Ćwiczenie – Konfiguracja dynamicznej i statycznej translacji NAT

Topologia

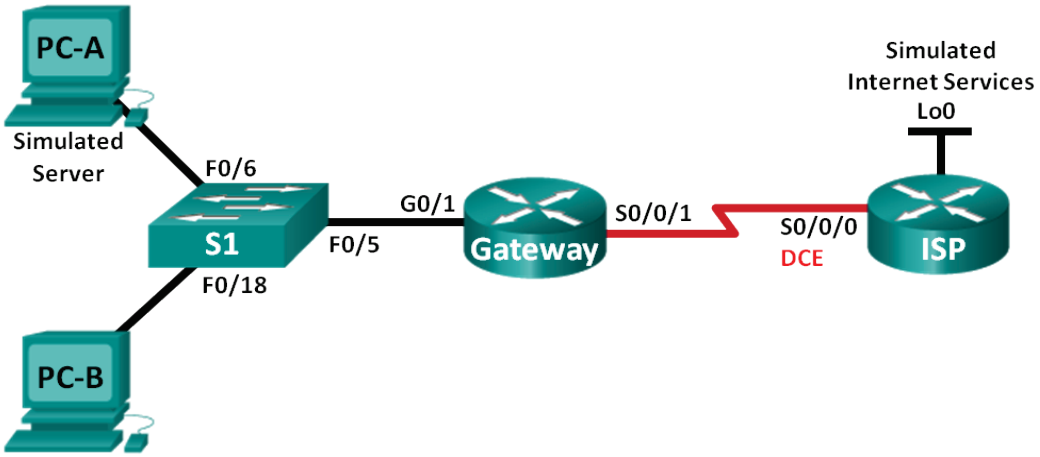

Tabela adresacji

Urządzenie	Interfejs	Adres IP	Maska podsieci	Brama domyślna
Gateway	G0/1	192.168.1.1	255.255.255.0	Nie dotyczy
	S0/0/1	209.165.201.18	255.255.255.252	Nie dotyczy
ISP	S0/0/0 (DCE)	209.165.201.17	255.255.255.252	Nie dotyczy
	Lo0	192.31.7.1	255.255.255.255	Nie dotyczy
PC-A (Symulowany Serwer)	Karta sieciowa	192.168.1.20	255.255.255.0	192.168.1.1
PC-B	Karta sieciowa	192.168.1.21	255.255.255.0	192.168.1.1

Cele

Część 1: Budowa sieci i sprawdzenie łączności

Część 2: Konfigurowanie i sprawdzenie statycznego NAT

Część 3: Konfigurowanie i sprawdzenie dynamicznego NAT

Wprowadzenie / Scenariusz

Translacja adresów sieciowych (ang. Network Address Translation - NAT) jest procesem, w którym urządzenie sieciowe, takie jak router Cisco, przydziela adres publiczny dla hostów wewnętrznej sieci prywatnej. Głównym powodem korzystania z NAT jest ograniczona liczba dostępnych publicznych adresów IPv4. Używanie NAT zmniejsza liczbę publicznych adresów IP, z których korzysta firma.

W tym ćwiczeniu, router ISP przydzielił dla firmy publiczną przestrzeń adresową IP 209.165.200.224/27. Zapewnia to firmie 30 publicznych adresów IP. Adresy od 209.165.200.225 do 209.165.200.241 są przeznaczone do przydzielenia statycznego, a adresy od 209.165.200.242 do 209.165.200.254 są przeznaczone do przydzielania dynamicznego. Od routera ISP do routera Gateway jest wykorzystywana trasa statyczna, a z routera Gateway do routera ISP jest używana trasa domyślna. Połączenie z Internetem jest symulowane na routerze ISP poprzez adres pętli sprzężenia zwrotnego (loopback).

Uwaga: Do realizacji ćwiczenia preferowane są routery Cisco 1941 Integrated Services Routers (ISR) z systemem Cisco IOS Release 15.2(4)M3 (universalk9 image) oraz przełączniki Cisco Catalyst 2960 z systemem Cisco IOS Release 15.0(2) (lanbasek9 image). W przypadku ich braku mogą zostać użyte inne routery i przełączniki z inną wersją systemu operacyjnego. W zależności od modelu i wersji IOS dostępne komendy mogą się różnić od prezentowanych w instrukcji. Na końcu instrukcji zamieszczono tabelę zestawiającą identyfikatory interfejsów routera.

Uwaga: Upewnij się, że routery i przełącznik zostały wyczyszczone i nie posiadają konfiguracji startowej. Jeśli nie jesteś pewny jak to zrobić, poproś o pomoc instruktora.

Wymagane zasoby

- 2 routery (Cisco 1941 z Cisco IOS Release 15.2(4)M3 universalk9 image lub podobny)
- 1 przełącznik (Cisco 2960 z Cisco IOS Release 15.0(2) lanbasek9 image lub podobny)
- 2 komputery PC (Windows 7, Vista, lub XP z programem do emulacji terminala, np. Tera Term)
- Kable konsolowe do konfiguracji urządzeń Cisco IOS poprzez porty konsolowe
- Kable sieciowe zgodne z topologią

Część 1: Budowa sieci i sprawdzenie łączności

W Części 1. należy zestawić sieć zgodnie z diagramem topologii i skonfigurować podstawowe ustawienia takie jak adresy IP interfejsów, trasy statyczne, dostęp do urządzeń i hasła.

Krok 1: Okabluj sieć zgodnie z diagramem topologii.

Połącz urządzenia jak pokazano na diagramie topologii.

Krok 2: Skonfiguruj komputery PC.

Krok 3: Zainicjalizuj i przeładuj routery i przełącznik.

Krok 4: Skonfiguruj podstawowe ustawienia na każdym z routerów.

a. Wyłącz opcję DNS lookup.

b. Skonfiguruj adresy IP, na routerach zgodnie z tabelą adresacji

c. Ustaw szybkość zegara na interfejsach szeregowych DCE na **128000**

d. Przypisz urządzeniom nazwy zgodnie z diagramem topologii.

e. Ustaw **cisco** jako hasło do trybu konsoli i trybu VTY.

f. Ustaw **class** jako hasło szyfrowane do trybu uprzywilejowanego EXEC.

g. Włącz logowanie synchroniczne (**logging synchronous**) aby zapobiec przerywaniu wprowadzania komend przez komunikaty pojawiające się na konsoli.

Krok 5: Utwórz symulowany serwer WWW na ISP.

a. Załóż lokalnego użytkownika o nazwie **webuser** z zaszyfrowanym hasłem **webpass**.

```
ISP(config)# username webuser privilege 15 secret webpass
```

b. Włącz usługę serwera HTTP na ISP.

```
ISP(config)# ip http server
```

c. Skonfiguruj usługę HTTP, żeby korzystała z bazy danych lokalnych użytkowników.

```
ISP(config)# ip http authentication local
```

Krok 6: Skonfiguruj routing statyczny.

a. Utwórz trasę statyczną z routera ISP do routera Gateway używając dla sieci przypisanego zakresu adresów publicznych 209.165.200.224/27.

```
ISP(config)# ip route 209.165.200.224 255.255.255.224 209.165.201.18
```

b. Utwórz trasę domyślną z routera Gateway do routera ISP.

```
Gateway(config)# ip route 0.0.0.0 0.0.0.0 209.165.201.17
```

Krok 7: Zapisz bieżącą konfigurację jako konfigurację startową.

Krok 8: Sprawdź połączenia sieciowe.

a. Wykonaj ping z hostów PC na interfejs G0/1 na routerze Gateway. Rozwiąż problemy jeśli testy się nie powiodły.

b. Wyświetl tablice routingu na obu routerach, aby sprawdzić, czy w tablicy routingu są trasy statyczne i czy są poprawnie skonfigurowane.

Część 2: Konfigurowanie i sprawdzenie statycznego NAT

Statyczny NAT wykorzystuje mapowanie (odwzorowywanie) typu jeden-do-jednego pomiędzy adresami lokalnymi i globalnymi, i mapowania te są niezmienne. Statyczny NAT jest szczególnie przydatny w przypadku serwerów internetowych lub urządzeń, które muszą być dostępne z Internetu pod stałym adresem.

Krok 1: Skonfiguruj mapowanie statyczne.

PC-A symuluje serwer lub urządzenie ze stałym adresem, do którego można uzyskać dostęp poprzez Internet. Mapowanie statyczne jest konfigurowane tak, aby kazać routerowi przenosić wewnętrzny adres prywatny serwera 192.168.1.20 na adres publiczny 209.165.200.225. Pozwala to użytkownikowi z Internetu na dostęp do PC-A.

```
Gateway(config)# ip nat inside source static 192.168.1.20 209.165.200.225
```

Krok 2: Określ interfejsy.

Wydaj na interfejsach komendy **ip nat inside** i **ip nat outside**.

```
Gateway(config)# interface g0/1
Gateway(config-if)# ip nat inside
Gateway(config-if)# interface s0/0/1
Gateway(config-if)# ip nat outside
```

Krok 3: Sprawdź konfigurację.

a. Wyświetl tabelę statycznego NAT za pomocą polecenia **show ip nat translations**.

```
Gateway# show ip nat translations
Pro Inside global      Inside local       Outside local      Outside global
--- 209.165.200.225    192.168.1.20       ---                ---
```

Jak jest modyfikowany wewnętrzny adres lokalny komputera?

192.168.1.20 = _____

Jaki jest przypisany wewnętrzny adres globalny?

_____

Jaki jest przypisany wewnętrzny adres lokalny?

_____

b. Wykonaj ping z PC-A na interfejs Lo0 (192.31.7.1) na ISP. Jeśli polecenie ping nie powiodło się, to znajdź i rozwiąż problemy. Wyświetl tabelę NAT na routerze Gateway.

```
Gateway# show ip nat translations
Pro Inside global      Inside local       Outside local      Outside global
icmp 209.165.200.225:1 192.168.1.20:1     192.31.7.1:1       192.31.7.1:1
--- 209.165.200.225    192.168.1.20       ---                ---
```

Gdy PC-A wysłał żądanie ICMP (ping) do 192.31.7.1 na ISP, to do tabeli NAT został dodany wpis z zaznaczonym protokołem ICMP.

Jaki numer portu został użyty w tej wymianie ICMP? _____

Uwaga: Może być konieczne wyłączenie zapory na PC-A aby ping zakończył się powodzeniem.

c. Z PC-A wykonaj połączenie telnet do interfejsu Lo0 na ISP i wyświetl tabelę NAT.

```
Pro Inside global        Inside local       Outside local      Outside global
icmp 209.165.200.225:1   192.168.1.20:1     192.31.7.1:1       192.31.7.1:1
tcp 209.165.200.225:1034 192.168.1.20:1034  192.31.7.1:23      192.31.7.1:23
--- 209.165.200.225      192.168.1.20       ---                ---
```

Uwaga: Wpis NAT dla żądania ICMP mógł zostać już usunięty z tabeli NAT, jeśli upłynął dla niego limit czasu.

Jaki protokół został użyty przy tej translacji? _____

Jakie są używane numery portów?

Wewnętrzny globalny / lokalny:_____

Zewnętrzny globalny / lokalny: _____

d. Ponieważ statyczny NAT został skonfigurowany dla PC-A, sprawdź, czy polecenie ping z ISP do PC-A na adres publiczny statycznego NAT (209.165.200.225) powiodło się.

e. Wyświetl tabelę NAT na routerze Gateway, żeby sprawdzić translacje adresów.

```
Gateway# show ip nat translations
Pro Inside global       Inside local       Outside local      Outside global
icmp 209.165.200.225:12 192.168.1.20:12    209.165.201.17:12  209.165.201.17:12
--- 209.165.200.225     192.168.1.20       ---                ---
```

Zauważ, że zewnętrzne adresy lokalny i globalny są takie same. Ten adres jest adresem źródłowym ISP w sieci zdalnej. Dla skutecznej komunikacji ping od ISP do PC-A, wewnętrzny adres globalny statycznego NAT (209.165.200.225) jest poddawany translacji na wewnętrzny adres lokalny PC-A (192.168.1.20).

f. Sprawdź statystyki NAT na routerze Gateway, za pomocą polecenia **show ip nat statistics**.

```
Gateway# show ip nat statistics
Total active translations: 2 (1 static, 1 dynamic; 1 extended)
Peak translations: 2, occurred 00:02:12 ago
Outside interfaces:
  Serial0/0/1
Inside interfaces:
  GigabitEthernet0/1
Hits: 39  Misses: 0
CEF Translated packets: 39, CEF Punted packets: 0
Expired translations: 3
Dynamic mappings:

Total doors: 0
Appl doors: 0
Normal doors: 0
```

```
Queued Packets: 0
```

Uwaga: To jest przykład wyjściowych danych wynikowych. Twoje dane wynikowe mogą być inne.

Część 3: Konfigurowanie i sprawdzenie dynamicznego NAT

Dynamiczny NAT korzysta z puli adresów publicznych i przydziela je na zasadzie pierwszy zgłoszony - pierwszy obsłużony. Kiedy urządzenie wewnętrzne wnioskuje o dostęp do sieci zewnętrznej, to dynamiczny NAT przydziela mu, dostępny w puli, publiczny adres IPv4. W wyniku działania dynamicznego NAT powstają mapowania między adresami lokalnym i globalnymi typu wiele-do-wielu

Krok 1: Wyczyść procesy NAT.

Przed przystąpieniem do dodawania dynamicznego NAT, wyczyść translacje i statystyki NAT z Części 2.

```
Gateway# clear ip nat translation *
Gateway# clear ip nat statistics
```

Krok 2: Zdefiniuj listę kontroli dostępu (ACL), która odpowiada zakresowi prywatnych adresów IP w sieci LAN.

ACL 1 jest używana w celu umożliwienia translacji sieci 192.168.1.0/24.

```
Gateway(config)# access-list 1 permit 192.168.1.0 0.0.0.255
```

Krok 3: Sprawdź czy nadal są aktualne konfiguracje NAT na interfejsach.

Wydaj komendę **show ip nat statistics** na routerze Gateway, żeby sprawdzić konfiguracje NAT.

Krok 4: Określ pulę możliwych do wykorzystania publicznych adresów IP.

```
Gateway(config)# ip nat pool public_access 209.165.200.242 209.165.200.254
netmask 255.255.255.224
```

Krok 5: Zdefiniuj NAT z listy wewnętrznych adresów źródłowych na pulę zewnętrzną.

Uwaga: Należy pamiętać, że w nazwie puli NAT jest rozróżniana wielkość liter, dlatego wpisana nazwa puli musi być dokładnie tą, która była wpisana w poprzednim kroku.

```
Gateway(config)# ip nat inside source list 1 pool public_access
```

Krok 6: Sprawdź konfigurację.

a. Wykonaj ping z PC-B na interfejs Lo0 (192.31.7.1) routera ISP. Jeśli polecenie ping nie powiodło się, to znajdź i rozwiąż problemy. Wyświetl tabelę NAT na routerze Gateway.

```
Gateway# show ip nat translations
Pro Inside global      Inside local       Outside local      Outside global
--- 209.165.200.225    192.168.1.20       ---                ---
icmp 209.165.200.242:1 192.168.1.21:1     192.31.7.1:1       192.31.7.1:1
--- 209.165.200.242    192.168.1.21       ---                ---
```

Jak jest zamieniany wewnętrzny adres lokalny komputera PC-B?

192.168.1.21 = _____

Gdy PC-B wysłał komunikat ICMP do 192.31.7.1 na ISP, to do tabeli NAT został dodany wpis z zaznaczonym protokołem ICMP.

Jaki numer portu został użyty w tej wymianie ICMP? _____

b. Otwórz przeglądarkę na PC-B i wpisz adres IP serwera WWW, symulowanego na ISP (interfejs Lo0). Gdy pojawi się monit, zaloguj się jako **webuser** z hasłem **webpass**.

c. Wyświetl tabelę NAT.

```
Pro Inside global        Inside local       Outside local      Outside global
--- 209.165.200.225      192.168.1.20       ---                ---
tcp 209.165.200.242:1038 192.168.1.21:1038 192.31.7.1:80     192.31.7.1:80
tcp 209.165.200.242:1039 192.168.1.21:1039 192.31.7.1:80     192.31.7.1:80
tcp 209.165.200.242:1040 192.168.1.21:1040 192.31.7.1:80     192.31.7.1:80
tcp 209.165.200.242:1041 192.168.1.21:1041 192.31.7.1:80     192.31.7.1:80
tcp 209.165.200.242:1042 192.168.1.21:1042 192.31.7.1:80     192.31.7.1:80
tcp 209.165.200.242:1043 192.168.1.21:1043 192.31.7.1:80     192.31.7.1:80
tcp 209.165.200.242:1044 192.168.1.21:1044 192.31.7.1:80     192.31.7.1:80
tcp 209.165.200.242:1045 192.168.1.21:1045 192.31.7.1:80     192.31.7.1:80
tcp 209.165.200.242:1046 192.168.1.21:1046 192.31.7.1:80     192.31.7.1:80
tcp 209.165.200.242:1047 192.168.1.21:1047 192.31.7.1:80     192.31.7.1:80
tcp 209.165.200.242:1048 192.168.1.21:1048 192.31.7.1:80     192.31.7.1:80
tcp 209.165.200.242:1049 192.168.1.21:1049 192.31.7.1:80     192.31.7.1:80
tcp 209.165.200.242:1050 192.168.1.21:1050 192.31.7.1:80     192.31.7.1:80
tcp 209.165.200.242:1051 192.168.1.21:1051 192.31.7.1:80     192.31.7.1:80
tcp 209.165.200.242:1052 192.168.1.21:1052 192.31.7.1:80     192.31.7.1:80
--- 209.165.200.242    192.168.1.22       ---                ---
```

Jaki protokół był używany w tej translacji? _____

Jakie numery portów zostały wykorzystane?

Wewnątrz: _____

Na zewnątrz: _____

Jaki dobrze znany numer portu i usługa zostały wykorzystane? _____

d. Sprawdź statystyki NAT na routerze Gateway, za pomocą polecenia **show ip nat statistics**.

```
Gateway# show ip nat statistics
Total active translations: 3 (1 static, 2 dynamic; 1 extended)
Peak translations: 17, occurred 00:06:40 ago
Outside interfaces:
  Serial0/0/1
Inside interfaces:
  GigabitEthernet0/1
Hits: 345  Misses: 0
CEF Translated packets: 345, CEF Punted packets: 0
Expired translations: 20
Dynamic mappings:
-- Inside Source
[Id: 1] access-list 1 pool public_access refcount 2
 pool public_access: netmask 255.255.255.224
        start 209.165.200.242 end 209.165.200.254
        type generic, total addresses 13, allocated 1 (7%), misses 0

Total doors: 0
Appl doors: 0
Normal doors: 0
Queued Packets: 0
```

Uwaga: To jest przykład wyjściowych danych wynikowych. Twoje dane wynikowe mogą być inne.

Krok 7: Usuń statyczny wpis NAT.

W kroku 7. zostanie usunięty statyczny wpis NAT i będziesz obserwował wpisy NAT.

a. Usuń, wprowadzony w Części 2, statyczny wpis NAT. Wpisz **yes**, gdy zostaniesz spytany o usunięcie pozycji podrzędnych.

```
Gateway(config)# no ip nat inside source static 192.168.1.20
209.165.200.225

Static entry in use, do you want to delete child entries? [no]: yes
```

b. Wyczyść translacje i statystyki NAT.

c. Wykonaj ping do ISP (192.31.7.1) z PC-A i PC-B.

d. Wyświetl tabelę i statystyki NAT.

```
Gateway# show ip nat statistics
Total active translations: 4 (0 static, 4 dynamic; 2 extended)
Peak translations: 15, occurred 00:00:43 ago
Outside interfaces:
  Serial0/0/1
Inside interfaces:
  GigabitEthernet0/1
Hits: 16  Misses: 0
CEF Translated packets: 285, CEF Punted packets: 0
Expired translations: 11
Dynamic mappings:
-- Inside Source
[Id: 1] access-list 1 pool public_access refcount 4
 pool public_access: netmask 255.255.255.224
        start 209.165.200.242 end 209.165.200.254
        type generic, total addresses 13, allocated 2 (15%), misses 0

Total doors: 0
Appl doors: 0
Normal doors: 0
Queued Packets: 0

Gateway# show ip nat translation
Pro Inside global      Inside local       Outside local      Outside global
icmp 209.165.200.243:512 192.168.1.20:512 192.31.7.1:512     192.31.7.1:512
--- 209.165.200.243    192.168.1.20       ---                ---
icmp 209.165.200.242:512 192.168.1.21:512 192.31.7.1:512     192.31.7.1:512
--- 209.165.200.242    192.168.1.21       ---                ---
```

Uwaga: To jest przykład wyjściowych danych wynikowych. Twoje dane wynikowe mogą być inne.

Do przemyślenia

1. Dlaczego NAT jest używany w sieci?

_____

_____

_____

2. Jakie są ograniczenia NAT?

_____

_____

_____

Tabela z zestawieniem interfejsów routera

Zestawienie interfejsów routera				
Model routera	**Interfejs Ethernet #1**	**Interfejs Ethernet #2**	**Interfejs Serial #1**	**Interfejs Serial #2**
1800	Fast Ethernet 0/0 (F0/0)	Fast Ethernet 0/1 (F0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
1900	Gigabit Ethernet 0/0 (G0/0)	Gigabit Ethernet 0/1 (G0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
2801	Fast Ethernet 0/0 (F0/0)	Fast Ethernet 0/1 (F0/1)	Serial 0/1/0 (S0/1/0)	Serial 0/1/1 (S0/1/1)
2811	Fast Ethernet 0/0 (F0/0)	Fast Ethernet 0/1 (F0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
2900	Gigabit Ethernet 0/0 (G0/0)	Gigabit Ethernet 0/1 (G0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)

Uwaga: Obejrzyj router, aby zidentyfikować typ routera oraz aby określić liczbę jego interfejsów. W ten sposób dowiesz się, jaka jest konfiguracja sprzętowa routera. Możesz to sprawdzić również z poziomu IOS poleceniem **show ip interface brief**. Nie ma sposobu na skuteczne opisanie wszystkich kombinacji konfiguracji dla wszystkich rodzajów routerów. Powyższa tabela zawiera identyfikatory możliwych kombinacji interfejsów szeregowych i Ethernet w urządzeniach. Tabela nie zawiera żadnych innych rodzajów interfejsów, mimo iż dany router może mieć jakieś zainstalowane. Przykładem może być interfejs ISDN BRI. Łańcuch w nawiasie jest skrótem, który może być stosowany w systemie operacyjnym Cisco IOS przy odwoływaniu się do interfejsu.