Univerzita Hradec Králové

Fakulta informatiky a managementu

Katedra informačních technologií

Cisco IP SLA a jeho využití

Bakalářská práce

Autor: Tomáš Matoulek

Studijní obor: Informační management

Vedoucí práce: Mgr. Josef Horálek, Ph.D.

Hradec Králové Srpen 2016

Prohlášení:

Prohlašuji, že jsem bakalářskou práci na téma Cisco IP SLA a jeho využití vypracoval samostatně s použitím odborné literatury a pramenů uvedených na seznamu, jenž tvoří přílohu této práce.

V Hradci Králové dne ……

Tomáš Matoulek

Poděkování:

Děkuji tímto panu Mgr. Josefu Horálkovi Ph.D. za cenné připomínky, rady, vstřícnost a konzultace při vypracování této bakalářské práce.

Anotace

Cílem této bakalářské práce je představit Cisco IP SLA službu, její funkčnost a využiti. Jedná se o Cisco proprietární technologii, která dokáže kontrolovat a sbírat data o funkčnosti sítě a jejích parametrů. Existuje několik typů měření, které se dají použít na určitý typ služby, jako například VoIP, kontrola DHCP,FTP a dalších. Tato služba dokáže monitorovat kritické parametry jedné linky případně všech IP prvků celkové trasy. Zabývat se tedy budeme základním využitím této technologie a unifikovaným IP SLA měřením pro zákazníky poskytovatele služeb. Okrajově bude řešena konfigurace technologií jako MPLS, QoS a NTP.

Kličová slova: Cisco, IP SLA, Sítě, MPLS, L3 VPN, Quality of Service, Network Time Protocol, Směrování, Traffic Engineering, VoIP, UDP, TCP, ICMP

Annotation

Title: Cisco IP SLA and its practical use

Main purpose of this Bachelor thesis is to introduce Cisco IP SLA as a service and its functionality and usage. It`s Cisco proprietary technology, that allows to scan and collect information about network performance and its parameters. There are several types of measurement, that can be used for certain types of service, such as VoIP, checking of DHCP, FTP and other services. This service can measure critical parameters of specific link or even every IP device of the whole path. We will explain basic use of this technology and unified IP SLA measurement for customers of the service provider. Additionally, we will deal with MPLS, QoS and NTP configurations.

Key words: Cisco, IP SLA, Networking, MPLS, L3 VPN, Quality of Service, Network Time Protocol, Routing, Traffic Engineering, VoIP, UDP, TCP, ICMP

OBSAH

Seznam obrázků:

Seznam tabulek:

1. Úvod

1.1. *Důvod výběru tématu bakalářské práce*

Jakožto zaměstnanec firmy zajišťující telekomunikační služby v pozici Specialista IP sítě mám na starosti zákazníka, jemuž poskytujeme datovou službu IP SLA pro dodržování výkonnostních parametrů. Service Level Agreement (SLA) je běžným právním dokumentem, který obsahuje předpokládaný rozsah a úroveň služby a také případně postihy za její nedodržení. Dále si myslím, že měření kvality služeb má v budoucnu velký potenciál, a to z důvodu narůstajících požadavků pro jednotlivé služby. Také dochází k neustálému rozvoji datových sítí, dramaticky se zvyšuje jejich počet, velikost a hlavně dochází k masivnímu nárůstu datové rychlosti. S rozšiřováním datových sítí je potřeba dodržovat určité parametry pro jejich funkčnost a bezchybnost, aby byl spokojený, jak uživatel, tak poskytovatel služeb.

1.2. *Cíl bakalářské práce*

Cílem je zpracování univerzální nabídky pro vytvoření měření výkonnostních parametrů v MPLS L3 VPN pro zákazníky poskytovatele služeb. Toto měření by mělo sloužit pro dodržování SLA smluv a pro-aktivní řešení problému, které můžou v síti vzniknout. Dle vyjednané smlouvy by se mělo jednat o měření parametrů jako: ztrátovost paketů, zpoždění (per direction, round trip), jitter (per direction, positive or negative). Cílem bakalářské práce je tedy dokázání, že Cisco proprietární řešení pro měření výkonnostních parametrů je efektivní technologií pro monitoring úrovně SLA. Dále se budu zabývat dvěma typy měření v dané topologii, kde jedním z nich bude měření v prioritní třídě s g.729a kodekem a druhé ve výchozí třídě.

U čtenáře této bakalářské práce se očekává základní znalost problematiky IP SLA a pokročilejší znalost v oblasti IP sítí jako MPLS, směrovací procesy, QoS a NTP.

2. Cisco IP SLA

2.1. *Co je Service Level Agreement (SLA)*

Jedná se o smlouvu mezi poskytovatelem služby a jejím zákazníkem. Tato smlouva obsahuje náležité parametry, které by daná služba měla splňovat. Definuje především klíčové parametry sjednané služby, jako kvalitu a rozsah. Dále popisuje způsobem řešení poruchy, dobu, rychlost reakce a odstranění poruchy, stanovení odpovědnosti za škody a další. V případě nedodržení těchto parametrů dochází k porušování dané smlouvy, nejčastěji pak dochází k finančnímu vyrovnání mezi účastníky smlouvy. [1]

2.2. *Co je IP SLA*

Cisco Internet Protocol (IP) Service Level Agreement (SLA) je proprietární technologie od společnosti Cisco, která efektivně monitoruje provoz na měření výkonnosti sítě měřením kritických parametrů (ztrátovost paketů, zpoždění jedním směrem, zpoždění round-trip) pro komunikaci. Díky využití Cisco IP SLA, je možné, odhalit a předcházet problémům, které by měly vliv na funkčnost a výkonnost sítě. S rostoucí popularitou hlasových a datových služeb v síti, poskytuje tato služba nejdůležitější parametry. Zobrazení IP SLA statistik může být pomocí protokolu SNMP, příkazové řádky a aplikaci Cisco RTTMON s MIBs. Tato technologie může být také využita s jinými technologiemi, jako je třeba policy-based routing, tedy změny směrování paketů v síti na základě aktuálních statistik. IP SLA bylo původně pojmenováno a předvedeno jako Response Time Reporter (RTR) v Cisco IOS software verzi 11.2, následně RTR bylo přejmenováno na Service Assurance Agent (SAA) ve verzi 12.0(5)T. Od verze 12.3(14)T se začal používat název IP SLA. [2]

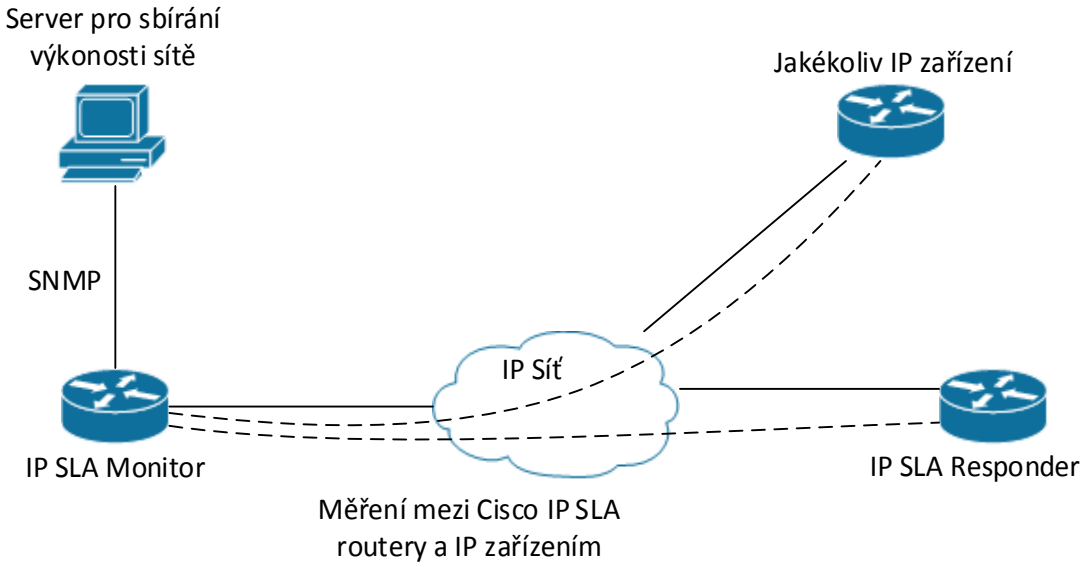
V základní topologii, kdy měříme end to end zařízení, je zapotřebí mít jeden cisco router pro generování paketů a hosta jako respondera. Responder v tomto případě může být jakýkoliv IP host, který je schopný odpovědět na požadavky typu ICMP echo, požadavek na připojení TCP a nebo HTTP GET. Pokud responder bude Cisco router, tak se nám otevírá více možností využití IP SLA a tím pádem můžeme měřit více kritických parametrů. Pro následné sbírání a zobrazování dat je potřeba nějaký network management system (NMS). Mnoho NMS podporují konfiguraci IP SLA z grafického rozhraní daného nástroje. Když je IP SLA

nakonfigurováno, tak router sbírá výsledky jednotlivých operací a ukládá dané statistiky v IOS RTTMON, následně pomocí SNMP NMS sbírá dané informace z MIB. [3]

IP SLA používá koncept operace. Každá operace definuje typ paketu, který router generuje, obsahuje cílovou i zdrojovou adresu a ostatní charakteristiky paketu. Konfigurace též obsahuje nastavení o čase, kdy má být daná operace vykonávána. Na jednom routeru může probíhat operací stejného ale i rozdílného typu. [3]

Například můžeme zároveň monitorovat:

- DHCP službu
- DNS službu
- End-to-End dobu odezvy



Obrázek 1: IP SLA monitoring[zdroj:autor]

2.3. *IP SLA monitor (generátor)*

Na IP SLA monitoru jsou definovány jednotlivé testy. Na základě konfigurovaných parametrů jednotlivých testů generuje IP SLA monitor specifický provoz, analyzuje výsledky a následně je zaznamenává pro budoucí vyhodnocení prostřednictvím CLI nebo SNMP. Jak již bylo řečeno, IP SLA monitor může být libovolný Cisco router vybavený IOS s příslušnou sadou funkcí podle zvolených typů testů. [4]

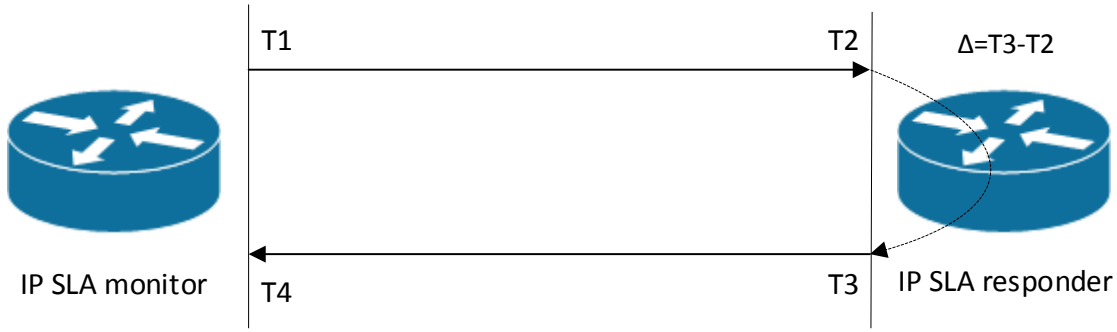
Na IP SLA monitoru představuje procesorové zatížení kritický ukazatel pro přesnost jednotlivých metrik, především přesný záznam časových značek, a proto je zde třeba klást důraz na vhodný návrh metodiky testování, aby procesorové zatížení routeru nepřekročilo 30%. S ohledem na tuto problematiku je doporučeno pro měření mít dedikovaný router, aby nebyl ovlivněn datový provoz ani dané měření. [4]

2.4. *IP SLA responder (odpovídač)*

IP SLA responder plní funkci odpovídače na testy generované IP SLA monitorem a musí být tedy schopen reagovat podle specifikovaného typu testu, opět tedy IOS s příslušnou sadou funkcí. IP SLA responder vkládá časové značky po přijetí a odeslání paketu do jeho payloadu a umožňuje tak z výsledného měření eliminovat čas procesování paketu na IP SLA responderu. U IP SLA responderu představuje procesorové zatížení také kritický parametr a tudíž je důležité nepřekročit 30% vytížení procesu, s ohledem na toto je třeba klást důraz na metodiku testování. [4]

Vytížení CPU	30%	60%	90%
Přesnost IP SLA	Výborná	Dobrá	Ovlivněná

Tabulka 1: Predikce přesnosti SLA ve využití procesoru[zdroj:autor]



Obrázek 2: Systém časových značek[zdroj:autor]

2.4.1. Plánování více IP SLA operací (Multioperations scheduler)

Normální naplánování IP SLA operace povoluje spustit jednu operaci v daném čase. V případě, že máme rozsáhlou síť s velkým počtem IP SLA sond pro monitorování výkonosti sítě, tak by bylo velice neefektivní a časově náročné plánovat vše po jedné operaci. Proto zde existuje příkaz „*ip sla group*“, je to takzvaný mnohonásobný operační plánovač. [2]

Mnohonásobný operační plánovač nám povoluje naplánovat celou skupinu IP SLA operací za pomocí jednoho příkazu v příkazové řádce. Tato funkce nám umožnuje monitorování provozu v rovnoměrně rozloženém časovém úseku. V příkazu se musí specifikovat určitý rozsah (ID) jednotlivých sond, a následně se již spouští jako celek. Tato funkce pomáhá minimalizovat procesorové využití, čímž se zvyšuje škálovatelnost sítě. [2]

Tato funkce používá následující konfigurační parametry:

- Číšlo (ID) dané operace (operation ID numbers) – Seznam všech IP SLA sond a jejich ID v dané skupině.
- Skupinové číslo (Group operation number) – Konfigurační parametr, jež obsahuje číslo dané skupiny.
- Časové opakování (Schedule period) – Množství času, po které je skupina IP SLA operací naplánována.
- Čas v paměti (Ageout) – Množství času, které drží v paměti operace, jenž aktivně nesbírají informace. Ve výchozím nastavení je ageout na dobu neurčitou.
- Životnost operace (Life) – Množství času, kde operace aktivně sbírá informace.
- Frekvence (Frequency) – Množství času, po které se každá IP SLA operace zrestauruje. Pokud je frekvence specifikována, tak to přepisuje frekvenci již v nadefinované operaci.
- Začátek operace (Start time) – Čas kdy daná operace začne sbírat informace. Operace může začít ihned nebo můžeme nastavit čas, kdy má začít.

2.5. *Výhody/Nevýhody IP SLA*

Výhody IP SLA plynou ze škálovatelnosti při použití. Dle definované operace jsme schopni efektivně monitorovat síť a pro-aktivně řešit jakýkoliv problém, tím jsme schopni zkrátit dobu řešení incidentního stavu při nefunkčnosti. Otestovat kvalitu hlasových služeb i video služeb, můžeme simulovat hlasový hovor a tím otestovat celý průběh sítě, a poté identifikovat nežádoucí vlivy v síti nebo otestovat jednotlivé kodeky hlasových služeb. Jsme schopni ověřit

nově nakonfigurovanou trasu s pohledu Quality of Service (QoS) služby a jsme schopni dělat i její průběžný monitoring.

Shrnutí:

- IP SLA monitoring
    - Monitorování a následné vyhodnocení SLA smluv
- Monitoring výkonnosti sítě
    - Měření jitteru, latence nebo ztrátovosti paketů v síti
    - Poskytuje nepřetržité, spolehlivé a předvídatelné měření.
- Edge to Edge monitoring dostupnosti
    - Provádí pro-aktivní monitoring a testování prvků v počítačové sítí
- VoIP monitoring
- Multiprocotol Label Switching (MPLS), Virutal Private Network (VPN) výkonnostní monitoring

Nevýhody této služby opět závisí na způsobu a použití. V případě, kdy potřebujeme opravdu pro-aktivní monitoring služby 24/7 z pohledu dodržování SLA smlouvy zákazníkem i dodavatelem, tak narážíme na problém provedení tohoto měření. Pokud zákazník požaduje měření kritických parametrů např. jitter, latence či ztrátovosti paketů, tak vzniká otázka, kdo toto měření bude provádět a jak se budou dané hodnoty vyhodnocovat. Nejlepší variantou pro obě strany, pokud to dané řešení podporuje je měření oběma stranami a to hned z několika důvodu. Měření zákazníka je ovlivňováno jeho datovým tokem, tedy pokud si zákazník bude plně vytěžovat linku datovým provozem, tak nastane problém s jeho měřením a to ztrátovost paketů, zvýší se skokově odezva a změní jitter, tedy zákazník bude službu reklamovat. Dodavatel je schopen se bránit vlastním měřením, kde si vyhradí část pásma linky pro dané měření a zároveň může prioritizovat provoz pomocí DSCP,COS značek v QoS politice. Hlavní nevýhodou tedy pravidelného měření je neustálé vytěžování linky dvojím

identickým měřením. V případě, kdy máme nízkou kapacitu linky a FUP, který může nastat pří využití technologie jako 3G/LTE, můžeme narazit na problém s tímto omezením.

Shrnutí:

- Pravidelná zátěž linky
- Z pohledu dodavatele nutno vyhradit pásmo pro dané měření
- Omezení při použití určitých přenosových technologii
- Maximální doporučené zatížení procesu IP SLA monitoru i responderu 30%

2.6. *Postup konfigurace*

Postup základní konfigurace probíhá v několika krocích. Jak už bylo řečeno, měření probíhá na základě posílání vygenerovaných paketů odesílatelem, přijmutí responderem a jeho odpovědí.

Základní body konfigurace:

- Nastavit požadovaný typ Cisco IP SLA operace
- Spustit danou operaci a nastavit jí parametry opakování
- Nastavit cílové zařízení jako responder

Příklad konfigurace:

IP SLA monitor:

```
ip sla 1
 <typ operace> <IP adresa SLA responderu> <port> source-ip <IP adresa Loopback rozhraní SLA monitoru> num-packets <počet paketů> interval <interval v ms>
ip sla schedule <číslo operace> start-time <čas startu> life <doba měření/nekonečně>
```

IP SLA responder:

```
ip sla responder
```

2.7. *Typy IP SLA měření*

2.7.1. Monitoring dostupnosti

- ICMP echo – operace IMCP echo měří end-to-end dobu odezvy mezi Cisco routerem a jakýmkoliv IP zařízením, které je schopno odpověď na ICMP echo. Při této operaci se bere v potaz doba z procesování paketu odesílatelem, ale nemůžeme zaručit dobu z procesování cílovým zařízením. Je to tedy efektivní nástroj na kontrolu dostupnosti, nicméně nám to nedá dostatek informací o síti nebo koncovém zařízení pro řešení problémů. [2]

- ICMP path echo – Měření end-to-end a hop-by-hop odezvy od jednotlivých prvků v síti. ICMP path echo se liší od ICMP echo tím, že nejdříve udělá traceroute cesty od zdroje k cíli, aby objevil všechny zařízení po cestě. Následně tedy můžeme měřit dobu odpovědi mezi zdrojem a jednotlivými prvky v cestě. [2]

- ICMP Jitter – Operace ICMP jitter je obdobná jako operace ICMP echo, navíc poskytuje měření latence, jitter a packet loss. [2]

- ICMP path jitter – Operace ICMP Path Jitter je velice podobná jako ICMP path echo, ale navíc provádí jitter operace mezi jednotlivými body v cestě jako latenci, jitter a ztrátovost paketů. Operace tedy zprvu zjistí prvky v síti za pomocí traceroute, aby následně mohla měřit parametry pro tyto jednotlivé prvky. [2]

- UDP echo – Operace UDP echo je obdobná, ale více užitečná, než ICMP echo, protože IP SLA responder rozumí UDP echo komunikaci, a proto operace bere v potaz proces, který zabere čas pro generování přesnějšího měření responderovy. [2]

- UDP jitter - Operace UDP Jitter je nejčastěji používané měření. Je zapotřebí mít synchronizovaný čas mezi generátorem paketů a responderem pomocí Network Time Protocolu(NTP) nebo Global Positioning systémem(GPS). Měří odezvu round-trip, one-way delay, one-way jiter, ztrátovost paketů. Slouží hlavně k měření provozu mezi sítěmi, které si posílají UDP pakety. Je to jediné měření, které podporuje mikrosekundovou přesnost, což jí dělá vhodnou pro monitorování video a hlasových

služeb. Tato operace má sekvenční informace o vygenerovaných paketech a časové značky na generátoru i responderu paketů. [2]

2.7.2. Síťový monitoring

- Data Link Switching Plus (DLSw+) - DLSw+ operace měří doby odpovědi mezi DLSw+ uzly. Tato operace v nich měří RTT, neúspěšné operace, chyby ve statistice a sekvenční chyby. [2]

- Frame Relay – Frame relay operace monitoruje fyzické linky frame relay konektivity. Tato operace podporuje mnoho frame relay statistik jako propustnost, ztrátovost paketů, celkový počet přenesených framů od zdroje k cíli. [2]

2.7.3. Aplikační monitoring

- Transmission Control Protocol (TCP) connect – operace TCP connect může být použita pro běžné monitorování dostupnosti sítě. Efektivnějším využitím může být monitorování doby odpovědi serveru, který je založen na TCP aplikacích. Typickým použitím může být monitorování databázi jako mySQL, MSSQL. [2]

- Hypertext Transfer Protocol (HTTP) - HTTP operace měří HTTP serveru reakční dobu mezi zdrojem a odpovědí HTTP serveru k zobrazení webové stránky. Doba odezvy HTTP je součtem tří individuálních round-trip měření. [2]

- File Transfer Protocol (FTP) – operace FTP měří dobu pro stažení souboru mezi zdrojovým zařízením a FTP serverem. Ve výchozím nastavení je použit pasivní režim, aktivní je možnost také nastavit. [2]

- Dynamic Host Control Protocol (DHCP) – DHCP operace měří čas odpovědi od DHCP serveru pro přidělení IP adresy. Je-li specifický DHCP server konfigurován pomocí příkazu „ip helper-adress“, tak DHCP operace posílá směrový požadavek přímo DHCP serveru pomocí za použití DHCPREQUEST paketu. Pokud není DHCP server definován, tak operace odešle broadcast paket pomocí DHCPDISCOVER na všechny IP zařízení v síti. Dále operace funguje s DHCP relay agenty. [2]

- Domain Name System (DNS) – DNS operace měří dobu odezvy od zdroje požadavku k DNS serveru pro přeložení doménového názvu. Efektivní přeložení doménového názvu v síti hraje významnou roli, protože velká odezva od DNS serveru může vést ke zpoždění odpovědí od aplikací. [2]

2.7.4. Hlasový monitoring

- VoIP UDP Jitter – Operace VoIP UDP Jitter slouží k měření kvality hlasového provozu za používání běžných hlasových kodeků a UDP provozu, který je podobný hlasovému provozu. Operace může navracet další dvě číselné hodnoty, které budou hodnotit kvalitu hlasu a těmi jsou MOS (mean opinion score) a ICPIF (the calculated planning impariemnt factor). Operace podporuje kodeky: G.711 A Law, G711 mu Law, G729A. Tato Operace **nesimuluje** RTP provoz. [2]

- VOIP RTP – Operace VoIP RTP je schopna simulovat hlasový provoz RTP streamem. Pro funkčnost této operace je zapotřebí na generátoru provozu mít digitální signálový procesor (DSP), který kóduje daný stream. Tato operace může měřit jitter, R-Factor, MOS a sekvenci paketů. [2]

2.8. *Sběr dat*

2.8.1. Simple Network Managemant Protocol (SNMP)

Protokol SNMP, celým názvem Simple Network Management Protocol. Je jednoduchý široce rozšířený standardizovaný protokol, který slouží ke správě zařízení v počítačových sítích. SNMP podporuje velká část zařízení, například tiskárny, počítačová čidla, síťové prvky. K Transportu dat používá protokol UDP, proto může docházet ke ztrátám paketů. Od verze 2 by již měla být zaimplementována kontrola doručení. Tento protokol prakticky funguje na principu agent/server. Agent přijímá požadavky od serveru a posílá mu zpět nasbíraná data. Server poté přijímá data od agentů, které následně zpracovává a ukládá. [3]

Stačí tedy mít nakonfigurované SNMP na Cisco monitoru a z MIB pomocí SNMP dotazů s daným OID jsme schopni sbírat informace o dané IP SLA sondě na jakýkoliv aplikační server. Následně je můžeme na aplikačním serveru zpracovávat do grafů, určovat určité hraniční hodnoty a případně zkompletovat s dohledovými nástroji.

2.8.2. Příkazová řádka Cisco

Pomocí příkazové řádky jsme schopni si zobrazit poslední operaci, které router vykonal. Dle dané operace jsou zde vidět určité parametry, zda daná operace proběhla, kdy a s jakým výsledkem. K zobrazení dané operace slouží příkaz *„show ip sla statistics <číslo sondy>“*.

Příklad výpisu udp-jitter operace 550 paketů interval mezi pakety 100ms:

```
router#show ip sla statistics 1
IPSLAs Latest Operation Statistics
IPSLA operation id: 1
Type of operation: udp-jitter
        Latest RTT: 21 milliseconds
Latest operation start time: 13:16:14 UTC Thu Apr 21 2016
Latest operation return code: OK
RTT Values:
        Number Of RTT: 550              RTT Min/Avg/Max: 4/21/69 milliseconds
Latency one-way time:
        Number of Latency one-way Samples: 502
        Source to Destination Latency one way Min/Avg/Max: 1/10/47 milliseconds
        Destination to Source Latency one way Min/Avg/Max: 2/11/56 milliseconds
Jitter Time:
        Number of SD Jitter Samples: 549
        Number of DS Jitter Samples: 549
        Source to Destination Jitter Min/Avg/Max: 0/8/25 milliseconds
        Destination to Source Jitter Min/Avg/Max: 0/5/68 milliseconds
Packet Loss Values:
        Loss Source to Destination: 0
        Source to Destination Loss Periods Number: 0
        Source to Destination Loss Period Length Min/Max: 0/0
        Source to Destination Inter Loss Period Length Min/Max: 0/0
        Loss Destination to Source: 0
        Destination to Source Loss Periods Number: 0
        Destination to Source Loss Period Length Min/Max: 0/0
        Destination to Source Inter Loss Period Length Min/Max: 0/0
        Out Of Sequence: 0      Tail Drop: 0
        Packet Late Arrival: 0  Packet Skipped: 0
Voice Score Values:
        Calculated Planning Impairment Factor (ICPIF): 0
        Mean Opinion Score (MOS): 0
Number of successes: 1
Number of failures: 0
Operation time to live: Forever
```

3. Technická část

Praktická část projektu je zaměřena na osvojení teoretických znalostí a vytvoření unifikovaného L3 VPN měření v rámci MPLS sítě. V této problematice se nebudu zabývat konfigurací MPLS. Vzhledem ke škálovatelnosti určitých technologii se bude jen okrajově zabývat nastavení QoS a NTP. Technickou část budu předvádět v malém měřítku, která bude dále škálovatelná na velká telekomunikační řešení. Návrh řešení je rozdělen do tří částí:

- Měření Customer Edge (CE) - Customer Edge (CE) – měření mezi CE směrovači navzájem, jedná se o měření, které postihuje jak páteřní, tak přístupovou část (například mezi pobočkami daného zákazníka nebo mezi centrálou a pobočkou)
- Měření Provider Edge (PE) - Customer Edge (CE) – Měření mezi CE směrovačem a nejbližším PE směrovačem (měření přístupové části sítě, které je závislé na přístupové technologii)
- Měření Provider Edge (PE) - Provider Edge (PE) – Měření mezi PE směrovači v rámci MPLS, jedná se tedy o měření full-mesh páteřní sítě

Každý typ měření bude používat vlastní metodiku.

Měření by mělo probíhat za předpokladu, že zdrojový i cílový směrovač jsou v dané síti daného poskytovatele.

Měřené budou výkonnosti parametry:

- Packet loss
- Delay
- Jitter

Návrh by měl zahrnovat parametry a metodiku měření, tedy jak bude dané měření probíhat, zda bude měření v prioritní frontě s vyhrazeným pásmem nebo měření v defaultní třídě. Například: Každou minutu je odesláno X paketů o velikosti Y bytů s odstupem Z ms mezi každým paketem.

3.1. *Metodika testování*

3.1.1. Typy testů

Pro testování dostupnosti síťové infrastruktury disponuje IOS IP SLA různými typy testů založenými na protokolu ICMP a UDP. S ohledem na požadované výkonnostní metriky v rámci MPLS, jsem pro toto měření vybral operaci UDP jitter.

Jak už bylo řečeno test UDP jiter je primárně určen pro diagnostiku síťové dostupnosti pro voice, video a jiné real-time aplikace (VoIP, video over IP, real-time konference). Je to jediný typ testu, který dokáže dosáhnout mikrosekundové přesnosti. Test UDP jiter generuje sekvenční informace a časové známky pro posílající i přijímající stranu.

Pro měření výkonnostních metrik v MPLS L3 VPN infrastruktuře budeme pracovat se dvěma variantami testu UDP jiter:

- UDP jiter s kodekem g.729a – určen pro měření v rámci prioritní třídě v prioritním provozu – **SLA-Voice**
- UDP jiter bez kodeku – určen pro měření v neprioritizovaných třídách – **SLA-Normal**

Zvolil jsem tyto dva testy tak, aby se dalo pozorovat více parametrů zákazníka. U varianty SLA-Voice jsme schopni odstínit datový tok zákazníka, takže naše měření budou více relevantní. Naopak ve variantě SLA-Normal jsem schopni pozorovat přímé chování v dané třídě v našem případě class-default fronty.

3.1.2. Parametry testů

U testu UDP jiter s kodekem budou konfigurovány následující parametry:

- cílová IP adresa – IP adresa příslušného SLA responderu
- cílový port – UDP port (16384)
- zdrojová IP adresa – IP adresa SLA monitoru
- kodek - typ kodeku (g729a), zvolený kodek určuje velikost paketu

- počet paketů – počet paketů vygenerovaný během jednoho provedení testu
- interval – interval mezi jednotlivými pakety (ms)
- tos – definice ToS (Type of Service)
- tag – identifikátor testu
- vrf – definice MPLS VPN
- frekvence – interval opakování testu (s)

U testu UDP jiter bez kodeku budou konfigurovány stejné parametry jako u testu s kodekem kro mě parametru kodek a data budou generovány v class-default třídě tedy s DSCP CS0 (ToS 0)

3.1.3. SLA-Voice varianta

Parametr	Hodnota
kodek	g.729a
velikost paketu	32B
počet paketů	550
interval	100ms
frekvence	60s (výchozí hodnota)
timeout(výchozí hodnota)	5000ms (výchozí hodnota)
threshold(výchozí hodnota)	5000ms (výchozí hodnota)
type of service	184(EF)

Tabulka 2: Parametry testu UDP jitter ve variantě SLA Voice[zdroj:autor]

Z uvedené tabulky vyplývá, že v této variantě budou generovány pakety o velikosti 32B po dobu 55s s intervalem mezi pakety 100ms a 5s je prodleva do dalšího testu, takže vlastní měření probíhá více jak 90% času z daného měřícího okna, které je dlouhé 60s.

Tento test bude vypovídat o lince jako takové a nebude tak závislý na datovém toku zákazníka. Bude aplikován jen na měření mezi zákaznickými pobočkami a to z důvodu vytíženosti daného měření.

Příklad konfigurace testu UDP jitter s kodekem pro prioritní třídu:

```
ip sla 1
 udp-jitter <IP adresa SLA responderu> 5000 source-ip <IP adresa SLA monitoru>
codec g729a codec-numpackets 550 codec-interval 100
 tos 184
 tag <označení daného měření>
 vrf <vrf>
 frequency 60
```

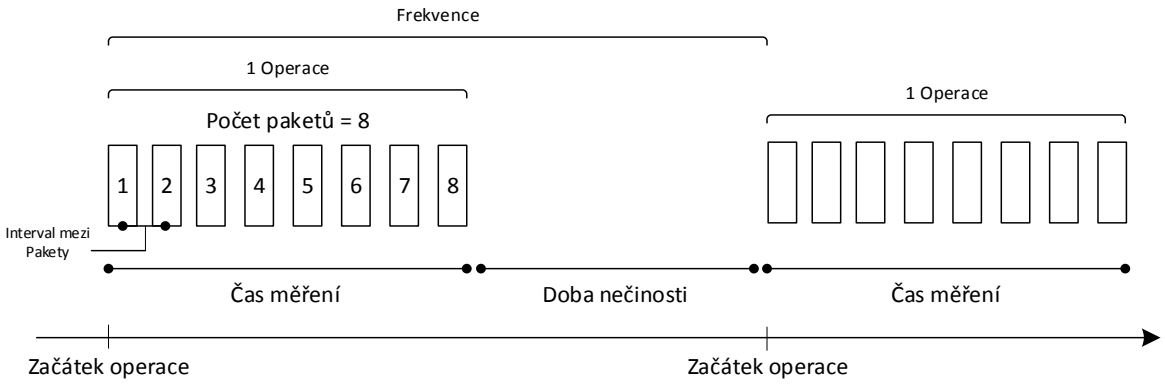
3.1.4. SLA-Normal varianta

Parametr	Hodnota
kodek	žádný
velikost paketu	20B+12B
počet paketů	100
interval	500ms
frekvence	60s (výchozí hodnota)
timeout	5000ms (výchozí hodnota)
threshold	5000ms (výchozí hodnota)
type of service	0 (class default)

Tabulka 3: Parametry testu UDP jitter ve variantě SLA normal[zdroj:autor]

Z uvedené tabulky vyplývá, že v této variantě budou generovány pakety o velikosti 32B po dobu 50s s intervalem mezi pakety 500ms a 10s prodleva do dalšího testu, takže vlastní měření probíhá více jak 80% času z daného měřícího okna, které je dlouhé 60s.

Tento test slouží pro simulaci zákaznického provozu a parametrů v defaultní QoS třídě. Tento test budu aplikovat ve všech možných řešeních.



Obrázek 3: Ilustrace parametrů SLA a vztahů mezi nimi[zdroj:autor]

Příklad konfigurace testu UDP jitter bez kodeku pro prioritní třídu:

```
ip sla 1
 udp-jitter <IP adresa SLA responderu> 16386 source-ip <IP adresa Loopback rozhraní SLA monitoru> num-packets 100 interval 500
 tos 184
 tag <označení daného měření>
 vrf <vrf>
 frequency 60
```

3.1.5. Spouštění testů

Testy budou rozloženy dle daného typu měření na skupiny a následně budou spouštěny hromadně pomocí příkazu ***ip sla group schedule***. Jak již bylo řečeno touto metodou, je možné efektivně a rovnoměrně rozložit zatížení IP SLA sond na procesor daného měřícího zařízení a to tím, že si IP SLA monitor bude sám rozkládat jednotlivé operace.

3.1.6. Nastavení Quality of Service (QoS)

Z pohledu moderních konvergovaných sítí, kde je snahou integrovat všechny služby sítě do jedné sjednocené sítě, je QoS mechanizmus nevyhnutelnou součástí moderních konvergovaných sítí.

Rostoucí požadavky na moderní konvergované datové sítě, které na rozdíl od starých datových sítí přenáší kromě typických dat i ostatní typy provozu reprezentované službami jako hlas, či video-stream v reálném čase. Tradiční datová síť byla určena výhradně pro přenos dat, kde určujícím parametrem sítě byla výhradně její šířka pásma. Tento přístup však při nasazování nových služeb do sítě jako je hlas, video a jiné interaktivní služby citlivé na odezvu a bezchybný přenos nebyl dostatečný. Proto bylo potřebné zabezpečit daným službám adekvátní kvalitu při doručování jednotlivých paketů. Na to, aby s nimi bylo možné odlišně zacházet, bylo nutné jednotlivé typy provozu rozlišovat. V QoS se na to používají mechanizmy inspekce a klasifikace paketů.

Nastavení QoS je tedy pro jednotlivé testy významným konfiguračním parametrem, který zajistí, že provoz generovaný jednotlivými testy bude klasifikován do stejné třídy provozu jako vlastní produkční provoz.

Pro určení třídy provozu je používán parametr type of service (ToS) v hlavičce IPv4 paketu. ToS je osmibitové číslo, které může nabývat hodnot 0-255. Při určení ToS budeme vycházet z definovaných hodnost DSCP (Differenciated Services Codepoint) pro jednotlivé třídy provozu, kdy binární vyjádření DSCP představuje prvních 6 bitu binárního vyjádření ToS. Poslední dva bity jsou využívány pro ECN (Explicit Congestion Notification). [3]

Pro určení správně dekadické hodnoty ToS na základě požadované hodnoty DSCP je možno použít následující tabulku:

DSCP	TOS (binárně)	TOS (dekadicky)
CS0	0	0
CS1	100000	32
AF11	101000	40
AF12	110000	48
AF13	111000	56
CS2	1000000	64
AF21	1001000	72
AF22	1010000	80
AF23	1011000	88
CS3	1100000	96
AF31	1101000	104
AF32	1110000	112
AF33	1111000	120
CS4	10000000	128
AF41	10001000	136
AF42	10010000	144
AF43	10011000	152
CS5	10100000	160
EF	10111000	184
CS6	11000000	192
CS7	11100000	224

Tabulka 4: DSCP/TOS značky[zdroj:autor]

QoS PE-CE:

Klasifikace provozu bude prováděna na základě parametru DSCP v IP hlavičce pro IPv4 provoz. Pro konfiguraci QoS jsem zvolil přístup jako u poskytovatele služeb, kterou jsem omezil jen na nutné minimum. Zákazník si objedná služby a její rychlost. V tomto případě jsem zvolil dvě policy-mapy směrem ke každé pobočce zákazníka a jednu unikátní na vstup od zákazníků. Jedna z policy-map obsahuje class-default shaping a je rodičovská druhé policy-mapy. Druhá policy-mapa obsahuje třídy sloužící k markování provozu viz. tab. 5.

Pro měření SLA provozu jsem zvolil prioritizovanou třídu, která slouží převážně pro hlasový provoz.

Třída	DSCP	CoS/EXP	Poznámka
SLA-Voice	CS3, EF	5	Prioritní třída (Hlasový provoz a SLA měření)
Critical	CS6	3	Kritický provoz citlivý na ztrátu, Směrovací protokoly
class-default	0	0	Provoz zákazníka, Internet, ostatní

Tabulka 5: Třídy provozu pro zákazníky[zdroj:autor]

Vstupní provoz od zákazníka nebude nijak přeznačkován na PE. U provozu ve třídě SLA-Voice se na PE routerech předpokládá použití vstupního policingu, který bude zahazovat vstupní provoz nad hodnotu 50% celkové šířky pásma vstupního rozhraní. Jedná se o bezpečnostní opatření, které by mělo být implementováno v každé MPLS síti a které chrání páteřní infrastrukturu před přetížením prioritním provozem.

Třída	DSCP	CoS/EXP	Povolená šířka pásma	Při překročení
SLA-Voice	CS3, EF	5	50%	Zahození paketů
Critical	CS6	3	-	-
class-default	0	0	-	-

Tabulka 6: Třídy provozu pro zákazníky a jejich omezení[zdroj:autor]

Konfigurace QoS PE-CE:

Zvolení parent policy-mapy:

```
policy-map zakaznik-parent
 class class-default
  shape average 5000000
   service-policy zakaznik
```

Child policy-mapa:

```
policy-map zakaznik
 class SLA-Voice
  priority 100
 class class-default
  bandwidth 4900
```

Unikátní policy-mapa konfigurována v příchozím směru od zákazníka:

```
policy-map FROM-CE
 class SLA-Voice
  police rate percent 50
  set mpls experimental imposition 5
 class Critical
  set mpls experimental imposition 3
```

```
class class-default
 set mpls experimental imposition 0
```

QoS PE-PE:

QoS v rámci páteřní infrastruktury je obdobný jako k zákazníkům. Vytvořil jsem policy-mapu OUT-MPLS, která je aplikována na výstupních rozhraních mezi PE routery. Tato policy-mapa obsahuje 3 třídy. Z pohledu poskytovatele služeb by bylo vhodnější změnit názvy daných tříd vůči zákaznickým, a zároveň by se předpokládala mnohem větší škála tříd.

Třída	DSCP	CoS/EXP	Garantovaná šířka pásma	Při překročení
SLA-Voice	CS3, EF	5	50% (z celkové šířky)	Zahození paketů
Critical	CS6	3	Zbývajících 60%	Pokud je celkové pásmo volné může danou hodnotu překročit
class-default	0	0	Zbývajících 40%	Pokud je celkové pásmo volné může danou hodnotu překročit

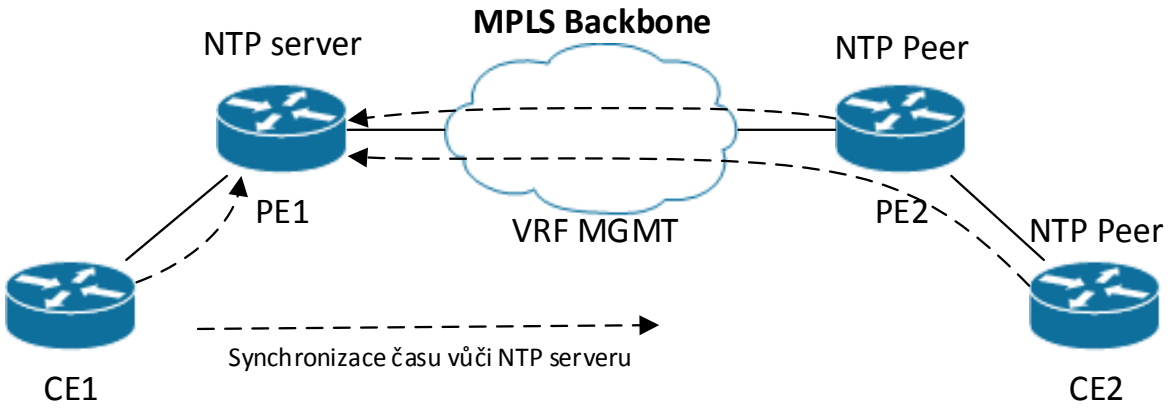
Tabulka 7: Třídy provozu pro páteřní provoz[zdroj:autor]

Páteřní infrastruktura je tedy omezená fyzickou rychlostí dané přenosové trasy. Výstupní provoz má opět bezpečnostní omezení na 50% z celkové šířky pásma v prioritní třídě.

3.1.7. Nastavení Network Time Protocol (NTP)

V rámci základní topologie se předpokládá synchronizace časů vůči jednomu NTP serveru. V tomto řešení bude NTP server představovat PE1 router v rámci MPLS. Viz. obr. 3. Na PE routerech je k tomuto vyhrazena zvláštní L3 VPN vrf nazvaná MGMT. Použil jsem systém prolévání vrf, kde importuji vrf zákazníka do páteřní vrf a naopak (Pozn. Tento systém prolévání není vhodný v rozsáhlejších MPLS řešeních)

Adresace:
PE1: Lo1:10.1.1.1/32 vrf:MGMT
PE2: Lo1:10.1.1.2/32 vrf:MGMT
CE1: Lo0:1.1.1.1/32
CE2: Lo0:2.2.2.2/32



Obrázek 4: Synchronizace času vůči NTP serveru[zdroj:autor]

Konfigurace NTP:

PE1:

```
interface Loopback1
 description NTP
 vrf forwarding MGMT
 ip address 10.1.1.2 255.255.255.255
!
ntp source Loopback1
ntp master 3
```

PE2:

```
interface Loopback1
 description NTP
 vrf forwarding MGMT
 ip address 10.1.1.2 255.255.255.255
!
ntp source Loopback1
ntp server vrf MGMT 10.1.1.1 prefer version 3
```

CE1 a CE2:

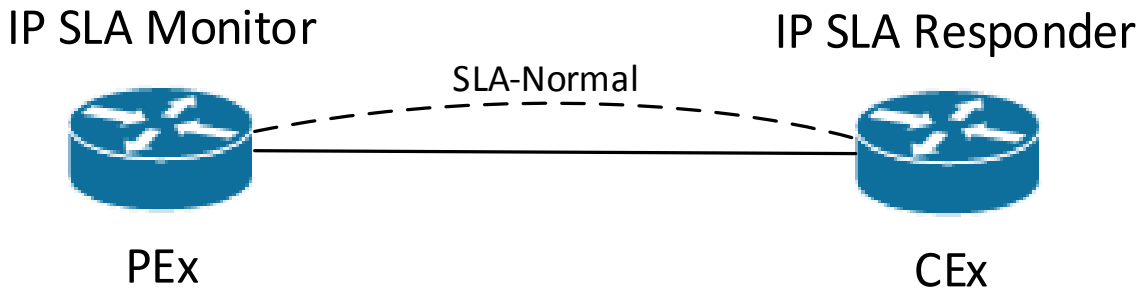
```
ntp source Loopback0
ntp peer 10.1.1.1
```

3.2. *Design*

3.2.1. Měření typu Provider Edge (PE) - Customer Edge (CE)

Tento typ měření bude měřit SLA metriky mezi koncovými zákaznickými CE routery a páteřními PE routery. Pro tento typ měření jsem zvolil design hub and spokes, kde hub představuje IP sla router (PE router) a spokes představují zákaznické CE routery. Toto měření může odhalit problém na dané přenosové technologie, která může pro poskytovatele služeb být pře prodávaná od jiného dodavatele síťových služeb, toto měření tedy může být i výstup při řešení problémů s externím dodavatelem pří dokazování nefunkční poskytované služby, například QoS netransparentnost nebo ztrátovosti paketů.

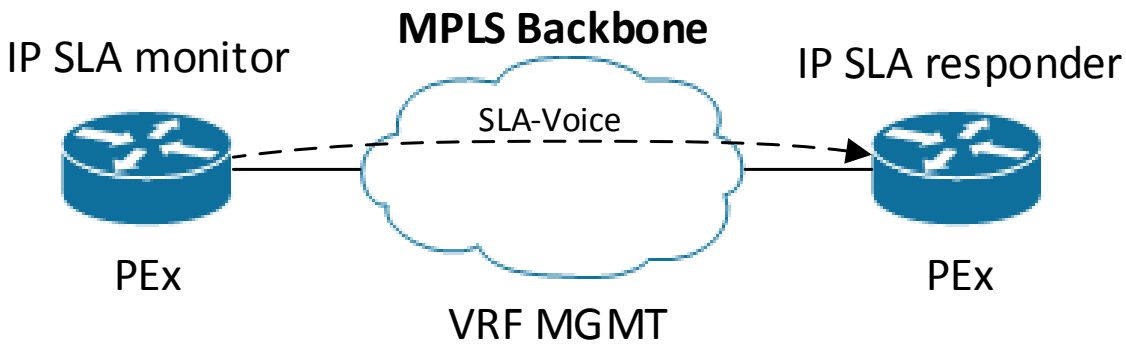
U měření typu PE-CE jsem zvolil jen variantu SLA-Normal z důvodu možného hardwarového vytížení procesoru na SLA monitoru, které by nastalo v případě přibývajících zákazníků a docházelo by k velkému nárůstu identického měření.



Obrázek 5: Měření PE-CE topologie[zdroj:autor]

3.2.2. Měření typu Provider Edge (PE) - Provider Edge (PE)

Tento typ měření bude měřit SLA metriky mezi páteřními PE routery v rámci MPLS sítě. Tento typ měření by měl být zvolen jako full-mesh, tedy měření kde každý PE router bude měřit ke všem ostatním PE routerům. Z pohledu MPLS infrastruktury nebude SLA měření probíhat na úrovni globálního routovacího procesu, ale bude pro něj vyhrazena dedikovaná MPLS VPN, takže bude možné definovat testy v jednotlivých páteřních QOS třídách. Tento test tedy bude určen pro odhalení a řešení problémů v rámci páteřní infrastruktury.

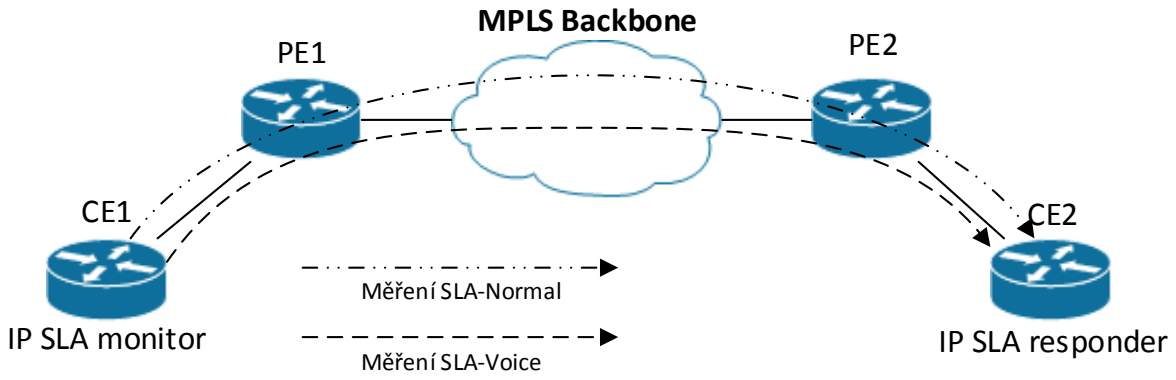


Obrázek 6: Měření PE-PE topologie[zdroj:autor]

3.2.3. Měření typu Customer Edge (CE) - Customer Edge (CE)

Tento typ měření bude měřit SLA metriky mezi koncovými body od zákazníka. Bude tedy monitorovat celou trasu, od jedné pobočky přes celou infrastrukturu poskytovatele až po další pobočku zákazníka. Z tohoto testu může vycházet SLA smlouva, například dodržení maximální odezvy z centrály do pobočky a zpět, případně maximální jitter mezi centrálou a pobočkou nebo maximální procento ztrátovosti.

V našem případě bude router CE1 monitor pro měření typu CE-CE. CE2 bude plnit funkci IP SLA respondera. Z CE1 budou generovány oba typy měření a to SLA-Voice i SLA-Normal. Zvolil jsem oba typy měření z toho důvodu, aby ve variantě SLA-Voice bylo možné odstínit vlivy zákaznického provozu na měření a ve variantě SLA-Normal naopak vidět celkové chování end-to-end konektivity.



Obrázek 7: Měření CE-CE topologie[zdroj:autor]

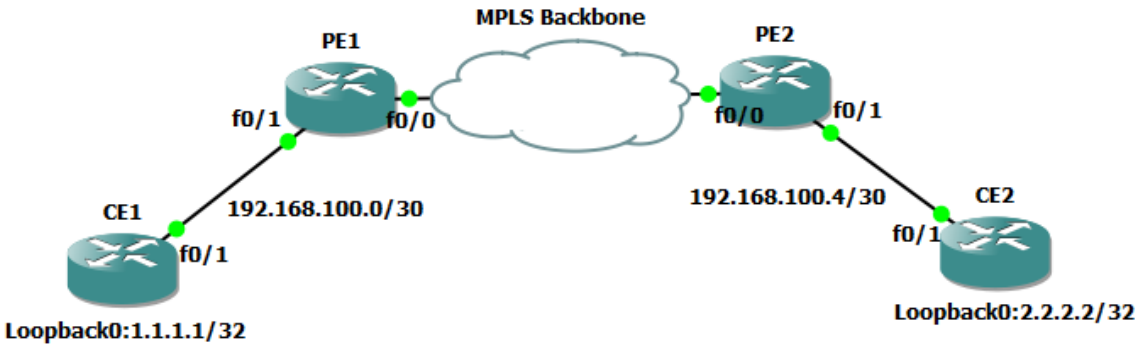
3.3. *Topologie*

Pro simulaci a konfigurace dané problematiky jsem zvolil 4 Cisco routery 7206. Tyto routery se hojně používali a používají v menších firmách poskytující L2/L3 VPN služby, tedy v menších topologiích sítově infrastruktury. Momentálně se C7206 neprodávají, jelikož nemají softwarovou ani hardwarovou podporou.

Celé řešení budeme simulat a konfigurovat v Graphical Network Simulatoru-3 (GNS3). GNS3 používá dynamips pro emulaci softwaru, který simuluje Cisco IOS.

Routery PE1 a PE2 simulují hraniční boxy v rámci MPLS infrastruktury, na niž je nakonfigurována zákaznická vrf a MPLS konfigurace. Routery CE1 a CE2 představují zákazníka se dvěmi pobočkami.

V mraku MPLS backbone je infrasturktura poskytovatele služeb v níž se nachazí MPLS interní routery (tzv. Provider-router) pro směrování MPLS značek, tedy routing jednotlivých zákazníků.



Obrázek 8: Topologie a IP adresace testovacího prostředí[zdroj:autor]

Měření mezi PE-PE bude generováno na PE1 a responder tohoto měření bude PE2. CE-PE měření bude probíhat z hraničních routerů u zákazníka, tedy CE1 bude responderem PE1 a CE2 bude responderem PE2. Berme v potaz, že CE1 je centrální pobočka zákazníka a odtud bude probíhat měření ke všem ostatním pobočkám v této topologii tedy CE1 generuje provoz jen na CE2, tedy CE2 bude responderem pro CE1.

4. Technická analýza

V prvé řadě provedeme konfiguraci IP SLA sond jednotlivých zařízení.

Postupně budeme provádět jednotlivé typy testů. Zaměříme se na měření výkonnostních parametrů jednoho zákazníka, kde budeme provádět simulaci datových toků. Jednotlivé datové toky budeme analyzovat a následně porovnávat jednotlivé stavy, tedy zatížený a nezatížený provoz.

Nejdříve uděláme měření typu PE-CE takzvané „poslední míle“, která může být poskytována od různých poskytovatelů datového připojení, kde se můžou objevit nežádoucí okolní vlivy, které můžou vysoce ovlivnit funkčnost datové linky a tím znehodnotit poskytující službu zákazníkovi. Poslední míle bývá v oblasti poskytování služeb nejčastěji problematická oblast.

Poté se zaměříme na měření typu PE-PE, kde hlavní vlivy má sám poskytovatel MPLS VPN, které nejčastěji způsobí malé zvýšení výkonnostního parametru RTT. Vzhledem ke škálovatelnosti a naddimenzovanému řešení většiny poskytovatelů MPLS VPN, zde nedochází k častým problémům.

Jako poslední typ měření provedeme měření typu CE-CE. Toto měření bývá kontrolním měření zákazníka, kde kontroluje všechny výkonnostní parametry celé přenosové trasy.

Následně budeme dělat analýzu a vyhodnocení IP SLA sond.

4.1. *Konfigurace jednotlivých měření*

4.1.1. Konfigurace IP SLA mezi PE - CE

Konfiguraci a demonstraci řešení budeme provádět mezi zařízeními PE1 a CE1. Konfigurace v našem řešení bude i mezi PE2 a CE2, nicméně ve virtuálním prostředí by nemělo smysl porovnávat daná měření.

Na IP SLA responderu nám stačí zapnout reakci zařízení na testovací pakety a to příkazem:

```
CE1(config)#ip sla responder
```

Nyní přistoupíme k nakonfigurování zařízení typu IP SLA monitor:

```
PE1(config)#ip sla 100
```

```
PE1(config-ip-sla)#udp-jitter 1.1.1.1 16386 source-ip 10.1.1.1 num-packets 100
interval 500
PE1(config-ip-sla-jitter)#tos 184
PE1(config-ip-sla-jitter)#vrf MGMT
PE1(config-ip-sla-jitter)#tag PE1-CE1
```

Těmito příkazy jsme nakonfigurovali IP SLA sondu s číslem 100, kde typ měření je operace udp-jitter s počtem paketů 100 a interval mezi pakety 500ms.

Nyní stačí IP SLA sondu spustit:

```
PE1(config)#ip sla schedule 100 start-time now life forever
```

Test funkčnosti IP SLA sondy pro PE-CE

```
PE1#show ip sla summary  destination 1.1.1.1
*100         udp-jitter  1.1.1.1          RTT=22      OK          56 seconds ago
```

4.1.2. Konfigurace IP SLA mezi PE – PE

Jak již bylo řečeno konfiguraci a demonstraci řešení budeme provádět mezi zařízeními PE1 a PE2 při normálním stavu a vytíženém stavu ve variantách SLA Normal.

Nejprve začneme s konfigurací respondera na zařízení PE2:

```
PE2(config)#ip sla responder
```

Následně budeme konfigurovat SLA Normal variantu na zařízení PE1:

```
PE1(config)#ip sla 1
PE1(config-ip-sla)#udp-jitter 10.1.1.2 16386 source-ip 10.1.1. codec g729a codec-
numpackets 550 codec-interval 100
PE1(config-ip-sla-jitter)#tos 184
PE1(config-ip-sla-jitter)#vrf MGMT
PE1(config-ip-sla-jitter)#tag PE1-PE2 Voice
```

Nyní opět spustíme IP SLA sondu:

```
PE1(config)#ip sla schedule 1 start-time now life forever
```

Kontrola funkčnosti IP SLA sondy:

```
PE1#show ip sla summary destination 10.1.1.2
*1           udp-jitter  10.1.1.2          RTT=28      OK          1 minute, 3
                                                                    seconds ago
```

4.1.3. Konfigurace IP SLA mezi CE – CE

Jako poslední provedeme konfiguraci mezi koncovými zařízeními v MPLS L3 VPN. Jak již bylo řečeno, zde budeme provádět oba typy měření a to z důvodu odstínění vlivů zákaznického provozu na měření.

Na CE2 zapneme funkci pro reakci na IP SLA testovací pakety:

```
CE2(config)#ip sla responder
```

Nyní na CE1 nakonfigurujeme jednotlivé varianty měření:

SLA Voice:

```
CE1(config)#ip sla 100
CE1(config-ip-sla)#udp-jitter 2.2.2.2 16386 source-ip 1.1.1.1 codec g729a codec-numpackets 550 codec-interval 100
CE1(config-ip-sla-jitter)#tos 184
CE1(config-ip-sla-jitter)#tag CE1-CE2 Voice
```

SLA Normal:

```
CE1(config)#ip sla 101
CE1(config-ip-sla)#udp-jitter 2.2.2.2 16386 source-ip 1.1.1.1 num-packets 100 interval 500
CE1(config-ip-sla-jitter)#tos 184
CE1(config-ip-sla-jitter)#tag CE1-CE2 Normal
```

Otestování funkčnosti jednotlivých variant:

```
CE1#show ip sla summary destination 2.2.2.2
*100         udp-jitter  2.2.2.2           RTT=44      OK          1 minute, 43
                                                                   seconds ago


*101         udp-jitter  2.2.2.2           RTT=49      OK          1 minute, 43
                                                                   seconds ago
```

4.2. *Testování scénářů*

Máme nakonfigurovány jednotlivé typy měření a nyní přejdeme k jednotlivým scénářům, které by mohly vzniknout v transportní síti z pohledu zákazníka, tak i poskytovatele služeb.

Hodnoty měření z jednotlivých zařízení při normálním datovém provozu.

PE1 - CE1 SLA Normal:

```
PE1#show ip sla statistics 100
IPSLAs Latest Operation Statistics

IPSLA operation id: 100
Type of operation: udp-jitter
        Latest RTT: 17 milliseconds
Latest operation start time: 14:40:10 UTC Sat Aug 6 2016
Latest operation return code: OK
RTT Values:
        Number Of RTT: 100              RTT Min/Avg/Max: 1/17/41 milliseconds
Latency one-way time:
        Number of Latency one-way Samples: 61
        Source to Destination Latency one way Min/Avg/Max: 0/10/31 milliseconds
        Destination to Source Latency one way Min/Avg/Max: 5/10/18 milliseconds
Jitter Time:
        Number of SD Jitter Samples: 99
        Number of DS Jitter Samples: 99
        Source to Destination Jitter Min/Avg/Max: 0/12/41 milliseconds
        Destination to Source Jitter Min/Avg/Max: 0/7/24 milliseconds
Packet Loss Values:
        Loss Source to Destination: 0
        Source to Destination Loss Periods Number: 0
        Source to Destination Loss Period Length Min/Max: 0/0
        Source to Destination Inter Loss Period Length Min/Max: 0/0
        Loss Destination to Source: 0
        Destination to Source Loss Periods Number: 0
        Destination to Source Loss Period Length Min/Max: 0/0
        Destination to Source Inter Loss Period Length Min/Max: 0/0
        Out Of Sequence: 0      Tail Drop: 0
        Packet Late Arrival: 0  Packet Skipped: 0
Voice Score Values:
        Calculated Planning Impairment Factor (ICPIF): 0
        Mean Opinion Score (MOS): 0
Number of successes: 8
Number of failures: 0
Operation time to live: Forever
```

PE1 - PE2 SLA Voice:

```
PE1#show ip sla statistics 1
IPSLAs Latest Operation Statistics
```

```
IPSLA operation id: 1
Type of operation: udp-jitter
        Latest RTT: 25 milliseconds
Latest operation start time: 14:51:37 UTC Sat Aug 6 2016
Latest operation return code: OK
RTT Values:
        Number Of RTT: 550              RTT Min/Avg/Max: 7/25/56 milliseconds
Latency one-way time:
        Number of Latency one-way Samples: 180
        Source to Destination Latency one way Min/Avg/Max: 0/7/31 milliseconds
        Destination to Source Latency one way Min/Avg/Max: 19/28/45 milliseconds
Jitter Time:
        Number of SD Jitter Samples: 549
        Number of DS Jitter Samples: 549
        Source to Destination Jitter Min/Avg/Max: 0/14/48 milliseconds
        Destination to Source Jitter Min/Avg/Max: 0/7/37 milliseconds
Packet Loss Values:
        Loss Source to Destination: 0
        Source to Destination Loss Periods Number: 0
        Source to Destination Loss Period Length Min/Max: 0/0
        Source to Destination Inter Loss Period Length Min/Max: 0/0
        Loss Destination to Source: 0
        Destination to Source Loss Periods Number: 0
        Destination to Source Loss Period Length Min/Max: 0/0
        Destination to Source Inter Loss Period Length Min/Max: 0/0
        Out Of Sequence: 0      Tail Drop: 0
        Packet Late Arrival: 0  Packet Skipped: 0
Voice Score Values:
        Calculated Planning Impairment Factor (ICPIF): 11
        MOS score: 4.06
Number of successes: 2
Number of failures: 0
Operation time to live: Forever
```

CE1 - CE2 SLA Voice:

```
CE1#show ip sla statistics
IPSLAs Latest Operation Statistics

IPSLA operation id: 100
Type of operation: udp-jitter
        Latest RTT: 48 milliseconds
Latest operation start time: 14:15:53 UTC Sat Aug 6 2016
Latest operation return code: OK
```

```
RTT Values:
        Number Of RTT: 550              RTT Min/Avg/Max: 1/35/71 milliseconds
Latency one-way time:
        Number of Latency one-way Samples: 526
        Source to Destination Latency one way Min/Avg/Max: 2/19/59 milliseconds
        Destination to Source Latency one way Min/Avg/Max: 2/16/43 milliseconds
Jitter Time:
        Number of SD Jitter Samples: 549
        Number of DS Jitter Samples: 549
        Source to Destination Jitter Min/Avg/Max: 0/8/56 milliseconds
        Destination to Source Jitter Min/Avg/Max: 0/6/34 milliseconds
Packet Loss Values:
        Loss Source to Destination: 0
        Source to Destination Loss Periods Number: 0
        Source to Destination Loss Period Length Min/Max: 0/0
        Source to Destination Inter Loss Period Length Min/Max: 0/0
        Loss Destination to Source: 0
        Destination to Source Loss Periods Number: 0
        Destination to Source Loss Period Length Min/Max: 0/0
        Destination to Source Inter Loss Period Length Min/Max: 0/0
        Out Of Sequence: 0      Tail Drop: 0
        Packet Late Arrival: 0  Packet Skipped: 0
Voice Score Values:
        Calculated Planning Impairment Factor (ICPIF): 11
        MOS score: 4.06
Number of successes: 8
Number of failures: 0
Operation time to live: Forever
```

CE1 - CE2 SLA Normal:

```
IPSLA operation id: 101
Type of operation: udp-jitter
        Latest RTT: 41 milliseconds
Latest operation start time: 14:15:53 UTC Sat Aug 6 2016
Latest operation return code: OK
RTT Values:
        Number Of RTT: 100              RTT Min/Avg/Max: 25/41/78 milliseconds
Latency one-way time:
        Number of Latency one-way Samples: 100
        Source to Destination Latency one way Min/Avg/Max: 19/29/43 milliseconds
        Destination to Source Latency one way Min/Avg/Max: 0/12/42 milliseconds
Jitter Time:
        Number of SD Jitter Samples: 99
        Number of DS Jitter Samples: 99
```

```
        Source to Destination Jitter Min/Avg/Max: 0/7/19 milliseconds
        Destination to Source Jitter Min/Avg/Max: 0/7/28 milliseconds
Packet Loss Values:
        Loss Source to Destination: 0
        Source to Destination Loss Periods Number: 0
        Source to Destination Loss Period Length Min/Max: 0/0
        Source to Destination Inter Loss Period Length Min/Max: 0/0
        Loss Destination to Source: 0
        Destination to Source Loss Periods Number: 0
        Destination to Source Loss Period Length Min/Max: 0/0
        Destination to Source Inter Loss Period Length Min/Max: 0/0
        Out Of Sequence: 0      Tail Drop: 0
        Packet Late Arrival: 0  Packet Skipped: 0
Voice Score Values:
        Calculated Planning Impairment Factor (ICPIF): 0
        Mean Opinion Score (MOS): 0
Number of successes: 16
Number of failures: 0
Operation time to live: Forever
```

Z výše uvedených dat vidíme parametry jednotlivých měření z IP SLA sond. Vidíme zde parametry jako round-trip-time, jitter, odezvu zdroje k cíli, odezvu od cíle ke zdroji, ztrátovost paketů, MOS a IPCIF. Dokážeme z toho také vyčíst čas, kdy byla daná operace naposledy vykonána, zda proběhla v pořádku, počet zdařilých operací, počet nezdařilých operací a životnost operace. Opravdu zajímavým parametrem jsou tzv. jednosměrné statistiky, ze kterých jsme schopni odvodit mnoho informací, které můžou být velmi důležitou součástí řešení poruchovosti na transportní sítí.

SLA Voice	Měření PE1-CE1	Měření PE1-PE2	Měření CE1-CE2
RTT (avg)	X	25ms	35ms
Latency S->D	X	7ms	19ms
Latency D->S	X	28ms	16ms
Jitter S->D	X	14ms	8ms
Jitter D->S	X	7ms	6ms
Packet loss	X	0	0
MOS	X	4,06	4,06
IPCIF	X	11	11

Tabulka 8: Souhrnná tabulka měření ve variantě SLA Voice za normálního datového provozu[zdroj:autor]

SLA Normal	Měření PE1-CE1	Měření PE1-PE2	Měření CE1-CE2
RTT (avg)	17ms	X	41ms
Latency S->D	10ms	X	29ms
Latency D->S	10ms	X	12ms
Jitter S->D	12ms	X	7ms
Jitter D->S	7ms	X	7ms
Packet loss	0	X	0

Tabulka 9: Souhrnná tabulka měření ve variantě SLA Normal za normálního datového provozu[zdroj:autor]

4.2.1. Scénář: Vytížení datové linky

Nyní se podíváme na variantu, kdy si sám zákazník vytíží linku vlastním provozem. Následně si začne stěžovat svému poskytovateli připojení na vysoké odezvy, velké odchylku jitteru, případně ztrátovosti paketů. Pro věrohodnost měření v simulovaném prostředí jsme si již vytvořili QoS politiku o velikosti pásma 5Mbit mezi zařízeními PE1-CE1 a PE2-CE2. Pro simulaci datového toku spustíme ping o velikosti 1500bytů s časovým limitem 0 pro odezvu a tím zaplníme datovou linku.

Kontrola zaplnění datové linky:

```
CE1#show policy-map int fa0/1
 FastEthernet0/1

  Service-policy output: zakaznik

    queue stats for all priority classes:
      Queueing
      queue limit 64 packets
      (queue depth/total drops/no-buffer drops) 0/0/0
      (pkts output/bytes output) 614739/45495386

    Class-map: Cust-Voice (match-any)
      614739 packets, 45495386 bytes
      30 second offered rate 6000 bps, drop rate 0000 bps
      Match:  dscp ef (46)
        614739 packets, 45495386 bytes
        30 second rate 6000 bps
      Match:  dscp cs3 (24)
        0 packets, 0 bytes
        30 second rate 0 bps
      Priority: 100 kbps, burst bytes 2500, b/w exceed drops: 0
```

```
  Class-map: class-default (match-any)
7610843 packets, 4398223737 bytes
30 second offered rate 6302000 bps, drop rate 167000 bps
Match: any
Queueing
queue limit 64 packets
(queue depth/total drops/no-buffer drops) 63/206590/0
(pkts output/bytes output) 7404254/4279906533
bandwidth 4900 kbps
```

Z výše uvedeného výstupu vidíme, že dochází k přehlcení datové linky a tím pádem k zahazování paketů na dané lince ve směru CE1-PE1. Nyní se podíváme na IP SLA měření mezi hraničními routery CE1 a CE2.

Měření CE1-CE2 SLA Voice:

```
CE1# show ip sla statistics 100
IPSLAs Latest Operation Statistics

IPSLA operation id: 100
Type of operation: udp-jitter
        Latest RTT: 34 milliseconds
Latest operation start time: 19:09:33 UTC Sun Aug 7 2016
Latest operation return code: OK
RTT Values:
        Number Of RTT: 550              RTT Min/Avg/Max: 1/34/74 milliseconds
Latency one-way time:
        Number of Latency one-way Samples: 526
        Source to Destination Latency one way Min/Avg/Max: 1/19/58 milliseconds
        Destination to Source Latency one way Min/Avg/Max: 2/15/48 milliseconds
Jitter Time:
        Number of SD Jitter Samples: 549
        Number of DS Jitter Samples: 549
        Source to Destination Jitter Min/Avg/Max: 0/13/49 milliseconds
        Destination to Source Jitter Min/Avg/Max: 0/11/55 milliseconds
Packet Loss Values:
        Loss Source to Destination: 0
        Source to Destination Loss Periods Number: 0
        Source to Destination Loss Period Length Min/Max: 0/0
        Source to Destination Inter Loss Period Length Min/Max: 0/0
        Loss Destination to Source: 0
        Destination to Source Loss Periods Number: 0
```

```
        Destination to Source Loss Period Length Min/Max: 0/0
        Destination to Source Inter Loss Period Length Min/Max: 0/0
        Out Of Sequence: 0      Tail Drop: 0
        Packet Late Arrival: 0  Packet Skipped: 18
Voice Score Values:
        Calculated Planning Impairment Factor (ICPIF): 11
        MOS score: 4.06
Number of successes: 20
Number of failures: 0
Operation time to live: Forever
```

Měření CE1-CE2 SLA Normal:

```
CE1# show ip sla statistics 101
IPSLA operation id: 101
Type of operation: udp-jitter
        Latest RTT: 211 milliseconds
Latest operation start time: 19:09:38 UTC Sun Aug 7 2016
Latest operation return code: OK
RTT Values:
        Number Of RTT: 77               RTT Min/Avg/Max: 184/211/236 milliseconds
Latency one-way time:
        Number of Latency one-way Samples: 77
        Source to Destination Latency one way Min/Avg/Max: 145/165/195 milliseconds
        Destination to Source Latency one way Min/Avg/Max: 23/45/63 milliseconds
Jitter Time:
        Number of SD Jitter Samples: 61
        Number of DS Jitter Samples: 76
        Source to Destination Jitter Min/Avg/Max: 0/7/24 milliseconds
        Destination to Source Jitter Min/Avg/Max: 0/8/22 milliseconds
Packet Loss Values:
        Loss Source to Destination: 23
        Source to Destination Loss Periods Number: 12
        Source to Destination Loss Period Length Min/Max: 1/4
        Source to Destination Inter Loss Period Length Min/Max: 1/23
        Loss Destination to Source: 0
         Destination to Source Loss Periods Number: 0
        Destination to Source Loss Period Length Min/Max: 0/0
        Destination to Source Inter Loss Period Length Min/Max: 0/0
        Out Of Sequence: 0      Tail Drop: 0
        Packet Late Arrival: 0  Packet Skipped: 0
Voice Score Values:
        Calculated Planning Impairment Factor (ICPIF): 0
        Mean Opinion Score (MOS): 0
Number of successes: 9
```

```
Number of failures: 0
Operation time to live: Forever
```

Z uvedených dat názorně vidíme, že opravdu dochází ke ztrátovosti paketů v defaultní třídě vlivem velkého datového toku, z původních hodnot se nám také skokově zvýšila odezva a jitter. Dokážeme také poznat, v jakém směru ztrátovost vzniká. V našem případě je to z CE1 na CE2.

Pokud se podíváme na měření v prioritní třídě SLA Voice, tak z původních hodnot vidíme, že nedošlo prakticky k žádné změně a tím pádem můžeme deklarovat, že linka je v pořádku a nedochází k nechtěnému zahazování paketů na přenosové technologii nebo v páteřní infrastruktuře poskytovatele. Porovnání mezi zatíženým a nezatíženým stavem je uvedeno v tabulce Tabulka 10: Porovnávací tabulka mezi zatíženým a nezatíženým stavem.

CE1-CE2	Normální stav		Zatížený stav	
Parametr	SLA Normal	SLA Voice	SLA Normal	SLA Voice
RTT (avg)	41ms	35ms	211ms	34ms
Latency S->D	29ms	19ms	165ms	19ms
Latency D->S	12ms	16ms	45ms	15ms
Jitter S->D	7ms	8ms	7ms	13ms
Jitter D->S	7ms	6ms	8ms	11ms
Packet loss	0	0	23	0
Packet loss S->D	0	0	23	0
Packet loss D->S	0	0	0	0
MOS	X	4,06	X	4,06
IPCIF	X	11	X	11

Tabulka 10: Porovnávací tabulka mezi zatíženým a nezatíženým stavem[zdroj:autor]

4.2.2. Scénář: Vytížení hlasové linky

Zákazník si stěžuje na špatnou kvalitu hovorů. Tento stav v případě, že je správně koncipována QoS politika nastane z toho důvodu, že zákazník má větší hlasový tok, než přidělené hlasové pásmo. V našem případě je šířka hlasového pásma 100Kbit. Datový tok u jednoho hovoru s kodekem G729a je cca 32Kbit/s. Proto zákazník může provést 3 hovory současně, které budou funkční. Simulaci hlasového toku opět provedeme příkazem ping, kde dané pakety označíme značkou DSCP EF.

Kontrola zaplnění hlasové třídy:

```
CE1#sh policy-map int fa0/1
 FastEthernet0/1

  Service-policy output: zakaznik

    queue stats for all priority classes:
      Queueing
      queue limit 64 packets
      (queue depth/total drops/no-buffer drops) 0/0/0
      (pkts output/bytes output) 661604/51762642

    Class-map: Cust-Voice (match-any)
      669687 packets, 52363554 bytes
      30 second offered rate 801000 bps, drop rate 23000 bps
      Match:  dscp ef (46)
        669687 packets, 52363554 bytes
        30 second rate 801000 bps
      Match:  dscp cs3 (24)
        0 packets, 0 bytes
        30 second rate 0 bps
      Priority: 100 kbps, burst bytes 2500, b/w exceed drops: 8035


    Class-map: class-default (match-any)
      797 packets, 60767 bytes
      30 second offered rate 1000 bps, drop rate 0000 bps
      Match: any
      Queueing
      queue limit 64 packets
      (queue depth/total drops/no-buffer drops) 0/0/0
      (pkts output/bytes output) 797/60767
      bandwidth 4900 kbps
```

Z uvedených dat vidíme, že došlo k zaplnění hlasové třídy a tím pádem k zahazování paketů v této třídě. V hlasové třídě máme také měření SLA Voice. V defaultní třídě není prakticky žádný provoz, proto nedochází k zahazování paketů v této třídě. Důležité opomenout je to, že třída Voice má prioritní přednost pro zpracování paketů před třídou class-default a z toho důvodu se může stát, že pakety ze třídy class-default budou mít nějaké zpoždění, nicméně by ani tak nemělo dojít k zahození paketu.

Nyní se podíváme na jednotlivá měření:

PE1-CE1:

```
PE1#show ip sla statistics 100
IPSLA operation id: 100
Type of operation: udp-jitter
        Latest RTT: 37 milliseconds
Latest operation start time: 21:26:26 UTC Sun Aug 7 2016
Latest operation return code: OK
RTT Values:
        Number Of RTT: 100              RTT Min/Avg/Max: 3/37/72 milliseconds
Latency one-way time:
        Number of Latency one-way Samples: 86
        Source to Destination Latency one way Min/Avg/Max: 0/15/28 milliseconds
        Destination to Source Latency one way Min/Avg/Max: 2/22/60 milliseconds
Jitter Time:
        Number of SD Jitter Samples: 99
        Number of DS Jitter Samples: 99
        Source to Destination Jitter Min/Avg/Max: 0/6/19 milliseconds
        Destination to Source Jitter Min/Avg/Max: 0/7/35 milliseconds
Packet Loss Values:
        Loss Source to Destination: 0
        Source to Destination Loss Periods Number: 0
        Source to Destination Loss Period Length Min/Max: 0/0
        Source to Destination Inter Loss Period Length Min/Max: 0/0
        Loss Destination to Source: 0
        Destination to Source Loss Periods Number: 0
        Destination to Source Loss Period Length Min/Max: 0/0
        Destination to Source Inter Loss Period Length Min/Max: 0/0
        Out Of Sequence: 0      Tail Drop: 0
        Packet Late Arrival: 0  Packet Skipped: 68
Voice Score Values:
        Calculated Planning Impairment Factor (ICPIF): 0
        Mean Opinion Score (MOS): 0
Number of successes: 6
Number of failures: 0
Operation time to live: Forever
```

V případě měření PE1-CE1 se nám nic nezměnilo. RTT i Jitter jsou v normě.

PE1-PE2:

```
PE1#show ip sla statistics 1
IPSLAs Latest Operation Statistics

IPSLA operation id: 1
```

```
Type of operation: udp-jitter
        Latest RTT: 119 milliseconds
Latest operation start time: 21:27:37 UTC Sun Aug 7 2016
Latest operation return code: OK
RTT Values:
        Number Of RTT: 550              RTT Min/Avg/Max: 31/60/120 milliseconds
Latency one-way time:
        Number of Latency one-way Samples: 423
        Source to Destination Latency one way Min/Avg/Max: 0/28/61 milliseconds
        Destination to Source Latency one way Min/Avg/Max: 10/32/59 milliseconds
Jitter Time:
        Number of SD Jitter Samples: 549
        Number of DS Jitter Samples: 549
        Source to Destination Jitter Min/Avg/Max: 0/5/69 milliseconds
        Destination to Source Jitter Min/Avg/Max: 0/5/47 milliseconds
Packet Loss Values:
        Loss Source to Destination: 0
        Source to Destination Loss Periods Number: 0
        Source to Destination Loss Period Length Min/Max: 0/0
        Source to Destination Inter Loss Period Length Min/Max: 0/0
        Loss Destination to Source: 0
        Destination to Source Loss Periods Number: 0
        Destination to Source Loss Period Length Min/Max: 0/0
        Destination to Source Inter Loss Period Length Min/Max: 0/0
        Out Of Sequence: 0      Tail Drop: 0
        Packet Late Arrival: 0  Packet Skipped: 0
Voice Score Values:
        Calculated Planning Impairment Factor (ICPIF): 12
        MOS score: 4.03
Number of successes: 28
Number of failures: 0
Operation time to live: Forever
```

V měření PE1-PE2, které probíhá ve variantě SLA Voice je vidět, že došlo k nárůstu latence. Vzhledem k tomu, že se jedná o simulované prostředí, tak tato situace může nastat, v reálném prostředí by takový to provoz neměl ohrozit páteřní infrastrukturu.

CE1-CE2 SLA Voice:

```
CE1#show ip sla statistics
IPSLAs Latest Operation Statistics

IPSLA operation id: 100
Type of operation: udp-jitter
```

```
        Latest RTT: 146 milliseconds
Latest operation start time: 21:15:33 UTC Sun Aug 7 2016
Latest operation return code: OK
RTT Values:
        Number Of RTT: 536              RTT Min/Avg/Max: 2/146/187 milliseconds
Latency one-way time:
        Number of Latency one-way Samples: 529
        Source to Destination Latency one way Min/Avg/Max: 3/103/141 milliseconds
        Destination to Source Latency one way Min/Avg/Max: 5/44/73 milliseconds
Jitter Time:
        Number of SD Jitter Samples: 522
        Number of DS Jitter Samples: 535
        Source to Destination Jitter Min/Avg/Max: 0/6/61 milliseconds
        Destination to Source Jitter Min/Avg/Max: 0/5/40 milliseconds
Packet Loss Values:
        Loss Source to Destination: 14
        Source to Destination Loss Periods Number: 11
        Source to Destination Loss Period Length Min/Max: 1/2
        Source to Destination Inter Loss Period Length Min/Max: 2/145
        Loss Destination to Source: 0
        Destination to Source Loss Periods Number: 0
        Destination to Source Loss Period Length Min/Max: 0/0
        Destination to Source Inter Loss Period Length Min/Max: 0/0
        Out Of Sequence: 0      Tail Drop: 0
        Packet Late Arrival: 0  Packet Skipped: 18
Voice Score Values:
        Calculated Planning Impairment Factor (ICPIF): 20
        MOS score: 3.12
Number of successes: 8
Number of failures: 0
Operation time to live: Forever
```

CE1-CE2 SLA Normal:

```
IPSLA operation id: 101
Type of operation: udp-jitter
        Latest RTT: 147 milliseconds
Latest operation start time: 21:15:33 UTC Sun Aug 7 2016
Latest operation return code: OK
RTT Values:
        Number Of RTT: 100              RTT Min/Avg/Max: 20/147/184 milliseconds
Latency one-way time:
        Number of Latency one-way Samples: 98
        Source to Destination Latency one way Min/Avg/Max: 15/101/136 milliseconds
        Destination to Source Latency one way Min/Avg/Max: 20/47/72 milliseconds
```

```
Jitter Time:
        Number of SD Jitter Samples: 99
        Number of DS Jitter Samples: 99
        Source to Destination Jitter Min/Avg/Max: 0/9/78 milliseconds
        Destination to Source Jitter Min/Avg/Max: 0/9/40 milliseconds
Packet Loss Values:
        Loss Source to Destination: 0
        Source to Destination Loss Periods Number: 0
        Source to Destination Loss Period Length Min/Max: 0/0
        Source to Destination Inter Loss Period Length Min/Max: 0/0
        Loss Destination to Source: 0
        Destination to Source Loss Periods Number: 0
        Destination to Source Loss Period Length Min/Max: 0/0
        Destination to Source Inter Loss Period Length Min/Max: 0/0
        Out Of Sequence: 0      Tail Drop: 0
        Packet Late Arrival: 0  Packet Skipped: 0
Voice Score Values:
        Calculated Planning Impairment Factor (ICPIF): 0
        Mean Opinion Score (MOS): 0
Number of successes: 12
Number of failures: 0
Operation time to live: Forever
```

Z měření SLA Voice mezi CE1 a CE2 vidíme, že došlo ke zhoršení parametrů pro hlasové technologie a dokonce ke ztrátovosti paketů. Latence se rapidně zvedla na průměrně 146ms, 14 paketů od zdroje k cíli nedošlo, hodnota MOS klesla na 3,12 a hodnota ICPIF stoupla na 20.

PE1-CE1	Normální stav		Zatížený stav	
Parametr	SLA Normal	SLA Voice	SLA Normal	SLA Voice
RTT (avg)	17ms	X	37ms	X
Latency S->D	10ms	X	15ms	X
Latency D->S	10ms	X	22ms	X
Jitter S->D	12ms	X	6ms	X
Jitter D->S	7ms	X	7ms	X
Packet loss	0	X	0	X
Packet loss S->D	0	X	0	X
Packet loss D->S	0	X	0	X
MOS	X	X	X	X
IPCIF	X	X	X	X

Tabulka 11: Souhrnná tabulka měření mezi PE1-CE1[zdroj:autor]

Naopak z měření SLA Normal mezi CE1 a CE2 jasně plyne, že nedošlo ke ztrátovosti paketů, nicméně jak již bylo řečeno, SLA Voice je v prioritní třídě a tím pádem může nastat situace, kdy se nám navýší latence a to se zde také stalo. Latence stoupla na průměrnou hodnotu 147ms.

PE1-PE2	Normální stav		Zatížený stav	
Parametr	SLA Normal	SLA Voice	SLA Normal	SLA Voice
RTT (avg)	X	25ms	X	60ms
Latency S->D	X	7ms	X	28ms
Latency D->S	X	28ms	X	32ms
Jitter S->D	X	14ms	X	5ms
Jitter D->S	X	7ms	X	5ms
Packet loss	X	0	X	0
Packet loss S->D	X	0	X	0
Packet loss D->S	X	0	X	0
MOS	X	4,06	X	4,03
IPCIF	X	11	X	12

Tabulka 12: Souhrnná tabulka měření mezi PE1-PE2[zdroj:autor]

V obou případech vidíme, že hlasový provoz byl generován od zákazníka CE1, protože ztrátovost i latence se rapidně zvedla od zdroje k cíli a zdroj generovaných měření je CE1.

Tímto měřením jsme tedy schopni vyhodnotit jednotlivé stavy, které můžou probíhat na dané lince. Můžeme rozlišit v jaké QoS třídě nám vzniká problém a tím proaktivně reagovat.

CE1-CE2	Normální stav		Zatížený stav	
Parametr	SLA Normal	SLA Voice	SLA Normal	SLA Voice
RTT (avg)	41ms	35ms	147ms	146ms
Latency S->D	29ms	19ms	101ms	103ms
Latency D->S	12ms	16ms	47ms	44ms
Jitter S->D	7ms	8ms	9	6ms
Jitter D->S	7ms	6ms	9ms	5ms
Packet loss	0	0	0	14
Packet loss S->D	0	0	0	14
Packet loss D->S	0	0	0	0
MOS	X	4,06	X	3,12
IPCIF	X	11	X	20

Tabulka 13: Souhrnná tabulka měření mezi CE1-CE2[zdroj:autor]

5. Závěr

Bakalářská práce popsala problematiku a princip měření výkonnostních parametrů za pomocí technologie IP SLA od společnosti Cisco Systems v transportní síti postavené na přepínacím mechanizmu MPLS s důrazem na směrování, kvalitu a přepínání v IP síti. Představila možnosti předcházení problémům, které můžou vznikat různými změnami v páteřní infrastruktuře, případně od třetích stran poskytovatelů služeb.

Technologie IP SLA byla popsána z teoretické i praktické části. Osvojili jsme si konfiguraci na zařízeních této technologie. Okrajově jsme se zabývali konfigurací služeb v rámci MPLS VPN.

Dále pojednávala o principu a metodách typu měření a vyhodnocení daných parametrů. Z testovacích scénářů jsme zjistili, že je to velice užitečná technologie pro řešení poruch. Také jsme viděli jednotlivé stavy chování při určitém typu provozu.

Zjistili jsme, že IP SLA je velice komplexní nástroj pro sledování sítě. Můžeme, tím sledovat velké množství provozu, a i služeb od běžné TCP nebo UDP komunikace až po VoIP, video, HTTP a FTP dostupnost.

Námi měřené výsledky jsou pouze laboratorní, ale pro důkaz funkčnosti dostačující.

6. Seznam zdrojů

1. **Cisco Systems, Inc.** Cisco IOS IP SLAs Overview. [Online] 2005. [Citace: 8. březen 2016.] http://www.cisco.com/c/en/us/td/docs/ios/12_4/ip_sla/configuration/guide/hsla_c/hsoverv.html.

2. —. IP SLAs Configuration Guide, Cisco IOS Release 15M&T. [Online] 2012. [Citace: 9. duben 2016.] http://www.cisco.com/c/en/us/td/docs/ios-xml/ios/ipsla/configuration/15-mt/sla-15-mt-book.pdf.

3. **Odom, Wendell.** *CCNP ROUTE 642-902 Official Certification Guide.* Indianapolis, Ind. : Cisco Press, 2010. ISBN 978-1-58720-253-7.

4. **Zoho Corporation.** IP Service Level Agreement Module. [Online] Manage Engine, 2011. [Citace: 2. Leden 2016.] https://www.manageengine.com/products/netflow/ipsla-monitor.html.

5. **Cisco Systems, Inc.** Cisco IP Service Level Agreement Video Operation. [Online] 2011. [Citace: 10. duben 2016.] http://www.cisco.com/c/en/us/products/collateral/ios-nx-os-software/ios-ip-service-level-agreements-slas/white_paper_c11-674560.html.

6. **Hucaby, David.** *CCNP Routing and Switching SWITCH 300-115 Offical Certification Guide.* Indianapolis, IN : Cisco Press, 2014. ISBN 978-1-58720-560-6.

7. **Alwayn, Vivek.** *Advanced MPLS design and implementation.* Indianapolis, IN : Cisco Press, 2001. ISBN 1-58705-020-X.

8. **WALLACE, Kevin.** *CCNP Routing and Switching ROUTE 300-101 Official Cert Guide.* Indianapolis, IN : Cisco Press, 2014. ISBN 978-1-58720-559-0.

7. Seznam použitých zkratek

CE	–	Customer Edge
CLI	–	Command line interface
Cos	–	Class of service
DHCP	–	Dynamic Host Configuration Protocol
DLSw+	–	Data-Link Switching
DNS	–	Domain Name System
DSCP	–	Differentiated services
ECN	–	Explicit Congestion Notification
end-to-end	–	označuje dvě koncová zařízení
Frame Relay	–	wan technologie – nástupce X.25
FTP	–	File Transfer Protocol
FUP	–	Fair Use Policy
hop-by-hop	–	označuje každý IP bod od zdroje k cíli
HTTP	–	Hyper Text Transfer Protocol
ICMP	–	Internet Control Message Protocol
ICPIF	–	The Calculated Planning Impairment Factor
ID	–	Identification Number
IP	–	Internet Protocol
Jitter	–	kolísání velikosti zpoždění paketů při průchodu sítí
VPN	–	Virutal Private Network
LTE	–	Long Term Evolution
MIB	–	Management Information Base
MOS	–	Mean opinion score
MPLS	–	Multi Protocol Label Switching
MSSQL	–	Microsoft Structured Query Language
mySQL	–	my Structured Query Language
NMS	–	Network Managemant System
NTP	–	Netowork Time Protocol
packet loss	–	označuje ztrátovost paketů
payload	–	datový obsah
PE	–	Provider Edge

per direction	–	označuje jeden směr
QoS	–	Quality of Service
round-trip	–	okružní cesta, označuje cestu od zdroje k cíli a od cíle ke zdroji
router	–	směrovač
RTR	–	Response Time Reporter
RTTMON	–	Round Trip Time Monitor
SAA	–	Service Assurance Agent
SLA	–	Service Level Agreement
SNMP	–	Simple Network Management Protocol
switch	–	přepinač
TCP	–	Transmission Control Protocol
threshold	–	označuje hranici
ToS	–	Type of Service
UDP	–	User Datagram Protocol
VoIP	–	Voice over Internet Protocol

8. Přílohy

Univerzita Hradec Králové
Faculty of Informatics and Management
Akademický rok: 2016/2017

Studijní program: Systems Engineering and Informatics
Forma: Combined
Obor/komb.: Informační management (im3-k)

Podklad pro zadání BAKALÁŘSKÉ práce studenta

PŘEDKLÁDÁ:	ADRESA	OSOBNÍ ČÍSLO
Matoulek Tomáš	Sokolovská 318, Trutnov - Dolní Předměstí	I1200898

TÉMA ČESKY:

Cisco IP SLA a jeho využití

TÉMA ANGLICKY:

Cisco IP SLA and its practical use

VEDOUCÍ PRÁCE:

Mgr. Josef Horálek, Ph.D. - KIT

ZÁSADY PRO VYPRACOVÁNÍ:

Cílem bakalářské práce je představit Cisco IP SLA službu, její funkčnost a využiti. Autor představí principy CISCO IP SLA a navrhne jejich využití a technické řešení v rámci měřením pro koncové zákazníky poskytovatele služeb.

SEZNAM DOPORUČENÉ LITERATURY:

Hucaby, David. CCNP Routing and Switching SWITCH 300-115 Offical Certification Guide. Indianapolis, IN : Cisco Press, 2014. ISBN 978-1-58720-560-6. Alwayn, Vivek. Advanced MPLS design and implementation. Indianapolis, IN : Cisco Press, 2001. ISBN 1-58705-020-X. WALLACE, Kevin. CCNP Routing and Switching ROUTE 300-101 Official Cert Guide. Indianapolis, IN : Cisco Press, 2014. ISBN 978-1-58720-559-0.

Podpis studenta: ..... **Datum:** 10.8.2016

Podpis vedoucího práce: ..... **Datum:** .....