
KAPITOLA 23

Překlady adres NAT

V této kapitole najdete informace a příkazy k následujícím tématům:

- Privátní IP adresy: RFC 1918
- Konfigurace dynamického NAT: překlad jedné privátní adresy na jednu veřejnou
- Konfigurace mechanismu PAT: překlad mnoha privátních adres na jednu veřejnou
- Konfigurace statického NAT: překlad jedné privátní adresy na jednu trvale definovanou veřejnou
- Zobrazení konfigurace NAT a PAT
- Řešení problémů s konfiguracemi NAT a PAT
- Příklad konfigurace PAT

Privátní IP adresy: RFC 1918

Následující tabulka uvádí intervaly adres definované v dokumentu RFC 1918, které může kdokoli používat jako interní privátní adresy. Jsou to tedy adresy „uvnitř mojí LAN“, které se pro přenos a směrování ve veřejném Internetu musí převést (přeložit) na veřejné adresy. Zmíněné adresy může pro své vnitřní potřeby používat libovolná síť, ale do veřejného Internetu směrovány být nesmí.

Privátní adresy		
Třída	Interval privátních adres RFC 1918	Prefix pro CIDR
A	10.0.0.0 – 10.255.255.255	10.0.0.0/8
B	172.16.0.0 – 172.31.255.255	172.16.0.0/12
C	192.168.0.0 – 192.168.255.255	192.168.0.0/16

Konfigurace dynamického NAT: překlad jedné privátní adresy na jednu veřejnou



Poznámka

Kompletní konfiguraci mechanismu NAT/PAT včetně názorného diagramu sítě najdete v ukázce konfigurace ke konci této kapitoly.

Krok 1: Na vzdáleném směrovači definujeme statickou cestu a určíme v ní, kam se mají veřejné adresy směřovat.

```
ISP(config)#ip
route 64.64.64.64
255.255.255.128
s0/0/0
```

Směrovači u poskytovatele (ISP) stanovíme, kam má odesílat pakety určené na adresy v síti 64.64.64.64 255.255.255.128.

Krok 2: Na lokálním směrovači, který bude provádět překlady NAT, definujeme fond dostupných veřejných IP adres.

```
Corp(config)#ip
nat pool scott
64.64.64.70
64.64.64.126 netmask
255.255.255.128
```

Privátní adresa dostane vždy přiřazenu první volnou veřejnou IP adresu z fondu.

Definuje následující fond:

Název fondu je `scott`. (Jako název je možné zadat libovolný řetězec.)

Začátek intervalu fondu je 64.64.64.70.

Konec intervalu fondu je 64.64.64.126.

Maska podsítě je 255.255.255.128.

Krok 3: Vytvoříme přístupový seznam (ACL), jenž popisuje, které privátní IP adresy se budou překládat.

```
Corp(config)#access-
list 1 permit
172.16.10.0 0.0.0.255
```

<p>Krok 4: Přístupový seznam napojíme na fond adres a tím aktivujeme překlad adres.</p>	<pre>Corp(config)#ip nat inside source list 1 pool scott</pre>	<p>Definujeme toto nastavení: Zdroj privátních adres pochází z ACL 1. Fond dostupných veřejných adres má název scott.</p>
<p>Krok 5: Definujeme rozhraní, která se nacházejí ve vnitřní síti (obsahují privátní adresy).</p>	<pre>Corp(config)# inter- face fastethernet 0/0</pre> <pre>Corp(config-if)#ip nat inside</pre>	<p>Přejde do režimu konfigurace rozhraní. Na jednom směrovači může být i více než jedno vnitřní rozhraní. Poté povolíme překlad adres z každého vnitřního rozhraní na veřejnou adresu.</p>
	<pre>Corp(config-if)#exit</pre>	<p>Návrat do globálního konfiguračního režimu.</p>
<p>Krok 6: Nakonec definujeme vnější rozhraní, tedy rozhraní, které vede do veřejné sítě.</p>	<pre>Corp(config)# inter- face serial 0/0/0</pre>	<p>Přejde do režimu konfigurace rozhraní.</p>
	<pre>Corp(config-if)#ip nat outside</pre>	<p>Definuje, které rozhraní bude mechanismem NAT považováno za vnější rozhraní.</p>

Konfigurace mechanismu PAT: překlad mnoha privátních adres na jednu veřejnou

V této konfiguraci se všechny privátní adresy překládají na jedinou veřejnou IP adresu a na více čísel portů.

<p>Krok 1: Na vzdáleném směrovači definujeme statickou cestu a určíme v ní, kam se mají veřejné adresy směřovat.</p>	<pre>ISP(config)#ip route 64.64.64.64 255.255.255.128 s0/0/0</pre>	<p>Směrovači u poskytovatele (ISP) stanovíme, kam má odesílat pakety určené na adresy v síti 64.64.64.64 255.255.255.128.</p>
<p>Krok 2: Na lokálním směrovači, který bude provádět překlady NAT, definujeme fond dostupných veřejných IP adres (nepovinný).</p>		<p>Tento krok provedeme v případě, že máme velké množství privátních adres na překlad. Jediná veřejná IP adresa může takto zvládnout i několik tisíc privátních adres. Bez fondu adres můžeme veškeré privátní adresy přeložit na IP adresu výstupního rozhraní (například sériové linky vedoucí k poskytovateli Internetu).</p>

	<pre>Corp(config)#ip nat pool scott 64.64.64.70 64.64.64.70 netmask 255.255.255.128</pre>	<p>Definuje následující fond:</p> <p>Název fondu je scott. (Jako název je možné zadat libovolný řetězec.)</p> <p>Začátek intervalu fondu je 64.64.64.70.</p> <p>Konec intervalu fondu je také 64.64.64.70.</p> <p>Maska podsítě je 255.255.255.128.</p>
Krok 3: Vytvoříme přístupový seznam (ACL), jenž popisuje, které privátní IP adresy se budou překládat.	<pre>Corp(config)#access- list 1 per- mit 172.16.10.0 0.0.0.255</pre>	
Krok 4, varianta 1: Přístupový seznam napojíme na fond adres a tím aktivujeme překlad adres.	<pre>Corp(config)#ip nat inside source list 1 interface serial 0/0/0 overload</pre>	<p>Zdroj privátních adres pochází z ACL 1.</p> <p>Adresy se budou překládat na veřejnou adresu, která je přiřazena k rozhraní serial 0/0/0.</p>
Krok 4, varianta 2: Přístupový seznam napojíme na fond adres a tím aktivujeme překlad adres.		<p>Jestliže se rozhodneme použít fond vytvořený v kroku 1...</p>
	<pre>Corp(config)#ip nat inside source list 1 pool scott overload</pre>	<p>Zdroj privátních adres pochází z ACL 1.</p> <p>Fond dostupných veřejných adres má název scott.</p> <p>Klíčové slovo overload stanovuje, že se pro překlady většího počtu adres budou používat čísla portů.</p>
Krok 5: Definujeme rozhraní, která se nacházejí ve vnitřní síti (obsahují privátní adresy).	<pre>Corp(config)# inter- face fastethernet 0/0</pre>	<p>Přejde do režimu konfigurace rozhraní.</p>
	<pre>Corp(config-if)#ip nat inside</pre>	<p>Na jednom směrovači může být i více než jedno vnitřní rozhraní.</p>
	<pre>Corp(config-if)#exit</pre>	<p>Návrat do globálního konfiguračního režimu.</p>
Krok 6: Nakonec definujeme vnější rozhraní, tedy rozhraní, které vede do veřejné sítě.	<pre>Corp(config)# inter- face serial 0/0/0</pre>	<p>Přejde do režimu konfigurace rozhraní.</p>
	<pre>Corp(config-if)#ip nat outside</pre>	<p>Definuje, které rozhraní bude mechanismem NAT považováno za vnější rozhraní.</p>



Poznámka

Příkazem **ip nat pool** můžeme podle potřeby do fondu zařadit také více než jednu adresu. Syntaxe vypadá následovně:

```
Corp(config)#ip nat pool scott 64.64.64.70 64.64.64.101 netmask
255.255.255.128
```

Takto vytvoříme fond 32 adres, který bude se všemi svými porty celý k dispozici pro překlady adres.

Konfigurace statického NAT: překlad jedné privátní adresy na jednu trvale definovanou veřejnou

<p>Krok 1: Na vzdáleném směrovači definujeme statickou cestu a určíme v ní, kam se mají veřejné adresy směřovat.</p>	<pre>ISP(config)#ip route 64.64.64.64 255.255.255.128 s0/0/0</pre>	<p>Směrovači u poskytovatele (ISP) stanovíme, kam má odesílat pakety určené na adresy v síti 64.64.64.64 255.255.255.128.</p>
<p>Krok 2: Na lokálním směrovači, který bude provádět překlady NAT, vytvoříme statické mapování.</p>	<pre>Corp(config)#ip nat inside source stat- ic 172.16.10.5 64.64.64.65</pre>	<p>Vnitřní adresa 172.16.10.5 se bude trvale překládat na veřejnou adresu 64.64.64.65. Příkaz musíme zadat zvlášť pro každou privátní IP adresu, kterou chceme staticky mapovat na veřejnou adresu.</p>
<p>Krok 3: Definujeme rozhraní, která se nacházejí ve vnitřní síti (obsahují privátní adresy).</p>	<pre>Corp(config)# interface fastethernet 0/0</pre>	<p>Přejde do režimu konfigurace rozhraní.</p>
<p>Krok 4: Nakonec definujeme vnější rozhraní, tedy rozhraní, které vede do veřejné sítě.</p>	<pre>Corp(config- if)#ip nat inside 0/0/0</pre>	<p>Na jednom směrovači může být i více než jedno vnitřní rozhraní. Přejde do režimu konfigurace rozhraní.</p>
	<pre>Corp(config- if)#ip nat out- side</pre>	<p>Definuje, které rozhraní bude mechanismem NAT považováno za vnější rozhraní.</p>



Upozornění

Nezapomeňte v konfiguraci směrovače definovat správné směrování paketů k poskytovateli internetových služeb a také dávejte pozor, aby směrovač poskytovatele věděl, kam posílat provoz pro definovaný fond NAT adres na lokálním směrovači. Bez těchto opatření, tedy pokud by směrovač poskytovatele nebyl obeznámen, kde se v síti fond veřejných IP adres nachází, by pakety opustily síť s veřejnou IP adresou, ale už by se nedokázaly vrátit.

Zobrazení konfigurace NAT a PAT

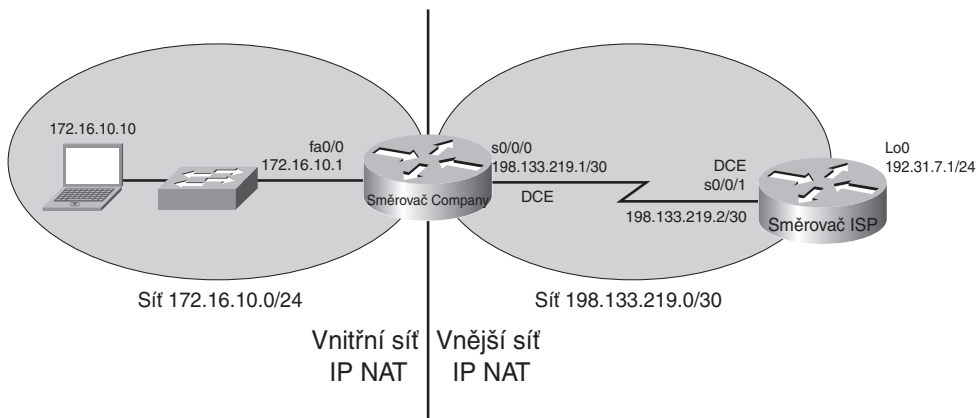
<code>Router#show ip nat translations</code>	Zobrazí překladovou tabulku
<code>Router#show ip nat statistics</code>	Vypíše statistiky mechanismu NAT
<code>Router#clear ip nat translations inside a.b.c.d outside e.f.g.h</code>	Vymaže z tabulky určitý překlad adres ještě před vypršením jeho časového limitu
<code>Router#clear ip nat translations *</code>	Vymaže celou překladovou tabulku ještě před vypršením časového limitu položek

Řešení problémů s konfiguracemi NAT a PAT

<code>Router#debug ip nat</code>	Zobrazí informace o každém překládaném paketu. S tímto příkazem zacházejte opatrně: může se stát, že procesor směrovače nezvládne tak velký objem výstupu zpracovat a celý systém tak začne váznout.
<code>Router#debug ip nat detailed</code>	O každém překládaném paketu zobrazí podrobnější informace.

Příklad konfigurace PAT

Nyní si řekneme, jak pomocí příkazů probraných v této kapitole provést konfiguraci mechanismu PAT, a to v příkladu sítě podle obrázku 23.1.



Obrázek 23.1: Konfigurace překladového mechanismu PAT

Směrovač poskytovatele ISP

router> enable	Přejde do privilegovaného režimu
router# configure terminal	Přejde do globálního konfiguračního režimu
router(config)# host ISP	Definuje hostitelský název
ISP(config)# no ip domain-lookup	Vypne vyhodnocování dotazů DNS (Domain Name System), aby nás každý překlep nezpomaloval
ISP(config)# enable secret cisco	Nastaví oprávněné tajné heslo na cisco
ISP(config)# line console 0	Vstoupí do režimu konfigurace konzolové linky
ISP(config-line)# password class	Nastaví heslo konzolové linky na class
ISP(config-line)# login	Zapíná ověřování hesla
ISP(config-line)# logging synchronous	Příkazy se zapisují na konec nového řádku
ISP(config-line)# exit	Návrat do globálního konfiguračního režimu
ISP(config)# interface serial 0/0/1	Přechod do režimu konfigurace sériového rozhraní
ISP(config-if)# ip address 198.133.219.2 255.255.255.252	Přiřadí IP adresu a síťovou masku
ISP(config-if)# clock rate 56000	Přiřadí hodinovou rychlost kabelu DCE na této straně linky
ISP(config-if)# no shutdown	Zapne rozhraní
ISP(config-if)# interface loop-back 0	Vytvoří zpětnovazební rozhraní 0 a přejde do režimu konfigurace rozhraní
ISP(config-if)# ip address 192.31.7.1 255.255.255.255	Přiřadí IP adresu a síťovou masku
ISP(config-if)# exit	Návrat do globálního konfiguračního režimu
ISP(config)# exit	Návrat do privilegovaného režimu
ISP# copy running-config startup-config	Uloží aktivní konfiguraci do paměti NVRAM

Firemní směrovač Company

router> enable	Přejde do privilegovaného režimu
router# configure terminal	Přejde do globálního konfiguračního režimu
router(config)# host Company	Definuje hostitelský název
Company(config)# no ip domain-lookup	Vypne vyhodnocování dotazů DNS (Domain Name System), aby nás každý překlep nezpomaloval
Company(config)# enable secret cisco	Nastaví oprávněné tajné heslo na cisco
Company(config)# line console 0	Vstoupí do režimu konfigurace konzolové linky
Company(config-line)# password class	Nastaví heslo konzolové linky na class

Firemní směrovač Company

Company (config-line) #login	Zapíná ověřování hesla
Company (config-line) #logging synchronous	Příkazy se zapisují na konec nového řádku
Company (config-line) #exit	Návrat do globálního konfiguračního režimu
Company (config) #interface fastethernet 0/0	Přechod do režimu konfigurace rozhraní
Company (config-if) #ip address 172.16.10.1 255.255.255.0	Přiřadí IP adresu a síťovou masku
Company (config-if) #no shutdown	Zapne rozhraní
Company (config-if) #interface serial 0/0/0	Přechod do režimu konfigurace rozhraní
Company (config-if) #ip address 198.133.219.1 255.255.255.252	Přiřadí IP adresu a síťovou masku
Company (config-if) #no shutdown	Zapne rozhraní
Company (config-if) #exit	Návrat do globálního konfiguračního režimu
Company (config) #ip route 0.0.0.0 0.0.0.0 198.133.219.2	Všechny pakety, jejichž cílová adresa není ve směrovací tabulce definována, se odešlou do směrovače u poskytovatele.
Company (config) #access-list 1 permit 172.16.10.0 0.0.0.255	Definuje adresy, jejichž průchod bude povolen; jsou to zároveň adresy, u kterých bude povolen překlad NAT.
Company (config) #ip nat inside source list 1 interface serial 0/0/0 overload	Zahájí překlady NAT, v nichž sloučí přístupový seznam 1 s rozhraním serial 0/0/0. Adresy v lokální síti budou překládané na jednu veřejnou adresu sériového rozhraní.
Company (config) #interface fastethernet 0/0	Přechod do režimu konfigurace rozhraní
Company (config-if) #ip nat inside	Umístění privátních vnitřních adres
Company (config-if) #interface serial 0/0/0	Přechod do režimu konfigurace rozhraní
Company (config-if) #ip nat outside	Umístění veřejných vnějších adres
Company (config-if) # Ctrl + Z	Návrat do privilegovaného režimu
Company #copy running-config startup-config	Uloží aktivní konfiguraci do paměti NVRAM