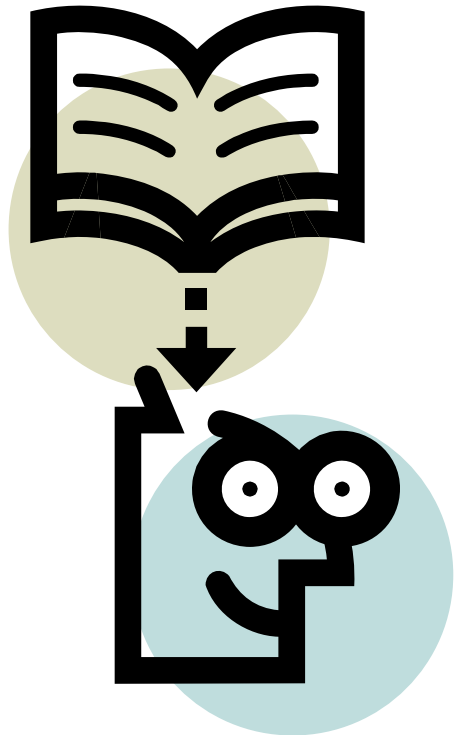
PBS

Wykład 6

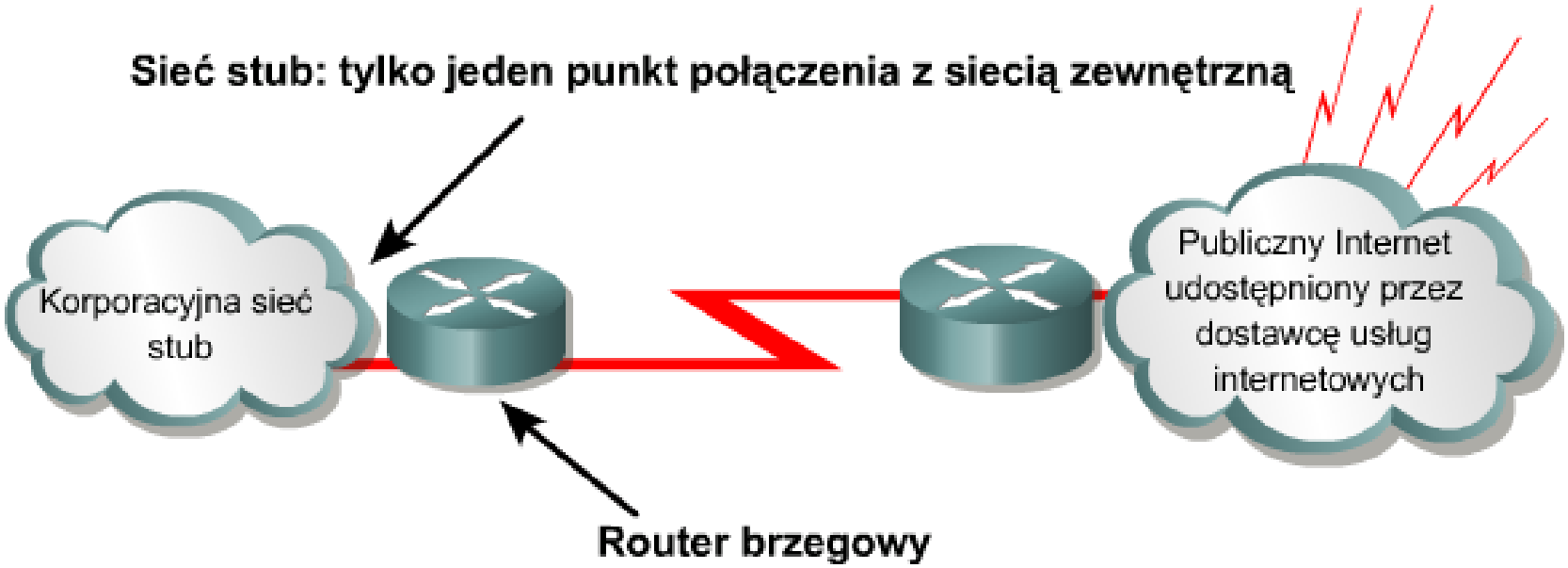
1. Filtrowanie pakietów
2. Translacja adresów
3. authentication-proxy



mgr inż. Roman Krzeszewski roman@kis.p.lodz.pl
mgr inż. Artur Sierszeń asiersz@kis.p.lodz.pl
mgr inż. Łukasz Sturgulewski luk@kis.p.lodz.pl

NAT

- Technologia NAT umożliwia ograniczenie liczby publicznych adresów IP i wykorzystanie prywatnych adresów IP w sieciach wewnętrznych



NAT – Podstawowe pojęcia

- **Wewnętrzny adres lokalny**

  – adres IP przypisany do hosta w sieci wewnętrznej. Ten adres IP zazwyczaj nie jest przypisany przez organizację InterNIC (ang. Internet Network Information Center) ani dostawcę usług. Najczęściej jest to adres prywatny zgodny ze standardem RFC 1918.

- **Wewnętrzny adres globalny**

  – legalny adres IP przypisany przez organizację InterNIC lub dostawcę usług. Adres ten reprezentuje dla sieci zewnętrznych jeden lub więcej wewnętrznych, lokalnych adresów IP.

NAT – Podstawowe pojęcia

- **Zewnętrzny adres lokalny**

  – adres IP zewnętrznego hosta, który znany jest hostom znajdującym się w sieci wewnętrznej.
- **Zewnętrzny adres globalny**

  – adres IP przypisany do hosta w sieci zewnętrznej. Ten adres przypisany jest przez właściciela hosta.

NAT - Cechy

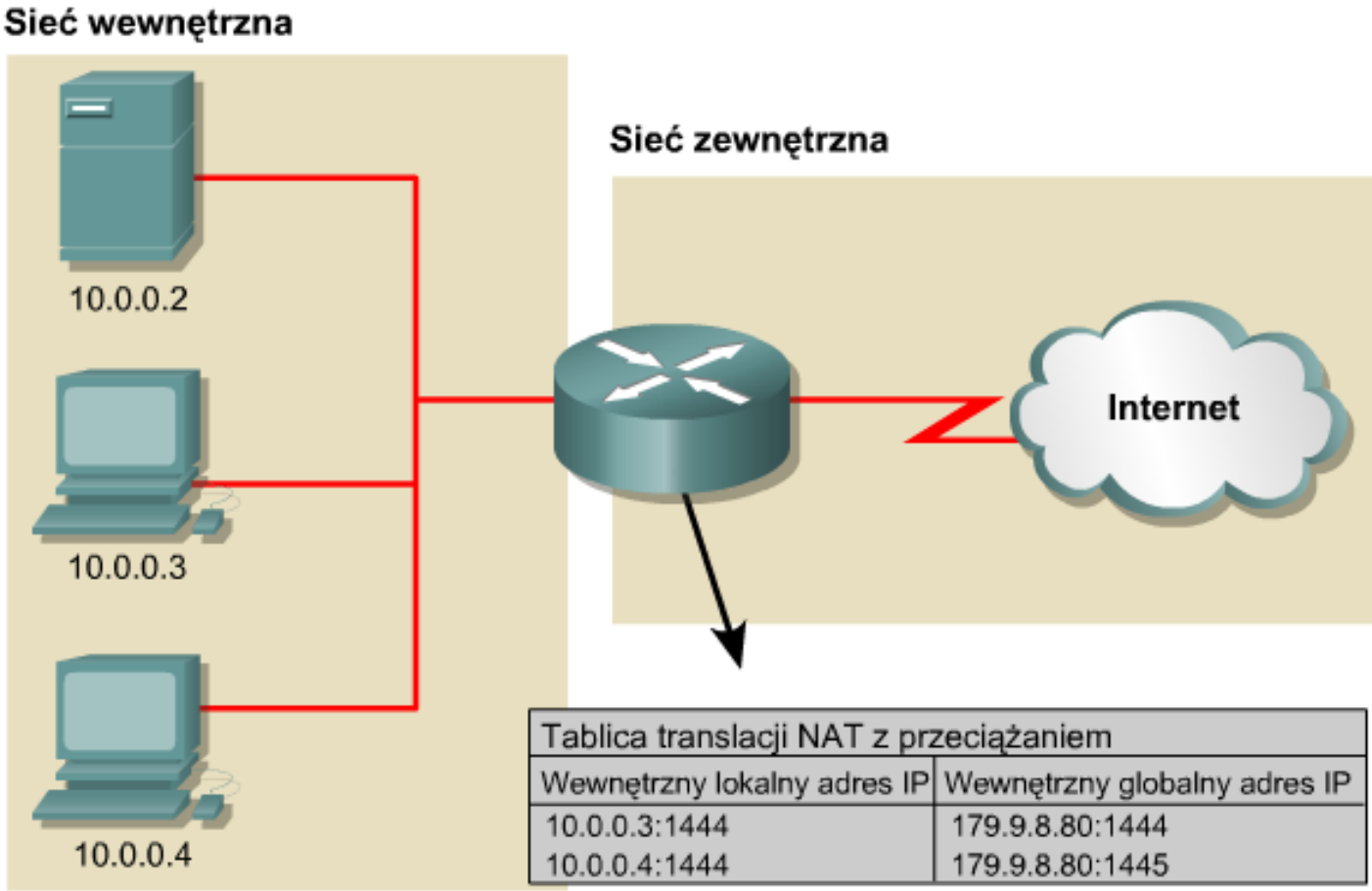
- **Statyczna translacja NAT**

  umożliwia utworzenie odwzorowania typu jeden-do-jednego pomiędzy adresami lokalnymi i globalnymi.

- **Dynamiczna translacja NAT**

  odwzorowuje mapę adresów prywatnych IP na adres publiczny.

NAT - Cechy

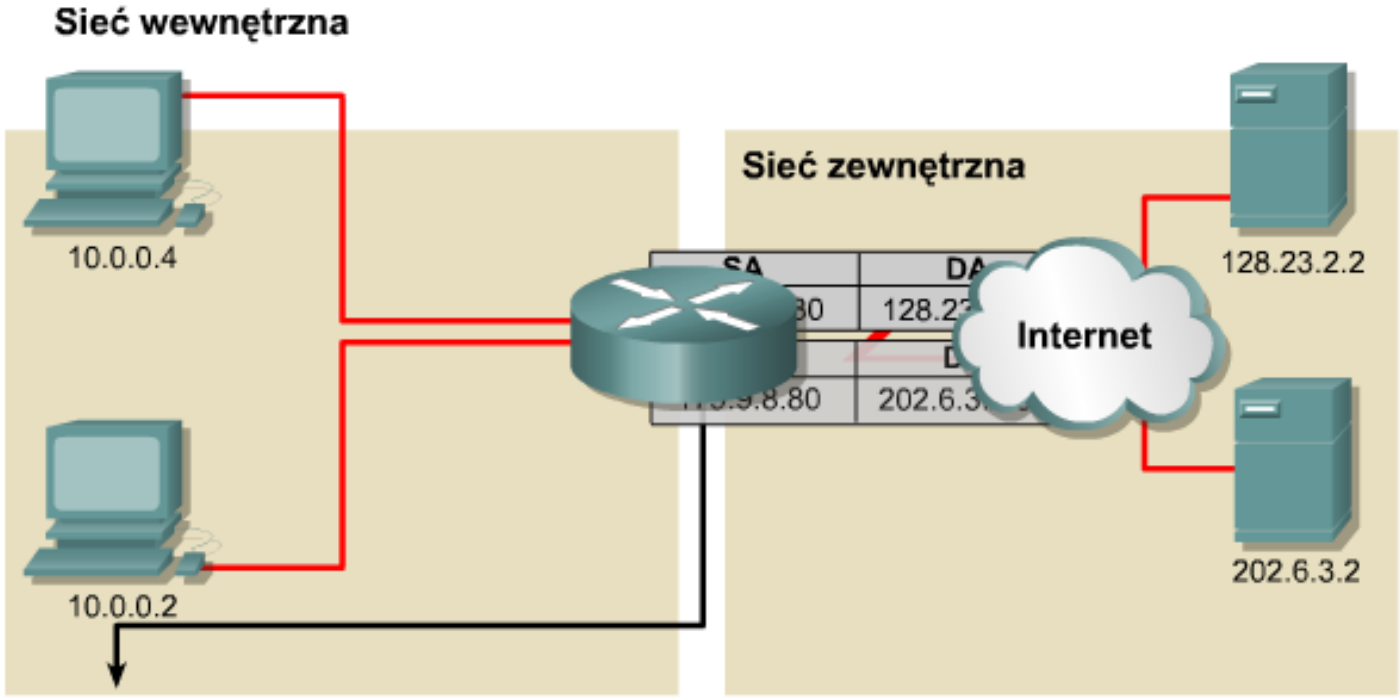


Tablica translacji NAT z przeciążaniem	
Wewnętrzny lokalny adres IP	Wewnętrzny globalny adres IP
10.0.0.3:1444	179.9.8.80:1444
10.0.0.4:1444	179.9.8.80:1445

PAT - Cechy

- W technologii PAT tłumaczone adresy są rozróżniane przy użyciu unikatowych numerów portów źródłowych powiązanych z globalnym adresem IP.

PAT - Cechy



Tablica translacji NAT z przeciążaniem			
Wewnętrzny lokalny adres IP	Wewnętrzny globalny adres IP	Zewnętrzny lokalny adres IP	Zewnętrzny adres globalny
10.0.0.2:1331 10.0.0.4:1555	179.9.8.80:1331 179.9.8.80:1555	202.6.3.2:80 128.23.2.2:80	202.6.3.2:80 128.23.2.2:80

NAT – Korzyści (1)

- Eliminacja konieczności ponownego przypisania adresów IP do każdego hosta po zmianie dostawcy usług internetowych (ISP). Użycie mechanizmu NAT pozwala na uniknięcie zmiany adresów wszystkich hostów, dla których wymagany jest dostęp zewnętrzny, a to wiąże się z oszczędnościami czasowymi i finansowymi.

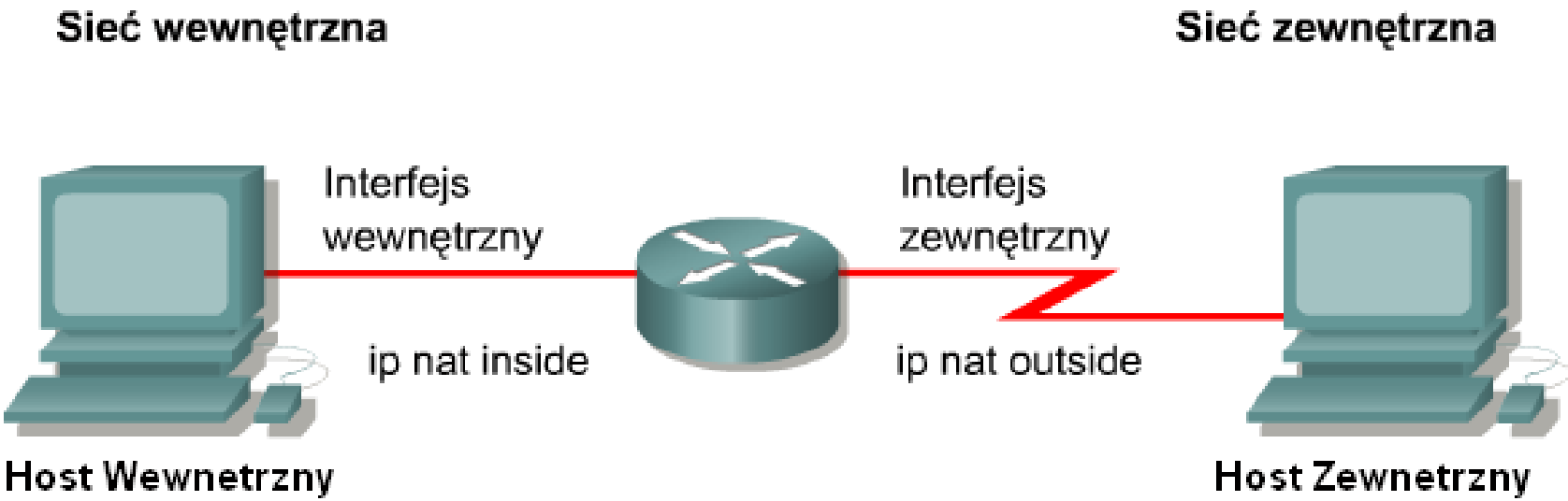
NAT – Korzyści

- Zmniejszenie liczby adresów przy użyciu dostępnej w aplikacji funkcji multipleksowania na poziomie portów. Gdy wykorzystywany jest mechanizm PAT, hosty wewnętrzne mogą współużytkować pojedynczy publiczny adres IP podczas realizacji wszystkich operacji wymagających komunikacji zewnętrznej. W takiej konfiguracji do obsługi wielu hostów wewnętrznych wymagana jest bardzo niewielka liczba adresów zewnętrznych. Pozwala to zaoszczędzić adresy IP.

NAT – Korzyści (2)

- Zwiększenie poziomu bezpieczeństwa w sieci. Ponieważ w wypadku sieci prywatnej nie są rozgłaszane wewnętrzne adresy ani informacje o wewnętrznej topologii, sieć taka pozostaje wystarczająco zabezpieczona, gdy dostęp zewnętrzny odbywa się z wykorzystaniem translacji NAT.

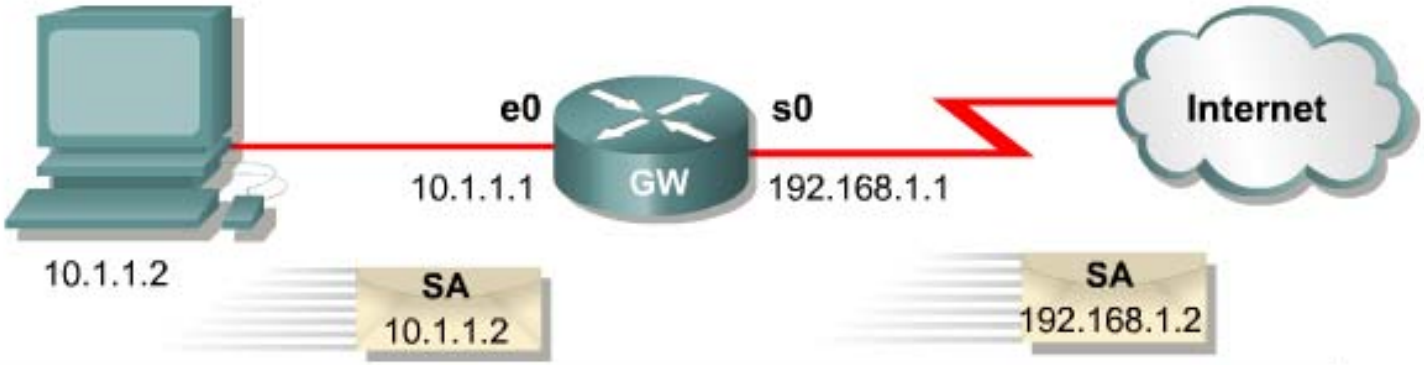
Konfiguracja mechanizmu NAT i PAT




```
Router(config-if)#ip nat inside
```

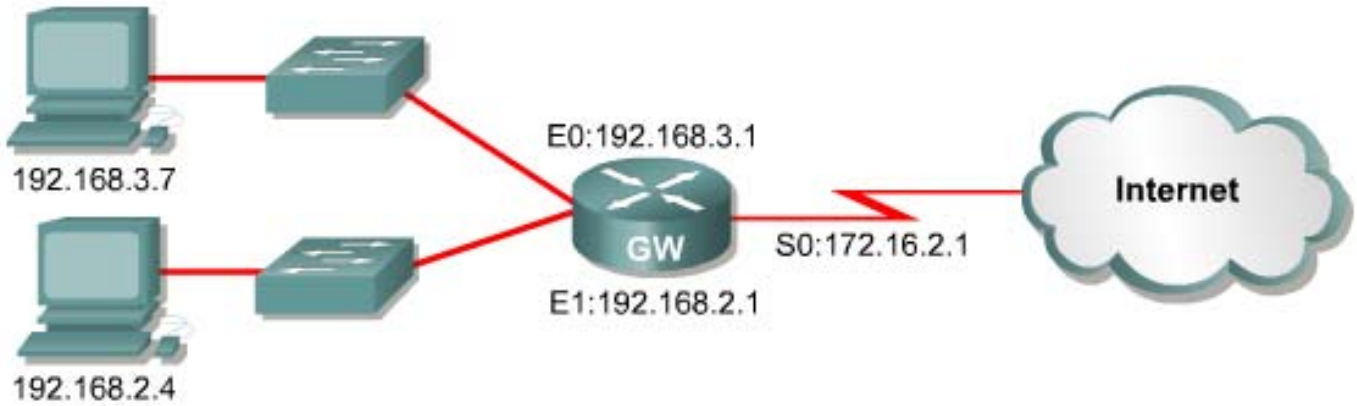
- Interfejs w routerze może zostać określony jako wewnętrzny lub zewnętrzny.
- Translacje wykonywane są między interfejsem wewnętrznym a zewnętrznym.

Konfiguracja NAT




```
hostname GW
!
ip nat inside source static 10.1.1.2 192.168.1.2
!
interface ethernet 0
  ip address 10.1.1.1 255.255.255.0
  ip nat inside
!
interface serial 0
  ip address 192.168.1.1 255.255.255.0
  ip nat outside
!
```

Konfiguracja PAT




```
interface ethernet 0
  ip address 192.168.3.1 255.255.255.0
  ip nat inside
!
interface ethernet 1
  ip address 192.168.2.1 255.255.255.0
  ip nat inside
!
interface serial 0
  ip address 172.16.2.1 255.255.255.0
  ip nat outside
!
ip nat inside source list 1 interface serial 0 overload
!
access-list 1 permit 192.168.2.0 0.0.0.255
access-list 1 permit 192.168.3.0 0.0.0.255
```

Weryfikowanie konfiguracji mechanizmu NAT i PAT

```
Router#show ip nat translations [verbose]
```

* verbose (opcjonalnie) Wyświetla dodatkowe informacje o każdym wpisie w tablicy translacji, łącznie z czasem utworzenia i użycia wpisu

```
Router#show ip nat translations
Pro Inside global     Inside local      Outside local  Outside global
172.16.131.1          10.10.10.1              ---            ---
```

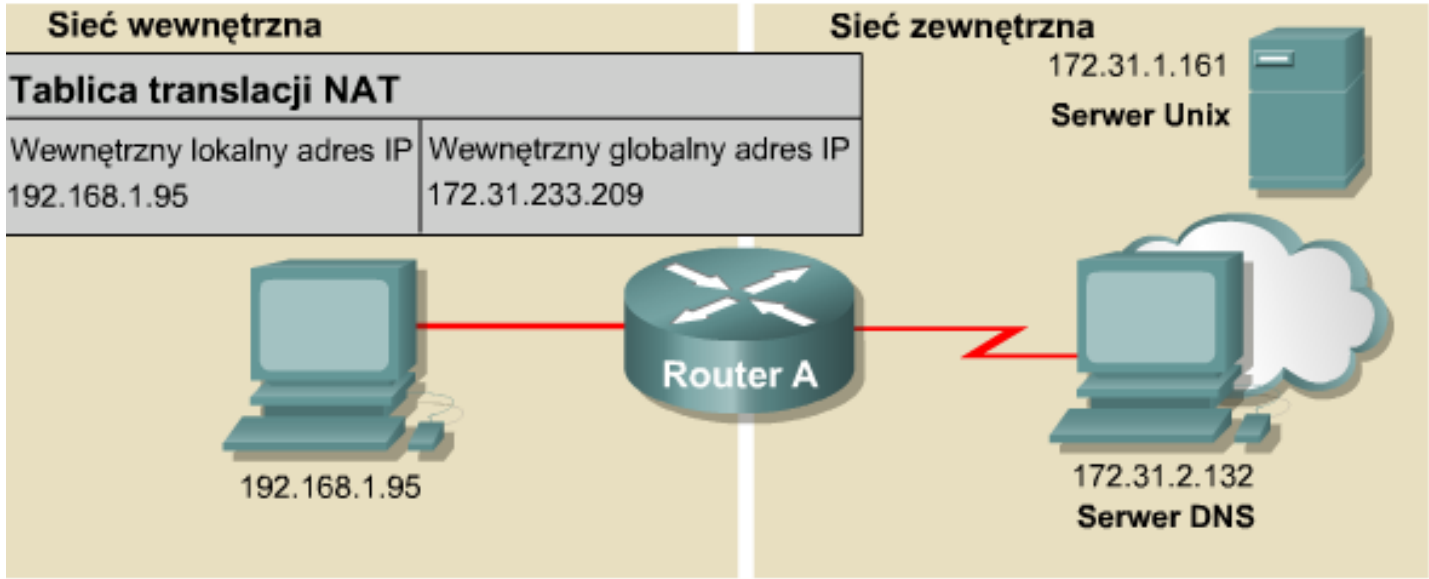
```
Router#show ip nat statistics
```

• Wyświetla statystykę translacji

```
Router#show ip nat statistics
Total active translations: 1 (1 static, 0 dynamic; 0 extended)
Outside interfaces:
Serial0
Inside interfaces:
Ethernet0, Ethernet1
Hits: 5 Misses:0
```

Polecenie	Opis
`show ip nat translations`	Wyświetla aktywne translacje
`show ip nat statistics`	Wyświetla statystykę translacji

Problemy z NAT i PAT




```
RouterA#debug ip nat
NAT:   s= 192.168.1.95    → 172.31.233.209,        d=172.31.2.132 [6825]
NAT:   s= 172.31.2.132,     d=172.31.233.209,    → 192.168.1.95 [21852]
NAT:   s= 192.168.1.95    → 172.31.233.209,        d=172.31.1.161 [6826]
NAT*:  s= 172.31.1.161,     d=172.31.233.209,    → 192.168.1.95 [23311]
NAT*:  s= 192.168.1.95    → 172.31.233.209,        d=172.31.1.161 [6827]
NAT*:  s= 192.168.1.95    → 172.31.233.209,        d=172.31.1.161 [6828]
NAT*:  s= 172.31.1.161      d=172.31.233.209,    → 192.168.1.95 [23313]
NAT*:  s= 172.31.1.161,     d=172.31.233.209,    → 192.168.1.95 [23313]
```

Zalety mechanizmu NAT

Z wykorzystaniem mechanizmu NAT wiąże się kilka korzyści, takich jak:

- Zastosowanie translacji NAT umożliwia ograniczenie liczby prawnie zarejestrowanych adresów dzięki umożliwieniu używania adresów prywatnych w sieciach intranet.
- Translacja NAT pozwala na dalsze wykorzystywanie istniejącego schematu adresowania i jednocześnie obsługuje nowy schemat przypisywania adresów spoza sieci prywatnej.

Mechanizm NAT w systemie IOS firmy Cisco obsługuje następujące typy ruchu, mimo że w tym przypadku adres IP przenoszony jest w strumieniu danych aplikacji:

- protokół ICMP
- protokół FTP (File Transfer Protocol), łącznie z poleceniami PORT i PASV
- usługi związane z przesyłaniem danych NetBIOS przez sieci TCP/IP, obsługą datagramów, nazw i sesji
- usługa RealAudio firmy Progressive Networks
- usługa CUSeeMe firmy White Pines
- zapytania DNS typu A i PTR
- oprogramowanie H.323/NetMeeting, wersja 12.0(1)/12.0(1)T lub nowsza
- VDOLive, wersje 11.3(4)11.3(4)T lub nowsze
- Vxtreme, wersje 11.3(4)11.3(4)T lub nowsze
- IP Multicast, wersja 12.0(1)T tylko dla translacji adresu źródłowego

Mechanizm NAT w systemie IOS firmy Cisco nie obsługuje następujących typów ruchu w sieci:

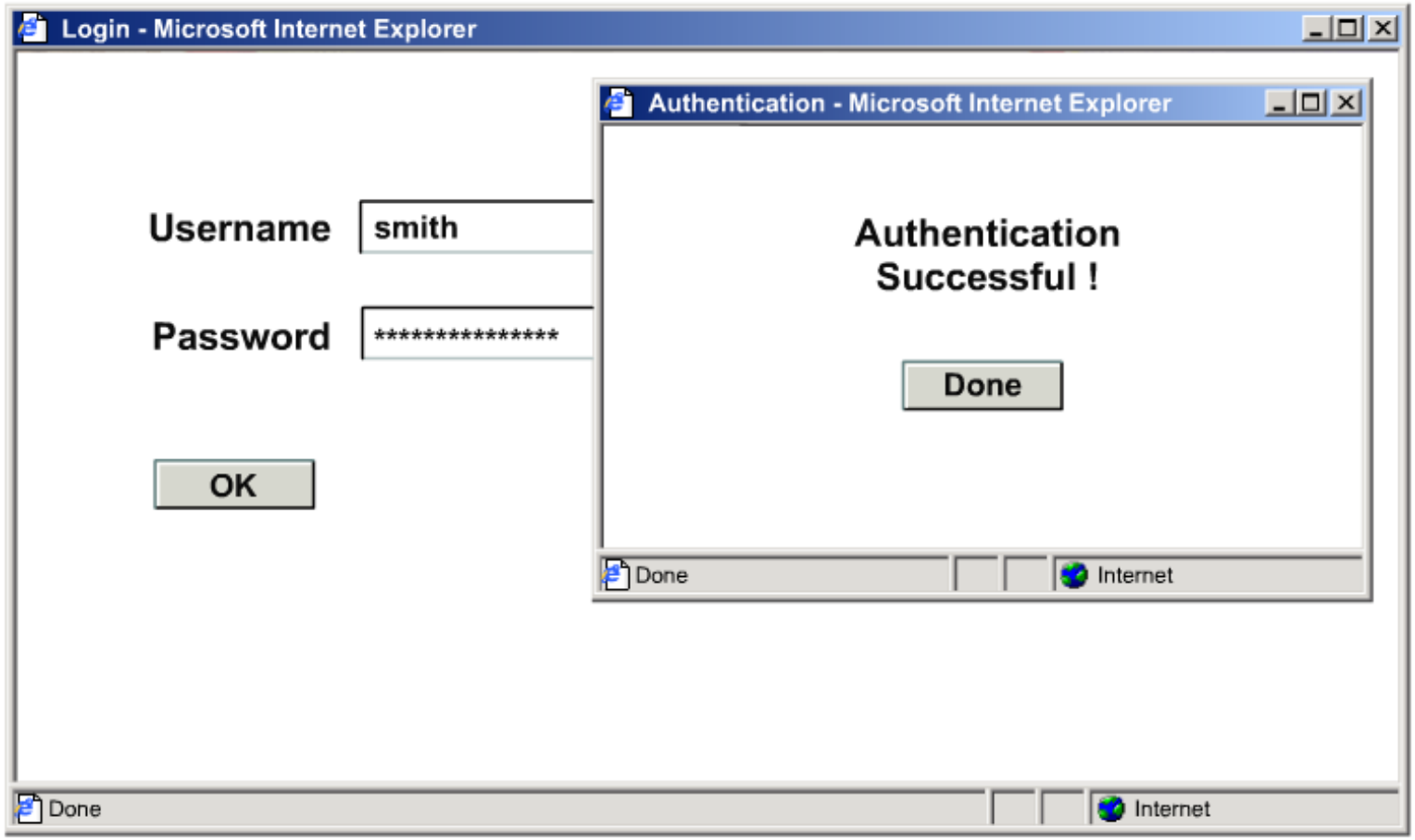
- aktualizacje tablic routingu
- przenoszenie stref DNS
- protokół BOOTP
- usługi talk, ntalk
- protokół SNMP (Simple Network Management Protocol),

Authentication Proxy
(Cisco IOS Firewall)

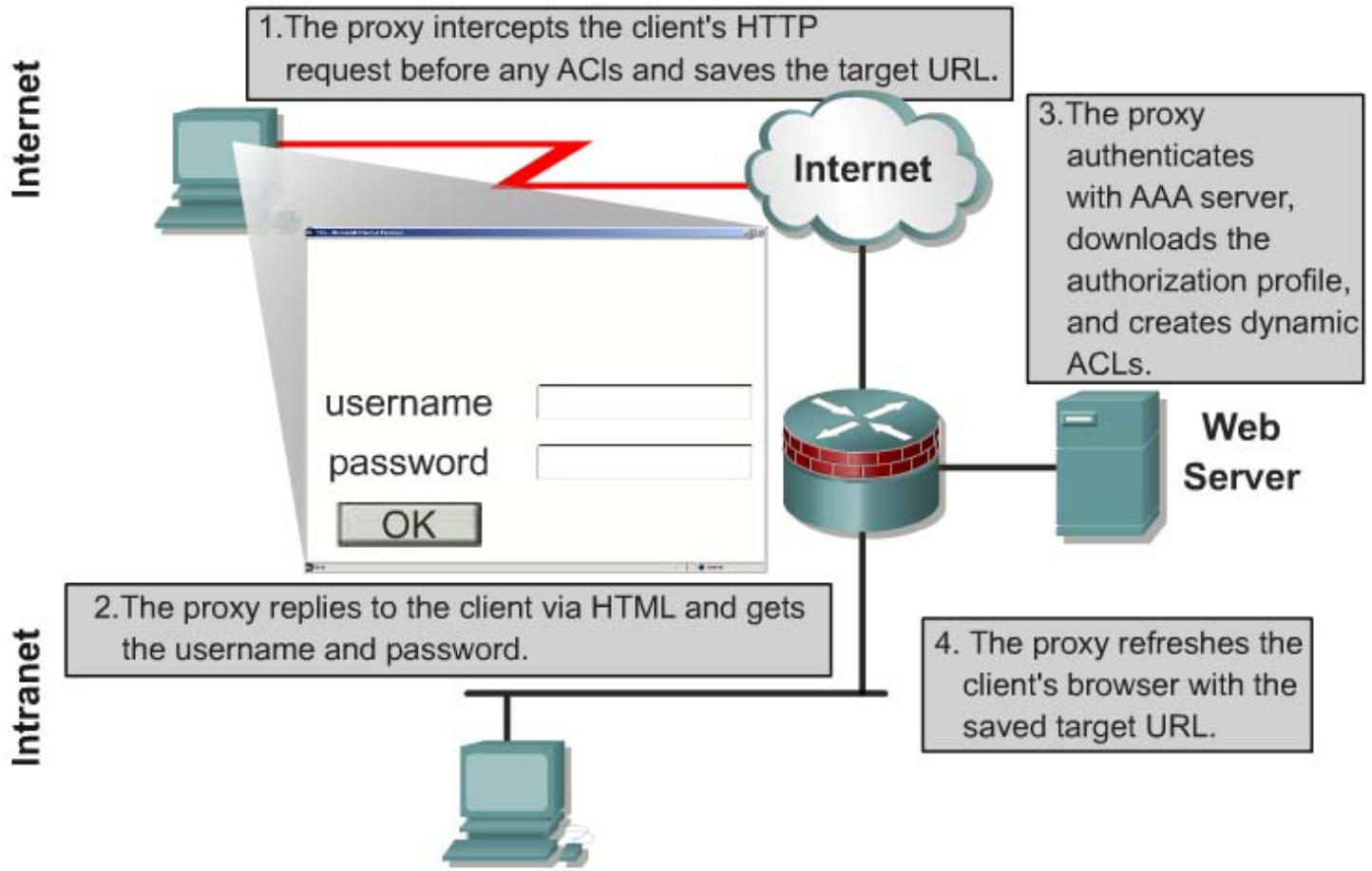
Co to jest Authentication Proxy ?

- Uwierzytelnienie bazujące na HTTP
- Zapewnia dynamiczne uwierzytelnienie i autoryzacje za pomocą protokołu TACACS+ i RADIUS
- Upoważnienie dla wszystkiego rodzaju ruchu sieciowego dla wszystkich plikacjiDziała na wszystkich typach interfejsów i ruch zarówno wychodzącego jak i przychodzącego
- Nie obsługuje AAA

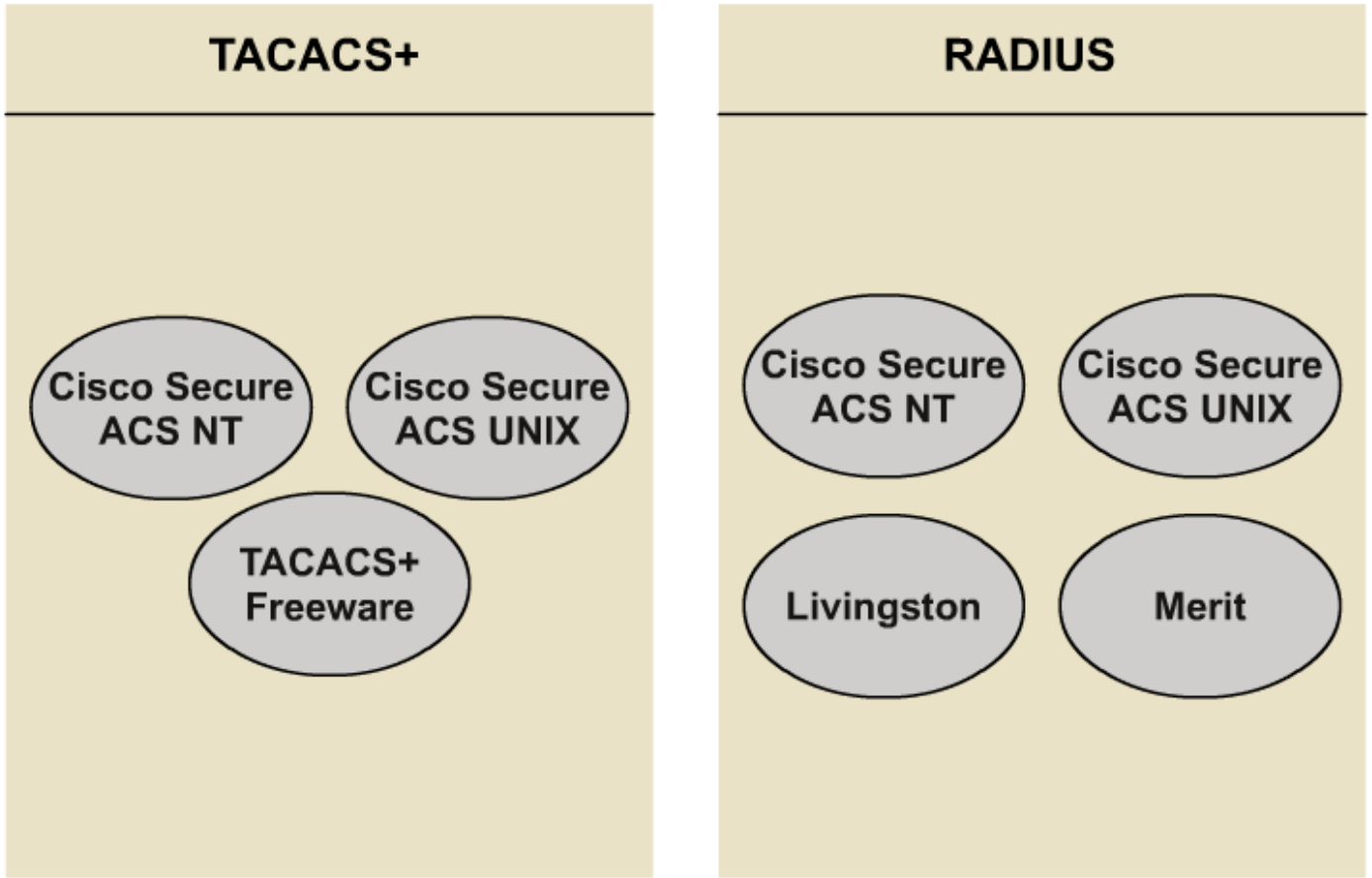
Co widzi użytkownik ?



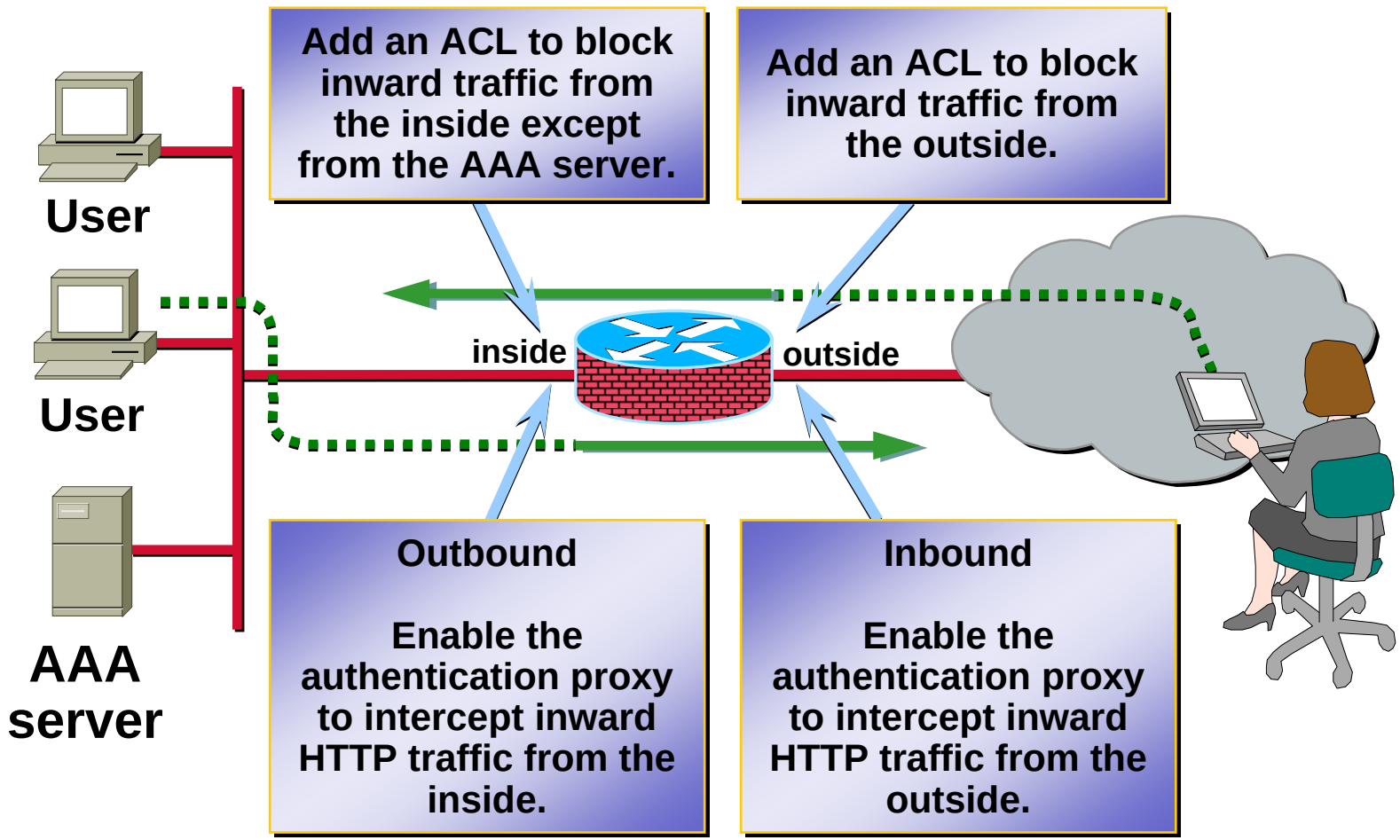
Działanie Authentication Proxy



Obsługiwane AAA Servers



Konfiguracja Authentication Proxy



Configuration Tasks

- Task 1—Configure the AAA server (CSACS).
- Task 2—Configure AAA on the router.
  - Enable AAA.
  - Specify AAA protocols.
  - Define AAA servers.
  - Allow AAA traffic.
  - Enable the router's HTTP server for AAA.
- Task 3—Authenticate the proxy configuration on the router.
  - Set the default idle time.
  - Create and apply authentication proxy rules.
- Task 4—Verify the configuration.

Wykład 4

KONIEC