack üzenettel válaszol:



A keret mezőinek, értékeinek és jelentéseinek értelmezése:

Next Seqno

Az a következő sorszám, amelyet a szerver küldött volna, ha a teszt megszakítás nélkül futott le. Ekkor ez az érték a Request-Session-ben a csomagok számával (NumPackets) egyezik meg.

Number of Skip Ranges

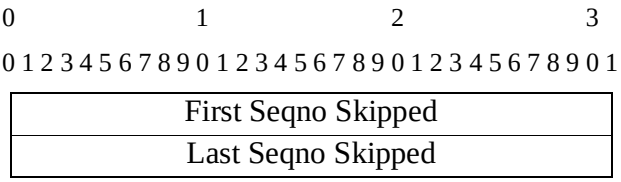
Ez jelzi, hogy hány rész volt ténylegesen kihagyva a küldés során.

Number of Records

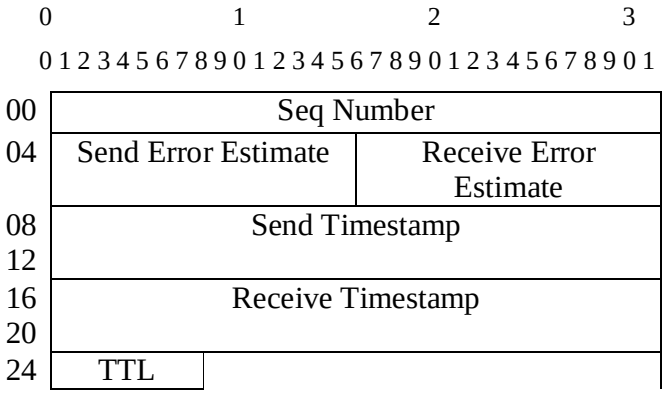
A csomagrekordok száma, amely a kért tartományra esik.

Következő lépésként a szerver elküldi az OWAMP-Test session adatait, mely az következő információkat tartalmazza.

- A Request-Session parancs másolatát, amely tartalmazza a pontszámokat.
- A Skip Range leírást, amely azt a két sorszámot jelenti, amelyek közt nem lett elküldve a csomag.



- A 16 oktetes HMAC-ot.
- Egy vagy több csomagrekordot, amelyek a beérkezés sorrendjében kerülnek kiküldésre.



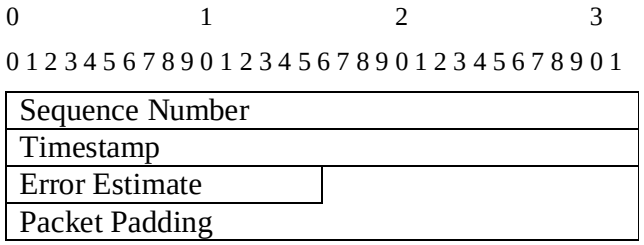
1.7.4.1.4 OWAMP Test protocol

1.7.4.1.4.1 Üzenet időzítések

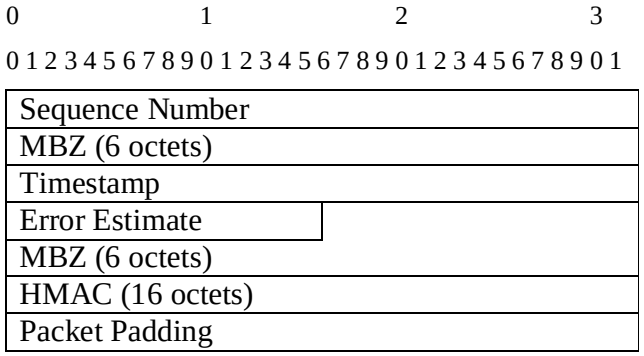
A teszt megkezdésekor a csomagok küldésének ütemezését egymástól függetlenül a slotok alapján határozza meg a küldő és a fogadó. Miután a Start-Sessions sikeresen végrehajtódott,

készen állnak a csomagok küldésére és fogadására, így a küldő azonnal megkezdheti a tesztelést az ütemezési tervnek megfelelően.

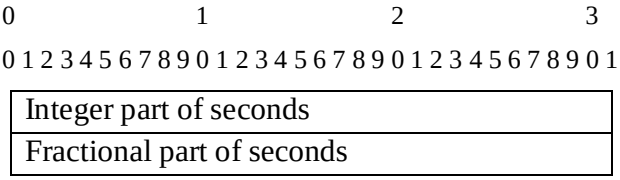
Az első ábra a tesztcsomag keretformátumát mutatja be.



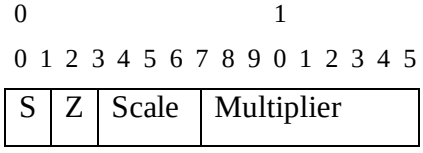
A második ábra a tesztcsomag formátumát mutatja be titkosított módban.



A harmadik ábra a timestamp keretformátuma.



A negyedik ábra az Error estimate keretformátuma:



A hiba becslésére a következő formulát használja: **Multiplier***2^(-32)*2^**Scale**

Az OWAMP teszt esetében a hitelesítéshez szükséges AES kulcsot az OWAMP-Control az AES kulcsból és a SID-ből származtatja.
Az OWAMP-test a HMAC kulcsot az OWAMP-Control HMAC kulcsából, és a SID-ből származtatja.

1.7.5 Y.1711

Az ITU-T létrehozott egy OAM ajánlást az MPLS számára, melynek segítségével definiálja az LSP mentén fellépő kapcsolódás ellenőrzési, gyors hiba detektálási és hibák diagnosztizálási módjait. Az Y.1711 OAM csomagokat a 14 es MPLS címkével különbözteti meg, melynek az értelmezése “OAM Alert Label”.

1.7.5.1 Kapcsolódás ellenőrzés (Connectivity Verification)

A CV funkcióval lehet az LSP kapcsolódási hiányosságait proaktívan detektálni, ezek a keretek másodpercenként kerülnek küldésre, valamint tartalmaznak egy Trail-Termination Source Identifier (TTSI) azonosítót, ami a LSR azonosítója. Adott körülmények között az alábbi hibás működés detektálását teszi lehetővé:

- Loss of Connectivity Verification (LOCV): Ha három periódus során nem kapja meg a CV OAM csomagokat, akkor a kapcsolatot megszakítottnak nyilvánítja.
- TTSI Mismatch: Ha a csomag TTSI értéke nem értelmezhető.
- TTSI Mismerge: Ha a kapott CV csomagok TTSI értékeinek egy része értelmezhető, illetve másik részük pedig nem.
- Excess: Ha három periódus során ötnél több CV csomagot kap.

1.7.5.2 Gyors hibadetektálás (Fast Failure Detection)

Ez egy proaktív funkció, lényegében hasonló a CV-hez, egyedül abban tér el, hogy ebben az esetben a periódus igény szerint állítható, és alapértelmezetten másodpercenként húsz csomagot küld, ezáltal a hibára nagyon kicsi reakcióidőn belül tud reagálni.

1.7.5.3 Forward Defect Indication (FDI)

Az LSP-n fellépő hiba helyétől kiindulva az LSR-ek FDI csomagokkal jelentik tovább a hibát a további eszközöknek.

1.7.5.4 Backward Defect Indication (BDI)

A hibától kiindulva, a vissza úton az LSR-ek BDI csomagokkal értesítik egymást, hogy az LSP-n hiba lépett fel.

1.7.6 Y.1731

Az ITU-T által kidolgozott OAM funkciók ajánlása Carrier ethernet hálózatokra, mely segítségével mérhető a késleltetés, a késleltetés szórása és a keretveszteség.

1.7.6.1 Ethernet Continuity Check (ETH-CC)

A MEG-ben a MEP-eknek nyújt segítséget, hogy proaktívan tudják észlelni a kapcsolati hibákat. A Continuity Check Messages (CCM) periodikusan 3.33 és 10 másodperc között kerül elküldésre, és az alábbi hiba okokat tudja jelezni.

- Loss of continuity (LOC): Ha 3.5 periódus alatt nem kapja meg a CCM csomagokat.

- Unexpected MEG level: A MEG level egy 3 bites szám, amely a hierarchia szintjét adja meg.
- Mismerge: Ha a kapott CCM egy olyan MEP-től érkezett, amelynek a MEP ID-ja nem ismert.
- Unexpected MEP: Ha a kapott CCM egy olyan MEP-től érkezett, amelynek a küldő MEP ID-ja nem ismert.
- Unexpected period: Amikor a küldés periódus mező a CCM-ben nem egyezik meg a várt a küldés periódus értékével.

1.7.6.2 Ethernet loopback function (ETH-LB)

Az Ethernet loopback lehetőséget nyújt arra, hogy ellenőrizze a szomszéd viszonyban lévő MEP-ek közti kapcsolatot. Első lépésként az egyik fél egy üdvözlő üzenetet küld a másik félnek, amelyre a szomszéd fél válaszol. Csak ezután van lehetőség a kétirányú kapcsolat szolgáltatáson belüli és kívüli tesztelésére.

Ethernet test (ETH-TST)
Olyan egyirányú teszt, amely során a csomagok nem kerülnek visszaküldésre a feladónak.

Ethernet Linktrace (ETH-LT)
On demand (igény szerinti) módon egy célhoz vezető útvonal felderítése és a hiba lokalizálása.

Alarm Indication Signal (ETH-AIS)
Ha a MEP hibát észlel, akkor másodpercenként periodikusan AIS, vagyis hibajelző üzenetet küld, amíg a hiba meg nem szűnik.

Lock (ETH-LCK)
A MEP kezdeményezi a lezárást, értesíti a szomszéd MEP-jeit, hogy álljanak le a szóban forgó forgalom továbbításával, amíg a lezárást fel nem oldja.

Remote Defect Indication (RDI)

Ha a MEP hibát észlel, akkor a szomszéd MEP-jeit egy RDI-al, vagyis egy távoli hibaüzenettel értesíti a hibáról.

Loss measurement (ETH-LM)

A MEP számára mérhetővé teszi a csomag eldobást. Minden MEP számon tartja azt, hogy az egyes MEP-ek számára mennyi csomagot küldött, illetve kapott azoktól. Mindezt az ETH_LM csomag fogja tartalmazni.

A csomagveszteséget két féle módon lehet számolni. Az egyik eset az, amikor csak a kapcsolat egyik végén „on-demand" módon számolják. A másik eset pedig az, amikor a kapcsolat két végén proaktívan számolják. A második esetben a csomagveszteséget a CCM üzenetek LM mezői fogják tartalmazni.

Delay measurement ETH-DM

A két MEP közötti csomag késleltetést és szórást igény szerinti „on-demand" módon lehet mérni. Egyirányú mérés esetén csak az egyik fél küld csomagokat a másiknak. Illetve lehetőség van két irányban mérni, abban az esetben mindkét fél küld csomagot a szomszédjának.

1.7.7 IEEE 802.1ag

Az IEEE is létrehozott egy OAM szabványt a Carrier Ethernet alapú hálózatok számára, amelynek segítségével a szolgáltatóknak lehetőségük nyílik end-to-end kapcsolati hibák kezelésére. A 802.1ag képes az ügyfelekkel szerződésben megkötött és szolgáltatott SLA-k minden egyes Ethernet Virtual Connection-jének történő (EVC) külön-külön megfigyelésére. Ez a szabvány három fő funkcióra, a continuity check-re, loopback-ra és linktrace-re épül.

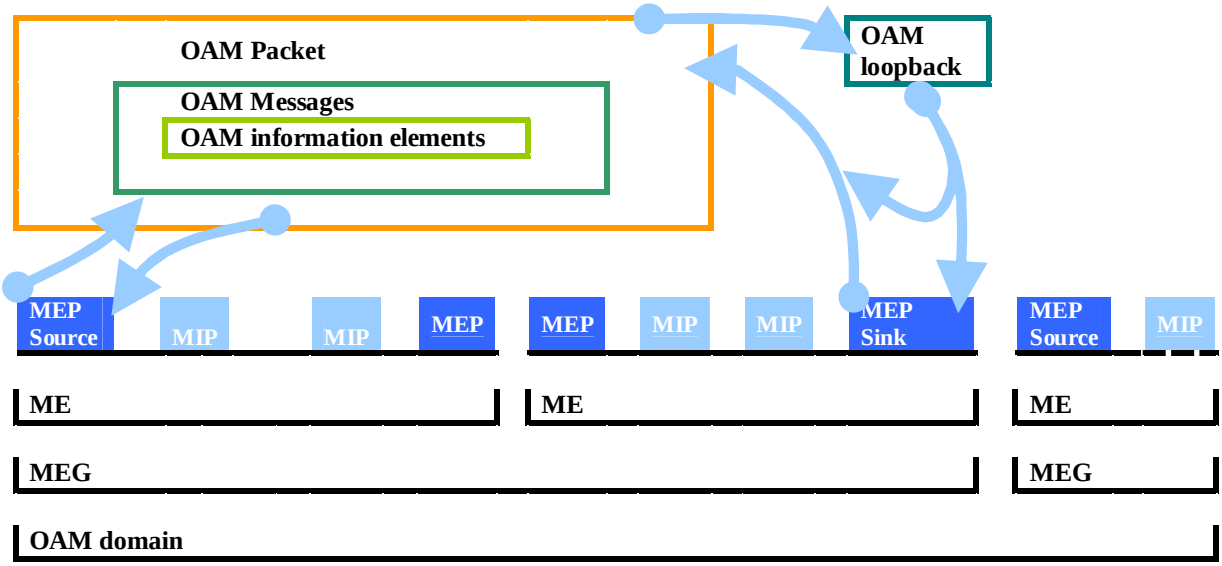
1.7.8 IEEE 802.3ah

Olyan IEEE szabvány, amely egy adott Ethernet szegmens menedzsmentjét rögzíti. Fizikai kapcsolat szintű menedzsmentet valósít meg, amely során lehetőség van kezelni kétirányú kapcsolatok esetében azt, ha az egyik irány megszakad. Továbbá a szegmens távoli eszközét loopback módba kapcsolhatja, amely biztosítja a szegmens tesztelését.

1.7.9 E-LMI

Az Ethernet Local Management Interface protokollt a Metro Ethernet Forum (MEF) hozta létre. A jelentősége abban rejlik, hogy az Ethernet menedzselhetőségét egészen az ügyfél hatásköréig tágítja, és a CE eszköz automatikusan kapja meg a VLAN-EVC hozzárendelést, illetve a QoS beállításokat. Ezzel a funkcióval kiküszöbölhetőek az emberi hibák, és hiba esetén gyorsabban tud reagálni a hálózat a változásokra.

1.7.10 MPLS-TP OAM referencia modell



12. MPLS-TP OAM referencia modell

OAM information element

Egy OAM alkalmazás által használt MEP-ek és MIP-ek közti elemi információ.

OAM Message

Olyan information element-ek, amelyek MEP-ek és MIP-ek között valamilyen OAM funkciót hajtanak végre.

OAM flow

Egy MEP által küldött OAM üzenetek sorozata.

OAM loopback

Egy csomópont azon képessége, hogy egy bizonyos utasításra megfelelő választ küldjön az utasítás küldőjének.

1.7.10.1 Continuity Check

A proaktív folytonossági ellenőrzésre vonatkozó leírásokat az RFC 5860 rögzíti. Ez a dokumentum rögzíti a CC-V üzeneteket, amelyek segítségével a két MEP között fellépő kapcsolati hibákat lehet észlelni, és reagálni azokra.

Loss of continuity defect (LOC)

Ha egy „sink“ MEP a „source” MEP-től a CC-V fogadó periódus három és félszereséig nem kap üzeneteket, akkor a kapcsolatot megszakadtnak veszi.

Mis-connectivity defect

Amikor egy CC-V üzenetet kap a „sink“ MEP-től, ellenőrzi a „source” MEP egyedi azonosítóját és a csomagolást. Ha nem ismeri ezeket a paramétereket, akkor hibát jelez és letiltja az ismeretlen MEP-től származó forgalmat.

Period Misconfiguration defect

Ez a hiba jelzi ha a „source” MEP-en és a „sink“ MEP-en az üzenetidőzítők nem egyeznek.

Unexpected encapsulation defect

Ez a jelzés akkor fordul elő, ha a „sink“ MEP egy ismeretlen csomagolású üzenetet kap. Ez csak egy figyelmeztetés és nincs közvetlen következménye.

Remote Defect Indication (RDI)

Ezzel jelzi a „sink” MEP a „source” MEP-nek, hogy egy jelzéskiesési állapot áll fenn. Ilyen körülmény lehet a „continuity defect”, vagy a „connectivity defect”, és amíg a körülmény fennáll, addig minden küldött CC-V üzenet tartalmazni fogja ezt a jelzést.

Alarm Indication Signal (AIS)

Amikor egy server MEP válaszjelzése kiesik, akkor értesíti a szomszédos eszközöket. Amíg a hiba fennáll, periodikusan AIS üzeneteket generál „downstream” irányba, így azok ez idő alatt vissza tudják fogni a másodlagos „loss of continuity defect” hibaüzeneteiket. Fontos megjegyezni, hogy a MIP-ek nem értelmezik az AIS üzeneteket.

Lock Reporting

Az RFC 5860-ban definiált Locked Report-ot (LKR) használja. Mikor egy szerver MEP le van zárva, akkor az MPLS-TP kliens LKR üzeneteket küld mindkét irányba, és így fogja vissza a másodlagos hibaüzeneteket.

Packet Loss Measurement (LM)

Az MPLS-TP Performance Monitoring (PM) része, amellyel egy útvonal QoS paramétereit lehet mérni. Az LM két számlálót tart számon: a két szóban forgó MEP közti ki és bemenő csomagok számát. A Packet Loss Measurement nagyon fontos elem a hibakeresési folyamat során, hiszen már az elején tisztázza a hibakeresést végző csoportok számára, hogy mely területek kiemelt fontosságúak a probléma megoldásának szempontjából. A két szomszédos MEP a Proaktív LM segítségével periodikusan küld és fogad OAM csomagokat, és ezekből teljesítmény statisztikát készít. Az OAM csomagok az ügyfél forgalmával együtt kerülnek továbbításra, és a számlálók

alapján kiszámolható, hogy hol kerül eldobásra az adott csomag. Egy adott MEP számára a „near-end packet loss” fogja jelenteni a bejövő forgalom csomagveszteségét, a „far-end packet loss” pedig a kimenő forgalom csomagveszteségét.

Packet Delay Measurement (PM)

Ennek segítségével végezhető az útvonal QoS paramétereinek ellenőrzése. A két szomszédos MEP egy adott időintervallum alatt proaktív módon DM csomagokat küld és fogad. A Packet Delay Measurement egyirányú vagy kétirányú is lehet. Egyirányú PM esetében a MEP OAM olyan csomagokat küld a szomszédjának, amelyek tartalmazzák a szükséges információkat az egyirányú késleltetés kiszámításához. Ehhez egy idő szinkronizálásáért felelős protokoll is szükséges. Kétirányú PM esetében mindkét fél OAM kéréseket küld a szomszédjának, melyre olyan OAM csomagokkal válaszolnak, amelyek tartalmazzák a szükséges információkat a kétirányú késleltetés kiszámításához.

Client Failure Indication (CFI)

Ha az ügyfél által használt OAM technológia nem támogatja az AIS üzenetet, akkor a CFI segítségével lehet megvalósítani a lokális vagy a távoli „Attachment Circuit” (AC) felügyeletét.

1.7.10.2 Connectivity Verification

Throughput Estimation

Ez egy igény szerinti „on-demand” szolgáltatáson kívüli funkció, mely lehetővé teszi az MPLS-TP útvonal sávszélességének az ellenőrzését. Az átviteli sebességet tetszőlegesen ellenőrizhetjük két MEP, vagy egy MEP és egy MIP között. A két fél közt végzendő teszthez be kell állítani az OAM csomag méretét, a becsomagolt minta típusát, és az útvonalra egy zárat kell tenni. A teszt alatt növekvő ütemben OAM csomagokat küld a két fél egymásnak, figyelik a csomagveszteséget, a kihasználtságot, és megállapítják az elméleti legnagyobb átviteli sebességet. A teszt lehet egyirányú, ebben az esetben csak az egyik fél küld OAM csomagokat a másiknak. A teszt kétirányú, ha a távoli fél a csomagokat visszairányítja a küldőjének, de mivel

ez csak a kétirányú minimum átviteli sebességet határozza meg, ezért érdemes inkább mindkét irányba külön egy egyirányú tesztet elvégezni.

Data plane Loopback

Lehetőség van arra, hogy egy útvonalon egy MEP vagy egy MIP visszairányítsa a forgalmat a küldőnek.

Route Tracing

Lehetővé teszi, hogy egy teljes MPLS-TP útvonalon lévő eszközöket felderítse a vonalhibáig.

Lock Instruct (LKI)

Ezzel a funkcióval egy MEP az útvonal hozzá közeli végéhez egyoldalúan zárat helyez, majd utasítja a szomszédját arra, hogy zárja le az MPLS-TP útvonal távoli részét is. A szomszéd MEP vagy elfogadja, vagy elutasítja ezt. Amíg a két fél nem oldja fel a zárat, addig az MPLS-TP útvonal zár alatt lesz.

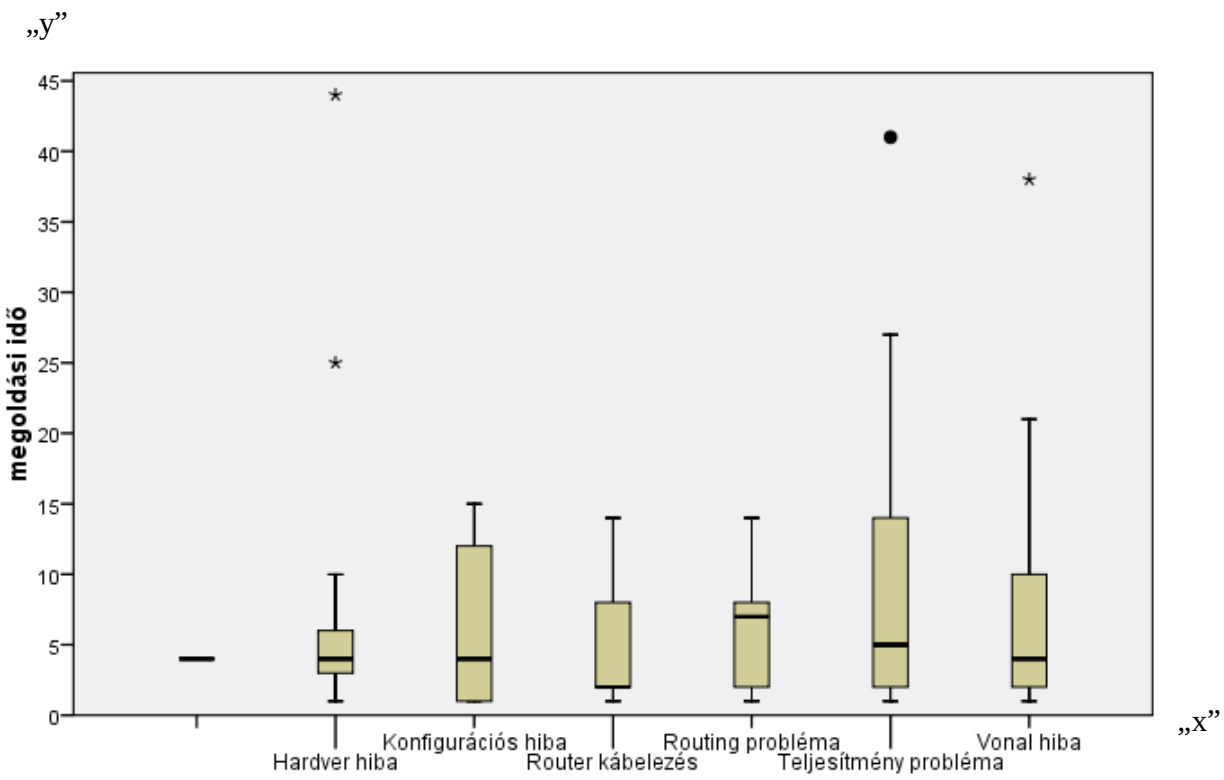
1.8 Hálózati problémák statisztikai felmérése

Jelenleg az IT Services Hungary Kft, debrecen hálózati szolgáltatásokat nyújtó Platform Provisioning and Operations részlegében dolgozok. Munkám során sokféle hálózati hibával találkozok, ezért kézenfekvő volt, hogy egy statisztikai felméréssel igazoljam az MPLS-TP létjogosultságát. Arra a kérdésre kerestem a választ, hogy a szolgáltatói hálózatokban előforduló hálózati hibák közül melyek fordulnak elő a leggyakoribban, és ezek milyen tendenciákat mutatnak.

A vizsgálat menete a következő volt. A beérkező hálózati problémákat hibakategóriákba soroltam be, majd ezeket összegeztem egy adatbázisban, végül mindezt SPSS-be importáltam. Hipotézisem az volt, hogy a teljesítménnyel kapcsolatos problémák növekvő tendenciát mutatnak és megoldásuk növekvő munkaidő ráfordítást igényelnek. A felmérést 2010. augusztus 1. és

2010. november 30. között végeztem el, mely idő alatt összesen 414 hibajegyet sikerült besorolnom. A diagramon az „y” tengelyen található a probléma megoldásával töltött napok száma, az „x” tengelyen pedig a hat leggyakoribb hálózati probléma kategória látható: hardver hiba, konfigurációs hiba, router kábelezés, routing probléma, teljesítmény probléma, vonalhiba.

Az SPSS-ben készített boxplot diagramból kiderül, hogy a legtöbb munkaerőt és munkaidőt a teljesítmény problémák megoldásának feladatai foglalják le. Az adatok szerint a megoldási idő mediánja 6 nap, és a hiba beérkezéstől a megoldásáig maximum 27 nap telt el. Második helyen a szintén teljesítmény problémákat okozó vonalhibák állnak. Ezeknek a mediánja 5 nap és a megoldásuk maximális időtartama akár 23 nap is lehet. A kiugró értékek kezelhetetlen problémákat jelentenek.



13. Hálózati problémák megoldásának időtartama

Mivel más probléma kategóriáknál nem tapasztalható ilyen hosszú megoldási idő, valamint az így megfigyelt tendenciák és a kiugró értékeik arra engednek következtetni, hogy a jelenleg használt hibakeresési folyamatok nem tartanak lépést a technológiai változásokkal, és az ügyfelek elvárásaival. Így igazoltnak látom az a feltevés, hogy a jövőben kiemelten kell foglalkozni e problémák megoldási stratégiájának újragondolásával és megoldási idejük csökkentésével. Fontos, hogy az új technológiai fejlődéssel együtt járó változások a hozzájuk kapcsolódó új hibakeresési folyamatokkal egy időben kerüljenek elsajátításra és alkalmazásra.

Összefoglalás:

Dolgozatomban ismertettem a jövőbeni hálózatoktól elvárt ügyfél követelményeket, és a szolgáltatókra háruló megoldások bevezetésének és továbbfejlesztések irányvonalát. Bemutattam az MPLS-TP alapú csomagkapcsolt hálózat alapelveit és a technológiával kapcsolatos szabványokat és módszereket. Kiemeltem az MPLS-TP hálózati referencia modelljét, amely az ügyfelek egyedi igényei szerint tovább bővíthető, és a szolgáltatók jelenleg használt hálózatára ráilleszthető. Ez egy olyan referencia modell, mely nagyon fontos viszonyítási pont az OAM-ben használatos hibakeresési és jelzési módszerek értelmezéséhez. A szolgáltatóknak erre a modellre alapozva javasolt felülvizsgálniuk, egyszerűsíteniük és átalakítaniuk a jelenleg használt hibakeresési folyamataikat. Mivel a szolgáltatási színvonal elsődlegesen a munkafolyamatok szervezettségén alapul, ezért a kidolgozott új technológiákhoz illeszkedő folyamatokat fel kell bontani részfolyamatokra, majd ezeket különböző kompetenciájú csoportokhoz kell rendelni, és a csoportok munkáját koordinálni.

A szolgáltatóknak fel kell készülniük a hálózataikból elavult technológiák felváltására, valamint a szolgáltatott teljesítmény és megbízhatóság növelésére. Ez a feladat sok szempontból is választás elé állítja majd a szolgáltatókat. Először alacsony beruházási költségű (CAPEX), jól skálázható, és hosszú távon elegendő erőforrással rendelkező eszközökbe kell befektetniük. Ezek után az alkalmazottaknak el kell sajátítaniuk az új technológiával és eszközökkel együttjáró új szaktudást, mivel csak így biztosíthatóak az alacsony üzemeltetési költséget (OPEX) eredményező hibakeresési és életciklusbeli folyamatok hatékony használata.

A dolgozatomban leírtakból is látszik, hogy a szolgáltatói hálózatok tervezésekor és üzemeltetésekor nagyon sok tényezőt kell figyelembe venni, és ezek alapján kell a lehető legjobb döntést meghozni. Mivel a jövőben is az ügyfelek fogják majd diktálni a követelményeket, nagyon fontos, hogy a szolgáltatók a jövőben egy hatékony OAM orientáltságú szemléletmódot valósítsanak meg. Célom az volt, hogy betekintést nyújtsak ebbe a témakörbe, és remélem sikerült alátámasztanom azt, hogy egy szolgáltató sikerességét az fogja meghatározni, mennyire képes a versenytársakat megelőzve megfelelni az ügyfelek követelményeinek.

Irodalomjegyzék

Könyvek:

[1] **Eric Osborne; Ajay Simha**: Traffic engineering with MPLS: Cisco Press, 2003.

[2] **Adrian Farrel; Igor Bryskin**: GMPLS: architecture and applications: Elsevier Inc, 2006.

[3] **Alwayn; Vivek:** Advanced MPLS design and implementation. Indianapolis: Cisco Press, 2001.

[4] **Tanenbaum; Andrew S.:** Számítógép-hálózatok. Budapest: Panem, 2004.

[5] **De Ghein; Luc:** MPLS fundamentals. Indianapolis: Cisco Press, 2007.

[6] **Sam Halabi; Bassam Halabi:** Metro ethernet: Cisco Press: 2003.

[7] **Sanjay Jha, Mahbub Hassan:** Engineering Internet QoS: ARTECH HOUSE, INC, 2002.

[8] **Zheng Wang:** Internet QoS: architectures and mechanisms for quality of service: Academic Press, 2001.

[9] **Uyless D. Black**: MPLS & label switching networks: Prentice Hall PTR, 2002.

[10] **Ina Minei, Julian Lucek:** MPLS-enabled applications: emerging developments and new technologies: John Wiley and Sons, 2008.

Cikkek:

[11] **Dieter Beller, Rolf Sperber**: MPLS-TP – The New Technology for Packet Transport Networks. 2009.

[12] Ethernet Operations, Administration, and Maintenance. Cisco Press. Cisco Press, 2007

RFC dokumentumok (https://datatracker.ietf.org/doc/search/)

[13] **Matthew Bocci; Stewart Bryant; Dan Frost; Lieven Levrau; Lou Berger**: A Framework for MPLS in Transport Networks. 2010. RFC5921.

[14] **Eric Gray; Scott Mansfield; Hing-Kam (Kam) Lam**: Network Management Requirements for MPLS-based Transport Networks. 2010. RFC5951.

[15] **Matthew Bocci; Stewart Bryant; Dan Frost**: MPLS Transport Profile Data Plane Architecture. 2010. RFC5960.

[16] **Dave Allan; Italo Busi; Ben Niven-Jenkins; Annamaria Fulignoli; Enrique Hernandez-Valencia; Lieven Levrau; Vincenzo Sestito; Nurit Sprecher; Huub van Helvoort; Martin Vigoureux; Yaacov Weingarten; Rolf Winter:** Operations, Administration and Maintenance Framework for MPLSbased Transport Networks. 2010. draft-ietf-mpls-tp-oam-framework-09.

[17] **Stewart Bryant; Prayson Pate:** Pseudo Wire Emulation Edge-to-Edge (PWE3) Architecture. 2005. RFC3985.

[18] **Loa Andersson; Lou Berger; Luyuan Fang; Nabil Bitar; Eric Gray, Attila Takacs; Martin Vigoureux; Elisa Bellagamba:** MPLS-TP Control Plane Framework. 2010. draft-ietf-ccamp-mpls-tp-cp-framework-03.

[19] **Dave Katz; Dave Ward:** Bidirectional Forwarding Detection. 2010 RFC5880.

[20] **Min Xiao; LiZhong Jin; Bo Wu; Jian Yang**: Throughput Estimation for MPLS based Transport Networks. 2010. draft-xiao-mpls-tp-throughput-estimation-01.

[21] **Stanislav Shalunov; Benjamin Teitelbaum; Anatoly Karp; Jeff W. Boote; Matthew J. Zekauskas**: A One-way Active Measurement Protocol (OWAMP). 2006. RFC4656.

[22] **Kaynam Hedayat; Roman M. Krzanowski, Ph.D.; Al Morton; Kiho Yum; Jozef Z. Babiarz**: A Two-Way Active Measurement Protocol (TWAMP). 2008. RFC5357.

[23] **George Swallow; Monique Morrow; Yuichi Ikejiri; Kenji Kumaki; Peter B. Busschbach; Rahul Aggarwal; Luca Martini; Thomas D. Nadeau; Carlos Pignataro**: Pseudo Wire Virtual Circuit Connectivity Verification (VCCV): Control Channel for Pseudo Wires. 2007. RFC5085.

[24] **Ben Niven-Jenkins; Deborah Brungard; Malcolm Betts; Nurit Sprecher; Satoshi Ueno**: Requirements of an MPLS Transport Profile. 2009. RFC5654.

[25] **Stephan Emile; Lei Liang; Al Morton:** IP Performance Metrics (IPPM): Spatial and Multicast. 2009. RFC5644.

[26] **Seisho Yasukawa; Adrian Farrel; Zafar Ali; George Swallow; Thomas D. Nadeau; Shaleen Saxena**: Detecting Data Plane Failures in Point-to-Multipoint Multiprotocol Label Switching (MPLS) - Extensions to LSP Ping. 2010. draft-ietf-mpls-p2mp-lsp-ping-13.

[27] **Italo Busi; Huub van Helvoort; Jia He**: MPLS-TP OAM based on Y.1731. 2010. draft-bhh-mpls-tp-oam-y1731-05.

[28] **Martin Vigoureux; David Ward; Malcolm Betts:** Requirements for Operations, Administration, and Maintenance (OAM) in MPLS Transport Networks. 2010. RFC5860.

[29] **Daniel O. Awduche; Lou Berger; Der-Hwa Gan; Tony Li; Vijay Srinivasan; George Swallow**: RSVP-TE: Extensions to RSVP for LSP Tunnels. 2001. RFC3209

[30] **Kenji Kumaki; Raymond Zhang; Yuji Kamite**: Requirements for Supporting Customer Resource ReSerVation Protocol (RSVP) and RSVP Traffic Engineering (RSVP-TE) over a BGP/MPLS IP-VPN. 2010. RFC5824.

[31] **Arthi Ayyangar; Kireeti Kompella; JP Vasseur; Adrian Farrel**: Label Switched Path Stitching with Generalized Multiprotocol Label Switching Traffic Engineering (GMPLS TE). 2008. RFC5150

Tanulmányok:

[32] **Istvan Kakonyi; Yves Hertogh**: Carrier Ethernet: Overview, Architecture and Technology Variants. 2009.

Internet

[33] MPLS/Tag Switching - http://www.cisco.com/en/US/docs/internetworking/technology/handbook/MPLS_Tag-Switching.html

[34] BGP Support for BFD http://www.cisco.com/en/US/docs/ios/12_2sr/12_2sra/feature/guide/srbgpbfd.html

Köszönetnyilvánítás

Ezúton szeretném megköszönni témavezetőmnek, Dr. Almási Bélának a dolgozat elkészítése során nyújtott szakmai segítségnyújtást, valamint építőjellegű kritikáit.