

Univerzita Komenského v Bratislave  
Fakulta matematiky, fyziky a informatiky

Protokol TRILL  
Bakalárska práca

Bratislava, 2022

Lenka Kudláčová

Univerzita Komenského v Bratislave  
Fakulta matematiky, fyziky a informatiky

Protokol TRILL  
Bakalárska práca

Študijný program: Aplikovaná informatika  
Študijný odbor: Informatika  
Školiace pracovisko: Katedra aplikovanej informatiky  
Školiteľ: RNDr. Jaroslav Janáček, PhD

Bratislava, 2022

Lenka Kudláčová



## ZADANIE ZÁVEREČNEJ PRÁCE

**Meno a priezvisko študenta:** Lenka Kudláčová  
**Študijný program:** aplikovaná informatika (Jednoodborové štúdium, bakalársky I. st., denná forma)  
**Študijný odbor:** informatika  
**Typ záverečnej práce:** bakalárska  
**Jazyk záverečnej práce:** slovenský  
**Sekundárny jazyk:** anglický

**Názov:** Protokol TRILL  
*TRILL Protocol*

**Anotácia:** Práca sa venuje predstaveniu protokolu TRILL a jeho porovnaniu s klasickými protokolmi používanými v počítačových sieťach s redundantnými linkami.

**Cieľ:**

- popísať protokol TRILL
- stručne popísať vybrané klasické alternatívy
- porovnať protokol TRILL s klasickými protokolmi, identifikovať výhody, nevýhody
- stanoviť odporúčania na výber protokolu pre bežné scenáre použitia

**Vedúci:** RNDr. Jaroslav Janáček, PhD.  
**Katedra:** FMFI.KI - Katedra informatiky  
**Vedúci katedry:** prof. RNDr. Martin Škoviera, PhD.  
**Dátum zadania:** 05.10.2021

**Dátum schválenia:** 06.10.2021

doc. RNDr. Damas Gruska, PhD.  
garant študijného programu

---

študent

---

vedúci práce

## Čestné prehlásenie

Čestne prehlasujem, že som túto bakalársku prácu na tému Protokol TRILL vypracovala sama pod vedením RNDr. Jaroslava Janáčka, PhD. s použitím literatúry uvedenej v závere tejto bakalárskej práce.

V Bratislave dňa 5. mája 2022.

.....

Lenka Kudláčová

## Pod'akovanie

Touto cestou by som sa veľmi rada pod'akovala môjmu vedúcemu bakalárskej práce RNDr. Jaroslavovi Janáčkovi, PhD. za odborné rady, ústretovosť, ochotu, pomoc a nasmerovanie správnym smerom.

## Abstrakt

Práca sa venuje predstaveniu protokolu TRILL, sú spomenuté vylepšenia oproti klasickému protokolu STP. Ďalej som protokol TRILL porovnala s alternatívnym protokolom SPB. Práca sa zaoberá popisom protokolu TRILL, taktiež popisom vybraných klasických alternatív pri problematike počítačových sietí s redundantnými linkami, stanovenie odporúčaní pre bežné využitie protokolu.

Kľúčové slová : TRILL, RBridge, IS-IS, STP, SPB

## Abstract

The work is devoted to the introduction of the TRILL protocol, improvements compared to the classic STP protocol are mentioned. Next, I compared the TRILL protocol with the alternative SPB protocol. The work focuses on the description of the TRILL protocol, as well as the description of selected classical alternatives in the issue of computer networks with redundant lines, setting recommendations for the common use of this protocol.

Keywords: TRILL, RBridge, IS-IS, STP, SPB

# Obsah

Úvod.....	9
1. OSI model.....	10
1.1. Linková vrstva.....	10
1.2. Sieťová vrstva .....	11
1.3. Porovnanie vrstvy 2 a 3.....	12
2. Protokol TRILL .....	13
2.1. Čo nové TRILL používa .....	14
2.2. Ako TRILL funguje .....	15
2.3. Posielanie rámcov .....	15
2.4. Formát hlavičky TRILL .....	19
2.4.1. Nickname RBridge .....	22
2.4.2. Rozšírenia hlavičky .....	23
2.4.3. TRILL OAM rámce.....	23
2.5. Link State Protocols (LSP).....	23
2.5.1. IS-IS.....	24
2.6. Point to Point Protokol a TRILL.....	25
2.7. Fungovanie RBridge-ov .....	25
2.8. Návrh implementácie RBridge.....	26
2.9. Primárne využitie TRILL protokolu .....	27
2.10. Vedľajšie využitie TRILL .....	29
3. Iné protokoly.....	29
3.1. STP protokol .....	29
3.2. SPB protokol .....	31
3.2.1. Porovnanie TRILL a SPB.....	32
3.3. Cisco FabricPath .....	34
3.3.1. Ďalšie podobné protokoly.....	35
4. Záver .....	36
Stránky – literatúra.....	37



## Úvod

V dnešnej dobe sa všetko vyvíja a nezaostávajú ani počítačové siete, ktoré napredujú veľkou rýchlosťou, či už napredujú softvérovo alebo aj hardvérovo, veď jedno napreduje s druhým súčasne. Kvôli požiadavkám na počítačové siete, ktoré často vyžadujú lepšiu škálovateľnosť alebo komplexnosť, sa musia zdokonaľovať aj protokoly sietí. V dnešnej dobe si veľa informácií a dát ukladáme na virtuálne disky, preto prístup k nim by mal byť čo najrýchlejší, a tým sa zároveň kladú požiadavky na tieto technológie. Osvedčené protokoly sa stali pomalé dokonca pri veľkom množstve komunikácie to nezvládali. Tento problém si všimla pani Perlman a začala hľadať spôsoby ako by sa to mohol zlepšiť konkrétne algoritmus Spanning Tree. S výskumnou skupinou vynašli protokol TRILL, ktorý všetky nedostatky STP protokolu zlepšuje ba i odstraňuje niektoré z nich. [15] [2] [14]

Pri sieťových protokoloch najprv popíšeme referenčný model OSI, následne sú v práci vybrané dve vrstvy, ktoré úzko súvisia s protokolom TRILL, a následne popísané bližšie a tiež je uvedený rozdiel v týchto vrstvách.

Cieľom práce je popísať protokol TRILL a aj popísať klasické alternatívy protokolu. Sú rozobrané jeho alternatívne protokoly. Určiť výhody a nevýhody TRILL protokolu. Popísať jeho zaradenie do bežného používania.

# 1. OSI model

Pri popise sieťových protokolov a architektúr sa zvyčajne využívajú spoločné normy, ktoré sa nazývajú referenčný model ISO OSI. Ide o architektúru zo siedmimi vrstvami, pričom každá vrstva má špecifickú funkčnosť a na každej vrstve sú definované rôzne protokoly. Všetky vrstvy spolu spolupracujú na prenose dát od jednej osoby alebo zariadenia k druhému. [24][25]

1. Prvá najnižšia vrstva je fyzická, tá obsahuje informácie vo forme bitov, ktoré len prenáša cez zariadenia ( kábel, hub, switch, modem, atď. ).
2. Linková vrstva je druhá vrstva modelu OSI. Táto vrstva prenáša rámce medzi susednými zariadeniami.
3. Sieťová vrstva je tretou vrstvou a slúži na prenos údajov a prenáša pakety.
4. Transportná vrstva je štvrtou vrstvou, ktorá poskytuje služby vyššej vrstve a preberá služby zo sieťovej vrstvy. Táto vrstva pracuje s údajmi označované ako segmenty.
5. Relačná vrstva je piatou vrstvou, ktorá má za úlohu nadviazať spojenie a udržať reláciu, autentifikáciu a tiež zaisťuje bezpečnosť. Táto vrstva prenáša dáta.
6. Prezentačná vrstva je šiestou vrstvou. Dáta z aplikačnej vrstvy sa tu spracujú podľa požadovaného formátu na prenos cez sieť. Táto vrstva pracuje s dátami.
7. Aplikačná vrstva je siedmou najvyššou vrstvou, túto vrstvu implementujú sieťové aplikácie, ktoré produkujú dáta. Tieto dáta sa musia prenášať cez sieť. Táto vrstva slúži ako také okno pre aplikačné služby na prístup k sieti a na zobrazovanie prijatých informácií používateľovi. [24][25]

Pretože protokol TRILL pracuje na druhej vrstve OSI modelu s využitím niektorých protokolov z tretej vrstvy OSI modelu, viacej sa zameriame na druhú a tretiu vrstvu OSI modelu. Aby sme mali lepší obraz ako presne fungujú a aké protokoly obsahujú ich trocha popíšeme. [24][25]

## 1.1. Linková vrstva

Túto vrstvu tiež poznáme ako vrstvu dátového spojenia (Data link layer). Táto vrstva je protokolovou vrstvou, ktorá prenáša dáta známe ako rámce medzi susednými sieťovými uzlami v sieti (WAN) alebo medzi uzlami v rovnakom segmente lokálnej siete (LAN). Vrstva poskytuje funkčné a procesné prostriedky na prenos dát medzi sieťovými zariadeniami a má prostriedky na detekciu a prípadnú opravu chýb, ktoré môžu nastať na fyzickej vrstve. [26][27] Táto vrstva pozostáva z dvoch podvrstiev:

1. Media Access Control (MAC) – táto podvrstva riadi prístup k médiu (napríklad CSMA/CD, CSMA/CA).
2. Logical Link Control (LLC) – táto podvrstva sa zaoberá adresovaním a multiplexingom.

Paket ktorý je prijatý zo sieťovej vrstvy bude ďalej rozložený na rámce na základe veľkosti rámca NIC (Network Interface Card). Linková vrstva musí korektne rozpoznať začiatok a koniec rámca, ako aj jeho samostatné časti. Má za úlohu overiť korektnosť prenosu postupnosti bitov medzi dvomi uzlami. Keď na linke nastane chyba napríklad v dôsledku šumu, táto vrstva môže požiadať o opakované zaslanie poškodenej postupnosti bitov. [26][27]

Funkcie linkovej vrstvy sú:

1. Rámčovanie – je funkcia, ktorá sa používa pridaním špeciálnych znakov v sade bitov na začiatok a koniec rámca.
2. Fyzické adresovanie – do hlavičky každého rámca pridá fyzické adresy (MAC adresu) príjemcu a odosielateľa .
3. Kontrola chýb – poskytuje mechanizmus kontroly chýb. Tento mechanizmus zachytáva a opakovane žiada o zaslanie poškodených alebo stratených rámcov.
4. Riadenie toku – zariadenie nemôže posielat' rámce rýchlejšie ako je príjemca schopný ich prijať, inak sa môžu rámce poškodiť, čiže riadenie toku koordinuje veľkosť údajov ktoré je možné odoslať pred prijatím potvrdenia.
5. Riadenie prístupu – keď jeden komunikačný kanál zdieľa viacero zariadení, podvrstva MAC pomáha určiť, ktoré zariadenie v danom čase vysiela a ostatný musia čakať kým odvysiela.[24]

Príklady protokolov linkovej vrstvy sú Ethernet pre lokálne siete, Point-to-Point Protocol (PPP), HDLC a ADCCP pre PPP (dual-node) spojenia. [27]

## 1.2. Sieťová vrstva

Táto vrstva slúži na prenos údajov medzi zariadeniami umiestnené v sieti. Tiež vyberá najkratšiu cestu z počtu dostupných ciest na prenos paketu a do každej hlavičky paketu je umiestnená IP adresa odosielateľa a príjemcu. [24]

Funkcie sieťovej vrstvy sú:

1. Smerovanie – Protokoly sieťovej vrstvy zistia a určia, ktorá cesta je najkratšia a najdostupnejšia od zdroja do cieľa. Táto funkcia sieťovej vrstvy je známa ako smerovanie.
2. Logické adresy – Prostredníctvom logických adries je možné prenos paketov z jedného zariadenia na druhé, aj medzi sieťami. Aby bolo možné jednoznačne identifikovať každé zariadenie v sieti, sieťová vrstva definuje IP adresy v sieťach, ktoré používajú IP protokol na sieťovej vrstve. Adresa zariadenie má dve časti – časť označujúca sieť do ktorej zariadenie patrí (napríklad ako v pošte : Mesto + PSČ), a časť označujúca konkrétny uzol (ako v pošte – ulica, číslo domu). IP adresa odlišuje výslovne každé zariadenie univerzálne od iného. [24]

### 1.3. Porovnanie vrstvy 2 a 3

Rozlíšenie medzi linkovou vrstvou a sieťovou vrstvou je dôležité pre pochopenie, ako prúdia informácie medzi dvomi počítačmi. Otázka by mohla byť, prečo potrebujeme dvojité adresovanie, čiže adresovanie na linkovej vrstve aj na sieťovej vrstve. [28]

Odpoveďou je, že každé adresovanie plní inú funkciu, nie sú totožné:

- Linková vrstva používa MAC adresy a je zodpovedná za doručenie medzi susednými zariadeniami .
- Sieťová vrstva používa IP adresy a je zodpovedná za doručenie paketov od odosielateľa k príjemcovi. [28]

Keď chceme dáta poslať v sieti, sieťová vrstva ich zapuzdrí do paketu, ktorý obsahuje IP hlavičky. IP hlavička bude obsahovať IP adresy odosielateľa a príjemcu. Takto zapuzdrené dáta sa pošlú na linkovú vrstvu, kde sa tieto dáta znovu zapuzdria do rámca, ktorý už obsahuje hlavičky MAC adresy. Táto MAC adresa bude obsahovať informácie, ako je zdrojová a cieľová MAC adresa aktuálneho router-a na ceste k cieľovému zariadeniu.

Medzi každým router-om je MAC hlavička vymenená za novú, aby sa dáta dostali na ďalší router. Táto MAC adresa slúži na cestovanie v sieti medzi zariadeniami. Prvý počítač vygeneruje IP hlavičku, ktorá bude odstránená až posledným počítačom. Preto IP hlavička rieši doručenie od odosielateľa k príjemcovi a každá z rôznych MAC hlavičiek je len na preposlanie medzi blízkymi susediacimi zariadeniami napríklad router-mi v sieti. [28]

## 2. Protokol TRILL

Pani Radia Perlman sa zamýšľala nad spôsobom ako zlepšiť algoritmus Spaning tree a spolu s výskumným tímom vymyslela TRILL protokol, neskôr ho štandardizovala Engineering Task Force(IEIF). [8]

V máji v roku 2009 bola vydaná informačná zmienka o protokole TRILL, ktorá hovorí o probléme protokolu STP a o možnom riešení tohto problému. Problémom STP protokolu je, že sa musí vyhýbať všetkým slučkám čiže aj tým dočasným. Spanning tree často vedie k neefektívnemu vyžívaniu topológie spojenia (blokuje redundantné linky). Možným riešením by boli funkcie moderných smerovacích protokolov sieťovej vrstvy, keby boli dostupné na linkovej vrstve. [2]

V roku 2011 bol vydaný prvý štandard vznikajúceho protokolu (RFC 6325), potom sa vydalo niekoľko aktualizácií a opráv RFC štandardu na ktorých spolupracovalo niekoľko spoločností a odborníkov. Posledný aktualizovaný štandard bol v apríli 2019 štandard RFC 8564 a posledným navrhovaným štandardom zatiaľ je RFC 9183 z Februára 2022 . [1]

Ciele nového protokolu TRILL sa stanovili kvôli dôležitosti opraviť nedostatky STP, a tak vytvoriť lepšiu variantu protokolu. Tieto ciele popisuje a definuje RFC 5556 [2] takto:

- Port musí byť radšej zablokovaný v prípade, že je jeho stav nejasný.
- Musí podporovať ľubovoľnú topológiu podsiete na linkovej vrstve.
- Musí podporovať nástroje na analýzu siete.
- Musí používať najvhodnejšie cesty k cieľovému zariadeniu.
- Musí zabezpečovať stabilitu siete a zároveň efektívne zabrániť slučkám v sieti.
- Musí využívať paralelné linky na prenos od rovnakého zdroja cez rovnaké zariadenia k rovnakému cieľu.
- Musí mať aktívne redundantné linky/cesty v sieti. [3]

Tak ako sa stanovili ciele pre zlepšenie používaného protokolu, tak isto sa stanovili aj požiadavky ktoré sa musia zachovať [3]:

- Ethernetový rámec nesmie byť pozmenený a musí byť doručený v rovnakej podobe ako bol odoslaný tj. cieľová stanica/zariadenie nesmie v rámci poznať rozdiel,
- možnosť posielania rámcov na unicast aj multicast a broadcast adresu, čiže na viac koncových zariadení (multi-destination),

- jednoduchá konfigurácia switch-ov – nesmie byť potrebné nič navyiac konfigurovať kvôli základnej funkčnosti protokolu,
- možnosť bezchybného fungovania klasických aj TRILL switch-ov v jednej sieťovej infraštruktúre.

Štandard RFC 6325 [5] definuje názvy špecifické pre TRILL. Názov „RBridge“ je skratkou pre „Routing Bridge“ čiže switch, ktorý ale obsahuje implementáciu protokolu TRILL. Názov switch je klasický ethernetový switch bez implementácie TRILL protokolu. [3] [10] Protokol TRILL poskytuje najlacnejšie cesty s nulovou alebo minimálnou konfiguráciou, taktiež umožňuje viacnásobné smerovanie s viacerými cieľmi a využitie viacnásobných ciest s rovnakou cenou. [11]

## 2.1. Čo nové TRILL používa

TRILL protokol spolu s RBridge naznačujú, že sa teraz použije niečo nové oproti STP alebo niečo čo sa uplatňuje na sieťovej vrstve [3]:

- Dvojité zapuzdrenie Ethernetového rámca. Najprv sa pôvodný rámec zapuzdrí s TRILL hlavičkou a potom s vonkajšou Ethernetovou hlavičkou, tak aby adresy cieľových zariadení switch nevidel. [3] [11]
- TRILL používa protokol IS-IS na vyhľadanie najvýhodnejšej a najrýchlejšej cesty v podsieti, protokol IS-IS je smerovací protokol na sieťovej vrstve. IS-IS poskytuje dynamické smerovanie medzi router-ami.[4] Čiže protokol IS-IS smeruje zapuzdrené rámce.
- Distribučné stromy a Reverse Path Forwarding (RPF) čiže kontrola smerovania opačnou cestou, kvôli distribúcii multi-destination prevádzky. [5][6]
- TRILL protokol by mal tiež zvýšiť počet koncových zariadení v jednej VLAN doméne, ale odporúčané maximálne množstvo cieľových zariadení sa nezmení. [2]
- Ethernetová sieť je citlivá k mnohým útokom. Napríklad na naplnenie MAC tabuliek. Preto tiež musí mať zabezpečenie Ethernetových sietí proti útokom. Bez ohľadu na implementovaný protokol riadenia by to mal riešiť. [3] [11]
- Mal by tiež využívať hierarchické smerovanie, MAC adresy sú v princípe nehierarchické, na rozdiel od IP adries. V prepínacej tabuľke musí mať každé koncové zariadenie musí mať svoj samostatný záznam. [3] [11]

## 2.2. Ako TRILL funguje

TRILL vytvára a udržiava prepojenie medzi RBridge-ami, používa IS-IS smerovanie. Susedné RBridge-e sa navzájom vyhľadajú pravidelnou inzerciou hlásení Hello, takže všetky RBridge-e vedia o všetkých svojich susediacich RBridge -och. [7] [11] Algoritmus najkratšej cesty (SPF) je tiež známy ako algoritmus Dijkstra. Na základe Link State Database (LSDB) každý RBridge používa algoritmus SPF na výpočet ciest vďaka preposlaným záznamom z iných RBridge-ov, čiže každý jeden RBridge môže vypočítať topológiu pre najmenej nákladné jednosmerné smerovanie a vypočítať rovnaké distribučné stromy pre rámce poslané na viac zariadení (multi-destination). [16] Protokol IS-IS funguje priamo na linkovej vrstve, preto sa v ňom nenachádzajú žiadne IP adresy, a môže byť spustený bez konfigurácie. Pre uľahčenie prenosu informácií TRILL, je ľahké ho rozšíriť definovaním nových TLV (typ, dĺžka, hodnota) prvkov, ktoré IS-IS používa. RBridge-e sú identifikované 2-bytovými nickname a IS-IS ID systémom ( je 6 bajtový jedinečný identifikátor RBridge v TRILL sieti ). Nickname sú predvolene automaticky pridelované ale je možnosť ich manuálne nakonfigurovať. V prípade že majú dva RBridge-e rovnaký nickname, tak si musí vybrať nový nickname ten RBridge, ktorý má nižšiu prioritu. Nickname sa používa preto lebo šetrí miesto v hlavičkách. Každý RBridge si vytvorí mapu celej siete. [11] [16]

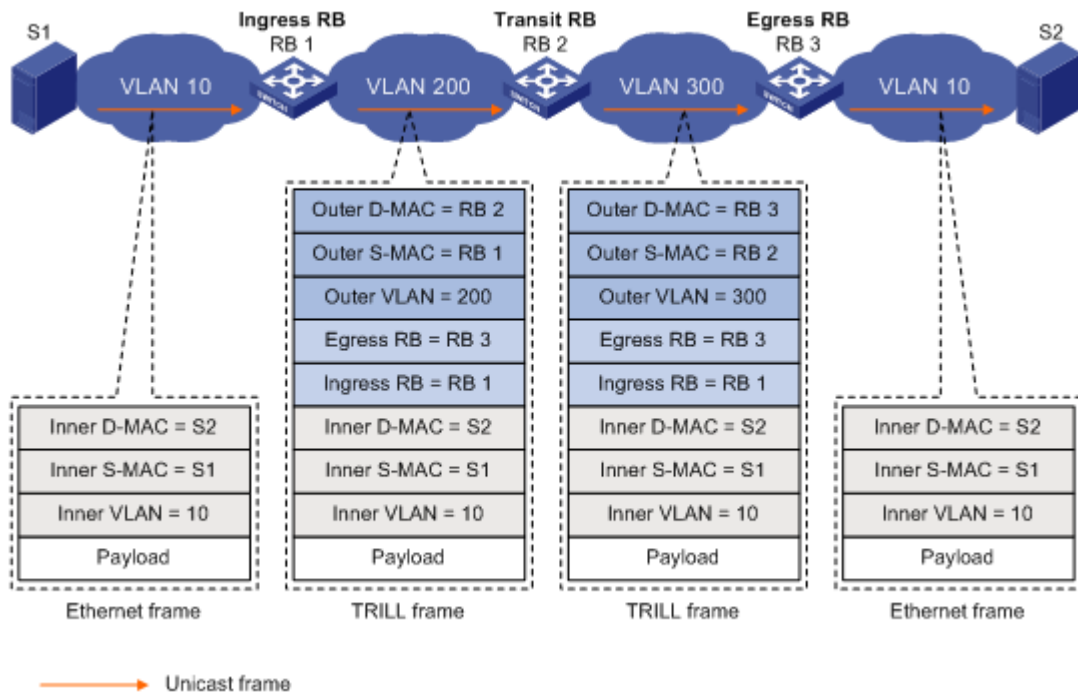
## 2.3. Posielanie rámcov

Pre poslanie toku dát vo vnútri VLAN siete, používa TRILL tieto mechanizmy [7]:

- Unicastové posielanie rámcov

- keď do TRILL siete príde unicastový rámec, vstupný RBridge (Ingress RBridge ) zabalí tzv. zapuzdrí pôvodný ethernetový rámec najprv s TRILL hlavičkou (dosť podobná IP hlavičke), a potom s vonkajšou ethernetovou hlavičkou (dosť podobná hlavičke klasického ethernetového rámca). Rovnakým systémom, ako switch-e preposielajú IP pakety, preposielajú RBridge-e rámce medzi blízkymi susedmi (hop-by-hop) podľa výstupného (egress) nickname RBridge -u v hlavičke TRILL. Vonkajšia ethernetová hlavička sa po každom preposlaní vymení za zodpovedajúcu vonkajšiu ethernetovú hlavičku, a zároveň sa zníži počet skokov - preposlaní v hlavičke TRILL o 1. U klasických zariadení sa vymení za zodpovedajúcu MAC adresu (čo som popísala vyššie), je to ten istý princíp. [7]

- Keď sa rámec dostane do výstupného RBridge -u, ten ho rozbalí (de-encapsuluje), aby mu zostal pôvodný ethernetový rámec, ktorý môže odoslať koncovému zariadeniu. Výstupný RBridge musí odstrániť vonkajšiu ethernetovú hlavičku a aj TRILL hlavičku, aby rámec rozbalil. [7]



Obr. 1: Posielanie unicastového rámca  
obrázok je prevzatý zo stránky [7]

Fungovanie switch -ov s RBridge -ami v jednej sieti a aj preposielanie TRILL rámcov, nám umožňuje vonkajšia ethernetová hlavička. [7]

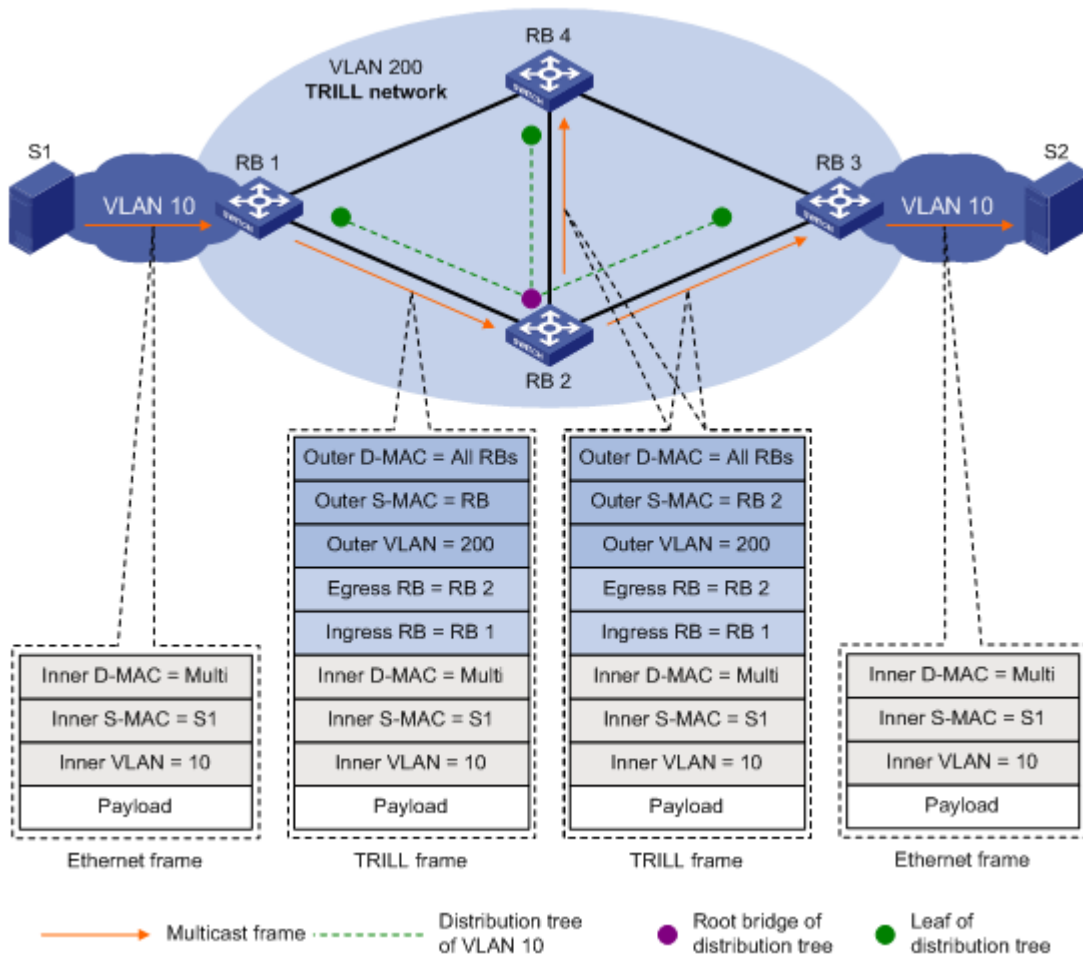
- RBridge vykonávajú v sieti TRILL funkcie, ktoré slúžia na posielanie rámca na viac cieľových zariadení, sú to tieto [7]:

- na základe databázy stavu spojenia – Link State Database (LSDB obsahuje všetky informácie o stave spojenia v sieti TRILL) vypočítavajú pre každú sieť VLAN distribučný strom TRILL.
- pomocou distribučného stromu TRILL, naviguje preposielanie rámcov na viac cieľov v každej VLAN sieti. [7]

Keď z VLAN siete príde multicastový rámec do TRILL siete, tak nastane zapuzdrenie multicast rámca do TRILL rámca, túto úlohu spraví vstupný RBridge. V rámci je zapísaný



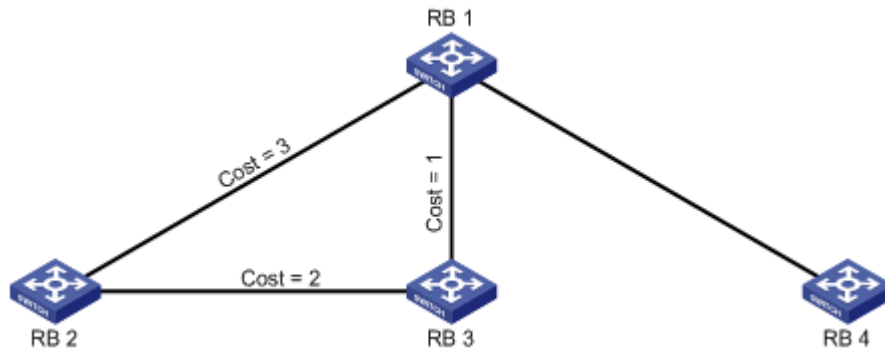
root bridge (RB2) distribučného stromu TRILL pre sieť VLAN a výstupný RBridge(RB3). Rámec bude distribuovaný po celom distribučnom strome TRILL a do všetkých častí podsiete (All RBs), keď dorazí do root bridge-u. Rámec rozbalí RB3 (RBridge) a odošle do cieľového zariadenia S2. V časti siete, ktorá nemá príjemcu a tak rámec zahodí sa nachádza RB4 (RBridge). Ak existuje viacero možností, ako distribučný strom vytvoriť, tak sú pravidlá pre tieto prípady, ktorými sa treba riadiť, môžeme použiť napríklad ECMP multicast. [7] [5] [14]



*Obr. 2: Posielanie multicastového rámca  
obrázok je prevzatý zo stránky [7]*

Na základe VLAN sietí do ktorých rámce patria, sú vybrané distribučné stromy na posielanie rámcov na viac cieľových zariadení. Závaž prenosu môže byť rozložená v prípade, že sú topológie distribučných stromov TRILL rôzne. Na poslanie rámcov v sieti kde je N prepojení s rovnakými cenami, sa vyberie prepojenie s najväčším ID pseudouzla (pseudouzol je vysvetlený v časti 2.7 ) pre každý distribučný strom TRILL. Napríklad sú

dve rovnako cenovo ohodnotené linky medzi RB1 a RB2. Potom cesta, ktorá má najväčšie ID pseudouzla priamo spája RB1 s RB2. Distribučný strom TRILL zakorenený v RB1 vyberá spojenie, tak ako aj distribučný strom TRILL zakorenený v RB4. (znázornené na obr.3). [7]



*Obr. 3: Znázorňuje multicast ECMP  
obrázok je prevzatý zo stránky [7]*

ECMP- Equal Cost Multiple Path, známe aj ako multicast ECMP sú podporované distribučnými stromami. Pre zlepšenie výkonu rozloženia záťaže, TRILL priraduje rovnako ohodnotené cesty k rôznym distribučným stromom TRILL, keď je povolený multicast ECMP. [7]

V prípade že existuje viacero cenovo ohodnotených ciest (N) v sieti TRILL sa vyberie cesta na poslanie rámcov, ktorá je rovnako cenovo ohodnotená. Túto cestu vyberá každý distribučný strom v poradí priority root bridge-u. Poradové číslo priority distribučného stromu TRILL začína od 0, budem ho značiť J. Táto cesta na posielanie rámcov sa vyberá cez  $J \bmod N$ . [7]

Na obrázku 3. si môžeme všimnúť:

- K distribučnému stromu TRILL s koreňom v RB1, je priradená cesta spájajúca RB1 s RB2
- K distribučnému stromu TRILL s koreňom RB4 je priradené spojenie spájajúce RB1 – RB3 – RB2. [7]

Rýchle prepínanie koreňov podporujú distribučné stromy TRILL. RB vymaže LPS záznam koreňa zo svojej databázy spojení (LSDB), vtedy keď zistí, že koreň distribučného stromu je nedostupný. Tým pádom sa musia prepočítať v sieti TRILL všetky distribučné stromy. Do

nových distribučných stromov sa prepne preprava na viac cieľových zariadení. TRILL používa mechanizmus pomenovaný Reverse Path Forwarding Check, ktorý má zabrániť vzniku dočasných slučiek pri cestovaní multi-destination rámcov. Fungovanie Reverse Path Forwarding Check spočíva v tom, že na základe použitého distribučného stromu kontroluje multi-destination rámce. Rámec musí byť zahodený vtedy, keď sa vráti inou cestou ako mechanizmus očakával. [12] [15]

## 2.4. Formát hlavičky TRILL

TRILL hlavička prešla niekoľkými úpravami do tejto podoby a je oslobodená od údajov, ktoré sa používajú na linkovej vrstve. [1] [5] TRILL na začiatku prenosu najprv zapuzdrí pôvodný Ethernetový rámec svojou hlavičkou. Táto hlavička sa skladá z týchto častí [5]:

<b>Version</b>	<b>Alert</b>	<b>Color</b>	<b>M</b>	<b>RESV</b>	<b>F</b>	<b>Hop Count</b>	<b>Egress Nickname</b>	<b>Ingress Nickname</b>	<b>Optional Flags Word</b>
2b	1b	1b	1b	4b	1b	6b	16b	16b	32b

Obr4.: Znázorňuje hlavičku TRILL ( podľa RFC 7780, zdroj [12] )

Hodnoty bitov „A“ a „C“ RBridge musí ignorovať pri výpočte hash hodnoty dátového rámca TRILL ako súčasť výberu rovnakého cenového ohodnotenia multipath. [12]

- V (Version) – 2-bitové celé číslo bez znamienka. Ak má hodnotu nula, tak je špecifikovaná verzia, táto časť slúži na označenie verzie protokolu. V prijatom zapuzdrenom rámci TRILL, RBridge vždy skontroluje pole „V“. RBridge musí rámec zahodiť v prípade ak má toto pole hodnotu, ktorú nevie rozpoznať. IETF Standards Action má na starosti pridelenie nových čísel verzií TRILL. [12]
- A (Alert) – 1 bit. Tento bit je špecifikovaný ako varovný bit. Tento bit nesmie používať RBridge na preposielanie rozhodnutí, ako je výber cesty ECMP(Equal Cost Multipath). Bit sa používa v súlade so špecifikáciami na identifikáciu rámcov TRILL OAM, čo vyžaduje aj špeciálne spracovanie.  
Ak má hodnotu 1 je to znak, že ide o možný rámec OAM a musí sa s ním špecificky zaobchádzať. Môže sa stať že má rámec nastavený tento bit a neobsahuje CFM

EtherType (Connectivity Fault Management EtherType), preto nie je považovaný za rámec OAM a musí sa zahodiť. RBridge ktorý podporuje OAM rámce, nesmie generovať rámce OAM pre RBridge-e, ktoré OAM nepodporujú. TRILL OAM rámce sú rámce, ktoré poskytujú indikáciu poruchy siete, lokalizáciu poruchy a informácie. [37]

- C (Color) – 1bit. Týmto bitom sa označujú dátové pakety TRILL na špecifické účely pre implementáciu. RBridge-e ktoré takéto rámce preposielajú, nesmú tento bit meniť. Tranzitné a výstupné RBridge-e môžu používať tento bit na označenie implementačne závislej linky alebo na štatistickú analýzu alebo iné typy štúdií alebo analýz. [12]
- M (Multi-destination) – 1bit. Tento bit označuje, že rámec má byť doručený skupine koncových zariadení cez distribučný strom. Tento distribučný strom je vybraný polom Nickname výstupného RBridge. [5]
  - ak je bit 0 (False) – obsahuje nickname výstupného RBridge pre známu Unicast MAC adresu.
  - ak je bit 1 (True) – obsahuje nickname výstupného RBridge, ktorý určuje distribučný strom. Tento nickname vyberie vstupný RBridge pre daný rámec TRILL. [5]
- RESV : 4 bits. Tieto bity musia byť odoslané ako nula, pretože sú rezervované. Väčšina hardvérových implementácií TRILL zachytáva a nepreosiela dátové rámce TRILL s nenulovými bitmi. TRILL switch prijímajúci dátový rámec TRILL s nejakým nenulovým bitom v RESV buď tento bit alebo bity majú špecifikované nejaké budúce použitie, o ktorých RBridge vie alebo tento rámec musí RBridge zahodiť. [12] [5]
- F : 1 bit. Ak je táto hodnota nulová, potom príznak nie je prítomný. Ale ak je bit „F“ nenulový v TRILL hlavičke, potom prvých 32 bitov po poli „Ingress Nickname“ poskytuje ďalšie príznaky. [12]

- Hop Count: 6-bitové celé číslo bez znamienka. Veľkosť tohto poľa však obmedzuje maximálny počet skokov. RBridge môže rozšíriť tohto pole na 9 bitov, tým sa maximálny počet skokov zvýši na 512, ale táto podpora, tohto rozšírenia je potrebná na všetkých RBridge-och na ceste TRILL rámca. Vstupný RBridge by mal „Hop Count“ nastaviť pre známe unicastové rámce. Aby sa neskôr na ceste umožnilo alternatívne smerovanie, mal by RBridge počítat' o niečo viac ako počet skokov medzi RBridge-ami, ktoré očakáva výstupný RBridge. Pomocou vstupného RBridge by mal byť nastavený počet skokov pre rámce s viacerými cieľmi, od najvzdialenejšieho RBridge na aspoň predpokladaný počet skokov. RBridge zahodí rámec s nulovým počtom skokov, inak sa toto číslo zníži o 1. Tento princíp je podobný mechanizmu Time to Live na sieťovej vrstve IPv4. Pre rámce s viacerými cieľmi sa zaviedlo niekoľko dodatočných opatrení, kvôli možnosti generovania viacerých kópií rámca. Toto generovanie môže spôsobiť cyklus obsahujúci jednu a viac vetiev distribučného stromu. Kvôli tomuto sú rámce s viacerými cieľmi podrobené kontrole presmerovania spätnej cesty (Reverse Path Forwarding) a iným kontrolám. Ako dodatočné opatrenie pre tieto rámce môže tranzitný RBridge RBm znížiť o viac ako 1 počet skokov, ale musí počet skokov znížiť aspoň o 1. Ak je počet skokov nulový, tak sa rámec zahodí. [12] [5]
- Egress Nickname: 16 bitový identifikátor. V závislosti od bitu M sú dva prípady obsahu nickname výstupného RBridge-u. Pre rámce TRILL ESADI je nickname vyplnená zdrojovým RBridge-om a pre dátové rámce TRILL ju vyplní vstupný RBridge. [5]
  - Keď M je nastavené na 0 (False), tak je rámec označený ako unicastový dátový rámec TRILL. Určuje RBridge, ktorý potrebuje odstrániť zapuzdrenie TRILL a poslať natívny rámec koncovému zariadeniu, toto sa určí poľom výstupný nickname čo je výstupný RBridge. Toto pole po nastavení počas celej cesty nesmie byť zmenené žiadnym RBridge-om. [5]
  - Keď je M nastavené na 1 (True), tak je rámec označený ako multi-destination dátový rámec TRILL alebo rámec TRILL ESADI. Pole výstupný nickname RBridge-u obsahuje nickname určujúcu distribučný strom. Tento strom sa použije ako cesta na poslanie rámca. Žiaden tranzitný RBridge nesmie

zmeniť tento nickname. [5]

- Ingress Nickname: 16 bitový identifikátor. Vstupný RBridge nastaví vstupnú nickname na svoju vlastnú nickname pre dátové rámce TRILL, a pre rámce TRILL ESADI na nickname zdrojového RBridge-u. Žiaden tranzitný RBridge nesmie zmeniť toto pole keď je nickname nastavené. [5]
- Optional Flags Word: tento bit "F" v hlavičke TRILL poskytuje ďalšie príznaky prvých 32 bitov po poli Ingress Nickname ak je nenulový. [12] [17]

Rámec ktorý TRILL zapuzdriľ, bude obsahovať tri hlavičky (vonkajšia, TRILL a vnútorná). Vonkajšia Ethernetová hlavička, slúži len na preposielanie medzi blízkymi susedmi a zároveň sa odstráni po každom skoku – preposlaní. Keď sa posieľa medzi jedným(RB1) a druhým(RB2) RBridge-om, určí RB1 ako zdrojový a RB2 ako cieľový. [16]

#### 2.4.1. Nickname RBridge

Nickname sa používajú pre šetrenie miesta v hlavičkách, slúži ako skratka pre IS-IS ID RBridge. Toto pole je 16 bitová dynamicky zadaná hodnota, tiež nickname slúži pre kompatibilnejšie zakódovanie. Vďaka tomuto je možné mať až  $2^{16}$  RBridge-ov v jednej sieti. Existuje tiež zopár predvolených označení, pre ktoré je zopár hodnôt rezervovaných. Hodnota 0x0000 označuje, že nickname nie je špecifikovaná a pre budúcu špecifikáciu sú určené hodnoty 0xFFC0 až 0xFFFF pričom natrvalo rezervovaná je hodnota 0xFFFF. [14] [5] [16] RBridge môže mať aj viacero Nickname, ktoré by mal používať aj po reštarte zariadenia. Ak sú nickname vybrané automaticky, tak majú nižšiu prioritu ako tie, čo sú nakonfigurované administrátorom siete. Aby sa zabránilo duplicitám nickname, RBridge si zvyčajne zvolí nickname pseudonáhodne alebo hashom svojich parametrov, čiže sa vyhýba tým nickname, ktoré už získali iné RBridge a podľa odporúčenia by RBridge mal počkať so zvolením do tej doby, kedy bude mať k dispozícii úplnú databázu všetkých RBridge v sieti, potom už nevyberie duplicitnú nickname. [14] Pre odstránenie duplicit nickname v podsieti sa spúšťa postup, ktorým sa zabezpečí odstránenie duplicity, tým pádom si jeden RBridge vytvorí novú nickname, a to len v prípade, keď sa príde na to že je viac rovnakých nickname v podsieti. RBridge spája protokol IS-IS na získanie jednej alebo viacerých unikátnych nickname v oblasti kampusu. [5]

### 2.4.2. Rozšírenia hlavičky

TRILL obsahuje aj možnosť rozšírenia TRILL hlavičky. To udáva pole s názvom RESV a bit F, zobrazené vyššie. Ak je F nula, potom nie je žiadne rozšírenie hlavičky, ale v prípade keď je tento bit vyplnený nasleduje oblasť rozšírenia hlavičky priamo za polom Ingress RBridge Nickname v hlavičke TRILL. Sú zabezpečené hop-by-hop príznaky, ingress-to-egress príznaky, príznaky ovplyvňujúce zatiaľ nešpecifikovanú triedu RBridge (napríklad bridge rozšírené o podporu viacúrovňového IS-IS v tejto TRILL sieti) a rôzne iné príznaky. [16] [17] [12]

### 2.4.3. TRILL OAM rámce

Tieto rámce sa používajú na rôzne účely napríklad na merania výkonnosti, overenie konektivity, kontroly kontinuity, monitorovania chýb ako aj na ich rýchle a efektívne odstraňovanie. Ako je uvedené vyššie rámce OAM sa identifikujú v hlavičke nastavením „A“ bitu s CFM Ethertype. Podľa možností rovnako ohodnoteného preposlania a na základe topológie si TRILL vyberie akúkoľvek cestu ktorú použije, čo umožňuje predvolené nastavenie. Niekedy je potrebné aby sa použili špecifické cesty, čiže OAM rámce musia sledovať cestu, ktorou prechádza konkrétny tok. RBridge -e musia rozpoznať OAM rámce, ktoré vyžadujú OAM spracovanie. Podobne ako pri natívnych rámcoch aj tieto rámce nemôžu opustiť TRILL sieť. OAM poskytuje možnosť nastaviť začiatočnú hodnotu a udržiavať viacero súbežných relácií OAM. Funkcie OAM, ktoré sa spúšťajú len na požiadanie alebo proaktívne musia súvisieť s kontrolami kontinuity a konektivity, taktiež sa musia dať spustiť na ľubovoľnom inom RBridge -i. [39]

## 2.5. Link State Protocols (LSP)

Protokoly stavu spojenia, sú protokoly, ktoré fungujú ako cestovná mapa. Každý router má úplný obraz o sieti. Každý router si najprv zistí koho má za suseda a periodicky testuje či je prístupný. Inými slovami vytvára informácie o sebe a o stave priamo pripojených ciest k susedným zariadeniam. Informácie o sebe a o svojich susedoch posiela do celej siete, to znamená že každý router má zoznam všetkých ciest a router-ov v sieti. [18] [16] [14] Toto smerovanie sa vždy snaží zachovať úplnú topológiu siete tým, že sa aktualizuje vždy, keď nastane nejaká zmena v sieti (napríklad výpadok komponentu/RBridgu v sieti). Každý router v sieti si uloží jeho nezmenenú kópiu. Po skončení preposielania informácií má každý

router kompletný obraz topológie siete. [5] [16] Aby mal každý router prehľad o svojich najlepších (najlacnejších) cestách k cieľovým zariadeniam, príde na rad algoritmus najkratšej cesty, ktorým si router nezávisle vypočíta svoje vlastné najlepšie cesty. Cieľom je aby každý router mal rovnaké informácie o prepojení a každý router si nezávisle vypočítal cesty. LSP protokoly sú založené na SPF (Short-Path-First) algoritme na nájdenie najlepšej cesty k cieľu. A v tomto algoritme sa LSA (Link-State Advertisement) nazýva to, keď prebehne aktualizácia smerovania. A keď prebehne aktualizácia smerovania LSA, potom sa použije algoritmus stavu spojenia na prepočítanie najkratšej cesty buď celej siete alebo jej aktualizovaných častí. [16] [18] [14]

Príkladom protokolov LSP sú protokoly IS-IS, OSPF, IGP alebo EGP. Protokol OSPF je primárne určený na IP smerovanie, ale IS-IS súčasne podporuje smerovanie niekoľkých protokolov. [18]

TRILL využíva IS-IS ako svoj smerovací protokol. IS-IS má niekoľko výhod:

- pracuje priamo cez linkovú vrstvu môže sa nakonfigurovať automaticky,
- je ľahké ho rozšíriť zavedením nových údajov TLV (Type Length Value) pre prvky TRILL. [16] [15]

### 2.5.1. IS-IS

Primárne bol vyvinutý pre model OSI, pre výhodnosť jeho funkcií, ktoré sa dajú ľahko rozšíriť. Formát Type Length Value (TLV) používa na preposielanie správ. Bez úpravy základnej infraštruktúry je možné pridať nové rozšírenia v IS-IS, aby podporoval nový protokol. TRILL aj FabricPath si ho vybrali aj s niekoľkými jeho modifikáciami, napríklad svoj riadiaci protokol. [38] IS-IS beží priamo na 2. vrstve takže sa môže automaticky konfigurovať. Bez potreby algoritmu Spanning-Tree, je schopný poskytnúť dostatočné informácie pre všetky router-e, aby si vypočítali rovnaké stromy. Na distribúciu rámcov pre viac cieľových zariadení TRILL potrebuje aspoň jeden strom. Sieťová vrstva používa inú inštanciu IS-IS, pretože si TRILL implementuje svoju vlastnú TRILL IS-IS inštanciu. TRILL IS-IS rámce musia byť odlišné od klasických sieťových IS-IS rámcov, aby RBridge-e vedeli rozoznať, aké zariadenie rámec poslalo. RBridge-e preposielajú klasické IS-IS rámce. [5] [15]



## 2.6. Point to Point Protokol a TRILL

Existujú siete kde sa v nejakých jej častiach používa protokol Point-to-Point. Z tohto dôvodu má TRILL dva samostatné Ethertype typy aby rozoznal zapuzdrenia hlavičky rámca. V sieťach kde sa využíva PPP na spojenie sieťových zariadení, môže byť výhodnejšie prejsť medzi Ethernetovými segmentmi siete cez PPP segment a tým pádom spojiť vzdialené siete s daným cloudom TRILL. LCP (Link Control Protocol) a metódu na dohodnutie používania viac-protokolového posielania cez PPP cesty definuje PPP protokol. Priame prepojenie Ethernetových rámcov cez PPP umožňuje protokol riadenia spojenia (BCP), žiaľ tento mechanizmus nie je vyhovujúci pre TRILL, ale je možné ho cez PPP spojenia zdokonaľiť. Na používanie IS-IS P2P Hellos je možné nakonfigurovať porty RBridge-u a toto prepojenie bude point-to-point cesta na iný RBridge. RBridge port nakonfigurovaný na používanie P2P Hellos, nemôže poskytovať služby cieľovému zariadeniu. Na prenos cez PPP cesty je Ethernetový rámec zapuzdrený s TRILL hlavičkou, ale vonkajšia už bude PPP hlavička namiesto Ethernetovej hlavičky. [5] [33]

## 2.7. Fungovanie RBridge-ov

RBridge-e podporujú viacnásobné smerovanie unicastového aj multicastového posielania, taktiež je možné bezpečné posielanie dát aj počas dočasných slučiek a poskytujú optimálne preposielanie bez konfigurácie. Toto všetko uskutočňujú pomocou zapuzdrenia hlavičky, ktorá obsahuje počet skokov a taktiež smerovania. RBridge vedia komunikovať a fungovať so súčasnými zariadeniami, a netreba nič ďalšie implementovať. [5] [15] [16]

RBridge-e si navzájom vymieňajú rámce TRILL IS-IS Hello, aby si vytvorili obraz siete a zároveň sa našli. Všetky riadiace rámce TRILL IS-IS sa posielajú na multicastovú adresu (All-IS-IS-RBridges), kde sa posiela aj TRILL Hellos. Tieto rámce sú spracované portmi RBridge-u (ale nepreposielané ďalej), transparentne sú preposielané bridge-ami a ukončia ich koncové stanice taktiež aj router-e. TRILL Hellos sú malé, nevyplnené a podporujú fragmentáciu niektorých informácií preto sa odlišujú od rámcov IS-IS LAN Hellos sieťovej vrstvy. RBridge-e si zvolia Designated RBridge (DRB) v jednej LAN na základe priority portu a informácií z vymenených správ Hellos. Rámce Hellos sa používajú na zistenie a nadviazanie susedstva prepojených systémov. Tiež sú nazývané aj ako IS-IS Hellos skrátene IHH. [13] [5]

Designated RBridge môže vytvoriť pseudouzol, ktorý je virtuálny. Tento uzol je dosť podobný pseudouzlu zo sieťovej vrstvy. DRB bude mať na starosti vytvorenie LPS v mene pseudouzlu a vytvorenie PDU s úplným poradovým číslom (protokol CSNP). [5]

Designated RBridge je tiež zodpovedný za vymenovanie Appointed Forwarder, čiže zvolenie RBridge-a, ktorý bude bránou do druhej VLAN siete. Avšak keď sa stane Appointed Forwarder veľmi preťažený, DR by mal túto funkciu preložiť na iný RBridge ak je k dispozícii na linke, ktorá nie je preťažená.[41]

RBridge vytvárajú distribučné stromy, ktoré sú obojsmerné a používajú sa na posielanie rámcov s viacerými cieľmi tzv. multi-destination. Každý distribučný strom vie o všetkých RBridge-och v sieti TRILL a môže mu poslať rámce. [13] [5]

Pri prenose rámcov sa RBridge takzvané učí, prvý rámec poslaný zo zariadenia, narazí na prázdne prepínacie tabuľky RBridge-ov. Automaticky zapíše port ktorým prišiel do prepínacej tabuľky a zdrojovú MAC adresu, princíp je rovnaký ako na klasickom Ethernetovom switch-i. RBridge-e sa učia z dekapulovaných TRILL rámcov aj zdrojové adresy, do tabuľky k MAC adrese si zapíše RBridge, ktorý spravil prvé zapuzdrenie natívneho rámca, túto informáciu zapíše ako „next hop“ - vstupný RBridge. [3]

## 2.8. Návrh implementácie RBridge

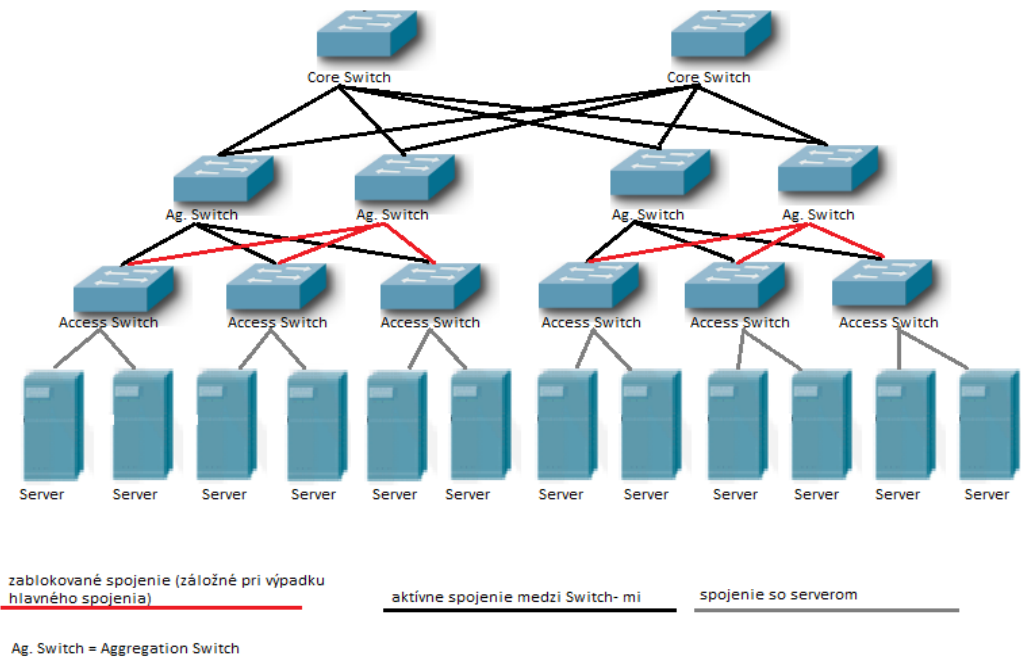
Tento návrh bude rozdelený na riadiacu rovinu a dátovú rovinu, čiže bude vysvetlený v dvoch častiach. Riadiaca rovina bude zodpovedná všetky časti smerovania preto je založená na protokole IS-IS. Vďaka protokolu IS-IS prijíma rozhodnutia o smerovaní na základe ceny linky a buduje topológiu. IS-IS používa topológiu stromu SPF (Short Path First) na smerovanie rámcov. Na základe výmen správ Link State DPU (LSP) medzi RBridge-ami sa vypočíta strom SPF. Informácie sú prenášané vo forme TLV (typ, dĺžka a hodnota). Smerový protokol IS-IS je založený na Link-state protokole. Aby vedel kam poslať rámce, musí najprv zistiť topológiu siete. Tú zistí tak, že cez každý RBridge-ový port odošle Hellos správu, svoj zoznam susedov (pokiaľ ich pozná) a prioritu portu. Nasledujú dva prípady. Prípad keď RBridge obdrží Hellos so svojou MAC adresou, z toho vyplýva že na porte je obojsmerná komunikácia. A prípad keď dostane Hellos s inou MAC adresou, potom MAC adresu odosielateľa pridá do svojej prepínacej tabuľky. Následne si zvolia DRB. Keď skončia s výmenou Hellos správ, začína výmena správ LSP, ktoré obsahujú nickname RBridge. Aby sa predišlo duplikovaniu správ, tak LSP ktoré sú v jednej LAN pošle v mene ostatných DRB. Každý RBridge si vypočíta svoju vlastnú tabuľku presmerovania na základe LSP a informáciách o susedstve pre každý RBridge v topológii. Na základe smerovacej tabuľky sa vypočíta každé preposlanie. Tieto dáta sa posunú dátovej rovine. [29]

Dátová rovina bude spracovávať všetky úlohy ohľadom rámcov, ich preposielania, zapuzdrenia a dekapulácie. Tiež poskytuje rozhodnutia o smerovaní na základe hlavičky TRILL. [29]

## 2.9. Primárne využitie TRILL protokolu

Najlepšie uplatnenie protokolu môže byť napríklad v rozsiahlych dátových centrách, prečo bol aj vytvorený. Kde na dosiahnutie efektívnej služby musia spĺňať z hľadiska efektívnosti a dostupnosti nové požiadavky a poskytovať rozsiahle služby. Tento problém sieťových architektúr pramení zo starých štandardov dizajnu, ako je napríklad Virtual LAN (802.1Q). V prípade že sa v prepínacej tabuľke nenachádza adresa cieľového zariadenia, Ethernet bude stále vysielat' rámce do všetkých portov okrem prijímacieho (pre predstavu tohto momentu, takto pracuje hub zariadenie). S veľkým počtom počítačov, ktoré navzájom komunikujú, to spôsobí obrovské zaťaženie všetkých prepínacích tabuliek. Táto technika zahltenia prepínacích tabuliek, bude viesť k celkovému zhoršeniu výkonu siete. Tieto prepínacie tabuľky sú zvyčajne uložené v Content Addressable Memory (CAM), čo je drahé. Vieme že STP vytvára stromovú topológiu, ktorá zabezpečí sieť bez možných slučiek. Pre menšie siete to je pomerne efektívne, ale v spojení STP a veľkej siete, tento mechanizmus má to niekoľko nevýhod (sú spomenuté v časti 3.1. ). [29]

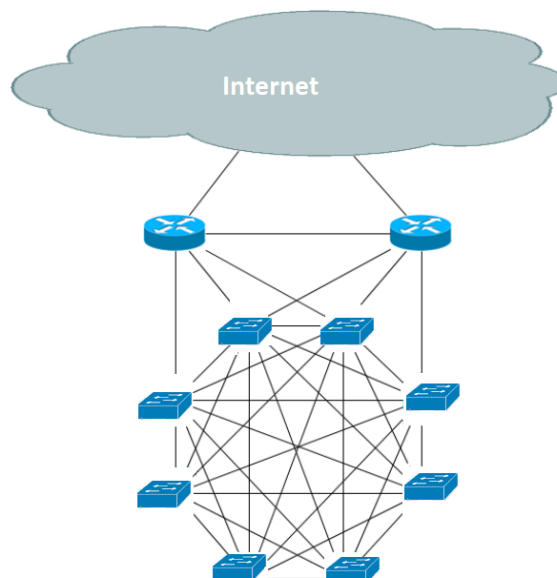
Dátové centrá majú zvyčajne sieť trojvrstvovej štruktúry. Vrstvy tejto štruktúry sú: základná vrstva (Core Layer), agregáčna vrstva (Aggregation Layer) a prístupová vrstva (Access layer). Každá vrstva má svoju funkciu, zariadenia na prístupovej vrstve sú pripojené k serveru a tiež sa označuje aj ako ToR (Top of Rack). Agregáčna vrstva má za úlohu zistiť narušenie a analyzovať sieť a tiež zariadenia na tejto vrstve sú pripojené k zariadeniam na ToR vrstve a poskytujú ďalšie služby. Základná vrstva má funkciu vysokorýchlostného posielania paketov z dátového centra ale aj paketov, ktoré prišli do dátového centra, to znamená že poskytuje konektivitu vyššej agregáčnej vrstve. Zariadenia na agregáčnej vrstve pracujú v L2 sieti, a zariadenia v základnej vrstve pracujú v L3 sieti. [32]



Obr.5: znázorňujúci sieťovú architektúru dátového centra

Obrázok je prevzatý a upravený z [32]

Protokol TRILL poskytuje rozsiahlu sieť linkovej vrstvy a nenáročnú podporu pre škálovateľnosť viacerých používateľov. V architektúre založenej na TRILL je spojenie typu any-to-any, to znamená že, každé zariadenie má priame spojenie s každým ďalším zariadením. [29]

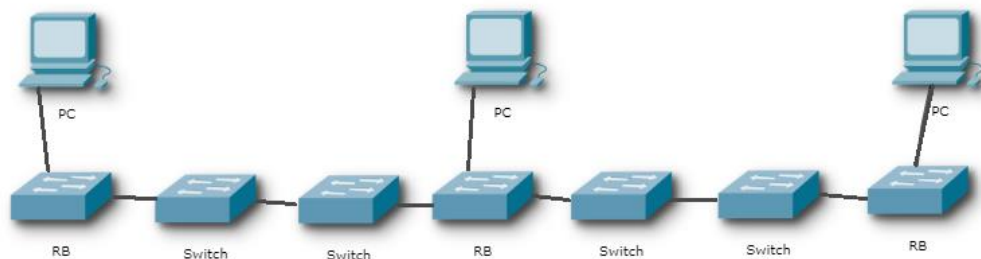


Obr.6: Znázorňuje dátové centrum s využitím TRILL

Obrázok je prevzatý a upravený z [29]

## 2.10. Vedľajšie využitie TRILL

Aj keď bol vyvinutý primárne pre dátové centrá, jeho využiteľnosť je väčšia. Keby sme logicky umiestnili napríklad len dva RBridge-e do obyčajnej siete (ktorá nie je malá), napríklad školskej, tak aby medzi jedným RBridge-om a druhým RBridge-om boli klasické switch-e, tak tieto switch-e nemusia poznať celú topológiu siete za RBridge-ami. To by znamenalo, že by sa dala ušetriť pamäť na prepínacích tabuľkách a zároveň zlepšiť stabilitu a škálovateľnosť siete. Vieme že každý jeden RBridge musí poznať celú topológiu siete, teda nie je veľmi múdre v obyčajnej sieti vymeniť všetky klasické switch-e za RBridge-e, pretože by sme neušetrili žiadnu pamäť a zároveň si spravili niečo ako medzi sieť, v konečnom dôsledku by záležalo od nás. Keďže TRILL protokol využíva smerovacie protokoly zo sieťovej vrstvy, nemožno ho jasne nazvať protokolom linkovej vrstvy, pretože je takým medzi-protokolom alebo lepšie povedané medzi vrstvou. Síce je značne nevýhodné, že do starých – klasických zariadení sa nedá implementovať a kvôli tomu je potrebný nový hardvér, ktorý ho implementuje. Preto by som navrhla vymeniť povedzme každý druhý switch za RBridge alebo vymeniť tie ktoré sú najvyťaženejšie a prepájajú viacej ciest.



Obr.6: Znázorňuje fungovanie klasických switch – ov a RBridge – ov v jednej sieti

## 3. Iné protokoly

V tejto kapitole sa budeme venovať starším protokolom, ktoré protokol TRILL nahradí ale aj alternatívnym protokolom, ktoré boli vyvinuté za podobným účelom ako protokol TRILL.

### 3.1. STP protokol

STP protokol vznikol na základe zabránenia vzniku slučiek v sieti. STP je štandardizovaný IEEE 802.1D v roku 1990. Tento algoritmus Spanning-Tree navrhla Radia Perlman. STP protokol je dnes už vymieňaný za novšie protokoly. [14] [40]

Switch-e spolu komunikujú vymieňaním správ a tým siet' ustália na jednu cestu bez slučiek. STP porty môžu byť buď v aktívnom stave posielania (forwarding) alebo v zablokovanom stave (blocking). STP k odstráneniu všetkých slučiek v topológii zablokuje toľko portov, koľko je potrebné. Najprv si všetky najlepšie cesty vyberá koreňový switch (Root Bridge), označí ich ako aktívne a ostatné cesty zablokuje. Každý switch na začiatku, vytvorí a odosiela správu Hello (BPDU teda dátovú jednotku mostového protokolu). Pokiaľ ale dostane správu, ktorá má nižšie ID bridge-u, potom ten switch ktorý tú správu poslal bude koreňový switch. Následne tento switch nebude koreňovým a prestane posilať svoje správy Hello a začne rozposilať správy koreňového switch-u. Koreňový switch – root bridge má zvyčajne všetky porty aktívne. Cez root bridge zvyčajne prechádza v podsieti väčšina komunikácie a dát. Root bridge je vybraný buď na základe nižšej hodnoty MAC adresy alebo na základe konfigurácie. [14] [40] [16]

Switch v jednej sieti, bude mať designated port, ktorý bude dostávať a preposilať dáta z tejto siete do inej časti siete. Switch, ktorý bude posilať a dostávať dáta z inej časti siete sa nazýva designated switch. Designated port môže mať ten switch, ktorý rozosiela správy Hello zo svojej LAN do inej časti siete. [14]

Ako viaceré protokoly aj STP má novšie verzie, Rapid Spanning Tree Protocol (RSTP) a Multiple Spanning Tree Protocol (MSTP). [40] [16]

- RSTP bol primárne zameraný na rýchlejšie zistenie konektivity v sieti, čo mu trvá málo sekúnd oproti STP. RSTP má možnosť portu komunikovať na danom porte s použitím protokolu STP, keď mu príde na daný port správa kde je použitý STP protokol. [16] [14]
- MSTP vychádza z RSTP, je možné vytvorenie viacerých stromových kostier, každá kostra blokuje iné redundantné cesty v sieti a počet týchto kostier nemusí byť rovný počtu VLAN. Priradí VLAN -y ku kostrám, a tým tento protokol rozkladá zaťaženie siete a komunikáciu z rôznych VLAN na viac kostier. Keď príde k nejakému prerušeniu jednej časti siete, vieme komunikáciu presmerovať cez inú kostru. [16] [14]

Hlavnou nevýhodou STP protokolu je stromová štruktúra protokolu, ktorá nevyužíva všetky cesty medzi zariadeniami, čím sa stáva pri veľkých sieťach náchylnou na preťaženie, keďže všetka premávka dát ide len po tejto stromovej štruktúre. Keďže blokuje redundantné trasy v sieti, čím zabraňuje vytvoreniu slučiek v sieti. Ďalšou nevýhodou je chybová situácia, kedy môže nastať zahltenie siete vplyvom aktivovania všetkých liniek to sú aktívne aj neaktívne, táto situácia môže nastať napríklad pri poruche a princíp fungovania sa nazýva „fail-open“. Pri možnom zahltení siete je toto zahltenie ťažké analyzovať a tiež STP nezaručuje stabilitu siete.[2][3]

### 3.2. SPB protokol

SPB najprv štandardizoval IEEE ako 802.1aq a neskôr aj IETF uvedený ako RFC 6329. Celým názvom Shortest Path Bridging poskytuje riešenie problému STP, na čo bol aj primárne zameraný. Pri riešení problémov STP, využíva na smerovanie a nájdenie najkratšej dostupnej cesty protokol IS-IS. SPB tiež umožňuje a podporuje virtualizáciu siete. [19] [30]

Jeho úplný názov je :“Štandard pre miestne a metropolitné siete: Virtuálne premostené lokálne siete – Premostenie najkratšej cesty.“

Tento štandard špecifikuje protokoly na výpočet aktívnych topológií, ktoré môžu zdieľať informácie o umiestnení stálych zariadení, a podporu VLAN pomocou viacerých identifikátorov VLAN podľa topológie a taktiež premostenie rámcov unicast a multicast s najkratšou cestou. [20]

SPB používa dva už existujúce štandardy IEEE a to IEEE 802.1ad, IEEE 802.1ah. [21]

- IEEE 802.1ad Provider Bridges, neformálne známy tiež ako Q – in – Q, ako dodatok k štandardu IEEE 802.1Q. Pôvodná špecifikácia 802.1Q umožňuje vloženie jednej hlavičky virtuálnej lokálnej siete (VLAN) do ethernetového rámca. [22] [3] [21]

- IEEE 802.1ah Provider Backbone Bridge, neformálne známy tiež ako MAC – in – MAC, je špecifický pre zapuzdrenie rámca do druhej ethernetovej hlavičky. Aby neboli viditeľne adresy odosielateľa rámca cez prenos backbone sieťou, dostane rámec navyše druhý pár MAC adres. Vďaka tomu sa nemusia backbone bridge-e učiť MAC adresy každého zariadenia. To zvyšuje flexibilitu nielen MAC adres, ale aj VLAN identifikátorov. [23] [3] [21]

Formát rámca 802.1ah umožňuje zjednodušenú virtualizáciu dátového centra, tým že

identifikátor služby (I-SID) je oddelený od VLAN ID a Backbone MAC adres. Cieľom je zbaviť sa všetkých vzájomných závislostí fyzickej siete a protokolov, a tiež od infraštruktúry fyzickej siete úplne oddeliť linkovú vrstvu. I-SID tiež poskytuje mechanizmus pre riadenie prevádzky. [34]

IEEE 802.1ad a IEEE 802.1ah ale neurčujú druhú ethernetovú hlavičku, ktorá by mala byť použitá pre doručenie konkrétneho rámca, tiež neupresňujú žiadny riadiaci protokol, ktorý by hľadal na linkovej vrstve optimálne cesty v sieti. Na vstupných rozhraniach do backbone siete sa tieto pravidlá manuálne nakonfigurujú. [21]

Protokol bude bez potreby manuálnej konfigurácie automaticky vykonávať:  
 - druhé ethernetové hlavičky podľa Q – in – Q, tiež sa toto pravidlo uvádza ako SPBV  
 - zapuzdrenie do druhej hlavičky podľa MAC – in – MAC, tiež sa toto pravidlo uvádza ako SPBM. [3]

Tento protokol bude na výpočet bezslučkovej cesty používať smerovací protokol IS-IS, ktorý používa Dijkstrov algoritmus. Čo zabezpečí, že bude možné prestať používať STP mechanizmus. Aby sa ethernetový rámec dostal k cieľu najvýhodnejšou cestou, musia byť činnosti SPBV a SPBM vzájomne vykonávané. V SPB sa automaticky pridáva druhá ethernetová hlavička. SPB môže byť okamžite nasadené do prevádzky bez potreby nového hardvéru, ktoré by ho implementovalo. Použitie nájde v sieťach, ktoré obsahujú veľa switchov s podporou Mac – in – Mac. [3]

### 3.2.1. Porovnanie TRILL a SPB

Oba protokoly vynikli ako náhrada za STP a boli vyvinuté pre zefektívnenie smerovania bez slučiek v sieti. Tieto protokoly sú si síce dosť podobné ale odlišujú sa v detailoch, ktoré vyplývajú z toho ako vznikli. V prostredí IETF ako náhrada SPT vznikol TRILL a používa protokoly sieťovej vrstvy. Zlepšuje zväčšenie škálovateľnosti linkových domén aj keď na to nebol zameraný. V prostredí IEEE vznikol SPB ako riadiaci protokol nahrádzajúce manuálnu konfiguráciu pre siete MAC – in – MAC. Zásluhou mechanizmov, ktoré používa sa dá jednoducho implementovať. [3] [34] Pre porovnanie dôležitých charakteristík protokolov TRILL a SPB sú uvedené v tabuľke:

<b>Protokol</b>	<b>SPB</b>	<b>TRILL</b>
Štandardizoval	IEEE aj IETF	IETF



Nahrádza STP	Áno	Áno
Použitý protokol pre tvorbu bezslučkovej topológie a hľadanie najvýhodnejších ciest	IS – IS	IS – IS
Možnosť použitia najvýhodnejších a násobných ciest k cieľu	Áno	Áno
Zapuzdrenie Ethernetových rámcov	Q-in-Q (pre SPBV), MAC-in-MAC (pre SPBM)	Formát TRILL + vonkajšia Ethernetová hlavička
Úprava hlavičky na každom prvku	Nie, iba na hraničných prvkoch	Áno, na hraničných aj tranzitných prvkoch
TTL položka v hlavičke rámca	Nie	Áno
Možnosť linkových nástrojov typu ping alebo traceroute	Nie	Áno
Odolnosť proti slučkám a iným prepínaním problémom	Stredná (ostáva malá pravdepodobnosť slučiek z dôvodu jednoduchosti)	Vysoká (slučky sú vylúčené za cenu väčšej zložitosti)
Potreba nového hardvéru	Nie nutne, rad hardvéru už zapuzdrenie podľa Q-in-Q alebo MAC-in-MAC zvládne	Áno, zapuzdrenie TRILL je nové
Univerzalita návrhu, možnosť kombinácie výhod oboch protokolov	SPB nemôže využiť pokročilejších vlastností smerovania v sieťovej vrstve	TRILL môže koexistovať s Q-in-Q a využívať škálovateľnosť VLAN identifikátorov. Skrývanie vnútorných MAC adries funguje natívne.
Použitie na sieťach typu	SP, neskôr DC	DC, neskôr SP
Doručovanie rámcov v inom poradí	Nie	Je to možné len v prípade, keď na začiatku nepoznáme MAC adresu príjemcu

Spracovanie výstupu pre multicast	Nevyžaduje sa	Vyžaduje sa z dôvodu zmeny výstupného portu hlavičky MAC
Agregácia služieb	Áno, je možné namapovať viacero sietí VLAN do Service Instance	Nie
OA&M	IEEE 802.1ag, ITU Y.1731 výkon a správa	N/A
Jednoduchosť odstránenia problému	Jednoduchšie vidieť celú cestu cez sieť. Kompletná sada IEEE/ITU ethernetových OAM nástrojov	Je potrebné kontrolovať premávku na princípe hop-by-hop a musíme poznať cestu. Nemá k dispozícii OAM nástroje.
Rozšírenia sieťovej vrstvy a IP VPN	Koncept IP/SPB	Žiadna integrácia
Škálovateľnosť	10 000+ s viacúrovňovým IS-IS	10 000+
Konvergencia	Výpočty stromu založené na zdrojovom uzle (počet stromov vypočítaný na základe počtu uzlov)	Samostatná inštancia EASDI/VLAN -každý port oznamuje všetky VLAN cez TRILL Hellos, na jeden port je možné odoslať až 4096 Hellos. Dynamická voľba Root Bridge, dynamická voľba zasielania.
ID systému	Názvy uzlov používajú zabezpečené systémové ID	Potenciálne kolízie Nickname pri spájaní sietí TRILL

tabuľka pochádza zo zdrojov [3][34]

### 3.3. Cisco FabricPath

Cisco protokol FabricPath je dosť podobný protokolu TRILL, tiež má podobné možnosti využitia a tiež používa k hľadaniu najkratšej cesty na smerovanie protokol IS-IS. Cisco FabricPath protokol má inú hlavičku ako protokol TRILL. Keby sme Cisco switch dali do siete s inými klasickými switch-mi musíme vypnúť FabricPath, aby mohol byť využitý tiež klasický implementovaný TRILL protokol. Porty FabricPath môžu používať iba siete FabricPath VLAN. Tento protokol FabricPath používa svoju FabricPath VLAN, ktorú

musíme nakonfigurovať a tiež musíme zmeniť režim portu FabricPath. Pretože FabricPath je založený na jednotlivých VLAN, a len tie VLAN budú používať infraštruktúru FabricPath, ktoré môžu používať tento režim. Takže môžeme rozdeliť siete VLAN na tie, ktoré budú používať FabricPath VLAN a klasické ethernetové VLAN. FabricPath protokol má aj svoje výhody, jednou z nich je väčšia funkcionálna, ktorú Cisco prináša o niečo skôr oproti protokolom, ktoré treba schváliť. [31] [14]

### 3.3.1. Ďalšie podobné protokoly

Výrobcovia sa budú snažiť o náhradu protokolu STP a vyriešiť problém slučiek na linkovej vrstve. Medzi také systémy sa radí aj QFabric od firmy Jupiter. QFabric vznikla zameraním na rozsiahlo ploché podsiete a ponúka lepšie možnosti škálovania a virtualizáciu siete ako tradičné dátové centrá. Tento systém QFabric môžeme v podstate vnímať ako jeden switch, čiže viacej switchov v QFabric podsieti sa tvári ako jedna logická entita. Celý systém QFabric je riadený ako jeden celok prostredníctvom skupiny *Director*. [14] [35]

Ďalšiu technológiu Virtual Cluster Switching predstavila spoločnosť Brocade, tiež je určená k riadeniu plochých podsietí a funguje na podobnom princípe ako QFabric. [14]

Ďalšou technológiou na zlepšenie riadenia toku v sieťach je Software-Defined Networking skrátene SDN. Tento protokol ukazuje nový prístup ako spravovať správanie siete dynamicky a aj schopnosť riadiť, meniť, inicializovať. SDN zavedením abstrakcie pre zasielanie údajov vyzdvihuje úlohu softvéru v sieťovej prevádzke. [14] [36]

## 4. Záver

V práci sme na úvod spomenuli a oboznámili sa s referenčným modelom ISO/OSI, aby sme vedeli kde je umiestnený a pracuje protokol TRILL. Bližšie sme popísali vrstvy, ktoré protokol TRILL využíva.

Ďalej sme sa venovali predstaveniu protokolu TRILL, popísali sme jeho vybrané časti, uviedli sme aké nedostatky protokolu STP má za úlohu vylepšiť. Tiež sme sa oboznámili s tým ako TRILL pracuje aj čo iné využíva k svojmu fungovaniu na linkovej vrstve. Tiež sme uviedli a rozobrali primárny vznik a využitie protokolu TRILL. Pokračovali sme navrhnutím použitia protokolu TRILL pre bežné scenáre použitia, ako aj sme sa zamysleli nad tým čo zlepšuje v tomto prípade.

Ku koncu práce sme spomenuli protokol STP a alternatívne protokoly TRILL. Popísali sme Spanning Tree Protokol, jeho vznik a fungovanie, taktiež sme uviedli aj jeho novšie verzie, ktoré sme v skratke popísali. Tiež sme spomenuli jeho nevýhody v sieti.

Pokračovali sme alternatívnym protokolom SBP. Popísali sme účel jeho vzniku a zameranie. Uviedli sme štandardy, ktoré SBP využíva k fungovaniu, s týmito štandardami sme sa oboznámili.

Ďalej sme pokračovali porovnaním TRILL a SBP protokolov, kde sme spomenuli ich výhody ako aj ich odlišnosti. Ďalej je spomenutý alternatívny protokol od spoločnosti Cisco nazvaný Cisco FabricPath. Spomenuli sme ako pracuje ako aj jeho odlišnosť od protokolu TRILL. Na koniec sme spomenuli zvyšné protokoly, ktoré sa zaoberali problematikou STP protokolu.

## Stránky – literatúra

[1] [online] Dostupné na: [https://www.rfc-editor.org/search/rfc\\_search\\_detail.php?title=trill&pubstatus%5B%5D=Any&pub\\_date\\_type=any](https://www.rfc-editor.org/search/rfc_search_detail.php?title=trill&pubstatus%5B%5D=Any&pub_date_type=any)

[citované: 21.10.2021]

[2] J. Touch, et al. *Transparent Interconnection of Lots of Links (TRILL): Problem and Applicability Statement*. Máj 2009[online]. Dostupné na: <https://www.rfc-editor.org/rfc/rfc5556.html>

[citované: 21.10.2021]

[3] Ing. Miroslav Matuška. *Seriál TRILL: Konečně náhrada za Spanning Tree?*. 7.10.2010 [online]. Dostupné na: <https://www.lupa.cz/serialy/trill/>

[citované: 21.10.2021]

[4] *IS -IS*. [online] Dostupné na: <https://www.pcmag.com/encyclopedia/term/is-is>

[citované: 21.10.2021]

[5] R. Perlman, et al. *Routing Bridges (RBridges): Base Protocol Specification*. Jún 2011 [online]. Dostupné na: <https://www.rfc-editor.org/rfc/rfc6325.html>

[citované: 21.10.2021]

[6] D. Eastlake 3rd, et al. *Transparent Interconnection of Lots of Links (TRILL) Use of IS -IS*. Júl 2011 [online]. Dostupné na: <https://www.rfc-editor.org/rfc/rfc6326.html>

[citované: 21.10.2021]

[7] H3C Technologies. *15-TRILL Configuration Guide*. [online]. Dostupné na: [http://www.h3c.com/en/Support/Resource\\_Center/HK/Switches/H3C\\_S10500/H3C\\_S10500/Technical\\_Documents/Configure/Configuration\\_Guide/H3C\\_S10500\\_CG-R7523P01-6W100/15/201609/951148\\_294551\\_0.htm](http://www.h3c.com/en/Support/Resource_Center/HK/Switches/H3C_S10500/H3C_S10500/Technical_Documents/Configure/Configuration_Guide/H3C_S10500_CG-R7523P01-6W100/15/201609/951148_294551_0.htm)

[citované: 27.10.2021]

[8] Robert Sheldon. *Spanning Tree Protocol(STP)*. August 2021[online]. Dostupné na: <https://www.techtarget.com/searchnetworking/definition/spanning-tree-protocol>

[citované: 27.10.2021]

[9] Adam Surák. *Transparent Interconnection of Lots of Links (TRILL) jako náhrada Spanning Tree*. Máj 2012[online]. Dostupné na: <http://wh.cs.vsb.cz/sps/images/8/88/TRILL.pdf>

[citované: 27.10.2021]

[10] IBM Systems and Technology Group . *IBM b-type Networks for High Performance and Scalable Computing Systems*. Máj 2010[online] Dostupné na: <https://docs.broadcom.com/doc/12379981>

[citované: 27.10.2021]

[11] Donald E. Eastlake 3rd. *The IETF TRILL Protocol Transparent Interconnection of Lots of Links*. Február 2013 [online]. Dostupné na: [https://conference.apnic.net/35/pdf/trillapricot8\\_1361288177.pdf](https://conference.apnic.net/35/pdf/trillapricot8_1361288177.pdf)

[citované: 27.10.2021]

[12] D. Eastlake 3rd, et al. *Transparent Interconnection of Lots of Links (TRILL): Clarifications, Corrections, and Updates*. Február 2016 [online]. Dostupné na: <https://www.rfc-editor.org/rfc/rfc7780.html#>

[citované: 27.10.2021]

[13] Donald E. Eastlake 3rd. *RBridges and the IETF TRILL Protocol*. December 2009[online]. Dostupné na: [https://archive.nanog.org/meetings/nanog48/presentations/Monday/Eastlake\\_RBridge\\_N48.pdf](https://archive.nanog.org/meetings/nanog48/presentations/Monday/Eastlake_RBridge_N48.pdf)

[citované: 27.10.2021]

[14] Bc. Tomáš Kmoníček. *Analýza využití protokolu TRILL v podnikové síti*. 2015 [online]. Dostupné na: [https://dk.upce.cz/bitstream/handle/10195/60413/KmonicekT\\_AnalyzaVyuziti\\_JH\\_2015.pdf?sequence=1&isAllowed=y](https://dk.upce.cz/bitstream/handle/10195/60413/KmonicekT_AnalyzaVyuziti_JH_2015.pdf?sequence=1&isAllowed=y)

[citované: 14.11.2021]

[15] Bc. Matej Hrnčířík. *Modelování L2 Protokolů zajišťujících bezsmýškovost*. 2012 [online]. Dostupné na: <https://docplayer.sk/204514332-Fakulta-informa%C4%8Dn%C3%ADch-technologi%C3%AD.html>

[citované: 14.11.2021]

[16] Zard Ali Khan. *Comparative Analysis of TRILL: A Research Study*. September 2017[online]. Dostupné na: [https://www.researchgate.net/publication/330888235\\_Comparative\\_Analysis\\_of\\_Trill\\_A\\_Research\\_Study](https://www.researchgate.net/publication/330888235_Comparative_Analysis_of_Trill_A_Research_Study)

[citované: 14.11.2021]

[17] D. Eastlake 3rd, et al. *Transparent Interconnection of Lots of Links (TRILL): Header Extension*. Máj 2014[online]. Dostupné na: <https://www.rfc-editor.org/rfc/rfc7179.html>

[citované: 14.11.2021]

[18] Libor Dostálek, Alena Kabelová. *Velký průvodce protokoly TCP/IP a systému DNS*. Praha: Computer Press 2000. ISBN 80-7226-323-4 [citované: 7.2.2022]

[19] AlcatelLucent. *Shortest Path Bridging (SPB)*. [online] Dostupné na: <https://www.al-enterprise.com/en/solutions/shortest-path-bridging>

[citované: 14.11.2021]

[20] Don Fedyk, Mick Seaman. *802.1aq – Shortest Path Bridging*. 29.3.2012 [online] Dostupné na: <https://1.ieee802.org/tsn/802-1aq-shortest-path-bridging/>

[citované: 27.12.2021]

[21] D. Fedyk, Ed., et al. *IS-IS Extensions Supporting IEEE 802.1aq Shortest Path Bridging*. April 2012 [online]. Dostupné na: <https://datatracker.ietf.org/doc/html/rfc6329#section-4>

[citované: 27.12.2021]

[22] Norman Finn. *MAC address transparency*. Máj 2006[online]. Dostupné na: <https://www.ieee802.org/1/files/public/docs2006/ad-nfinn-mac-address-transparency-0506.pdf>

[citované: 27.12.2021]

[23] CISCO. *Understanding Basic 802.1ah Provider Backbone Bridge*. 9.3.2018 [online]. Dostupné na: <https://www.cisco.com/c/en/us/support/docs/routers/asr-9000-series-aggregation-services-routers/212882-understanding-basic-802-1ah-provider-bac.html>

[citované: 27.12.2021]

[24] Sandeep Jain. *Layers of OSI Model*. 18.10.2021[online]. Dostupné na: <https://www.geeksforgeeks.org/layers-of-osi-model/>

[citované: 3.1.2022]

[25] RNDr. Jaroslav Janáček. *Referenčný model ISO OSI*. [online]. Dostupné na: <http://www.dcs.fmph.uniba.sk/siete/OSI.pdf>

[citované: 3.1.2022]

[26] Roman Pramberger. *Data Link Layer*. [online] Dostupné na: <https://osi-model.com/data-link-layer/>

[citované: 3.1.2022]

[27] *Linková vrstva*. [online] Dostupné na: <https://www.sciencedirect.com/topics/computer-science/data-link-layer>

[citované: 3.1.2022]

[28] Ed Harmoush. *OSI Model*. [online] Dostupné na: <https://www.practicalnetworking.net/series/packet-traveling/osi-model/>

[citované: 3.1.2022]

[29] Ahmed Amamou, Kamel Haddadou, Guy Pujolle. *A TRILL-based multi-tenant data center network*. 5.8.2014 [online]. Dostupné na: <https://www.sciencedirect.com/science/article/pii/S1389128614000851#b0020>

[citované: 3.1.2022]

[30] Peter Ashwood-Smith. *Shortest Path Bridging IEEE 802.1aq Tutorial and Demo*. Október 2010 [online]. Dostupné na: [https://archive.nanog.org/meetings/nanog50/presentations/Sunday/IEEE\\_8021aqShortest\\_Path.pdf](https://archive.nanog.org/meetings/nanog50/presentations/Sunday/IEEE_8021aqShortest_Path.pdf) [citované: 5.1.2022]

[31] Haider Khalid. *What is Cisco FabricPath?*. 11 Február 2018 [online]. Dostupné na : <https://ourtechplanet.com/what-is-cisco-fabricpath/>

[citované: 17.1. 2021]



[32] OPTCORE. *Do you know the data center network architecture*. 26.9.2018 [online]. Dostupné na: <https://www.optcore.net/do-you-know-the-data-center-network-architecture/> [citované: 15.5.2022]

[33] J. Carlson et al. *PPP Transparent Interconnection of Lots of Links (TRILL) Protocol Control Protocol*. August 2011[online]. Dostupné na: <https://www.rfc-editor.org/rfc/rfc6361.html> [citované:10.1.2022]

[34] Avaya. *Compare and Contrast SPB and TRILL*. [online]. Dostupné na: [http://www.techdata.ca/business/avaya/DataCenterSolutions/files/A%20-%20Why%20Avaya/2%20-%20Learn%20More%20About%20VENA/SPB-TRILL Compare Contrast-DN4634.pdf](http://www.techdata.ca/business/avaya/DataCenterSolutions/files/A%20-%20Why%20Avaya/2%20-%20Learn%20More%20About%20VENA/SPB-TRILL%20Compare%20Contrast-DN4634.pdf) [citované:10.1.2022]

[35] Jupiter networks. *QFabric System Overview*. 26 Marec 2021 [online]. Dostupné na: <https://www.juniper.net/documentation/us/en/software/junos/qfx3000-g-deployment/topics/concept/qfabric-overview.html> [citované:17.1.2022]

[36] s.Denazis, et al. *Software-Defined Networking(SDN): Layers and Architecture Terminology*. Január 2015 [online]. Dostupné na: <https://datatracker.ietf.org/doc/html/rfc7426> [citované:17.1.2022]

[37] Andersson, et al. *Guidelines for the Use of the "OAM" Acronym in the IETF*. Jún 2011 [online]. Dostupné na : <https://www.rfc-editor.org/rfc/rfc6291> [citované:21.1.2022]

[38] Cisco. *Using TRILL, FabricPath, and VXLAN: IS-IS Intra Domain Routing Protocol*. 14 Február 2014 [Online]. Dostupné na: <https://www.ciscopress.com/articles/article.asp?p=2176197> [citované: 21.1.2022]

[39] T. Senevirathne et al. *Requirements for Operations, Administration, and Maintenance (OAM) in Transparent Interconnection of Lots of Links (TRILL)*. Marec 2013[online].  
Dostupné na : <https://www.rfc-editor.org/rfc/rfc6905.html>

[40] Wendell Odom, Rus Healy, Naren Mehta. *Směrování a přepínání sítí Autorizovaný výukový průvodce*. Brno: Computer Press 2009. ISBN 978-80-251-2520-5  
[citované: 16.2.2022]