Jak NIX.CZ přešel na VxLAN/EVPN aneb od dvojité hvězdy ke kruhu

root.cz/clanky/jak-nix-cz-presel-na-vxlan-evpn-aneb-od-dvojite-hvezdy-ke-kruhu

Marian Rychtecký

Od dvojité hvězdy ke kruhu

V roce 2019 sdružení NIX.CZ provozovalo dva nezávislé uzly NIX.CZ a NIX.SK, které byly odděleny a byly provozně zcela nezávislé. Já jsem stál před zásadním rozhodnutím – jak zajistit rozvoj sdružení, stoupající počet portů, kapacity a hlavně spojení dvou uzlů do jednoho.

Spojení obou uzlů jsme nakonec provedli v polovině roku 2019 a z hlediska topologie sítě se nejednalo o velkou komplikaci. Ke konci téhož roku se sdružení rozhodlo rozšířit o další lokalitu: Vídeň. To již znamenalo **změnu topologie** a obecně kompletní revizi struktury celé sítě. NIX byl od roku 1997, kdy začal fungovat, vždy provozován jako čistě L2 infrastruktura. Ještě v roce 2020 byl NIX po spojení obou uzlů v topologii dvojité hvězdy (dual star). To však bylo nutné změnit s ohledem na připojení třetího města.

Spojením tří měst vznikla **kruhová topologie** a jelikož L2 infrastruktura se v topologii kruhu příliš bezpečně a efektivně řídit nedá, zvolil jsem přechod na routovanou síť s virtualizovaným rozšířením. Nakonec jsem vybral technologii VxLAN, která byla nová a v prostředí internetového uzlu poměrně unikátní. Tento měsíc jsme přestavbu celé sítě dokončili a nyní je celá infrastruktura NIX.CZ přemigrována na nové přepínače naplno tak využívá technologii VxLAN/EVPN.

Poznámka: V následujícím článku budu v některých částech uvádět jména výrobců a zařízení z důvodu autenticity. Uvedení konkrétních jmen není známkou naší nespokojenosti a nebo výhrad ke konkrétnímu zařízení či výrobci. V našem prostředí jsme použili zařízení na vlastní

zodpovědnost a v některých případech nebylo využití funkcí v době pořízení zcela zdokumentováno pro náš případ užití a proto jsme mohli narazit na nesrovnalosti.

Proč Leaf-Spine pro NIX?

V NIX.CZ se velmi dlouhou dobu používaly **šasi přepínače**, velká zařízení, které je nutné vybavit kartami rozhraní, dle vašeho přání. Použití má velmi mnoho praktických důvodů, hlavně při velké hustotě portů. V našem případě se však ukázalo, že kombinace některých typů karet není vůbec podporovaná – např. kombinace 1G portů a 400G portů v jednom zařízení je velký problém z důvodu potřeby obrovských bufferů.

- 
- 

- 

Dalších 7 fotografií

Leaf-spine je **dvouúrovňová architektura** sítí, která rozlišuje role prvků sítě na takzvané prvky „leaf“ (list) a „spine“ (páteř). Síťový prvek v roli „leaf“ agreguje provoz typicky ze serverů, přičemž prvky v roli „spine“ přepínají nebo routují data mezi různými prvky „leaf“. Protože zapojení této topologie je každý s každým (full-mesh), zvýšení kapacity sítě je možné dosáhnout přidáním zařízení typu „leaf“.

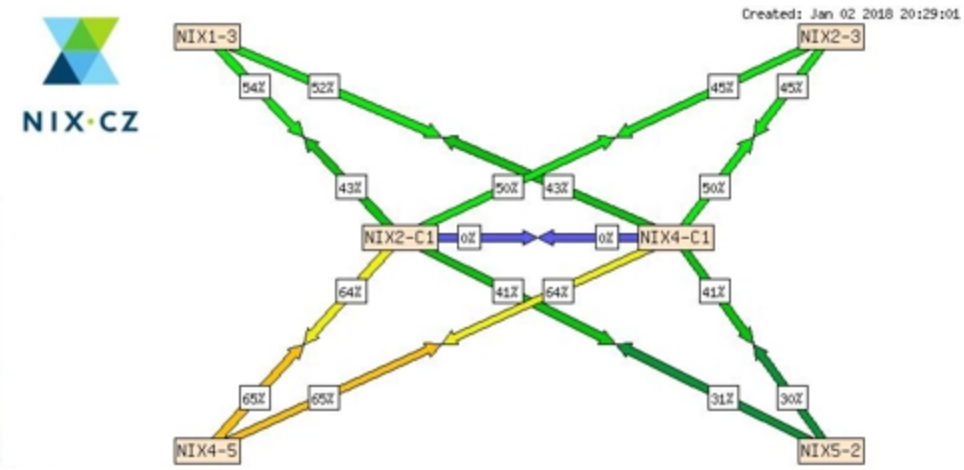
Jedním z dalších důležitých důvodů rozhodnutí použít topologii Leaf-Spine složenou ze několika samostatných zařízení, místo jednoho obrovského šasi, je **úspora elektrické energie,** což se o pár let později ukazuje jako docela dobrý nápad. Výhodou je také lepší životní cyklus zařízení, které je možné posouvat v síti dle potřeby. To je u šasi verzí velmi nákladné a nepraktické.

Virtualizovaná L2 síť

Vybudovat virtualizovanou L2 síť byl nejpravděpodobnější scénář a velmi nás lákala i myšlenka udržování **L3 sítě**, místo pouze sítě fungující na některém z L2 protokolů. V zásadě i proto, že L2 protokoly jako Fabric-Path, Trill nebo SPB se z podpory výrobců vytratily a skončily v propadlišti dějin.

Jediným rozumným řešením na výběr tedy zůstalo značkování/balení do MPLS/VPLS nebo VxLAN. Nakonec jsme po několika týdnech testování a konzultací dospěli k názoru, že vhodné bude jít cestou co nejjednodušší konfigurace změn a vybrali jsme **VxLAN**.

Zbývalo tedy ještě rozhodnout, jaký typ „control-plane“ zvolit. Z důvodu konzistence dat, zajištěného ověřeným protokolem BGP jsme se rozhodli, že půjdeme cestou **EVPN**. V té době s nasazením VxLAN/EVPN v prostředí IXP nebyla žádná zkušenost (alespoň ne nám známá). Museli jsme tedy vše nastudovat, naplánovat, vyzkoušet v malém měřítku a také nasadit.



Topologie NIX.CZ v roce 2018

Autor: NIX.CZ

Jdeme na to!

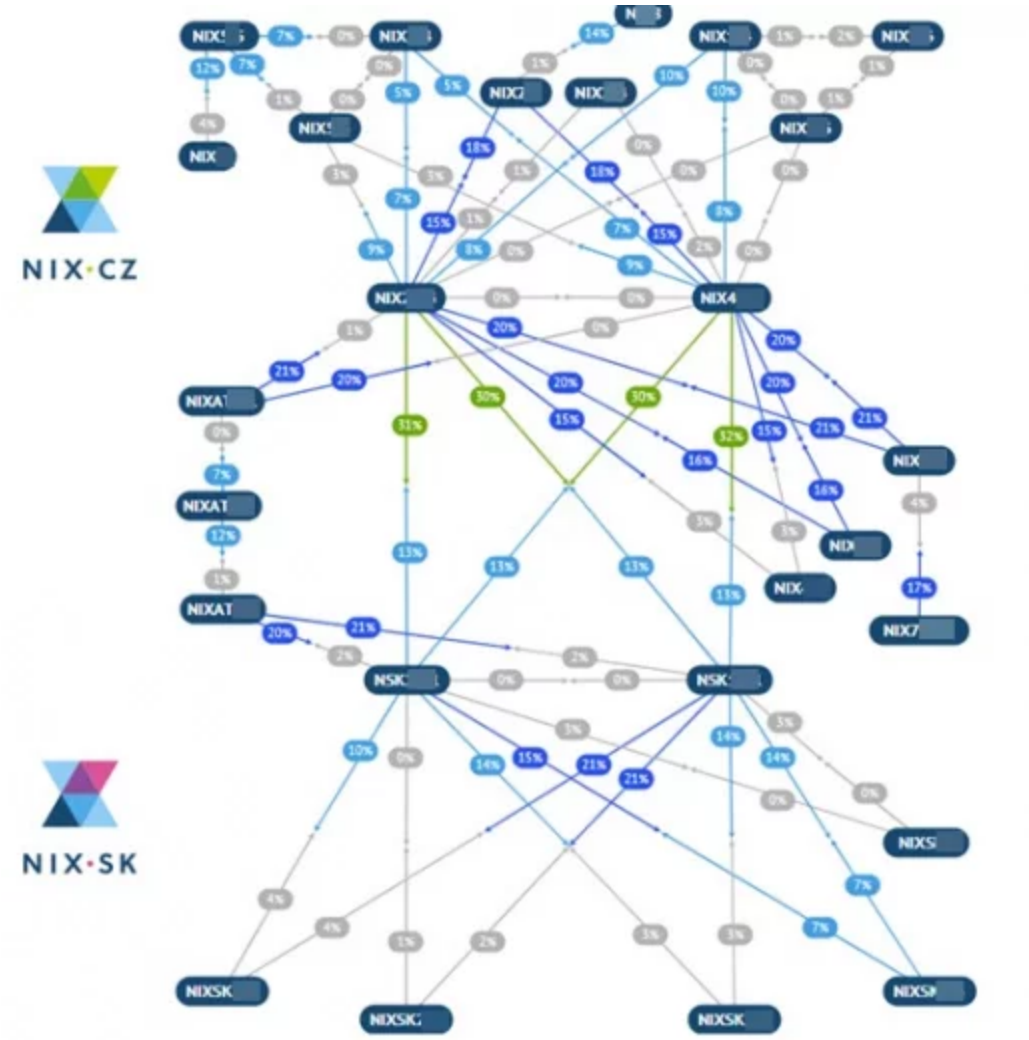
Do karet nám hrálo, že ve slovenské části sítě byly provozovány dva přepínače Nexus 7010, u kterých výrobce vyhlásil **konec podpory** a museli jsme je nahradit do konce roku 2020. I přes kovidové restrikce a nejistotu objednaná zařízení dorazila a my jsme začali připravovat přechodový mechanismus. Bylo nutné osadit dva nové „core“ přepínače do Prahy a ty nastavit jako bránu do nového světa VxLAN/EVPN směr Bratislava.

Tato zařízení jsme již objednali s podporou 400G rozhraní, abychom mohli zároveň na začátku roku 2021 připojit první síť linkovou rychlostí 2×400G. Výměna zařízení v Bratislavě znamenala stihnout za jednu noc odpojení 50 optických kabelů, demontáž původního 130kg

přepínače, montáž nových přepínačů, správné zapojení kabelů, připojení linek směr Praha a přenastavení sítě z L2 na L3. To celé na **třech místech** koordinovaně.

Největším problémem byla nefunkční technologie „Fabric-Peering“, kterou jsme plánovali použít místo původní konfigurace vPC. Ukázalo se, že zamýšlená kombinace **dvou různých ochran** v reálném prostředí není podporována. Pod tlakem si člověk až moc intenzivně uvědomuje, jak čas utíká, když se něco nedaří. Problém se mi nakonec podařilo identifikovat a včas najít řešení. V šest hodin ráno bylo hotovo, ale hlavu jsem měl řádně zamotanou.

Při této první migraci jsme si opět potvrdili, jak je výměna zařízení komplexní úkol. Chce to **systém a automatizaci**.



Topologie NIX.CZ v roce 2022

Autor: NIX.CZ

Máte dokumentaci? Mohl bych ji vidět?

Po prožití několika nočních akcí mi velmi rychle došlo, že ačkoli **dokumentace** původní sítě byla poměrně přesná, údaje bylo nutné hledat v několika různých systémech, které neměly přímou vazbu. To vyžadovalo velké množství úsilí a dlouhé hodiny příprav.

Společně s kolegy jsme se tedy rozhodli, že vytvoříme nový systém, kde bude vše odpovídat reálné situaci po přepojení a data budou k sobě svázaná. Proto jsme začali v roce 2020 plnit nový systém, založený na platformě Netbox. V době kdy jsme s Netboxem začínali, neuměl moc věcí a **modelování** naší sítě v něm znamenalo vyvinout velké úsilí. Vydrželi jsme a nyní z naší tříleté snahy těžíme.

Při plánování přechodu na VxLAN/EVPN v Praze byl hlavní důraz kladen na co nejkratší výpadky pro klienty. Bez fyzického přepojení to ovšem zajistit nelze, a tak jsme museli novou kabeláž připravit dopředu. Toho jsme chtěli také využít. Společně jsme se rozhodli, že ta největší datacentra kompletně **překabelujeme** a vymyslíme nový a lepší systém, který bude přehlednější, zabere méně místa a sníží riziko chyb při přepojování.

Nová lokalita – Vídeň

Odhodláni vyzkoušet si nový design sítě, migrační skripty, nové kabeláže a ještě k tomu na zcela novém místě jsme vyrazili instalovat novou lokalitu ve Vídni. Nová instalace je vždy jednodušší než úprava staré za provozu. Po spuštění Vídně a zapojení této lokality do naší VxLAN fabriky jsme nyní měli kompletní kruhovou topologii, kterou jsme nově mohli **řídit na třetí vrstvě**.

Bohužel v roce 2020 přišel kovid a doby dodávek techniky se extrémně **prodloužily**. Jen stěží bylo možné vycestovat do vedlejšího okresu, natož do cizí země. Tento neplánovaný zásah shůry jsme chtěli využít a začali plánovat přechod pražských datacenter na nový design.

Praha – jak na to

Praha byla velká výzva, z původního zapojení nezůstalo nic. Ihned poté, co jsme připojili (tenkrát) novou technologií 400Gbit/s společnost O2, jsme identifikovali největší přispěvatele provozu a ty jsme přepojili jako první do stejného přepínače. To byl však pouze první krok.

Kvůli omezení osmi 400G portů jsme postavili kruh pokrývající další pražská datacentra s kapacitou 1,6Tbit/s na jedno datacentrum v plné redundanci. Do finální konfigurace nám chyběla potřebná zařízení, která měla v době kovidové dodací termíny neznámé, fakticky to znamenalo většinou minimálně **rok a více**. Museli jsme si poradit a zvolit cestu řízeného přepojování páteřní sítě. Jakmile byla hotová páteřní vrstva, začali jsme postupně migrovat zákazníky na nové přepínače.

V průběhu roku 2022 jsme dočasnou topologii přepojili na nově dodané přepínače Nexus, které disponují 32 rychlými 400G porty a od této doby je páteřní síť kompletní.

- 
- 
- 

Dalších 13 fotografií

Ansible, Python a další

Každý zákazník musel být přepojený do nových přepínačů, včetně nových kabelů, vytvoření nové dokumentace a přenesení **konfigurace** do nových přepínačů.

Abychom udělali co nejméně chyb při přenosu konfigurací, napsali jsme si první verzi migračního nástroje, který „překládal“ původní konfigurační soubory na novou syntaxi pro VxLAN/EVPN. Ten využíval hlavně **Ansible** a sadu knihoven v Pythonu.

Vše docela slušně fungovalo, až na rychlost. Ladění CLI příkazů v tomto prostředí bylo **zdlouhavé** a kombinací konfigurací mnoho. Největší vrásky nám působily problémy, kdy konfigurace zadaná přes CLI manuálně fungovala, ale pokud jsme ji poslali jako dávku, selhala bez zjevné chyby.

Po této poměrně trpké zkušenosti, jsme se nakonec rozhodli, že využijeme jiný způsob – DME (Data Managment Engine) API a u tohoto způsobu jsme již zůstali.

Napsali jsme si tedy druhou sadu skriptů, které zajistily převod konfigurací. Tyto nové skripty byly zodpovědné za konfiguraci VLAN, VNI, mapování, port-channelů a podobně. Vstupním formátem je dobře známá konfigurace **Cisco CLI** a výstupem je sada volání REST HTTPS s objekty JSON, které přepínač patřičně nastaví.

Přepínače Nexus 9300 jsou vybaveny rozhraním REST API, díky kterému lze ovládat zařízení na úrovni objektů uspořádaných v logickém stromu (podobně jako SNMP). Uvnitř tyto přepínače pracují pouze s tímto konfiguračním modelem a vše ostatní se překládá. Například známé CLI je pouze **emulace** a příkazy z CLI se interně překládají do interního objektového stromu. Tímto způsobem se konfigurace i ukládá. Díky DME REST API je možné objekty ovládat přímo.

Pomocí této vlastnosti lze data z přepínačů i získávat. Zkoušeli jsme „Streaming Telemetry“, ale nakonec jsme skončili u čtení dat **vlastním systémem**. Největší výhodou je rychlost, REST API je opravdu rychlé a vyřízení požadavků probíhá v rámci milisekund. Nevýhodou je, že tímto nízkoúrovňovým přístupem můžete přepínač velmi rychle dostat do nechtěného stavu. Opatrnost a intenzivní testování je zcela na místě.

Port Security – IXP vs. DC

Smyčky jsou hlavním nepřítelem každé L2 sítě. Pokud provozujete své datacentrum, pravděpodobně máte pod kontrolou i infrastrukturu, která je do vaší L2 sítě připojená a tudíž bezpečnost a konzistenci portů na straně VxLAN/EVPN fabriky nemusíte příliš řešit. Naopak **stěhování MAC adres** z jednoho kouta sítě do druhého je zcela legitimní a žádaný proces, například kvůli stěhování virtuálních strojů mezi hypervizory.

V internetovém uzlu je situace opačná, přestěhování MAC adres je v drtivé většině případů považováno za chybu a je potřeba s ní správně naložit. V ideálním světě tedy chcete, aby MAC adresy byly **definovány napevno** a vůbec se v síti bez vašeho vědomí neobjevovaly jinde. V síti jako je NIX.CZ je poměrně běžné, že se MAC adresy objeví na jiném místě, než by měly. Tento jev sledujeme i několikrát za týden, hlavně v nočních hodinách a souvisí to hlavně s údržbami síťových, nebo transportních zařízení připojených do společné peeringové sítě. Zcela běžně vidíme (neúmyslný) únos MAC adresy související se smyčkou na straně připojené sítě. Klasickým problémem je vrácení námi zaslaného provozu zpět do našeho rozhraní.

Výše popsané rozdíly jsou hlavním problémem použití datacentrové technologie v režimu IXP. Bohužel technologie EVPN je **definovaná pro datacentra** a počítá pouze s přenosem MAC (MAC mobility) a

nikoli s prevencí. Každý výrobce tak musí „port-security“ definovat po svém a nám se povedlo, díky usilovné práci kolegů, nechat implementovat správné nastavení bezpečnosti rozhraní v NX-OS (feature port-security).

V aktuální verzi NX-OS tak můžete funkci „port-security“ použít. Hlavní změna implementace je ve vnímání statické MAC na vzdáleném přepínači. V nově vydaném NX-OS je MAC adresa naučená na zabezpečeném portu propagována do EVPN s **příznakem** (sticky bit) a vzdálený přepínač tak ví, že pokud by se stejná MAC objevila lokálně, má lokální výskyt ignorovat a nikoli jej oznámit všem okolo.

Dalším problémem, na který jsme narazili, byla rychlost distribuce naučených MAC adres. Pokud máte na rozhraní nastavený limit, řekněme na dvě MAC adresy, a zákazník vám během krátké chvíle (několik milisekund) pošle data z dalších 100 MAC adres, pak zabezpečení portu zareaguje a **port shodí**. Než k tomu dojde (proces shození několik milisekund trvá) MAC adresy, které jsou nad rámec povolených, jsou i přesto přes BGP signalizovány do celé EVPN. Za pár dalších milisekund jsou opět odebrány (zdrojový port je shozen a MAC vyčistěny). Nicméně i tento jev způsobí kolizi a únos MAC adres na velmi krátký okamžik. Pokud je takový krátký okamžik 1ms, pak na 400Gbit rozhraní přijdete o 50 MB dat.

Pokud jste dočetli až sem, možná vás napadlo, proč neuděláme jednoduše MAC ACL nebo proč nenastavíme MAC na portu napevno. Inu, protože to na této platformě **není podporované**. Můžete sice vytvořit MAC ACL na portu a data filtrovat podle zdrojové MAC, ale bohužel tím nevypnete učení MAC adres a tak provoz poslaný do portu sice není přeposlán dále, ale naučená MAC adresa je unesena stejně. Stejný problém je s MAC nastavenými napevno: pokud tuto funkci zapnete, musíte ovšem vypnout funkci „port-security“ a pak se vám port nedeaktivuje v případě porušení bezpečnostní politiky.

Co se nepovedlo

Během implementace jsme samozřejmě narazili na několik záležitostí, které nás zaskočily, nebo **překvapily**. Některé z nich jsme museli testovat pouze na živé síti, protože v laboratorních podmínkách se je nepodařilo nasimulovat. Nepříjemným aspektem byla i změna v dokumentaci výrobce, který podporu některých námi používaných funkcionalit v čase měnil.

Fabric-Peering – aneb vPC (Virtual Port-channel) spojený pomocí EVPN. Původní nápad byl nabídnout zákazníkům připojených pomocí technologie LACP možnost se připojit do jakýchkoli dvou přepínačů v síti. Dokumentace hovoří o možnosti použití EVPN ESI, ale v praxi se ukázalo, že použití těchto rozšířených vlastností EVPN je možné, ale není vhodné pro sítě, kde není možné zajistit kompletní bezpečnost připojených prvků. Zúžili jsme proto návrh na podporu LACP na dva sousední přepínače a velmi se mi líbil nápad použití Fabric-Peeringu. Pokud znáte technologii vPC, věžte, že fabric-peering vám umožní stejné vlastnosti, ale bez použití „peer-link“, čímž se ušetří porty na přepínači. Nebudu vás napínat, nakonec jsme fabric-peering i vPC ze sítě téměř zrušili. Hlavním důvodem je obtížnost diagnostiky, nepredikovatelné chování při smyčkách zákaznických portů a zejména chybějící podpora zabezpečení portů v kombinaci s EVPN.

Port-security – asi největší kámen úrazu, na který jsme narazili. Chybějící podpora ochrany portů na použitých přepínačích byla po dlouhé dva roky noční můrou, ale snažili jsme se s tímto neduhem technicky vypořádat. Celkem jsme našli tři problémy s bezpečnostní portů:

1. *Únos MAC ze strany Layer 2* - tento scénář se nejvíce projevil v průběhu migrace. Původní přepínače Nexus 7710 byly umístěny za pár nových typů VxLAN/EVPN přepínačů. Spojení mezi těmito dvěma světy bylo na úrovni páteřních portů a tudíž nemhola být použita „port-security“. Pokud některá z připojených sítí poslala svou linkou rámec se zdrojovou MAC jiné sítě a tento rámec dorazil důvěryhodnými páteřními linkami až do nových přepínačů, EVPN chtěla zajistit přenos adresy na nový port. Na straně L2 se přepínače naučily MAC v kolizi z nového směru (směrem k Nexus 7710) a EVPN chtělo MAC přestěhovat i v rámci EVPN na nový směr, ale díky vlastnostem se toto přesměrování zamítlo a síť zůstala rozdělena na dva světy. Původní síť L2 směrovala provoz na (špatné) nové místo, fabrika EVPN směrovala provoz na původní (správné) místo. To mělo za následek nepříjemné chvíle, kdy došlo k (nechtěnému) únosu MAC významného operátora a do té doby, než se manuálně tabulka MAC vyčistila, byl jeden jeho router nedostupný. Tomuto problému jsme se věnovali velmi intenzivně, až jsme nakonec vyvinuli vlastní skript, který „čištění“ MAC prováděl sám. Přesný popis, včetně zdrojového kódu je na umístěn na GitHubu.
2. *Únos MAC ze strany VxLAN/EVPN* - tento scénář se nejvíce projevil také v průběhu migrace. Jedná o velmi podobný průběh událostí, s tím rozdílem, že ke kolizi dojde na již migrovaném portu přepínače, který má port-security zapnuté, ale má povolenou více než jednu dynamickou MAC – typicky dvě. Pokud se objevila na portu připojené sítě právě jedna další MAC a ta způsobila kolizi, systém se opět ze situace nezotavil automaticky, ale vyžadoval manuální zásah.

3. *Záplava MAC adres* – objevili jsme i situaci, kdy při síťové smyčce se na zákaznickém portu objeví ve velmi malém časovém okně (typicky jednotky milisekund) desítky nebo stovky MAC adres. I přesto, že port-security měla povoleno jednu nebo dvě MAC, zahlcení portu novými MAC znamená zahájení procesu shození portu pro překročení limitu povolených adres. Kvůli tomu, že je celý proces paralelizován, je zahájeno shození portu a čištění přepínací tabulky na přepínači, ale zároveň všechny adresy MAC (i ty které překročí limit) jsou pomocí EVPN přeneseny řídícím protokolem na ostatní přepínače a ty je zařadí do své přepínací tabulky. Datový tok se tak přesune na nový port, který MAC ohlásil jako poslední. Protože přepínače disponují rychlými CPU, zpracování těchto aktualizaci BGP je velmi rychlé a proběhne dříve, než jiný proces dokončí shození portu. Po shození portu a vyčistění lokální přepínací tabulky na portu zákazníka, který způsobil záplavu, se poté všechny MAC, které záplavu způsobily, vyčistí a EVPN oznámí stažení MAC a tím dojde k nápravě celé situace. Existuje však několik desítek milisekund, kdy je provoz směrován na port sítě, jež způsobila záplavu.

V důsledku těchto zjištění, jsme přistoupili k razantní změně provozního řádu a nově povolujeme pouze **jednu dynamickou MAC** adresu v peeringovém segmentu.

Pokud byste chtěli vědět více, můžete si shlédnout videozáznam mé přednášky na YouTube.

IP unnumbered na paralelních linkách – není podporována (do verze NXOS 10.2(3)) a zapříčinila dva vážné incidenty, při kterých některé připojené sítě nedostávaly BUM (Broadcast, Unknown unicast, Multicast) provoz z náhodných MAC po krátkodobém výpadku L3 páteřních linek. Tento problém jsme analyzovali několik nocí a nazval

bych jej hledáním jehly v kupce sena. V provozu kolem 5 Mpps hledáte jeden paket ARP, který je zahozen a analyzujete, proč se tak stalo. Peklo.

userCfgdFlags – použití REST API má své výhody. Nám se bohužel stalo, že jsme si nevšimli změny v dokumentaci při přechodu NXOS z verze 9.2.x na 10.3.x, že v API přibyl jeden parametr, kterým musíte explicitně říct, které parametry jste uživatelsky změnili – jde o jakousi rekapitulaci. Nenastavením rekapitulace se sice konfigurace uloží, ale po dalším restartu se vám vybrané parametry nepřenesou do běžící konfigurace a vy skončíte po restartu přepínače bez nastavených portů. Správně musíte tedy uvést při nastavování portu i následující:

```
"l1PhysIf": {
    "attributes": {
    "id": "eth1/1",
    "layer": "Layer2",
    "mode": "trunk",
    "mtu": "9192",
    "trunkVlans": "100",
    "userCfgdFlags": "admin_layer,admin_mtu,admin_state"
    }
}
```

Alternativní zápis v CLI (tak, jak jsme zvyklí):

```
interface Ethernet1/1
  switchport
  switchport mode trunk
  switchport trunk allowed vlan 100
  mtu 9192
```

Zvýrazněná část musí být použita, pokud provozujete NXOS verze 10.2 nebo vyšší.

Unknown unicast – zatím posledním problémem, který jsme řešili bylo zamezení přenosu „unknown unicastu“. Pokud ve vaší síti dojde k náhlému odpojení zákazníka a zákaznický port je náhle shozen, jeho

MAC adresa se v tu chvíli pro celou vaši síť stane neznámou a ve výchozím nastavení se přepínače k takovému provozu chovají jako k broadcastu. Všechen provoz s cílovou MAC je tak posílán do všech portů. Nyní si představte, že takovou sítí, která se náhle odpojila je velký poskytovatel obsahu s provozem 200Gbit/s. Na dobu asi 40 sekund tedy musíte takový provoz zablokovat, jinak se přetíží všechna zákaznická rozhraní.

Co bych vzkázal svému druhému já zpátky do roku 2019

- Ukládej si víc poznámek,
- nauč se dokumentaci výrobce zpaměti a nevěř jí,
- ulož si lokálně dokumentaci výrobce, když ji čteš, zítra může být jiná,
- co je za hranicí sítě je nebezpečné a tomu nevěř,
- novější software neznamená lepší (ale mnohdy pomůže a je menší zlo),
- bude kovid, kup všechno najednou a nebudeš muset čekat měsíce na dodávky,
- problémy s technikou budou, důležitá je podpora.

Co nás čeká dál

Díky úspěšnému startu potřebná kapacita stoupala velkou rychlostí a celý kruh Praha – Bratislava – Vídeň – Praha postavený na 4×100 Gbit/s **přestává stačit**. Jsme těsně před dokončením navýšení kapacit mezi jednotlivými lokalitami na 2×400Gbit/s a používáme již 400G linky. V lednu otevřeme pro připojení další lokalitu ve Frankfurtu nad Mohanem a připojíme ji do celé sítě dalšími 400G linkami.

V příštím roce **navýšíme kapacity** mezi lokalitami, ale zejména budeme plánovat rozvoj na další období. Zvažuji zapojení lepších protokolů pro řízení provozu a budu s napětím sledovat dění kolem vývoje modulů a rozhraní s vyšší kapacitou než 400Gbit/s. Čeká nás

také obnova interních systémů, zpracovávajících statistické údaje o provozu, detekce anomálií a monitoringu. Chtěl bych se věnovat zvýšení uživatelského komfortu zákaznické sekce.

Co ještě děláme

Díky tomu, že NIX.CZ spoluorganizuje konference CSNOG a Peering Days, naše sdružení vyvíjí systém pro organizování, registraci a plánování schůzek. Aplikace v posledním roce zaujala další organizátory podobných akcí a jsme hrdí na to, že jsme mohli podpořit již **sedm setkání**. Celkem tak aplikaci aktivně využilo přibližně 4 000 účastníků. Tento nástroj jsme pojmenovali Meet a informace o něm naleznete na nix.cz/meet.

Pro vlastní potřebu jsme vyvinuli vlastní sady **knihoven pro Python**, které nám umožňují řízení a monitoring přepínačů Nexus 9300. Díky vlastnímu pojetí jsme nyní schopni získávat informace o stavu rozhraní velmi rychle a zpracovávat tak velké množství dat. Zatím jsme s tímto projektem na začátku, ale máme velmi mnoho nápadů, jak s daty dále naložit, včetně zpracování knihovnami LLM. Je to sice práce na několik let, ale pokud byste mi v roce 2019 ukázali dnešní síť NIXu, nevěřil bych, že to dokážeme. Budeme mít i nadále smělé plány a nápady, které se dnes zdají nereálné, ale zítra již budou mít obrysy.

Velká výzva ke zdokonalení

Jsme na konci. Na konci článku, nikoli cesty. Zcela otevřeně přiznám, že přestavba uzlu NIX.CZ byla zatím největší výzva, kterou jsem zažil. Každý incident a anomálie jsou pro mě pokaždé nejlepšími příležitostmi, jak se dále zdokonalit, naučit a více porozumět problematice. Nic z toho bych ale nemohl dokázat bez podpory celého týmu kolegů a kolegyň, kteří/které trpí mé neustálé nové nápady.

Velký dík za vytrvalou podporu patří spolupracujícím zástupcům výrobců a distributorů a zahraničním kolegům a přátelům za inspiraci. Pevně věřím, že NIX.CZ se bude dále rozvíjet tak, aby i nadále nabízel služby na vysoké úrovni. Podporoval komunitu a rozvoj internetu v Česku, na Slovensku a v dalších zemích, kde působí nebo jednou třeba působit bude.