



**Akademia Górniczo-Hutnicza
im. Stanisława Staszica w Krakowie**

Urządzenia Teleinformatyki:

Ograniczanie ruchu sieciowego za pomocą list ACL

Wstęp

Czym jest ACL?

Access Control List, w skrócie ACL, służy do ograniczania ruchu sieciowego. W skrócie można powiedzieć, że jej działanie przypomina trochę Firewall. Dla Standard ACL polega to na tworzeniu w Routerach list adresów źródłowych IP, które chcemy przepuszczać lub blokować. Istnieje również Extended ACL, która umożliwia nam przepuszczanie lub blokowanie nie tylko źródłowego IP, lecz również docelowego IP a także portów (serwisów sieciowych).

Aby utworzyć ACL, musimy nadać jej numer. Zgodnie z przyjętą konwencją:

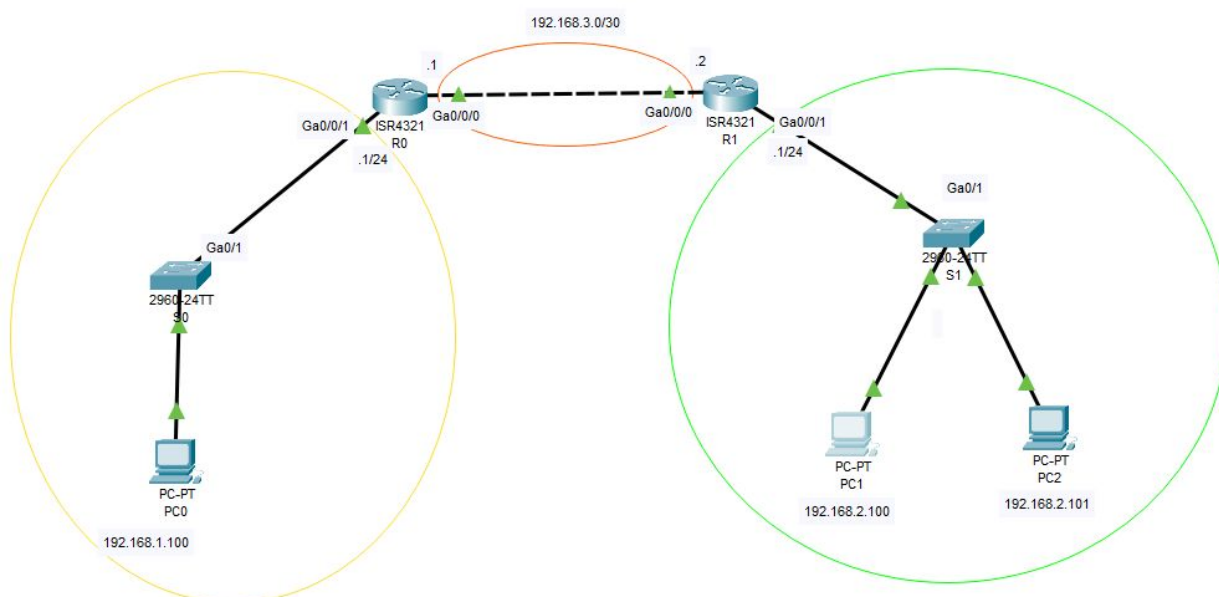
Protokół	Zakres
Standard ACL	1-99, 1300-1999
Extended ACL	100-199, 2000-2699

Przydatne do Ext. ACL mogą okazać się numery portów odpowiadające danym serwisom:

- Telnet - TCP 23,
- FTP - TCP 21,
- www - TCP 80,
- SNMP - UDP 161,
- DNS - TCP/UDP 53,
- SMTP - TCP 25,
- TFTP - UDP 69,
- RIP - UDP 520,
- BGP - TCP/UDP 179,
- SSH - TCP/UDP 22
- HTTPS - TCP/UDP 443.

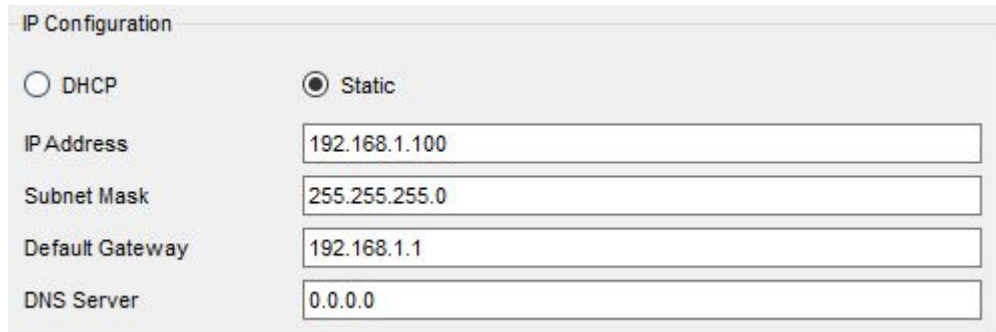
Tworzenie topologii ćwiczeniowej

Jako pierwsza topologia zostanie skonfigurowana sieć z trzema podsieciami. Dwie z PC i jedna pomiędzy routerami. Propozycja adresów klasy C. Schemat sieci:



rys. 1. Przykład sieci

Na początek należy ustawić IP, maskę i gateway dla PC. W tym celu klikamy na ikonę PC i w zakładce Desktop → IP Configuration.



IP Configuration	
<input type="radio"/> DHCP	<input checked="" type="radio"/> Static
IP Address	192.168.1.100
Subnet Mask	255.255.255.0
Default Gateway	192.168.1.1
DNS Server	0.0.0.0

rys. 2. Przykład IP dla PC0

- Konfiguracja Routerów zgodnie z przyjętą adresacją:

```
R1>en
R1#conf t
R1(config)#interface gigabitEthernet 0/0/X
R1(config-if)#ip addr aaa.aaa.aaa.aaa mmm.mmm.mmm.mmm
R1(config-if)#no sh
```

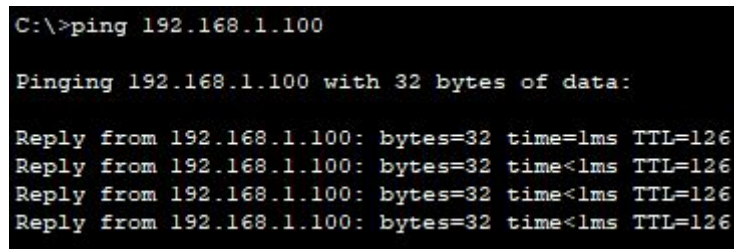
- Ustawienie tras statycznych na każdym z Routerów:

```
R0(config)#ip route 192.168.2.0 255.255.255.0 192.168.3.2
R1(config)#ip route 192.168.1.0 255.255.255.0 192.168.3.1
```

- Na tym etapie należy sprawdzić czy PC pingują się nawzajem.

W tym celu w Desktop odpalamy Command Prompt i wpisujemy polecenie
>ping aaa.aaa.aaa.aaa

Powinniśmy zaobserwować poniższy rezultat (możliwe, że pierwsze dwie próby połączenia skończą się niepowodzeniem i komunikatem "Request timed out."):



```
C:\>ping 192.168.1.100

Pinging 192.168.1.100 with 32 bytes of data:

Reply from 192.168.1.100: bytes=32 time<1ms TTL=126
Reply from 192.168.1.100: bytes=32 time<1ms TTL=126
Reply from 192.168.1.100: bytes=32 time<1ms TTL=126
Reply from 192.168.1.100: bytes=32 time<1ms TTL=126
```

rys. 3. Odpowiedź na polecenie ping

Konfiguracja ACL

- Zasady tworzenia ACL

Standard ACL tworzymy na porcie routera **najbliżej podsieci docelowej**

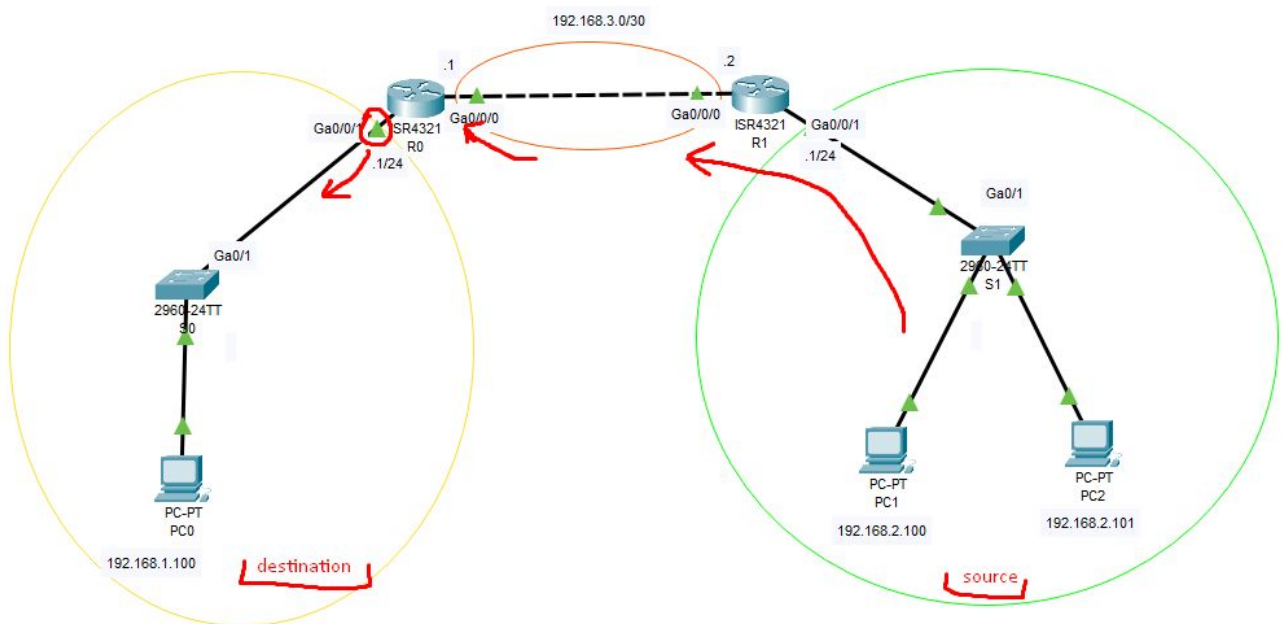
Extended ACL tworzymy na porcie routera **najbliżej podsieci źródłowej**

Powiedzmy, że chcemy utworzyć ACL, która będzie blokowała ruch przychodzący z PC2 do PC1.

Co potrzebujemy wiedzieć zanim przystąpimy do konfiguracji?

1. Standard czy extended?
Blokujemy tylko IP źródłowe, więc starczy nam **Standard**
2. Jaki numer listy?
Standard, czyli dowolna z zakresu **1-99**
3. Na jakim porcie?
Najbliżej podsieci docelowej, czyli u nas port **Ga0/0/1 w routerze R0**
4. Jaki kierunek ruchu?
Ruch "wlatuje" do routera na ga0/0/0 i "wylatuje" do podsieci z ga0/0/1. Jeżeli chcemy mieć najbliżej docelowych, to będzie to ga0/0/1, czyli **outbound**.

Możemy więc zmodyfikować nasz poglądowy schemat:



rys. 4. Kierunek przepływu pakietów

- Tworzenie listy

`R0(config)#access-list 1 deny 192.168.2.101 0.0.0.0` (lub `deny host 192.168.2.101`)

`R0(config)#access-list 1 permit any`

po wpisaniu `show run` możemy zobaczyć stworzoną przez nas ACL-kę:

```

!
access-list 1 deny host 192.168.2.101
access-list 1 permit any
! deny any
!
!

```

rys. 5. Początkowa konfiguracja ACL

Jak można zauważyć, dopisałem na końcu zasadę “deny any”. Nie jest to widoczne w konfiguracji, jednak każda ACL ma domyślnie na końcu taką właśnie zasadę. W związku z tym nasza konfiguracja może też wyglądać tak:

```
R0(config)#access-list 1 permit 192.168.2.101 0.0.0.0
```

- Przypisanie listy do interfejsu

Lista została stworzona na routerze, jednak należy jeszcze “powiedzieć” interfejsowi, że musi z niej korzystać.

W tym celu wykonujemy komendy:

```
R0(config)#interface GigabitEthernet 0/0/1
R0(config-if)#ip access-group 1 out           // out bo outbound
```

Możemy sprawdzić konfigurację portu:

```

interface GigabitEthernet0/0/1
ip address 192.168.1.1 255.255.255.0
ip access-group 1 out
duplex auto
speed auto

```

rys. 6. ACL przypisana do portu

Sprawdzamy czy nasza ACL działa poprzez pingowanie PC0 z PC2.

```

C:\>ping 192.168.1.100

Pinging 192.168.1.100 with 32 bytes of data:

Reply from 192.168.3.1: Destination host unreachable.
Reply from 192.168.3.1: Destination host unreachable.
Reply from 192.168.3.1: Destination host unreachable.
Reply from 192.168.3.1: Destination host unreachable.

```

rys. 7. Test działania ACL

Jeżeli wszystko działa, możemy przejść dalej.

- Dodawanie zasad do ACL

Przypomnijmy, że nasza ACL wygląda następująco:

```
access-list 1 deny 192.168.2.101 0.0.0.0
access-list 1 permit any
```

Ćw. 1 Dodaj do sieci źródłowej trzeci PC, zmodyfikuj ACL tak, aby blokowała również ruch z PC2. Przetestuj działanie utworzonej ACL. Czy wszystko działa tak jak powinno?

Po wykonaniu ćwiczenia, ACL powinna wyglądać tak:

```
!
access-list 1 deny host 192.168.2.101
access-list 1 permit any
access-list 1 deny host 192.168.1.102
!
```

rys. 7. ACL po ćw. 1

Skoro reguła została dodana, dlaczego ruch cały czas przechodzi?

Otóż ACL sprawdza reguły “od góry do dołu”, czyli po kolei

1. Czy ruch przychodzi z .101? Nie, czyli kolejna reguła
2. Czy jest to dowolny adres (any)? Tak

Jak widać druga reguła spełnia warunki, więc ACL nie przeszukuje listy dalej.

- Usuwanie ACL

Aby usunąć ACL, należy usunąć ją z routera i osobno z interfejsu na którym jest przypisana.

```
R0(config)#no access-list 1
R0(config)#interface gigabitEthernet 0/0/1
R0(config-if)#no ip access-group 1 out
```

Ćw. 2 Stwórz nową ACL, która będzie blokowała ruch z PC1 i PC2 na PC0. Przetestuj poleceniem ping, czy wszystko działa zgodnie z założeniami.

rozwiązanie:

```
R0(config)#access-list 2 deny host 192.168.2.100
R0(config)#access-list 2 deny host 192.168.2.101
R0(config)#access-list 2 permit any
R0(config)#interface gigabitEthernet 0/0/1
R0(config-if)#ip access-group 2 out
```

Ćw. 3 Stwórz nową **Extended** ACL blokującą ruch z PC1 i PC2 na PC0. Przetestuj poleceniem ping, czy wszystko działa zgodnie z założeniami.

Podpowiedź:

```
Rx(config)# access-list access_list_number (deny/permit) protocol source_IP  
source_IP_wildcard dest_IP dest_IP_wildcard
```

rozwiązanie:

```
R1(config)#access-list 100 deny ip 192.168.2.100 0.0.0.0 192.168.1.0 0.0.0.255  
R1(config)#access-list 100 deny ip 192.168.2.101 0.0.0.0 192.168.1.0 0.0.0.255  
R1(config)#access-list 100 permit ip any any  
R1(config)#interface gigabitEthernet 0/0/1  
R1(config-if)#ip access-group 100 in
```

Ćw. 4 Do podsieci .1.X dodaj serwer o dowolnym adresie. Skonfiguruj ACL tak, aby PC z podsieci .2.X miały dostęp tcp do serwera ale nie do PC w podsieci .1.X.
Aby sprawdzić, przez PC z .2.X wejdź w Web Browser i wpisz adres serwera.
W Command Prompt komenda ping nie powinna działać (Destination host unreachable.)

rozwiązanie:

```
R1(config)#access-list 100 permit tcp 192.168.2.0 0.0.0.255 host 192.168.1.101 eq 80  
R1(config)#interface gigabitEthernet 0/0/1  
R1(config-if)#ip access-group 100 in
```

eq → equal, numer portu

