



Vážení čtenáři,

vítám vás u čtení dalšího vydání čtvrtletního .news. Pevně věřím, že budou novinky, které přináší, pro vás zajímavé.

Podobně jako v minulém čísle i tentokrát se budeme věnovat technologii DNSSEC. Ač je tu už nějaký měsíc, stále ještě není tato technologie

mezi poskytovateli internetových služeb příliš rozšířena. Proto nás potěšilo, že se symbolicky s příchodem jara objevují první vlaštovky. Od března tohoto roku je podepsaná doména jednoho z největších internetových knihkupectví v České republice, doména kosmas.cz. Společnost Kosmas si uvědomuje důležitost takové ochrany i význam této technologie jak pro sebe, tak pro své zákazníky. Další takovou vlaštovkou s DNSSEC na křídly je společnost Internet Info provozující například významné informační servery Root.cz a Lupa.cz. Pevně věřím, že tito vizionáři budou mít vliv i na další důležité provozovatele internetových portálů.

Tak jako obvykle i v tomto čísle najdete vybraný příspěvek z našeho blogu. Kolega Emanuel Petr se rozhodl detailně rozebrat situaci, která vznikla díky zadání chybné informace při konfiguraci směrovače. Příspěvek z blogu měl úspěch a proto i pokračování, které s několikadenním odstupem vyšlo na serveru Lupa.cz. Jeho autory jsou kolegové Ondřej Surý a Emanuel Petr.

Dovolte mi na závěr jednu informaci, která s tímto vydáním .news zatím nesouvisí. To, že čtete toto periodikum, je důkazem, že se zajímáte o dění ve sdružení, že vás zajímají nové technologie a věci související s rozvojem Internetu. Proto mi dovolu, aby vás pozval na konferenci Internet a Technologie 09, která se bude konat 4. června v Praze v Klubu Lávk. Více informací najdete na internetových stránkách této **konference**. A nyní už mi už pouze zbývá vám popřát příjemné čtení.

Ondřej Filip
Výkonný ředitel sdružení CZ.NIC

ENUM oslavil v lednu dva roky v komerčním provozu

Ve čtvrtek 22. ledna oslavilo sdružení CZ.NIC dva roky od spuštění systému ENUM do ostrého provozu. Ten umožňuje přenášet běžné telefonní hovory přes internet tak, že volající nemusí za skutečné hovory platit minutové poplatky. Počet jeho uživatelů stále roste, v registru ENUM domén bylo k 22. lednu evidováno 4 834 domén, které představovaly 664 399 potenciálních telefonních čísel. Počet domén se tak oproti loňskému roku zvýšil o 65 procent. Tato čísla řadí Českou republiku mezi země, kde se ENUM používá nejvíce. Přestože ENUM a volání přes internet nabízí oproti klasické telefonii mnoho výhod, je IP telefonie stále ještě pořád doménou technicky zdatných uživatelů

či firem. Situace a podmínky na trhu se ale postupně mění v její prospěch, a to nejen proto, že firmy i domácnosti uvažují nad tím, jak nejvíce ušetřit. Právě cena je totiž jednou z řady předností volání přes internet. Na trhu se objevují mobilní telefony schopné volat přes internet, rozšiřuje se rychlé připojení k internetu, uživatelé se už nenechávají odradit těmi, kteří o IP telefonii šíří zkreslené informace. Toto vše do telekomunikací přinese obdobně razantní změnu podobnou té, kterou přinesl internet i do jiných oborů. V blízké budoucnosti by také měla vzniknout v mezinárodní spolupráci značka, podle níž se pozná, zda je daný produkt nebo služba vhodná pro telefonování po internetu. Jejím smyslem je především

e.num

W E M A N A G E N U M B E R S

usnadnit zájemcům orientaci v nabídce na trhu, a zjednodušit tak přechod k IP telefonii.

Sdružení CZ.NIC spustilo český registr ENUM domén pro veřejný, komerční provoz 22. ledna 2007. Domény ENUM v tuto chvíli registruje 21 registrátorů, ve své síti systém podporují telekomunikační operátoři IPEX, CL-NET a NETWAY. ENUM využívá v současné době z evropských zemí také například Rakousko, Německo, Polsko, Finsko, Rumunsko, Holandsko, Velká Británie a Irsko.

ONDŘEJ FILIP V MAG

Výkonný ředitel CZ.NIC Ondřej Filip je od konce loňského roku jedním z členů organizace MAG (Multistakeholder Advisory Group), která je poradním orgánem generálního tajemníka OSN pro organizaci Internet Governance Fora.

ROZHOVORY S PŘEDSTAVITELI CZ.NIC V MÉDIÍCH

I o druhém výročí technologie ENUM v České republice bylo interview s Pavlem Tůmou, projektovým manažerem sdružení, v pořadu **Nula-jednička**, který vysílá Český Rozhlas Leonardo. Rozhovor s Ondřejem Filipem o vzniku kořene DNSSEC otiskl v březnu server **Lupa.cz**.

SÉRIE ČLÁNKŮ A SOUTĚŽ NA MOBILMANIA.CZ

Sérii článků na téma VoIP a ENUM, jejichž autory jsou zaměstnanci sdružení CZ.NIC, a společnou soutěž o manažerský mobilní telefon přinesla březnová spolupráce sdružení a specializovaného serveru **Mobilmania.cz**.

VÍTE, ŽE

... blog zaměstnanců sdružení (.blog) je od února zařazen mezi zdroje informací, které jsou součástí českého kulturního dědictví?

V únoru potkaly změny i čtvrtletník sdružení CZ.NIC (.news)

Česká národní knihovna mu přidělila ISSN, tedy osmimístný číselný kód, kterým se jednoznačně identifikují názvy periodik a ostatních takzvaných pokračujících zdrojů vydávaných kdekoli na světě.

O finanční odměnu se v soutěži VIP podělilo sedm projektů

Vyvíjej Inovuj Programuj

Sdružení CZ.NIC oznámilo 3. února výsledky prvního ročníku soutěže pro mladé talenty v oblasti ICT - „VIP - Vyvíjej, Inovuj, Programuj“. Do ní mohli zájemci v loňském roce přihlásit projekty zaměřené na vývoj nového open-source softwaru nebo inovaci softwaru používaného v oblasti internetových technologií, služeb či infrastruktury. Finanční částku v celkové výši 271 tisíc si mezi sebe rozdělilo sedm projektů, které

soutěžící zpracovali a zaslali na adresu sdružení do 15. ledna tohoto roku.

V prvním kole soutěže přihlásili zájemci celkem 32 projektů, z nichž loni v říjnu vybrala pětičlenná porota 12, kterým podle obtížnosti a významu přidělila finanční částky od 10 do 55 tisíc korun.

Jednotliví soutěžící si tak mohli na konci soutěže rozdělit až 405 tisíc korun.

Do 15. ledna ale přišlo na adresu sdružení pouze sedm z 12 vybraných projektů. U nich porota posuzovala, v jakém rozsahu byla splněna jednotlivá zadání, která si na začátku určili samotní soutěžící. Kvalita odevzdaných prací porotce soutěže velice překvapila. Tři z projektů, z nichž dva se věnují technologii DNS, dokonce porota ocenila vyšší částkou, než jakou původně navrhla. Ve všech těchto případech se jednalo o práce, které realizovali vysokoškoláci.

Protože byl o soutěž mezi mladými lidmi zájem, rozhodli se její pořadatelé, že ještě v tomto roce vyhlásí její druhý ročník. Informace o pokračování soutěže „VIP – Vyvíjej, Inovuj, Programuj“ budou zveřejněny v průběhu tohoto roku jak na stránkách sdružení, tak na internetové adrese projektu [VIP](#). První ročník soutěže mediálně podpořily informační portály Root.cz, ABC Linuxu, IT Systems a měsíčník Connect.

Název projektu	Autor	Umístění hotového projektu
DnsResolver .NET	Dušan Janošik	http://projects.djanosik.cz/dnsnet/
MapTiler – generátor mapových dlaždic pro interaktivní webové mapy	Petr Přidal	http://help.maptiler.org/cz-nic-vip
Resize Image pulg-in pro Firefox	Ondřej Klejch	http://www.klejch.eu/imageresize/
UniMaxima	Martin Dózsa	http://aiya.ms.mff.cuni.cz/webcalc/
Unbound bindings pro jazyk Python, využití jako lokální DNS	Marek Vavruša,	http://www.fit.vutbr.cz/~vasicek/nic-vip/
White/Gray/Black List pro potlačení spamu	Zdeněk Vašíček	
WrapSix	Michal Zima	http://wrapsix.tuxportal.cz/
LDNS Python wrapper (pyLDNS) a jeho využití pro automatickou kontrolu konfigurace DNS serveru	Karel Slaný, Miroslav Macek, Ivo Kolomazník	http://www.fit.vutbr.cz/~slany/nic-vip/

Sdružení otevřelo Akademii CZ.NIC pro širokou veřejnost



Akademie

Od 1. dubna nabízí sdružení široké veřejnosti specializované kurzy zaměřené na internetové technologie. Ty budou probíhat v prostorách Akademie CZ.NIC, výukovém centru, které je na taková, vysoce odborná školení vybavené. Zájemci o kurzy se mohou přihlásit na internetových stránkách www.nic.cz/akademie, kde najdou vedle rozpisu kurzů také další informace o lektorech, anotace kurzů a třeba i sekci e-Akademie pro samostatné vzdělávání.

Takto specializované kurzy v nabídce jiných vzdělávacích center v České republice nejsou.

V Akademii CZ.NIC je v tuto chvíli možné absolvovat tři kurzy – DNS, DNSSEC a ENUM. O těchto technologiích budou přednášet jak zaměstnanci CZ.NIC, tak odborníci z praxe. V případě DNS a DNSSEC to bude Ondřej Surý, technický ředitel sdružení. Kurzy na téma ENUM povede Lukáš Macura ze Slezské univerzity v Opavě a Petr Hruška z CZ.NIC. Nabídka kurzů se bude do budoucna rozrůstat. V plánu jsou například školení na téma IPv6, směrování, kryptografie a další.

První kurzy proběhly v Akademii CZ.NIC už na konci loňského roku. Tato setkání ale nebyla veřejná, zúčastnili se jich pouze členové sdružení a registrovaní. Zkušební kurzy měly ukázat, jaký by o takové přednášky mohl být zájem; zároveň si na nich přednášející vyzkoušeli jednotlivé kurzy před známým publikem.

Akademie CZ.NIC je dalším z projektů zaměřených na osvětu v oblasti internetu a internetových technologií. Podle počtu účastníků, kteří se dosavadních kurzů zúčastnili, je vidět, že by o taková školení mohl být mezi veřejností zájem.

Kurzy jsou určené především pro techniky, kteří ve svých společnostech spravují DNS, starají se o bezpečnost dat, odpovídají za telekomunikační systémy nebo dohlíží na jiné síťové systémy. Zajímavé ale mohou být i pro všechny ostatní, kteří mají o tyto technologie zájem a chtějí se o nich dozvědět více.



DNSSEC chrání doménu internetového knihkupectví Kosmas



On-line nákupy na www.kosmas.cz, jednom z největších internetových knihkupectví v České republice, jsou nyní bezpečnější. Internetová doména společnosti Kosmas je

totiž od 17. března zabezpečena technologií DNSSEC. Ta tak teď chrání tuto doménu před napadením nebo zfalšováním údajů uložených v DNS.

O ochranu technologií DNSSEC by měli usilovat všichni poskytovatelé internetových služeb, kteří mají zájem o co největší zabezpečení svých dat. Vedení společnosti Kosmas si uvědomujeme, že bezpečnost, obzvláště při on-line obchodování, je velice důležitá. Proto se rozhodli pro zavedení technologie DNSSEC pro svou klíčovou doménu. Díky této službě se tak také výrazně sníží riziko odcizení hesel a čísel kreditních karet při on-line nakupování.

Zástupci společnosti Kosmas uvedli, že zavedení DNSSEC pro doménu Kosmas.cz nebylo nijak složité ani časově náročné. Díky jejich registrátorovi, společnosti Active 24, jenž tuto službu nabízí svým zákazníkům, došlo k implementaci DNSSEC během velice krátké doby.

Zavedení DNSSEC je důležité pro všechny, kteří se na internetu pohybují, v první řadě ale pro poskytovatele internetových služeb a koncové uživatele. Společnost Kosmas je jedním z prvních poskytovatelů služeb, která takto své zákazníky chrání. Ti tuto službu jistě ocení. Teď totiž mohou skutečně věřit tomu, komu po internetu posílají své peníze za objednané zboží. V případě koncových uživatelů je důležité, aby tuto technologii podporovali jejich poskytovatelé připojení k síti. Po nich by uživatelé měli požadovat zavedení DNSSEC. Jestli jsou nebo nejsou jednotliví uživatelé chráněni při přístupu na internet, poznají všichni zájemci v testu na stránkách www.dnssec.cz.

Kořen DNSSEC je na světě



Přestože je již několik správců domén nejvyšší úrovně, kteří ve svých

registrech zavedly technologii DNSSEC, stále ještě chybí možná to nejdůležitější – podpis úplně nejvyšší, nebo-li kořenové zóny.

Pokud teď tedy chceme plně validovat záznamy ve všech podepsaných zónách, musíme si stáhnout klíče všech sedmi organizací a starat se o jejich aktualizaci. Toto je ale celkem nepraktické; každý správce domény má jiný způsob, jak klíče zveřejňuje. V praxi to tedy funguje tak, že každý ISP, který validaci provádí, buď sleduje aktuálnost obvykle té, pro něj nejzajímavější domény a ostatní ignoruje nebo používá úložiště klíčů mechanismu DNSSEC Lookaside Validation – DLV. DLV je poměrně elegantní řešení. Přesto ne každý má důvěru v konkrétního provozovatele DLV, které navíc není zcela obecně přijaté a standardizované řešení.

Vzhledem k tomu, že k podepsání kořenové zóny z mnoha důvodů ještě nedošlo, rozhodla se organizace IANA, která se jinak o změny v kořenové zóně stará, jednat a vytvořila prozatímní řešení, do doby než se spory vyjasní a dojde k podpisu. Tak vznikl takzvaný ITAR – Interim Trust Anchor Repository. Toto řešení je technologicky odlišné od DLV a je z hlediska typu použitého DNS resolveru zcela neutrální. Další výhodou je, že ITAR spravuje důvěryhodná organizace, která se o změny v kořenové zóně stará a má tedy autentizační mechanismy pro komunikaci se správci domén nejvyšší úrovně. Předností je i poměrně přesná specifikace toho, za jakých podmínek je služba provozována, a dále také toho, co se stane po podpisu zóny. Na závěr je třeba dodat, že na rozdíl od DLV slouží ITAR pouze pro domény nejvyšší úrovně. Ač se vznik technologického řešení nemusí zdát důležitý, ve skutečnosti je důležitý velice. Může totiž přesvědčit registry, kteří čekají s implementací DNSSEC na podpis kořene, k urychlení svých aktivit.

Evropská unie má zájem o DNSSEC



Evropská agentura pro bezpečnost sítí a informací (ENISA) slouží institucím EU a členským státům unie jako centrum pro odborné konzultace v oblasti bezpečnosti sítí a informací. Na konci ledna uspořádala

tato organizace v řeckých Aténách jednodenní workshop pod názvem Zvýšení odolnosti DNS. Smyslem setkání bylo prodiskutovat současný stav nasazení technologie DNSSEC v evropských zemích, označit problémy jež jejímu dalšímu rozšiřování brání a především, pokusit se najít cestu, jakou by ENISA mohla k tomuto rozšiřování přispět.

Na workshop přijelo přibližně 15 zástupců společností, které mají k tomuto tématu co říct. Kromě vyslanců evropských národních registrů, které DNSSEC zavedly (Bulharsko, Švédsko a České republiky), zde byli také například odborníci z RIPE NCC nebo holandského NINet Labs.

V průběhu setkání přišlo na řadu mnoho zajímavých témat, z nichž se ta nejzajímavější týkala nelehkého prosazování bezpečnostní technologie u veřejnosti a různých alternativních možností využití této technologie.

Všechny zastoupené registry se snaží různými komunikačními kampaněmi podpořit zavedení DNSSEC. Ve Švédsku, kde je tato technologie v provozu nejdéle, zveřejnili v rámci jedné takové kampaně na stránkách www.kaminskybug.se snímek, v němž ukazují, jak snadné je zaútočit na některé domény a upravit jejich obsah. V Aténách bylo na úvod setkání ukázáno toto video v nezkrácené podobě. Zveřejnění této verze bylo prý z bezpečnostních důvodů ve Švédsku zakázáno.

Dalším krokem vyplývajícím z tohoto setkání bude příprava dokumentů, které shrnou to podstatné, co bylo během workshopu řečeno. Zástupci agentury ENISA také oznámili, že se budou v rámci Evropy snažit o to, aby ostatní zástupci národních registrů přijali zavedení technologie DNSSEC jako jednu ze svých hlavních priorit.

CZ.NIC na konferencích



První tři měsíce nového roku byly bohaté na prezentace zaměstnanců sdružení na odborných konferencích; ty se věnovaly bezpečnosti v ICT.

Sérii vystoupení členů managementu CZ.NIC odstartoval 11. února projektový manažer sdružení Pavel Tůma na první konferenci sdružení ČIMIB (Český institut manažerů informační bezpečnosti) s názvem **Aktuální témata řešení internetové bezpečnosti**. Na toto vystoupení navázal Pavel Tůma o týden později v hotelu Diplomat. Zde se konala již tradiční jednodenní konference **Security 2009**, na níž byl poprvé prezentován v reálném prostředí útok, kterému může právě DNSSEC zabránit. Zájem o tuto prezentaci proto nebyl i z tohoto důvodu překvapující.

V únoru se také poprvé uskutečnila konference s názvem **Trendy v internetové bezpečnosti**, v jejímž programu byl také DNSSEC Workshop. Během odpolední tříhodinové prezentace zde technický ředitel sdružení Ondřej Surý popsal zájemcům DNSSEC doslova "od shora dolů" a v závěrečné diskusi doplnil v odpovědích na otázky vše, co v průběhu svého vystoupení nevysvětlil do úplného detailu.

V rámci 34. setkání organizace **ICANN**, které se konalo na začátku března ve středoamerickém Mexico City, vystoupili s přednáškami na téma DNSSEC a jeho zavádění v doméně .CZ a ENUM výkonný ředitel sdružení Ondřej Filip a projektový manažer CZ.NIC Pavel Tůma. ■

Další díl úspěšného semináře pro právníky hostilo Brno



Na začátku února uspořádalo sdružení CZ.NIC ve spolupráci s Pracovní skupinou pro právo a ICT Právnické fakulty Masarykovy univerzity v Brně další, již tradiční seminář určený pro odbornou právníkou veřejnost, která

se věnuje doménovým jménům, jejich právním aspektům a otázkám, které v souvislosti s nimi vznikají. Kromě obecného technického úvodu do problematiky si účastníci, mezi kterými byli zástupci advokátů, podnikových právníků, soudců i studentů, mohli vyslechnout přednášku doktora Víta Horáčka z Rozhodčího soudu při Hospodářské komoře České republiky a Agrární komoře České republiky věnovanou postupu a praxi Rozhodčího soudu při rozhodování sporů o doménová jména, a to nejen doménová jména .cz, ale i řešení sporů o .eu domény. S velkým zájmem se setkala prezentace JUDr. Radima Polčáka z Masarykovy univerzity; ta byla zaměřená na některé nejasnosti a kontroverze v současném světě domén, ať už jde o rozhodčí řízení, postavení doménové autority a jejich povinností či samotnou právní povahu doménového jména. Neodmyslitelnou součástí semináře bylo vystoupení JUDr. Petra Hostaše, právního zástupce sdružení CZ.NIC, který mluvil především o praktických otázkách: postup řešení sporu, uplatňované žalobní nároky či možná součinnost sdružení. Velmi pozitivně byla přijata závěrečná panelová diskuse, již se zúčastnili všichni přednášející a posluchači prostor pro diskusi využili v maximální míře.

U návštěvníků akce se seminář opět setkal s pozitivním ohlasem. Sdružení CZ.NIC jej jistě i v budoucnu zařadí mezi své vzdělávací a osvětové aktivity. Tentokrát mohou zájemci očekávat témata, která se více či méně dotýkají domén a světa Internetu z pohledu práva, a to nejen v České republice, ale i v zahraničí, protože ani Internet nezná hranice. ■

Vybráno z .blogu As path prepending



(autor: Emanuel Petr,
administrátor CZ.NIC
publikováno: 25. února 2009)

AS path je BGP povinný atribut. Obsahuje seznam čísel autonomních systémů (ASNs), přes které je prefix (rozsah adres) propagován. Například AS path pro ripe.net 193.0.19.25 může vypadat:

```
test@juniper> show route protocol bgp 193.0.19.25
```

```
inet.0: 275156 destinations, 374067 routes (275106 active,  
0 holddown, 76 hidden)
```

+ = Active Route, - = Last Active, * = Both

```
193.0.18.0/23      *[BGP/170] 1w0d 17:01:53, localpref 100  
                  AS path: 15685 1299 3333 I  
                  > to 10.0.0.254 via ge-0/0/0.0
```

Má-li směrovač k danému prefixu více cest, může být délka AS path při výběru **nejlepší cesty** rozhodující.

AS path prepending neboli „umělé“ prodloužení AS path se užije v případě **multihomingu**, kdy chceme pro příchodí provoz preferovat jeden **upstream** před druhým.

Dne 16. 2. 2008 si takto svoji cestičku v globální směrovací tabulce do Uherského Hradiště/Broda (AS47868) prodloužila společnost SUPRO-NET. Využila zmiňované možnosti "AS path prependingu" pro svůj druhý upstream a nešetřila. Běžně stačí svoje AS znásobit jednociferným číslem. Ale 251x se ukázalo, jako velké sousto pro starší směrovače/staré verze IOSu či jakékoliv implementace BGP, které si neporadí s delším AS path. Následkem bylo rozpojení BGP sezení, velké BGP updaty a výpadky konektivity.

Článek na renesys.com popisuje, že to nebyl úmysl, ale chyba správce a bug routeru MikroTik.

Že prefixy s delším AS path nejsou ojedinělé, se můžete přesvědčit na <http://bgpmon.net/maxASpath.php>

Velmi dlouhé AS path jsou nerozumné, protože zbytečně zabírají systémové prostředky na směrovačích. Nejsou však v rozporu s [RFC4271](#). V BGP UPDATE zprávě jsou pro délku atributu vyhrazeny 2 Byty (64KB), takže AS path je omezeno snad jen samotnou velikostí BGP UPDATE zprávy, která je 4KB.

Zajímalo mě, jak se k tomu staví jednotlivé implementace. Zkoušel jsem příkazy pro omezení délky AS path, možnosti prodloužení AS path a nakonec import prefixu s velmi dlouhým AS path. Testovány byly tyto implementace Cisco, Juniper, Quagga a BIRD.

Cisco Systems

Testováno s IOS 12.4(11)T2.

Cisco ve starších IOSech mělo s delším AS path vážné problémy! Jak se jim vyvarovat?

Od IOS 12.0(17)S by měl být implementován příkaz „**bgp maxas-limit**“

```
#bgp maxas-limit ?
<1-2000> Number of ASes in the AS-PATH attribute
```

pokud příkaz není dostupný, můžete použít „ip as-path access-list“ a „filter-list/route-map“ nebo sáhnout po novějším IOS.

Maximální hodnota 2000 u „bgp maxas-limit“ je taková Cisco hrátko, protože v aktuální dokumentaci uvádí <1-255>. I když je Vám umožněno zadat více, bude limit pro importované prefixy stále 255, a to i v případě, neuvedete-li příkaz „bgp maxas-limit“ vůbec.

A aby to nebylo tak jednoduché, je tu ještě odlišnost ve výpisech.
sh ip bgp neighbors 10.0.0.22 route ...zobrazuje přijaté a akceptované prefixy

V případě „bgp maxas-limit“ s hodnotou < 255, nejsou ve výstupu prefixy s delším AS path logicky zobrazeny. Ale s hodnotou >= 255 nebo bez samotného příkazu pro omezení AS path, jsou zobrazeny jako akceptované, nejsou však zařazeny do směrovací tabulky. Ukázka omezení délky AS path na 15:

```
cisco(config)#router bgp 64501
cisco(config-router)#bgp maxas-limit 15
```

Při překročení limitu 15 ASNs se prefix ignoruje a důvod je zalogován.

```
*Feb 19 20:12:27.057: %BGP-6-ASPATH: Long AS path 25192
25192 25192 25192 25192 25192 25192 25192 25192 25192
25192 25192 25192 25192 15685 1299 3333
received from 10.0.0.20: More than configured MAXAS-LIMIT
```

Pravděpodobně jako prevence dlouhých AS path, je v IOS prodloužení AS path omezeno na maximálně 10 ASNs pro jednotlivé příkazy.

```
cisco(config)# route-map prepend-as permit 10
cisco(config-route-map)#set as-path prepend 64501 64501 64501
64501 64501 64501 64501 64501 64501 64501 64501
cisco(config-route-map)#set as-path prepend last-as 10
```

Při pokusu zadat více, skončíte s chybovou zprávou.

```
cisco(config-route-map)#set as-path prepend 64501 64501
64501 64501 64501 64501 64501 64501 64501 64501 64501
64501
% Cannot have more than 10 as-paths prepended
% Cannot have more than 10 as-paths prepended
```

Pokud upravujete AS path pro prefix, který nemá původ u Vás, můžete přidat dalších 20 ASNs aplikací route-mapy při importu.

```
cisco(config-router)#neighbor 10.0.0.22 route-map prepend-as ?
in Apply map to incoming routes
out Apply map to outbound routes
```

Celkem lze prodloužit AS path až o 40 ASNs + 1 ASN implicitně. Tranzitní AS s Cisco směrovači si musí dát pozor na novou chybu a omezit AS path. V opačném případě může dojít při exportu k přerušení BGP spojení.

Juniper Networks

Testováno s JUNOS verzí 9.2R2.15.

Alternativou pro „**bgp maxas-limit number**“ je AS path regulární výraz, který následně aplikujeme ve směrovací politice.

AS path regulární výraz pro 91 ASNs a více.

```
[edit policy-options]
test@juniper# set as-path maxas-limit "{.91,}"
```

Rozšíření importovací politiky o zamítnutí všech prefixů s delším AS path než 90.

```
[edit policy-options policy-statement nix-import term reject-long-
-aspath]
test@juniper# set from as-path maxas-limit
test@juniper# set then reject
Výsledná konfigurace.
```

```
[edit policy-options ]
test@juniper# show
policy-statement nix-import {
...
term reject-long-aspath {
from as-path maxas-limit;
then reject;
}
...
}
set as-path maxas-limit "{.91,}"
```

Odmítnuté prefixy pak naleznete takto:

```
test@juniper> show route receive-protocol bgp 10.0.0.21 hidden
```

```
inet.0: 249888 destinations, 249891 routes (249886 active,
0 holddown, 4 hidden)
Prefix          Nexthop      MED        Lclpref    AS path
10.123.0.0/16   10.0.0.1      0              64501 64501
64501 ... výpis zkrácen ... 64501 64501 64501 64501 64501 64501 I
10.124.0.0/16   10.0.0.25     0              64501 64501
64501 ... výpis zkrácen ... 64501 64501 64501 64501 64501 64501 I
```

Také Juniper omezuje vytvoření velmi dlouhých AS path. Prodloužit AS path se dá třemi příkazy:

as-path-prepend as-path-string ... omezuje na 30 ASNs nebo na maximální délku řetězce 256
as-path-expand last-as count n ... n = kolikrát se poslední ASNs zopakuje a to v rozmezí 1..32
as-path-expand as-path-string ... omezuje na 30 ASNs nebo na maximální délku řetězce 256

Maximálně tedy můžeme prodloužit AS path o 62 ASNs.

V případě překročení limitu 30ti ASNs pro daný příkaz dostaneme chybovou zprávu:
AS path too complex
error: configuration check-out failed

A pokusíme-li zadat řetězec delší než 256 znaků, budeme informováni o invalidním řetězci a prefix nebude vůbec propagován.

```
test@juniper# commit
[edit policy-options policy-statement export-limited term allow-ripe-
-prefix then as-path-prepend]
'as-path-prepend "25192 25192 25192 25192 25192 25192 25192
25192 25192 25192 25192 25192 25192 ... výpis zkrácen ... 25192
25192 25192 25192 25192 25192 25192 25192 25192 25192 25192
25192 "'
Insufficient buffer space for string
[edit policy-options policy-statement export-limited term allow-ripe-
-prefix then as-path-prepend]
'as-path-prepend "25192 25192 25192 25192 25192 25192 25192
25192 25192 25192 25192 25192 25192 ... výpis zkrácen ... 25192
25192 25192 25192 25192 25192 25192 25192 25192 25192 25192
25192 "'
Policy: Invalid string
commit complete
```

Quagga

testovaná verze 0.99.9

Omezení délky AS path na 30 ASNs:

```
ip as-path access-list maxas-path deny ( [0-9]+)(30)$
ip as-path access-list maxas-path permit . *
```

Aplikujeme na přichozí prefixy:

```
neighbor 10.0.0.21 filter-list maxas-path in
```

Quagga neumožní prodloužit AS path více než o 24 ASNs.

Při pokusu zadat více, dostaneme chybovou zprávu a BGP démon se nespustí. Přes VTY sice můžete zadat více, ale příkaz bude tiše ignorován.

```
There is no such command.
Error occured during reading below line.
set as-path prepend 64502 64502 64502 64502 64502 64502 64502
64502 64502 64502 64502 64502 64502 64502 64502 64502
64502 64502 64502 64502 64502 64502 64502 64502 64502
3333
```

The Bird

testovaná verze 1.0.12

Omezení délky AS path na 35 ASNs:

```
protocol bgp {
  export all;
  import filter {
    if bgp_path.len > 35 then reject;
    accept;
  };

  local as 64502;
  neighbor 10.0.0.20 as 25192;
}
```

Filtr můžete testovat pohodlně z příkazové řádky BIRD klienta. V ukázce má importovaný prefix 193.0.18.0/23 délku AS path 35.

```
# ./birdc -s birdctl
BIRD 1.0.12 ready.
bird> show route all filter {if bgp_path.len > 35 then reject; accept;}
193.0.18.0/23   via 10.0.0.20 on eth0 [bgp1 17:21] (100) [AS3333i]
  Type: BGP unicast univ
  BGP.origin: IGP
  BGP.as_path: 25192 25192 25192 25192 25192 25192 25192 25192
25192 25192 25192 25192 25192 25192 25192 25192 25192 25192
25192 25192 25192 25192 25192 25192 25192 25192 25192 25192
25192 25192 25192 25192 25192 15685 1299 3333
  BGP.next_hop: 10.0.0.20
  BGP.local_pref: 0
bird> show route all filter {if bgp_path.len > 34 then reject; accept;}
bird>
```

Prodloužení AS path je omezeno interní velikostí atributů 1KB. Limitu je většinou dosaženo při cca 250 ASNs. Při překročení, obdržíme chybovou zprávu a BGP prefix nebude správně propagován.

```
20-02-2009 14:08:35 <ERR> BGP: attribute list too long,
ignoring the remaining attributes
```

Import prefixu s velmi dlouhým AS path

A jak si poradily jednotlivé implementace s importem prefixu, jehož AS PATH čítala 560 ASNs. Takto dlouhý BGP update byl vytvořen úpravou zdrojových kódů BIRD.

Cisco	import zvládne, ale prefix nezařadí do směrovací tabulky
Juniper	OK
Quagga	OK
BIRD	OK

Závěr

Máte-li na svém směrovači alespoň verze, které byly testovány, tak nebudete mít při samotném importu prefixu s dlouhým AS path problém.

Na směrovačích Cisco se však objevila nová chyba. Překročíte-li při prodloužení AS path délku 255 ASNs a tento prefix vypropagujete, bude BGP sezení přerušeno a následně cyklicky restartováno. Detailně se této nové chybě budu věnovat v dalším článku.

Dodatek:

3. 2009 - Quagga má obdobný problém při exportu s AS path > 255, a to i bez dodatečného prependingu. Ve verzi 0.99.10 byla chyba opravena.
3. 2009 - Rozbor Cisco chyby je součástí článku [Proč a zda Supronet shodil Internet](#).

Emanuel Petr

Zdroje:

<http://www.renesys.com/blog/2009/02/the-flap-heard-around-the-world.html>

http://wiki.nil.com/Limit_the_maximum_BGP_AS-path_length

<http://bgpmon.net/maxASpath.php>

http://www.cisco.com/en/US/docs/ios/iproute/command/reference/irp_bgp1.html#wp1013932

<http://www.juniper.net/>

<http://www.quagga.net/>

<http://bird.network.cz/>

<http://www.ietf.org/rfc/rfc4271.txt>

<http://blog.ioshints.info/2009/02/oversized-as-paths-cisco-ios-bug.html>