Wykład 1: Listy kontroli dostępu ACL

Routing & Switching

Cisco | Networking Academy®
Mind Wide Open™

Wykład 1

1.1 Działanie IP ACL

1.2 Standardowe listy ACL IPv4

1.3 Rozszerzone listy ACL IPv4

1.4 Przetwarzanie pakietów za pomocą list ACL

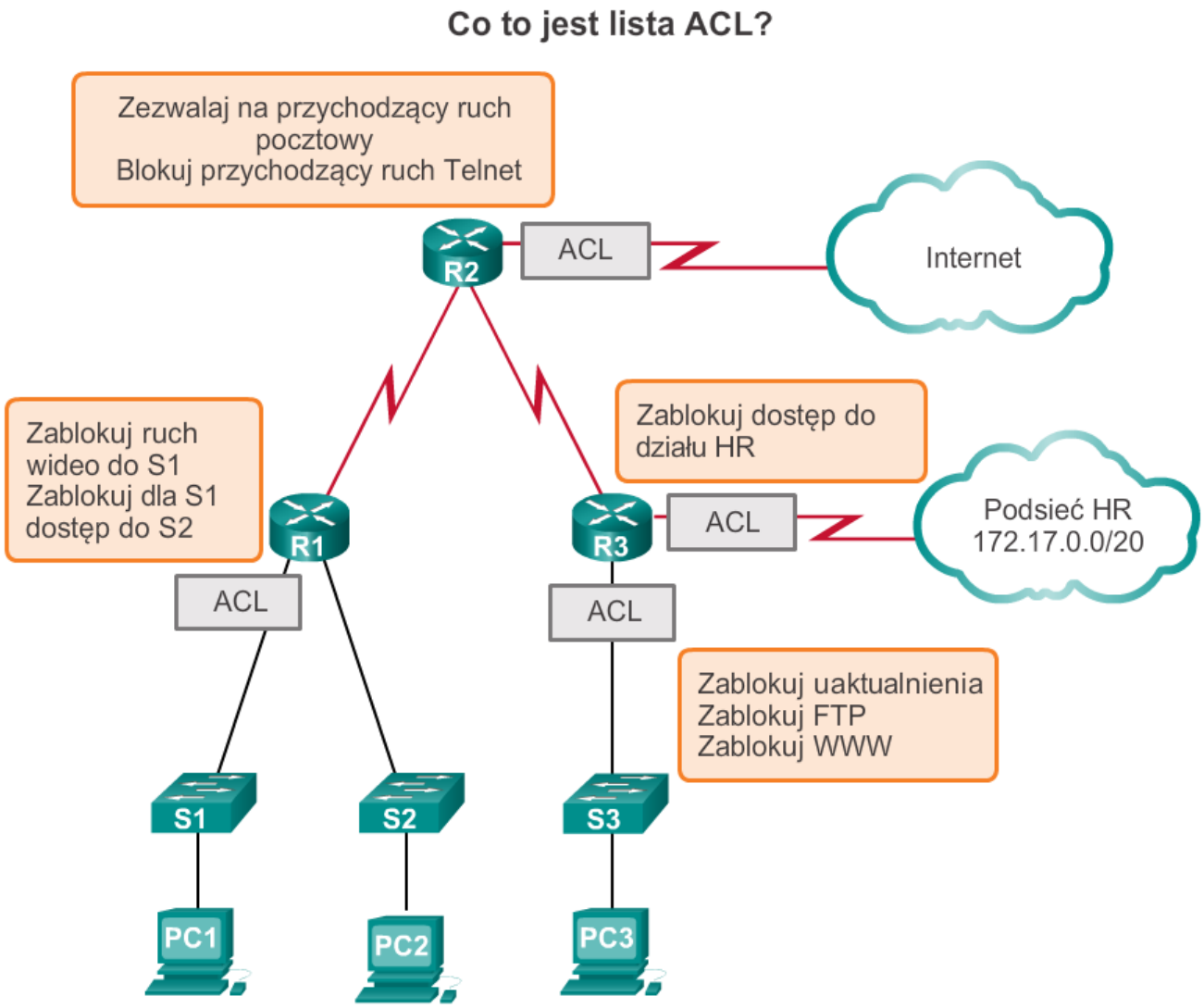
1.5 Rozwiązywanie problemów z listami ACL

1.6 Listy ACL IPv6

1.7 Podsumowanie

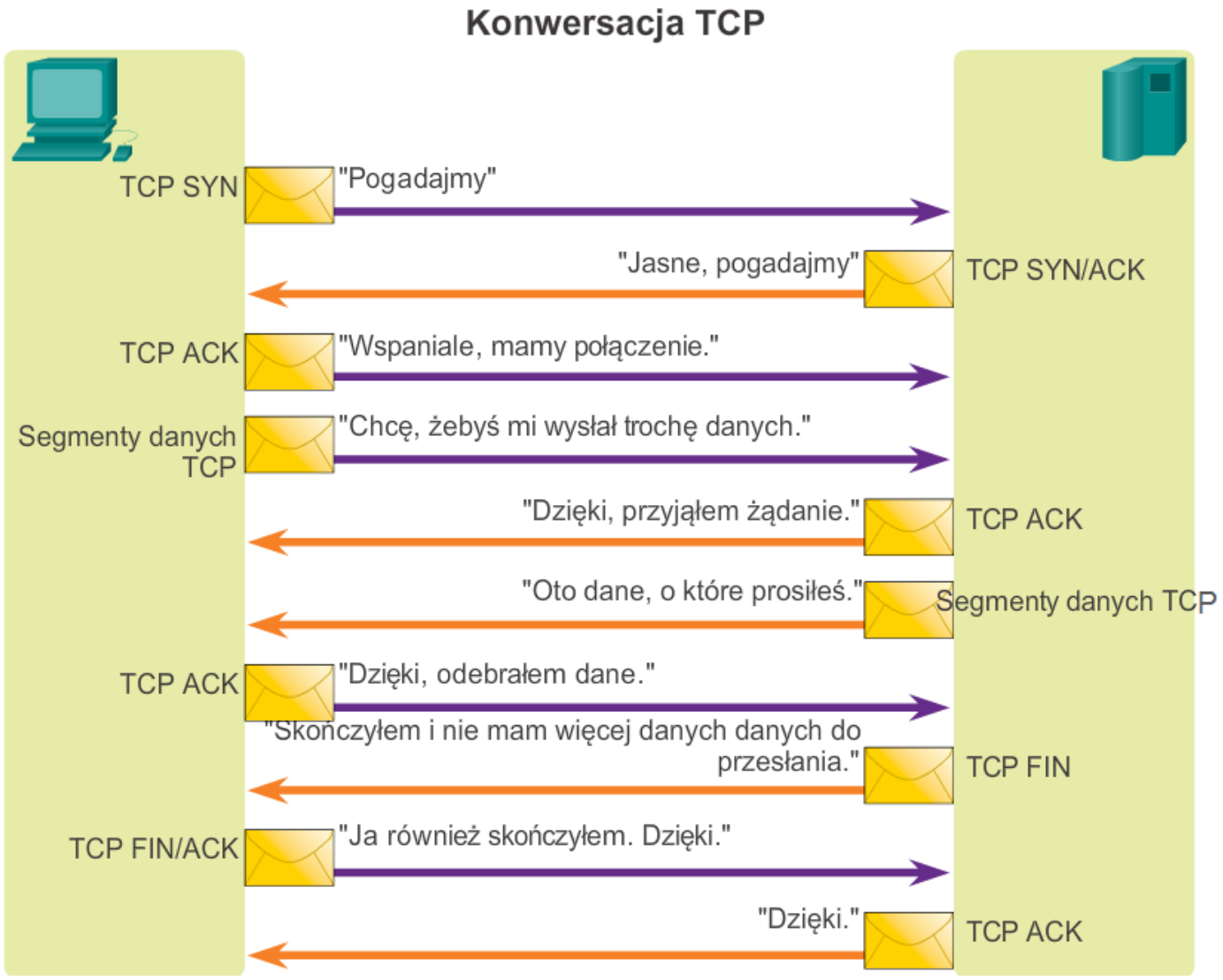
Rola list ACL

Czym jest lista ACL?



Rola list ACL

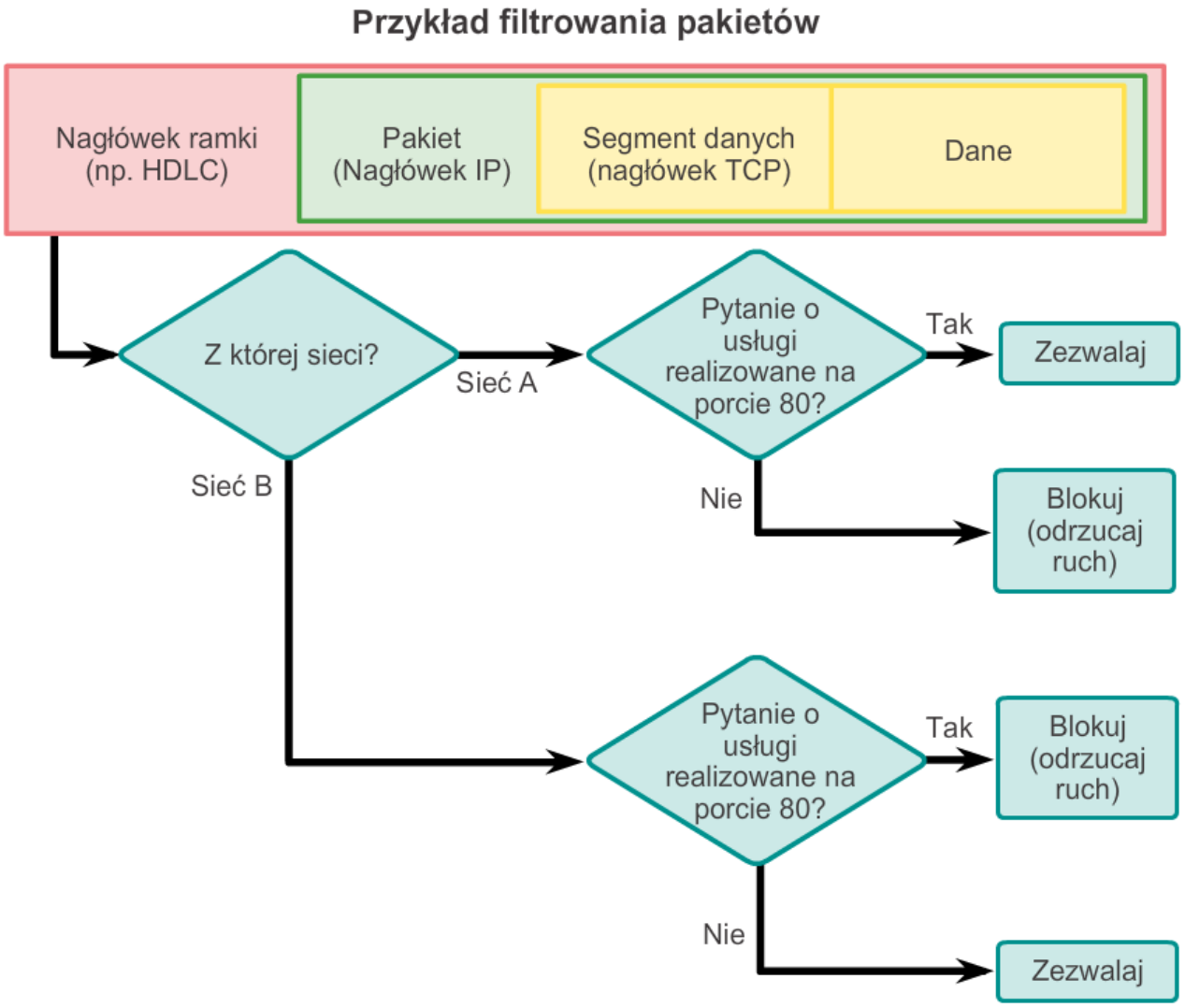
Konwersacja TCP



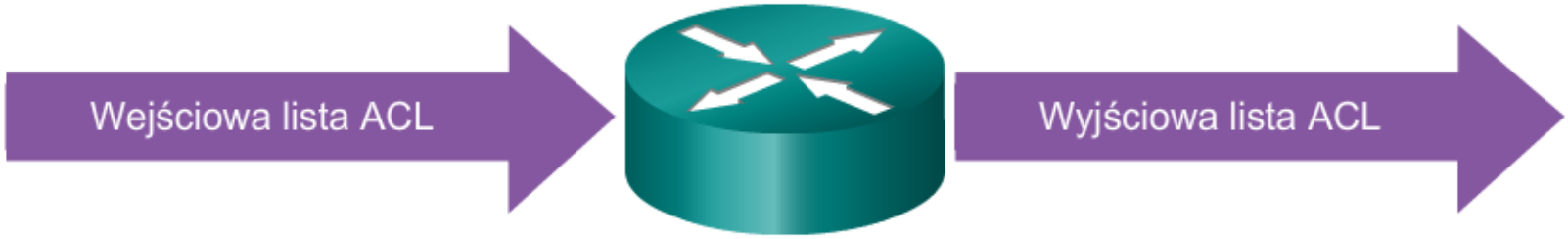
Filtrowanie pakietów

- Filtrowanie pakietów, zwane też statycznym filtrowaniem pakietów, zapewnia kontrolę dostępu do sieci poprzez analizę pakietów wchodzących i wychodzących a następnie przepuszczanie lub blokowanie ich na podstawie zadanych kryteriów, takich jak np. adres źródłowy IP, docelowy adres IP czy protokół.
- Rolę filtra pakietów spełnia router, którego zadaniem jest przepuszczanie lub odrzucanie ruchu na podstawie ustalonych reguł.
- ACL to sekwencyjna lista komend zezwalających lub odmawiających, zwanych wpisami kontroli dostępu (ACE).

Filtrowanie pakietów (cd.)



Operacja ACL



Wejściowa lista ACL filtruje pakiety docierające do routera na określonym interfejsie, zanim zostaną wysłane do procesu routingu a potem do interfejsu wyjściowego.

Wyjściowa lista ACL filtruje pakiety wychodzące, po przetworzeniu ich w procesie routingu, niezależnie od użytego interfejsu wejściowego.

Na końcu każdej listy ACL umieszczona jest niejawna odmowa. Wpis ten jest automatycznie dodawany na końcu każdej listy ACL nawet wówczas, gdy nie został jawnie ustawiony.

Niejawna odmowa powoduje odrzucenie całego ruchu. Z tego powodu listy ACL, które nie posiadają co najmniej jednej reguły, będą blokować cały przechodzący przez nie ruch.

Rodzaje list Cisco ACL IPv4

Standardowe listy ACL

```
access-list 10 permit 192.168.30.0 0.0.0.255
```

Standardowe listy ACL filtrują pakiety IP tylko w oparciu o adres źródłowy.

Rozszerzone listy ACL

```
access-list 103 permit tcp 192.168.30.0 0.0.0.255 any eq 80
```

Rozszerzone listy ACL filtrują pakiety IP na podstawie kilku atrybutów, takich jak:

- adresy IP źródłowe i docelowe,
- źródłowe i docelowe porty TCP i UDP,
- typ protokołu (numer protokołu) (na przykład: IP, ICMP, UDP, TCP, itp.).

Porównanie standardowych i rozszerzonych list ACL IPv4

Numeracja i nazewnictwo list ACL

Numerowana lista ACL:

Przypisz numer na podstawie protokołu, względem którego będzie wykonywane filtrowanie:

- (od 1 do 99) i (od 1300 do 1999): standardowa lista IP ACL,
- (od 100 do 199) i (od 2000 do 2699): rozszerzona lista IP ACL.

Nazywana lista ACL:

Przypisz nazwę w celu identyfikowania listy ACL:

- nazwy mogą zawierać znaki alfanumeryczne,
- sugeruje się, aby nazwę pisać WIELKIMI LITERAMI,
- nazwy nie mogą zawierać spacji ani znaków interpunkcyjnych,
- wewnątrz listy ACL wpisy mogą być dodawane lub usuwane.

Wprowadzenie do masek blankietowych w listach ACL

Maski blankietowe oraz maski podsieci różnią się sposobem, w jaki osiągane jest dopasowanie bitów 1 i 0. Reguły dopasowania masek blankietowych są następujące:

- Bit 0 maski blankietowej - dopasowanie odpowiadającego bitu adresu IP.
- Bit 1 maski blankietowej - zignorowanie odpowiadającego bitu adresu IP.

Maski blankietowe są często określane jako maski odwrotne (ang. inverse mask). Powodem jest fakt, że w przeciwieństwie do maski podsieci, gdzie bit 1 oznaczał dopasowanie a bit 0 brak dopasowania, w masce blankietowej sytuacja jest odwrotna.

Maski blankietowe w listach ACL

Przykłady masek blankietowych Hosty/Podsieci

Stosowanie masek blankietowych (wieloznacznych) w celu dopasowywania do hostów i podsieci IPv4

Przykład 1

	Adres dziesiętny	Adres binarny
Adres IP	192.168.1.1	11000000.10101000.00000001.00000001
Maska blankietowa (wieloznaczna)	0.0.0.0	00000000.00000000.00000000.00000000
Wynik	192.168.1.1	11000000.10101000.00000001.00000001

Przykład 2

	Adres dziesiętny	Adres binarny
Adres IP	192.168.1.1	11000000.10101000.00000001.00000001
Maska blankietowa (wieloznaczna)	255.255.255.255	11111111.11111111.11111111.11111111
Wynik	0.0.0.0	00000000.00000000.00000000.00000000

Przykład 3

	Adres dziesiętny	Adres binarny
Adres IP	192.168.1.1	11000000.10101000.00000001.00000001
Maska blankietowa (wieloznaczna)	0.0.0.255	00000000.00000000.00000000.11111111
Wynik	192.168.1.0	11000000.10101000.00000001.00000000

Przykłady masek blankietowych
Zakres przyporządkowania

Example 1

	Decimal	Binary
IP Address	192.168.16.0	11000000.10101000.00010000.00000000
Wildcard Mask	0.0.15.255	00000000.00000000.00001111.11111111
Result Range	192.168.16.0 to 192.168.31.255	11000000.10101000.00010000.00000000 to 11000000.10101000.00011111.11111111

Example 2

	Decimal	Binary
IP Address	192.168.1.0	11000000.10101000.00000001.00000000
Wildcard Mask	0.0.254.255	00000000.00000000.11111110.11111111
Result	192.168.1.0	11000000.10101000.00000001.00000000
	All odd numbered subnets in the 192.168.0.0 major network	

Obliczanie masek blankietowych

Obliczanie maski blankietowej może być nie lada wyzwaniem. Najszybszą metodą jest po prostu wykonanie odejmowania maski podsieci od pełnej maski 255.255.255.255.

Przykład 1

	255.255.255.255
-	255.255.255.000
	000.000.000.255

Przykład 2

	255.255.255.255
-	255.255.255.240
	000.000.000.015

Przykład 3

	255.255.255.255
-	255.255.254.000
	000.000.001.255

Maski blankietowe w listach ACL

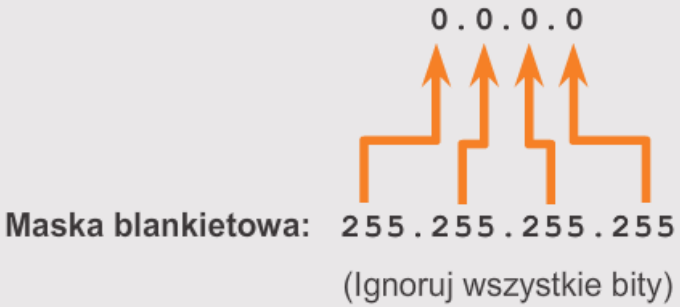
Słowa kluczowe dla masek blankietowych

Przykład 1

- 192.168.10.10 0.0.0.0 oznacza zgodność ze wszystkimi bitami adresu
- Maskę blankietową można skrócić, poprzedzając adres IP słowem kluczowym **`host`** (**`host 192.168.10.10`**)

Przykład 2

- 0.0.0.0 255.255.255.255 ignoruje wszystkie bity w adresie
- skracamy to wyrażenie za pomocą słowa kluczowego **`any`**



Przykłady użycia słów kluczowych dla masek blankietowych

Przykład 1:

```
R1(config)# access-list 1 permit 0.0.0.0 255.255.255.255
R1(config)# access-list 1 permit any
```

Przykład 2:

```
R1(config)# access-list 1 permit 192.168.10.10 0.0.0.0
R1(config)# access-list 1 permit host 192.168.10.10
```

Ogólne wytyczne dotyczące tworzenia list ACL

- Używamy list ACL na routerach pełniących funkcję zapory sieciowej, pomiędzy siecią wewnętrzną a zewnętrzną taką jak np. Internet.
- Używamy list ACL na routerach umieszczonych pomiędzy dwoma częściami własnej sieci, aby kontrolować ruch pomiędzy wybranymi segmentami sieci wewnętrznej.
- Listy ACL powinny być też definiowane na routerach brzegowych, czyli routerach znajdujących się na granicach twoich sieci.
- Definiujemy listy ACL dla każdego protokołu sieciowego skonfigurowanego na interfejsach routera brzegowego.

Ogólne wytyczne dotyczące tworzenia list ACL (cd.)

Zasada trzy N

- Jedna lista ACL na protokół - Aby kontrolować przepływ ruchu na interfejsie, należy zdefiniować listę ACL dla każdego protokołu włączonego na tym interfejsie.
- Jedna lista ACL na kierunek - Jedna lista kontroli dostępu ACL kontroluje ruch na interfejsie w jednym kierunku. Aby kontrolować ruch przychodzący i wychodzący, należy utworzyć dwie oddzielne listy ACL.
- Jedna lista ACL na interfejs - Listy kontroli dostępu ACL mogą kontrolować ruch na wybranym interfejsie, na przykład GigabitEthernet 0/0.

Wytyczne do tworzenia list ACL

Najlepsze praktyki

Zasada	Korzyści
Tworząc listy ACL uwzględniaj politykę bezpieczeństwa organizacji.	Zapewni to realizację podstawowych założeń dotyczących bezpieczeństwa organizacji.
Przygotuj opis akcji jakie będą wykonywane za pomocą list ACL.	Pomoże to uniknąć przypadkowego tworzenia potencjalnych problemów związanych z dostępem do sieci lub hostów.
Do tworzenia list ACL używaj edytora tekstu.	Pomoże to stworzyć bibliotekę list ACL używanych wielokrotnie.
Testuj listy ACL w sieci testowej przed zastosowaniem ich w sieci produkcyjnej.	Ta zasada pozwoli na zmniejszenie liczby błędów.

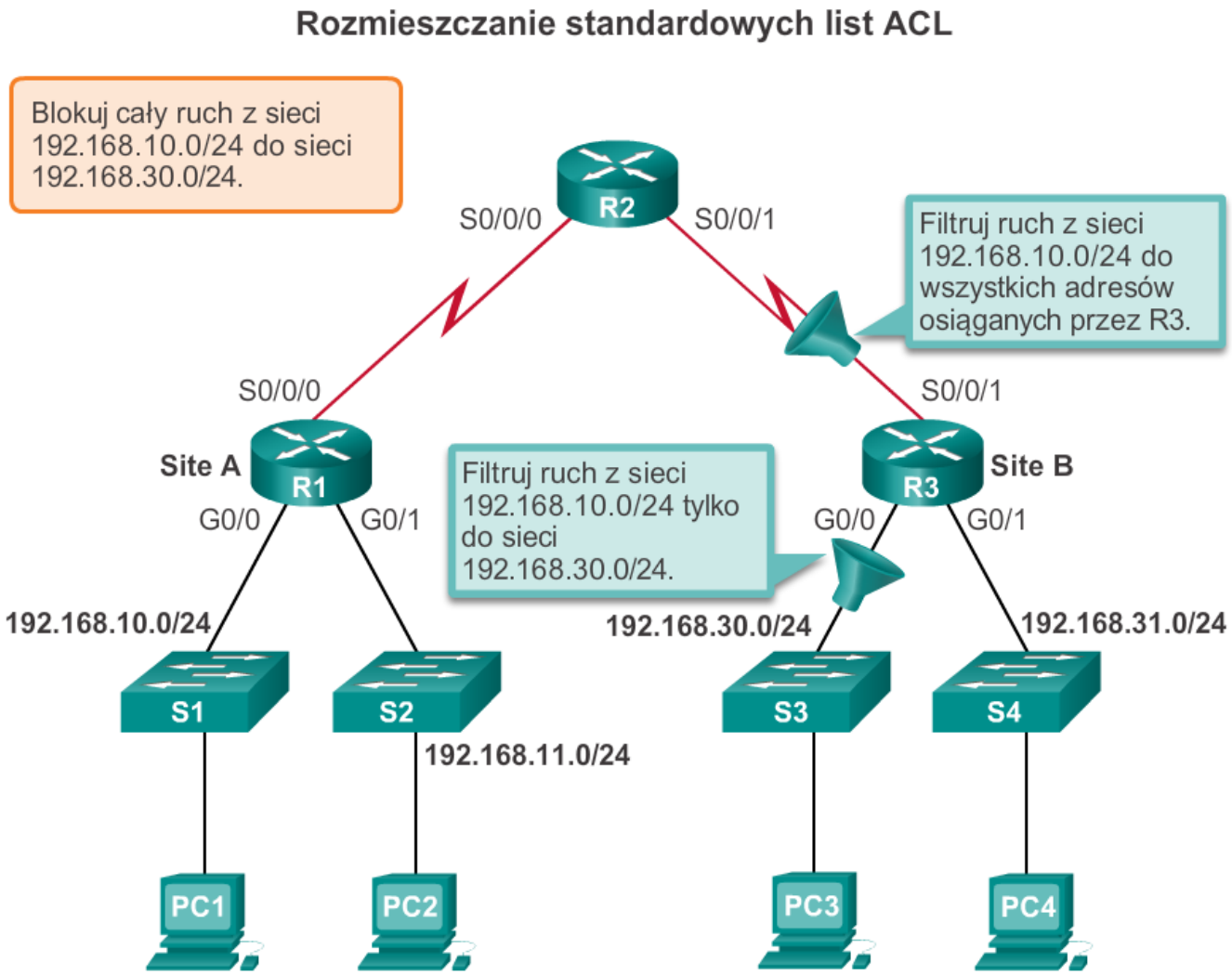
Gdzie należy umieścić listy ACL

Listy ACL należy umieszczać w miejscach, w których mają one największy wpływ na wydajność. Podstawowe reguły to:

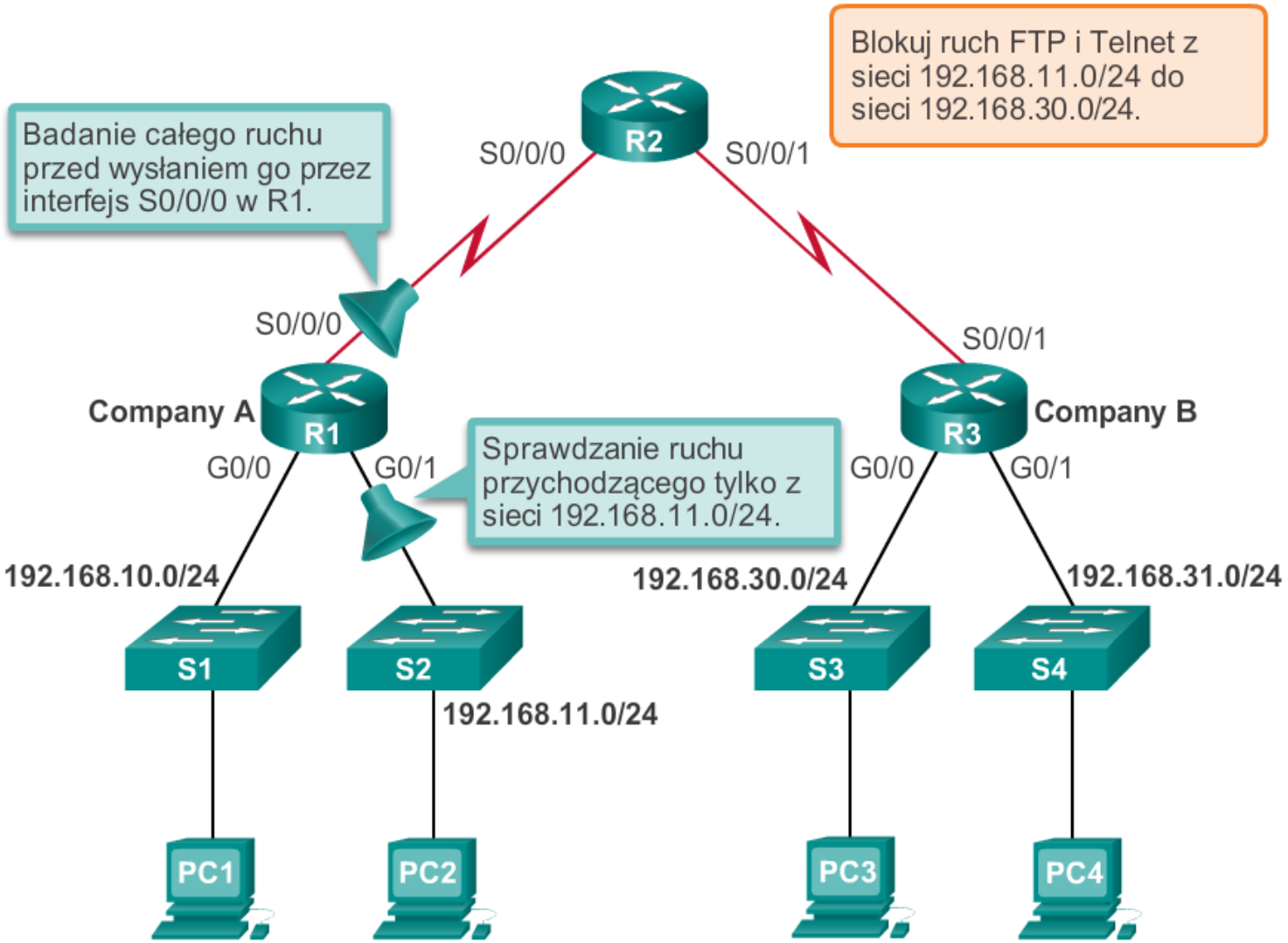
- Rozszerzone listy ACL - Umieszczamy je tak blisko źródła filtrowanego ruchu jak tylko jest to możliwe.
- Standardowe listy ACL - Ponieważ standardowe listy ACL nie uwzględniają adresów docelowych, należy umieszczać je blisko sieci docelowej.

Umieszczenie listy kontroli dostępu ACL może także zależeć od: zakresu kontroli administratora sieci, przepustowości zaangażowanych sieci i łatwości konfiguracji.

Rozmieszczanie standardowych list ACL

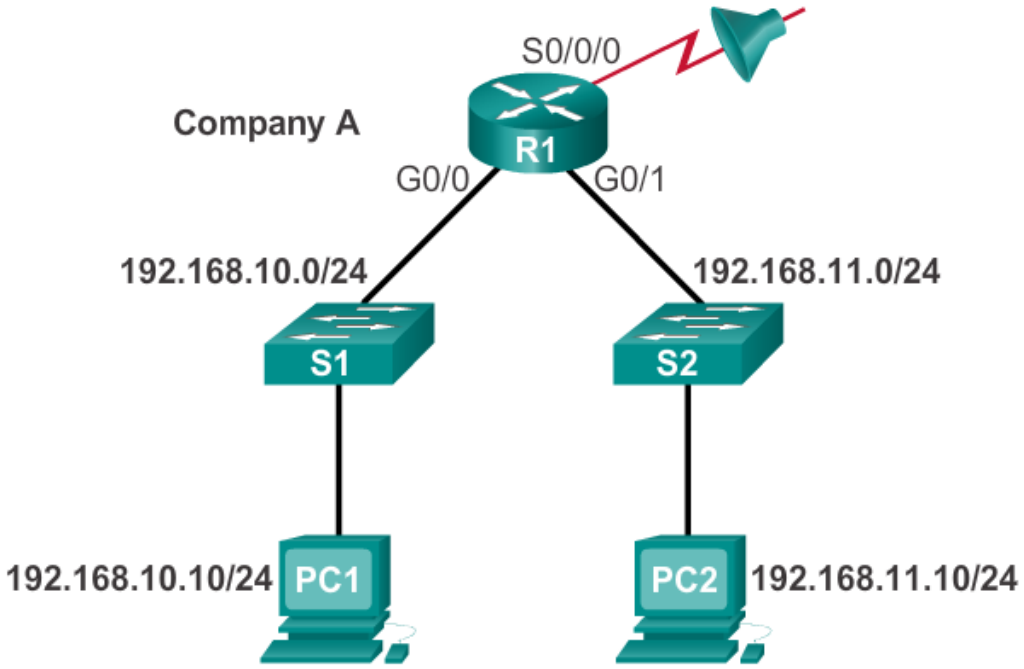


Rozmieszczanie rozszerzonych list ACL



Konfigurowanie standardowych list ACL IPv4

Wprowadzenie do kryteriów reguł



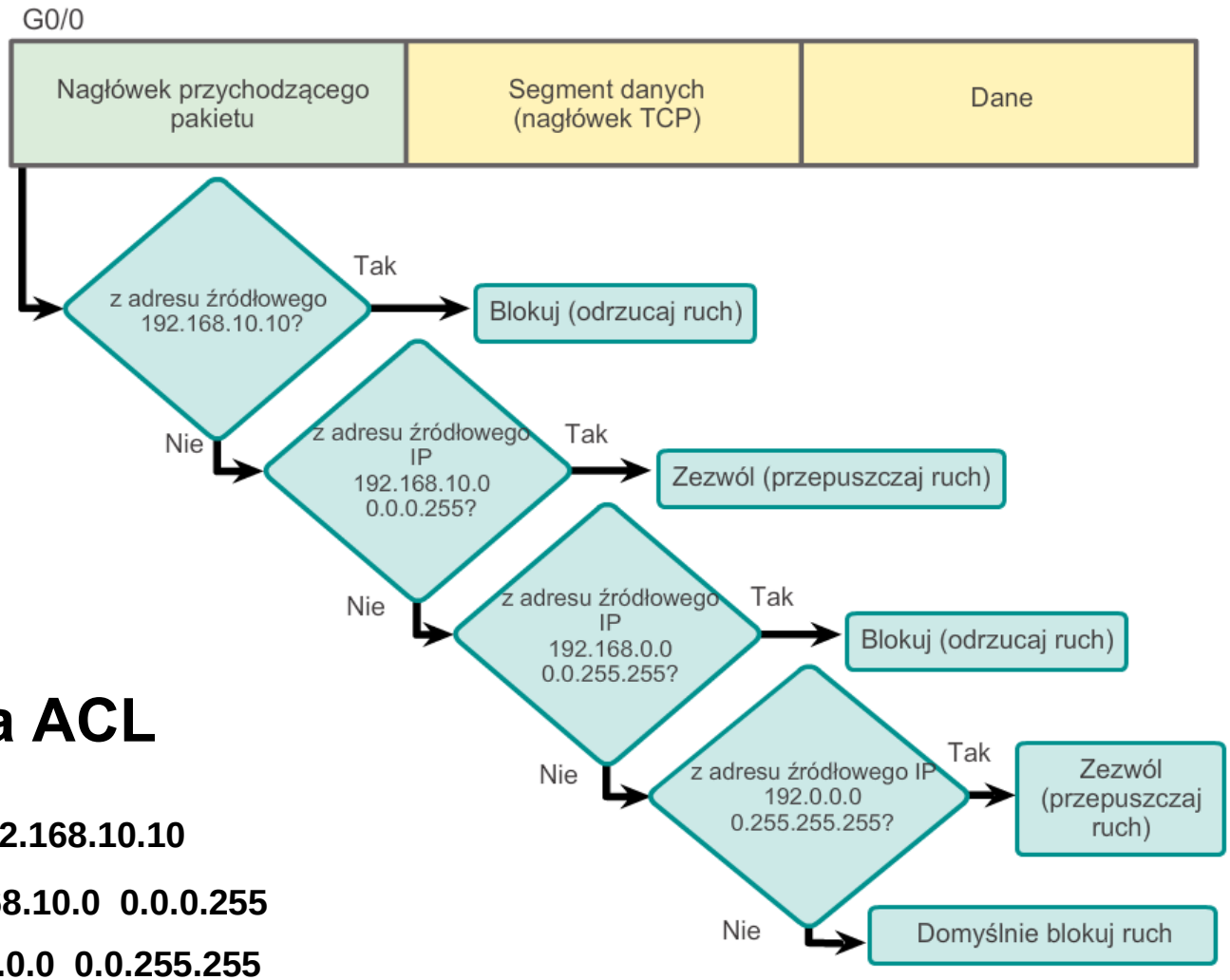
ACL 1

```
R1(config)# access-list 1 permit ip 192.168.10.0 0.0.0.255
```

ACL 2

```
R1(config)# access-list 2 permit ip 192.168.10.0 0.0.0.255
R1(config)# access-list 2 deny any
```

Konfiguracja standardowej listy ACL



Przykładowa lista ACL

- **access-list 2 deny host 192.168.10.10**
- **access-list 2 permit 192.168.10.0 0.0.0.255**
- **access-list 2 deny 192.168.0.0 0.0.255.255**
- **access-list 2 permit 192.0.0.0 0.255.255.255**

Konfiguracja standardowej listy ACL (cd.)

Pełna składnia dla standardowej listy ACL jest następująca:

Router(config)# **access-list** *numer-listy-dostępu* {**deny | permit remark}** *źródło* [*maska-blankietowa-źródła*] [**log**]

Aby usunąć listę ACL, należy użyć polecenia konfiguracji globalnej **no access-list**.

Polecenie **remark** służy do dokumentacji i sprawia, że lista dostępu jest o wiele łatwiejsza do zrozumienia.

Logika wewnętrzna

- Cisco IOS stosuje wewnętrzną logikę podczas przyjmowania i przetwarzania standardowych poleceń listy dostępu. Jak omówiono poprzednio, polecenia listy dostępu są przetwarzane sekwencyjnie. Dlatego tak ważna jest kolejność, w której wprowadzane są polecenia.

```
R1(config)# access-list 3 deny 192.168.10.0 0.0.0.255
R1(config)# access-list 3 permit host 192.168.10.10
% Access rule can't be configured at higher sequence num as
it is part of the existing rule at sequence num 10
R1(config)#
```

ACL 3: Wpis określający hosta koliduje z wcześniejszym wpisem określającym zakres adresów.

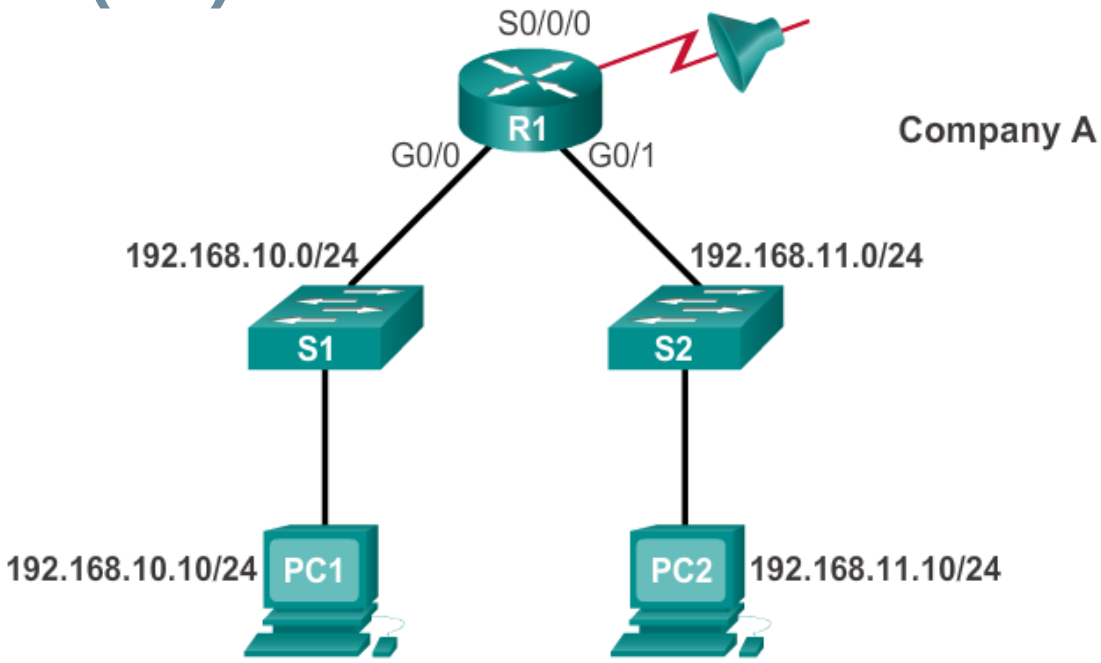
Przypisywanie standardowych list ACL do interfejsów

Gdy skonfigurowana jest standardowa lista ACL, jest przypisana do interfejsu za pomocą polecenia **ip access-group** w trybie konfiguracji globalnej:

Router(config-if)# **ip access-group** { *numer-listy-dostępu* | *nazwa-listy-dostępu* } { **in** | **out** }

Aby usunąć listę ACL z interfejsu, należy najpierw wpisać na interfejsie polecenie **no ip access-group**, a następnie wpisać polecenie globalne **no access-list**, aby usunąć całą listę ACL.

Przypisywanie standardowych list ACL do interfejsów (cd.)




```
R1(config)# no access-list 1
R1(config)# access-list 1 deny host 192.168.10.10
R1(config)# access-list 1 permit 192.168.10.0 0.0.0.255
R1(config)# interface s0/0/0
R1(config-if)# ip access-group 1 out
```

Tworzenie nazywanych standardowych list ACL

```
Router(config)# ip access-list [standard | extended] name
```

Nazwa w postaci łańcucha alfanumerycznego musi być unikatowa i nie może zaczynać się od cyfry.

```
Router(config-std-nacl)# [permit | deny | remark] {source
[source-wildcard]} [log]
```

```
Router(config-if)# ip access-group name [in | out]
```

Przypisywanie nazywanej listy ACL do interfejsu.

Konfiguracja standardowych list ACL IPv4

Komentowanie list ACL

Przykład 1: Tworzenie komentarzy dla numerowanej listy ACL

```
R1(config)# access-list 1 remark Do not allow Guest workstation
through
R1(config)# access-list 1 deny host 192.168.10.10
R1(config)# access-list 1 remark Allow devices from all other
192.168.x.x subnets
R1(config)# access-list 1 permit 192.168.0.0 0.0.255.255
R1(config)# interface s0/0/0
R1(config-if)# ip access-group 1 out
R1(config-if)#
```

Przykład 2: Tworzenie komentarzy dla nazywanej listy ACL

```
R1(config)# ip access-list standard NO_ACCESS
R1(config-std-nacl)# remark Do not allow access from Lab
workstation
R1(config-std-nacl)# deny host 192.168.11.10
R1(config-std-nacl)# remark Allow access from all other networks
R1(config-std-nacl)# permit any
R1(config-std-nacl)# exit
R1(config-std-nacl)# interface G0/0
R1(config-if)# ip access-group NO_ACCESS out
R1(config-if)#
```

Edycja standardowych numerowanych list ACL

Edytowanie numerowanych list ACL za pomocą edytora tekstu

Konfiguracja

```
R1(config)# access-list 1 deny host 192.168.10.99
R1(config)# access-list 1 permit 192.168.0.0 0.0.255.255
```

Krok 1

```
R1# show running-config | include access-list 1
access-list 1 deny host 192.168.10.99
access-list 1 permit 192.168.0.0 0.0.255.255
```

Krok 2

```
<edytor tekstu>
access-list 1 deny host 192.168.10.10
access-list 1 permit 192.168.0.0 0.0.255.255
```

Krok 3

```
R1# config t
Enter configuration commands, one per line. End with CNTL/Z.
R1(config)# no access-list 1
R1(config)# access-list 1 deny host 192.168.10.10
R1(config)# access-list 1 permit 192.168.0.0 0.0.255.255
```

Krok 4

```
R1# show running-config | include access-list 1
access-list 1 deny host 192.168.10.10
access-list 1 permit 192.168.0.0 0.0.255.255
```

Edycja standardowych numerowanych list ACL (cd.)

Edytowanie numerowanych list ACL z wykorzystaniem numerów sekwencyjnych

Konfiguracja

```
R1(config)# access-list 1 deny host 192.168.10.99
R1(config)# access-list 1 permit 192.168.0.0 0.0.255.255
```

Krok 1

```
R1# show access-lists 1
Standard IP access list 1
    10 deny   192.168.10.99
    20 permit 192.168.0.0, wildcard bits 0.0.255.255
R1#
```

Krok 2

```
R1# conf t
R1(config)# ip access-list standard 1
R1(config-std-nacl)# no 10
R1(config-std-nacl)# 10 deny host 192.168.10.10
R1(config-std-nacl)# end
R1#
```

Krok 3

```
R1# show access-lists
Standard IP access list 1
    10 deny   192.168.10.10
    20 permit 192.168.0.0, wildcard bits 0.0.255.255
R1#
```

Edycja standardowych nazywanych list ACL

Wstawianie wiersza do nazywanej listy ACL

```
R1# show access-lists
Standard IP access list NO_ACCESS
    10 deny   192.168.11.10
    20 permit 192.168.11.0, wildcard bits 0.0.0.255
R1# conf t
Enter configuration commands, one per line.  End with
CNTL/Z.
R1(config)# ip access-list standard NO_ACCESS
R1(config-std-nacl)# 15 deny host 192.168.11.11
R1(config-std-nacl)# end
R1# show access-lists
Standard IP access list NO_ACCESS
    10 deny   192.168.11.10
    15 deny   192.168.11.11
    20 permit 192.168.11.0, wildcard bits 0.0.0.255
R1#
```

Uwaga: polecenie **no** *sequence-number* named-ACL używane jest do kasowania konkretnego wiersza.

Weryfikacja list ACL

```
R1# show ip interface s0/0/0
Serial0/0/0 is up, line protocol is up
  Internet address is 10.1.1.1/30
<output omitted>
  Outgoing access list is 1
  Inbound  access list is not set
<output omitted>

R1# show ip interface g0/0
GigabitEthernet0/0 is up, line protocol is up
  Internet address is 192.168.10.1/24
<output omitted>
  Outgoing access list is NO_ACCESS
  Inbound  access list is not set
<output omitted>
```

```
R1# show access-lists
Standard IP access list 1
    10 deny   192.168.10.10
    20 permit 192.168.0.0, wildcard bits 0.0.255.255
Standard IP access list NO_ACCESS
    15 deny   192.168.11.11
    10 deny   192.168.11.10
    20 permit 192.168.11.0, wildcard bits 0.0.0.255
R1#
```

Modyfikacja list ACL IPv4

Statystyki list ACL

```
R1# show access-lists
Standard IP access list 1
    10 deny   192.168.10.10 (4 match(es))
    20 permit 192.168.0.0, wildcard bits 0.0.255.255
Standard IP access list NO_ACCESS
    15 deny   192.168.11.11
    10 deny   192.168.11.10 (4 match(es))
    20 permit 192.168.11.0, wildcard bits 0.0.0.255
R1#
```

```
R1# show access-lists
Standard IP access list 1
    10 deny   192.168.10.10 (8 match(es))
    20 permit 192.168.0.0, wildcard bits 0.0.255.255
Standard IP access list NO_ACCESS
    15 deny   192.168.11.11
    10 deny   192.168.11.10 (4 match(es))
    20 permit 192.168.11.0, wildcard bits 0.0.0.255
R1#
```

Licznik dopasowania dla warunku został zwiększony.

Numery sekwencyjne w standardowej liście ACL

- Kolejna część logiki wewnętrznej IOS obejmuje wewnętrzne sekwencjonowanie standardowych poleceń ACL.
  W pierwszej kolejności skonfigurowane są wpisy blokujące trzy zakresy sieci, następnie 5 wpisów dotyczących hostów. Wpisy dotyczące hostów są prawidłowe i zostały zaakceptowane, ponieważ ich adresy IP nie należą do zakresów zdefiniowanych wcześniej.
- Polecenie **show** służy do weryfikacji listy ACL, ale niekoniecznie w kolejności, w jakiej zostały wprowadzone. Kolejność wpisów jest ustalana przez system IOS przy użyciu specjalnej funkcji hashującej. Celem jest zoptymalizowanie procesu wyszukiwania wpisów dotyczących hosta na liście poleceń ACL.

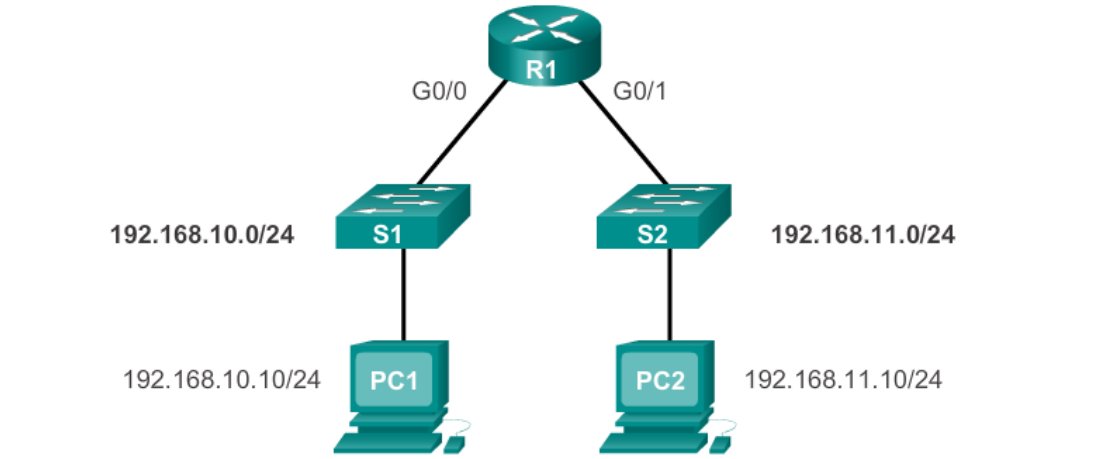
Konfigurowanie standardowej listy ACL w celu zabezpieczenia portu VTY

Filtrowanie ruchu Telnet lub SSH jest zazwyczaj domeną rozszerzonych list ACL, ponieważ podlega mu protokół wyższego poziomu. Ponieważ jednak jest użyte polecenie **access-class** do filtrowania przychodzących czy wychodzących sesji Telnet/SSH przez adres źródłowy, mogą zostać użyte standardowe listy ACL.

Router(config-line)# **access-class** *numer-listy-dostępu* { **in** [**vrf-also**] | **out** }

Weryfikacja standardowej listy ACL użytej do zabezpieczenia portu VTY

```
R1#show access-lists
Standard IP access list 21
    10 permit 192.168.10.0, wildcard bits 0.0.0.255 (2 matches)
    20 deny   any (1 match)
R1#
```




```
PC1>ssh 192.168.10.1

Login as: admin
Password: *****
R1>
```

```
PC2>ssh 192.168.11.1
ssh connect to host 192.168.11.1 port
22: Connection refused

PC2>
```

Struktura rozszerzonej listy ACL IPv4

Rozszerzone listy ACL

Rozszerzone listy ACL mogą filtrować ruch związany z:

- adresem źródłowym,
- adresem docelowym,
- protokołem,
- numerami portów.

Rozszerzone listy ACL (cd.)

Używanie numerów portów w listach ACL

```
access-list 114 permit tcp 192.168.20.0 0.0.0.255 any eq 23
access-list 114 permit tcp 192.168.20.0 0.0.0.255 any eq 21
access-list 114 permit tcp 192.168.20.0 0.0.0.255 any eq 20
```

Używanie słów kluczowych w listach ACL

```
access-list 114 permit tcp 192.168.20.0 0.0.0.255 any eq telnet
access-list 114 permit tcp 192.168.20.0 0.0.0.255 any eq ftp
access-list 114 permit tcp 192.168.20.0 0.0.0.255 any eq ftp-data
```

Konfigurowanie rozszerzonych list ACL

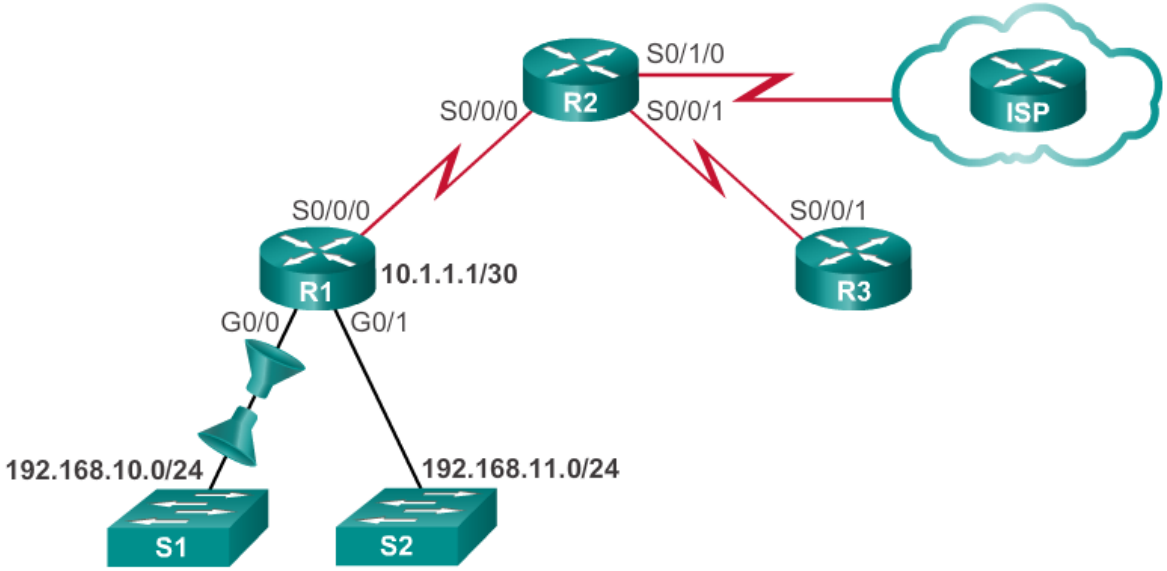
Poszczególne kroki proceduralne przy konfigurowaniu rozszerzonych list ACL są takie same, jak w przypadku list standardowych.
Najpierw należy skonfigurować listę ACL, a następnie przypisać ją do interfejsu. W celu umożliwienia obsługi dodatkowych funkcji, zmieniona została składnia polecenia a wymagane parametry są bardziej złożone.

```
access-list access-list-number {deny | permit | remark}
protocol source [source-wildcard] [operator operand]
[port port-number or name] destination [destination-wildcard]
[operator operand] [port port-number or name][established]
```

Konfigurowanie rozszerzonych list ACL

Parametr	Opis
access-list-number	Identyfikuje listę kontroli dostępu za pomocą liczby z przedziału od 100 do 199 (dla rozszerzonych list ACL IP) i od 2000 do 2699 (dla dodatkowych list ACL IP).
deny	Blokuje dostęp, jeśli warunki są spełnione.
permit	Zezwala na dostęp, jeśli warunki są spełnione.
remark	Używane do wpisywania uwagi lub komentarza.
protocol	Nazwa lub numer protokołu sieci Internet. Typowe słowa kluczowe to **icmp**, **ip**, **tcp** lub **udp**. Aby dopasować dowolny protokół sieci Internet (w tym ICMP, TCP i UDP), użyj słowa kluczowego **ip**.
source	Numer sieci lub hosta, z którego jest wysyłany pakiet.
source-wildcard	Bity maski blankietowej stosowane dla źródła.
destination	Numer sieci lub hosta, do którego wysyłany jest pakiet.
destination-wildcard	Bity maski blankietowej stosowane dla celu.
operator	(Opcjonalnie) Porównuje porty źródłowe lub docelowe. Dopuszczalne są operatory **lt** (mniejszy od), **gt** (większy od), **eq** (równy), **neq** (nierówny) oraz **range** (zakres zawierający).
port	(Opcjonalnie) Liczba dziesiętna bądź nazwa portu TCP lub UDP.
established	(Opcjonalnie) Tylko dla protokołu TCP: Oznacza ustanowienie połączenia.

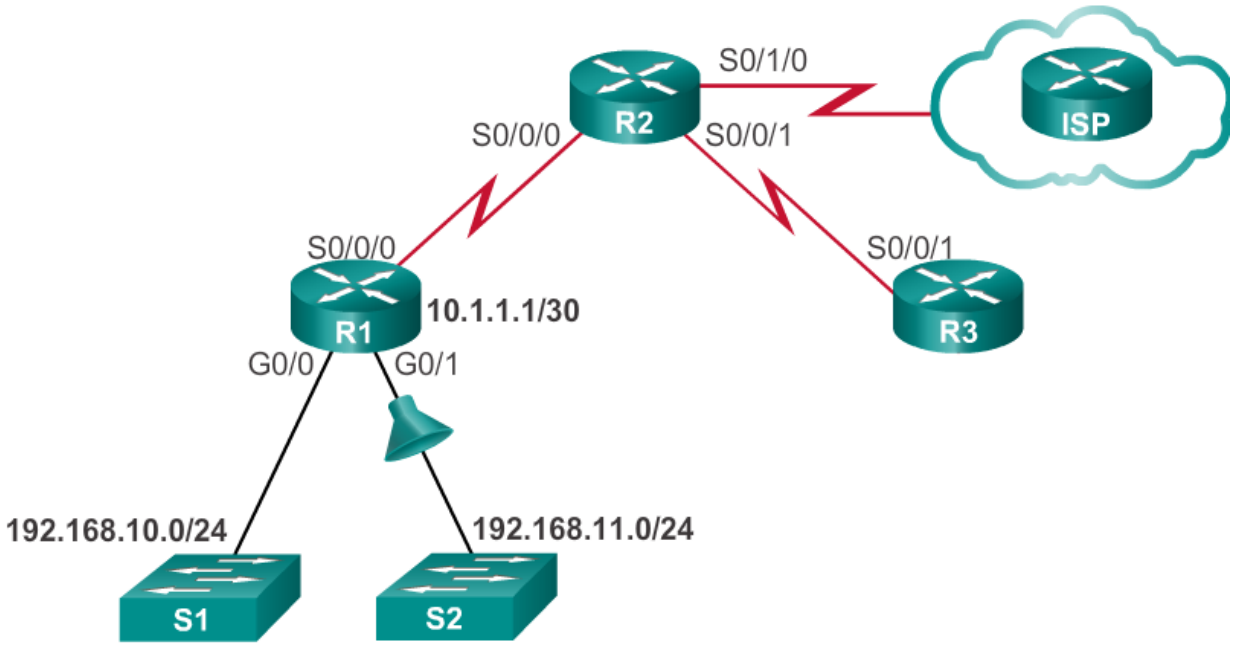
Przypisywanie rozszerzonych list ACL do interfejsów




```
R1(config)#access-list 103 permit tcp 192.168.10.0 0.0.0.255 any eq 80
R1(config)#access-list 103 permit tcp 192.168.10.0 0.0.0.255 any eq 443
R1(config)#access-list 104 permit tcp any 192.168.10.0 0.0.0.255 established
R1(config)#interface g0/0
R1(config-if)#ip access-group 103 in
R1(config-if)#ip access-group 104 out
```

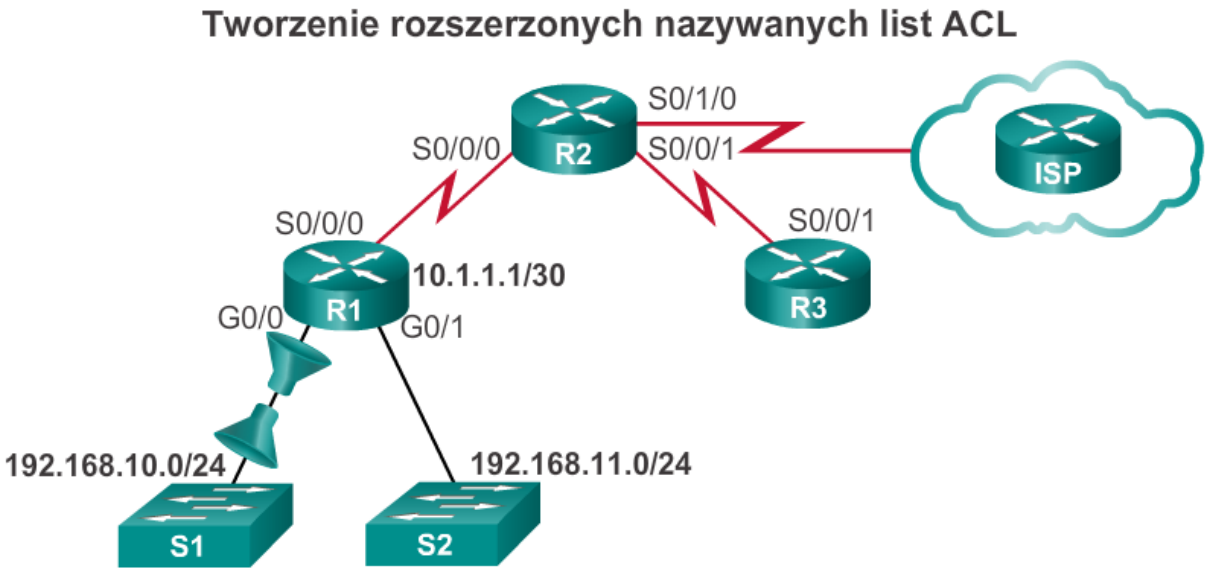
Filtrowanie ruchu za pomocą rozszerzonych list ACL

Rozszerzona lista ACL służąca do blokowania FTP




```
R1(config)# access-list 101 deny tcp 192.168.11.0 0.0.0.255
192.168.10.0 0.0.0.255 eq ftp
R1(config)# access-list 101 deny tcp 192.168.11.0 0.0.0.255
192.168.10.0 0.0.0.255 eq ftp-data
R1(config)# access-list 101 permit ip any any
R1(config)# interface g0/1
R1(config-if)# ip access-group 101 in
```

Tworzenie rozszerzonych nazywanych list ACL




```
R1(config)# ip access-list extended SURFING
R1(config-ext-nacl)# permit tcp 192.168.10.0 0.0.0.255 any eq 80
R1(config-ext-nacl)# permit tcp 192.168.10.0 0.0.0.255 any eq 443
R1(config-ext-nacl)# exit
R1(config)# ip access-list extended BROWSING
R1(config-ext-nacl)# permit tcp any 192.168.10.0 0.0.0.255 established
R1(config-ext-nacl)# exit
R1(config)# interface g0/0
R1(config-if)# ip access-group SURFING in
R1(config-if)# ip access-group BROWSING out
```

Weryfikacja rozszerzonych list ACL

```
R1#show access-lists
Extended IP access list BROWSING
    10 permit tcp any 192.168.10.0 0.0.0.255 established
Extended IP access list SURFING
    10 permit tcp 192.168.10.0 0.0.0.255 any eq www
    20 permit tcp 192.168.10.0 0.0.0.255 any eq 443
R1#
R1#show ip interface g0/0
GigabitEthernet0/0 is up, line protocol is up
  Internet address is 192.168.10.1/24
<output omitted for brevity>
  Outgoing access list is BROWSING
  Inbound  access list is SURFING
<output omitted for brevity>
```

Edycja rozszerzonych list ACL

Edycję rozszerzonych list ACL przeprowadza się analogicznie jak w przypadku standardowych list ACL. Można to zrobić na dwa sposoby:

- Metoda 1 - Użycie edytora teksu
- Metoda 2 - Użycie numerów sekwencyjnych

Logika wejściowych list ACL

- Pakiety, zanim zostaną przekierowane, są sprawdzane przez wejściową listę ACL.
- Przychodzący pakiet jest przekierowany dalej, jeśli lista ACL zezwala na to.
- Przychodzący pakiet jest odrzucany, jeśli jest blokowany przez listę ACL.
- Jeśli pakiet przychodzący nie spełnia żadnych wymagań listy ACL, wtedy jest on "bezwzględnie odrzucony".

Logika wyjściowych list ACL

- Pakiety są wstępnie sprawdzane przed wysłaniem do interfejsu wychodzącego. Pakiety są odrzucane, jeśli przekierowanie nie istnieje.
- Jeśli interfejs wychodzący nie ma przypisanej listy ACL, to pakiety są wysyłane bezpośrednio do tego interfejsu.
- Jeśli istnieje lista ACL na interfejsie wychodzącym, pakiety są testowane przed wysłaniem.
- Pakiet wychodzący jest wysyłany z interfejsu, jeśli ma zezwolenie listy ACL.

Logika wyjściowych list ACL (cd.)

- Wychodzący pakiet jest odrzucany, jeśli jest blokowany przez listę ACL.
- Jeśli pakiet wychodzący nie spełnia żadnych wymagań listy ACL, wtedy jest on "bezwzględnie odrzucony„.

Logika pełnego procesu ACL

- Gdy pakiet przychodzi do interfejsu wejściowego routera, podlega tym samym procesom routera, niezależnie od tego czy istnieją listy ACL, czy też nie. Gdy ramka jest wprowadzana do interfejsu, router sprawdza czy adres docelowy warstwy 2 w ramce odpowiada jego własnemu adresowi warstwy 2 na interfejsie lub czy adres ten jest adresem rozgłoszeniowym.
- Jeśli adres ramki został zaakceptowany, informacja o ramce jest usuwana, a router sprawdza, czy istnieje lista ACL interfejsu wejściowego. Jeśli lista ACL istnieje, dla pakietu sprawdzane są instrukcje w niej zawarte.

Logika pełnego procesu ACL (cd.)

- Jeśli pakiet został przepuszczony przez listę wejściową, porównywany jest z wpisami tablicy routingu i wybierany jest interfejs wyjściowy. Jeśli istnieje wpis tablicy routingu dla adresu docelowego, pakiet jest kierowany do interfejsu wyjściowego, w przeciwnym wypadku jest odrzucany.
- Następnie router sprawdza czy na interfejsie wyjściowym jest przypisana lista ACL. Jeśli lista ACL istnieje, dla pakietu sprawdzane są instrukcje w niej zawarte.
- Jeśli na interfejsie nie ma listy ACL lub gdy pakiet został przepuszczony, jest ponownie enkapsulowany w ramkę warstwy 2 i wysyłany przez interfejs wyjściowy do następnego urządzenia.

Proces decyzyjny standardowej listy ACL

- Standardowe listy ACL sprawdzają wyłącznie adres źródłowy IPv4. Miejsce przeznaczenia pakietu i zaangażowane porty nie są brane pod uwagę.
- Oprogramowanie Cisco IOS sprawdza adresy w poleceniach zawartych w ACL. Wystąpienie pierwszego dopasowania powoduje podjęcie decyzji czy dany adres ma zostać zaakceptowany czy odrzucony. Ponieważ po wystąpieniu pierwszego dopasowania, oprogramowanie przestaje sprawdzać następne wpisy, bardzo istotna jest kolejność reguł na liście ACL. Jeśli dopasowanie nie wystąpi, adres zostaje odrzucony.

Proces decyzyjny rozszerzonej listy ACL

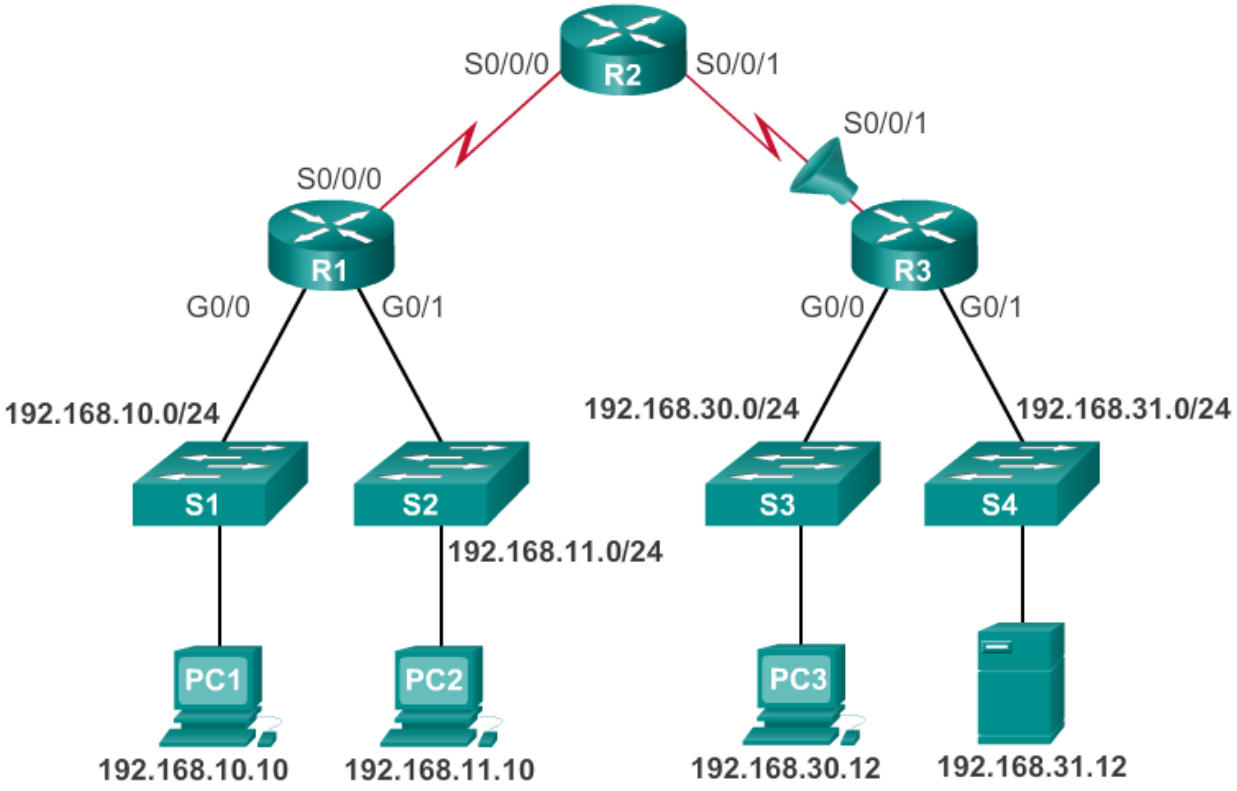
Lista ACL dokonuje najpierw filtrowania na podstawie adresu źródłowego, dalej portu i protokołu źródłowego. Następnym krokiem jest filtrowanie na podstawie adresu docelowego, potem docelowego portu i protokołu i ostatecznie podjęcie decyzji co do przepuszczenia lub odrzucenia pakietu.

Rozwiązywanie problemów z typowymi błędami list ACL - Przykład 1

Host 192.168.10.10

nie ma połączenia

z 192.168.30.12



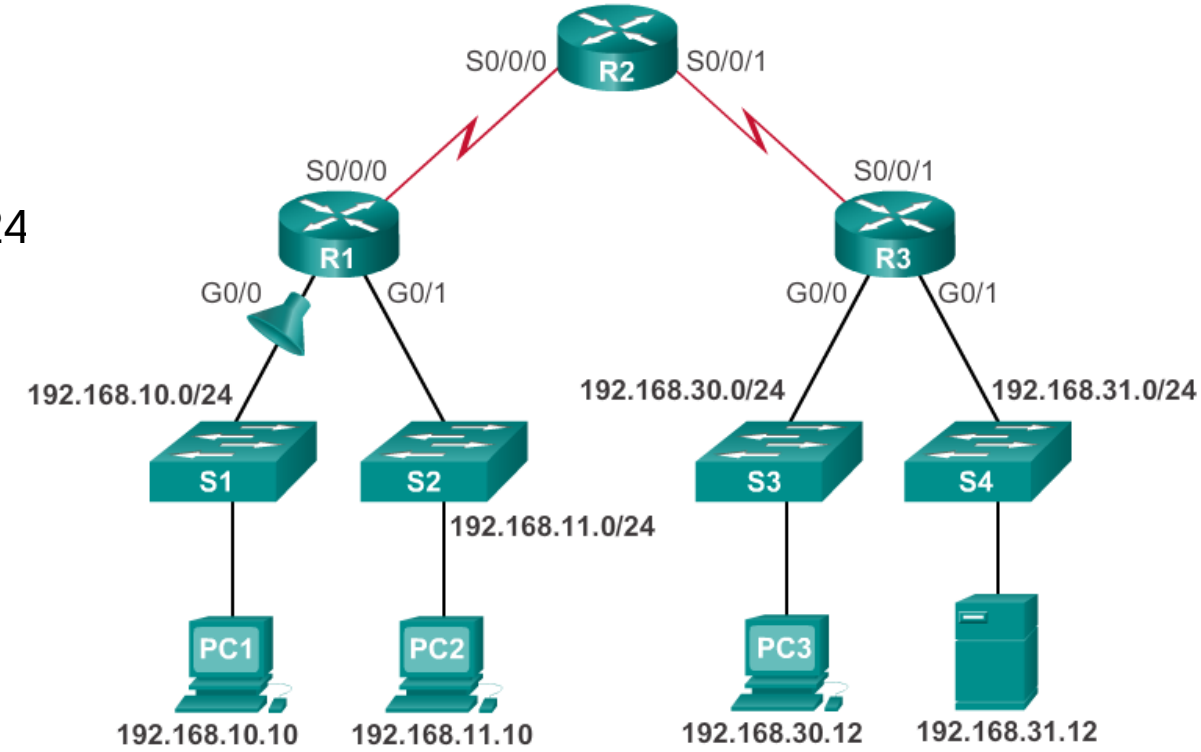

```
R3#show access-lists
Extended IP access list 110
    10 deny tcp 192.168.10.0 0.0.0.255 any (12 match(es))
    20 permit tcp 192.168.10.0 0.0.0.255 any eq telnet
    30 permit ip any any
```

Rozwiązywanie problemów z typowymi błędami list ACL - Przykład 2

Sieć192.168.10.0 /24

nie może użyć

TFTP do połączenia
się z siecią 192.168.30.0 /24

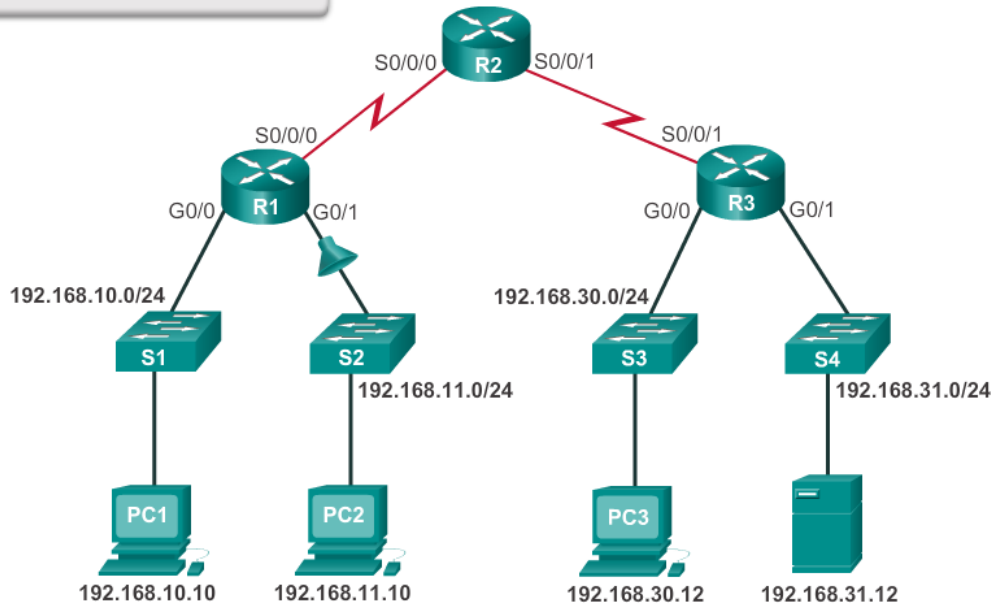



```
R1#show access-lists 120
Extended IP access list 120
    10 deny tcp 192.168.10.0 0.0.0.255 any eq telnet
    20 deny tcp 192.168.10.0 0.0.0.255 host 192.168.31.12 eq smtp
    30 permit tcp any any
```

Rozwiązywanie problemów z typowymi błędami list ACL - Przykład 3

Sieć 192.168.11.0 /24 może korzystać z usługi Telnet do połączenia się 192.168.30.0 /24, ale zgodnie z polityką firmy, połączenie to nie powinno być dozwolone.

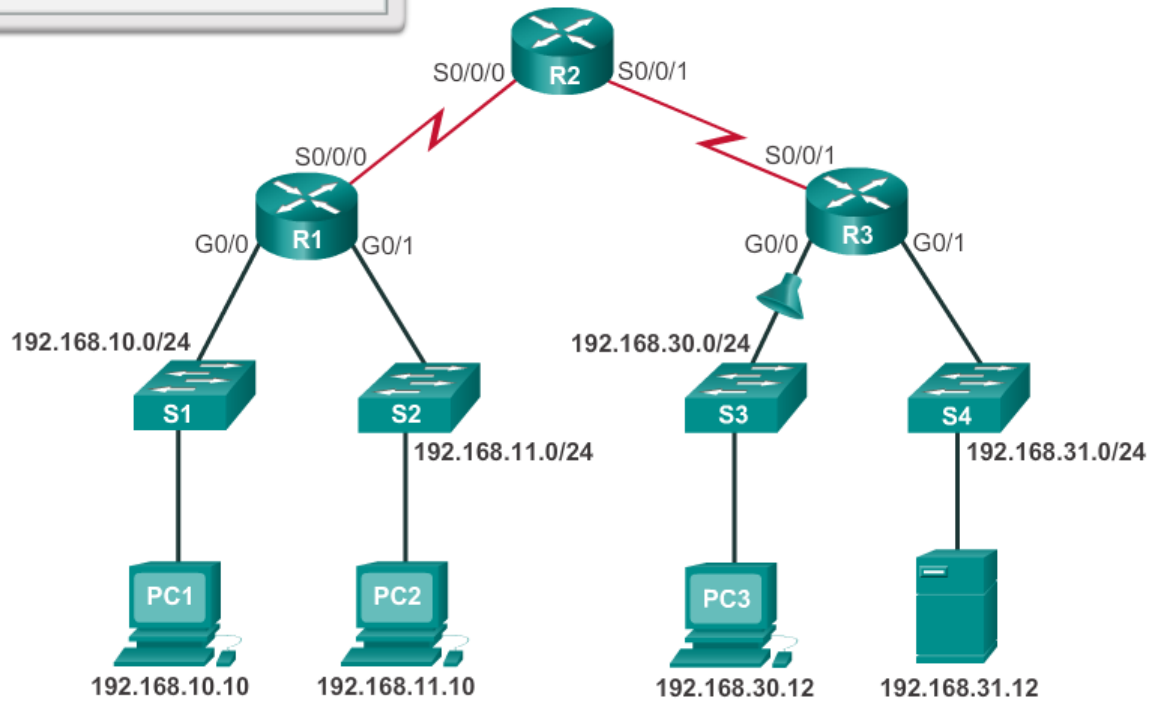
```
R1#show access-lists 130
Extended IP access list 130
    10 deny tcp any eq telnet any
    20 deny tcp 192.168.11.0 0.0.0.255 host 192.168.31.12 eq smtp
    30 permit tcp any any (12 match(es))
```



Rozwiązywanie problemów z typowymi błędami list ACL - Przykład 4

Host 192.168.30.12 jest w stanie połączyć się z 192.168.31.12 przy pomocy protokołu Telnet, lecz zgodnie z polityką firmy, takie połączenie nie powinno być możliwe.

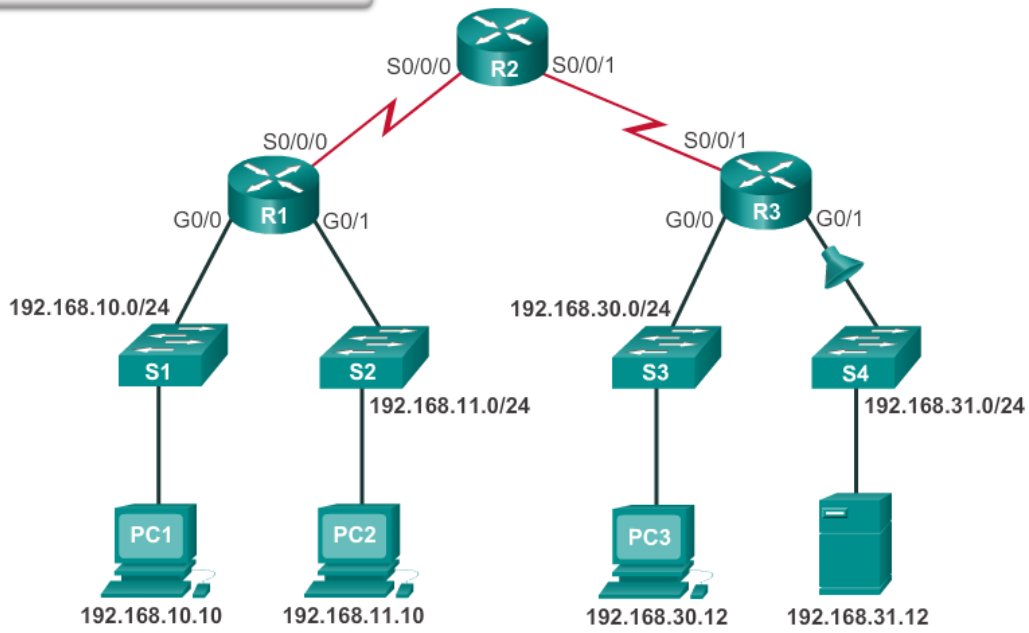
```
R3#show access-lists 140
Extended IP access list 140
    10 deny tcp host 192.168.30.1 any eq telnet
    20 permit ip any any (5 match(es))
```



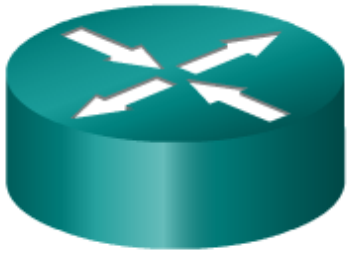
Rozwiązywanie problemów z typowymi błędami list ACL - Przykład 5

Host 192.168.30.12 jest w stanie połączyć się z 192.168.31.12 przy pomocy protokołu Telnet, lecz zgodnie z polityką bezpieczeństwa, takie połączenie nie powinno być możliwe.

```
R2#show access-lists 150
Extended IP access list 150
    10 deny tcp any host 192.168.31.12 eq telnet
    20 permit ip any any
```



Rodzaje list ACL IPv6



Listy ACL dla IPv4

- standardowe
  - numerowane
  - nazywane
- rozszerzone
  - numerowane
  - nazywane

Listy ACL dla IPv6

- tylko nazywane
- funkcjonalność jest podobna do rozszerzonej listy ACL IPv4

Porównanie list ACL IPv4 i IPv6

Mimo, że listy ACL w protokołach IPv4 i IPv6 są bardzo podobne, występują między nimi trzy istotne różnice.

- Stosowanie listy ACL IPv6

  IPv6 korzysta z polecenia **ipv6 traffic-filter**, aby wykonać tę samą funkcję dla interfejsów IPv6.

- Brak masek blankietowych

  Używana jest długość prefiksu, która określa, w jakiej części adres źródłowy lub docelowy IPv6 będzie dopasowany.

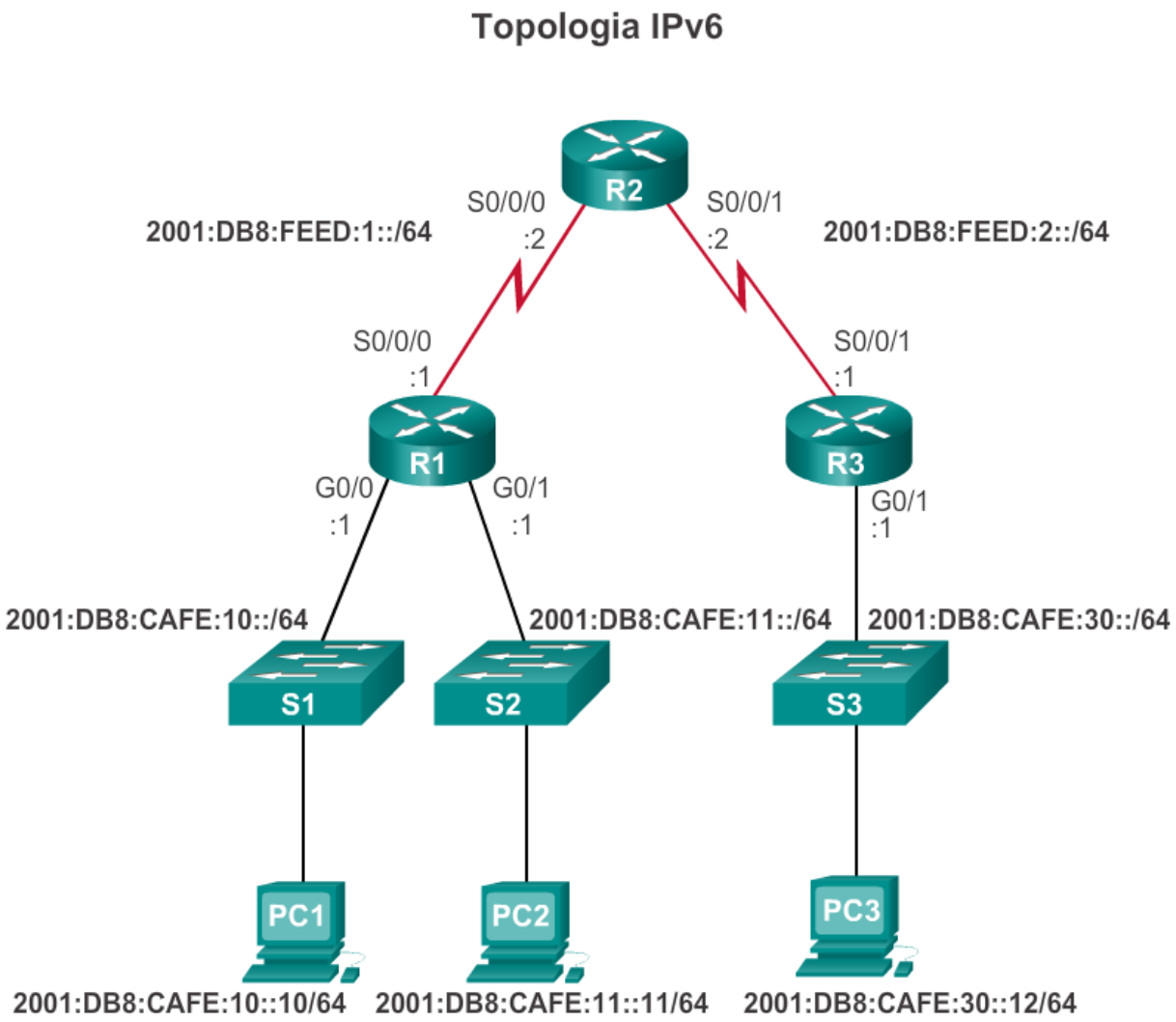
- Dodatkowe domyślne instrukcje

  permit icmp any any nd-na

  permit icmp any any nd-ns

Konfigurowanie list ACL IPv6

Konfiguracja topologi IPv6



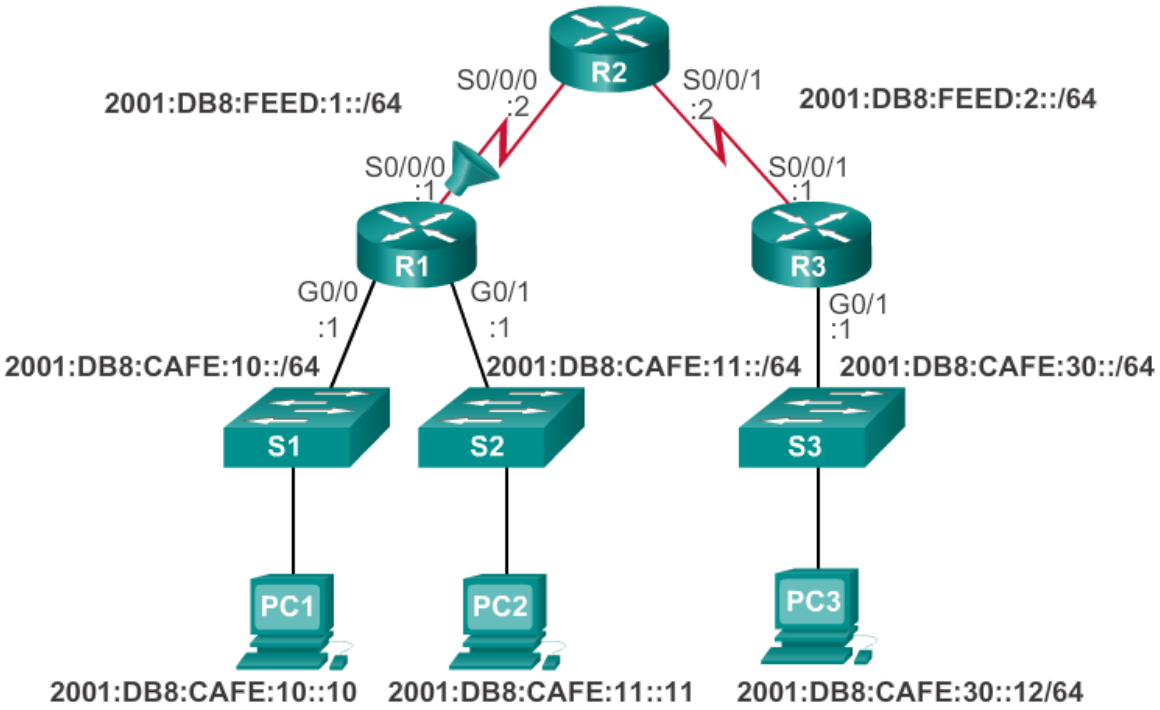
Konfiguracja list ACL IPv6

Konfiguracja IPv6 ACL składa się z trzech podstawowych kroków:

1. Aby stworzyć listę ACL IPv6, w trybie konfiguracji globalnej należy użyć polecenia **ipv6 access-list *nazwa*.**
2. W trybie konfiguracji nazywanej listy ACL, należy skorzystać z komunikatu **permit** lub **deny** w celu stwierdzenia, czy pakiet ma być przekazany dalej czy odrzucony.
3. Do trybu uprzywilejowanego wracamy przy pomocy polecenia **end**.

```
R1(config)# ipv6 access-list access-list-name
R1(config-ipv6-acl)# deny | permit protocol {source-ipv6-
prefix/prefix-length | any | host source-ipv6-address} [operator
[port-number]] {destination-ipv6-prefix/ prefix-length | any |
host destination-ipv6-address} [operator [port-number]]
```

Przypisanie listy ACL IPv6 do interfejsu




```
R1(config)#interface s0/0/0
R1(config-if)#ipv6 traffic-filter NO-R3-LAN-ACCESS in
```

Przykłady list ACL IPv6

Blokowanie ruchu FTP

```
R1(config)#ipv6 access-list NO-FTP-TO-11
R1(config-ipv6-acl)#deny tcp any 2001:db8:cafe:11::/64 eq ftp
R1(config-ipv6-acl)#deny tcp any 2001:db8:cafe:11::/64 eq ftp-data
R1(config-ipv6-acl)#permit ipv6 any any
R1(config-ipv6-acl)#exit
R1(config)#interface g0/0
R1(config-if)#ipv6 traffic-filter NO-FTP-TO-11 in
R1(config-if)#
```

Ograniczenie dostępu

```
R3(config)#ipv6 access-list RETRICTED-ACCESS
R3(config-ipv6-acl)#remark Permit access only HTTP and HTTPS to Network 1
R3(config-ipv6-acl)#permit tcp any host 2001:db8:cafe:10::10 eq 80
R3(config-ipv6-acl)#permit tcp any host 2001:db8:cafe:10::10 eq 443   1
R3(config-ipv6-acl)#remark Deny all other traffic to Network 10
R3(config-ipv6-acl)#deny ipv6 any 2001:db8:cafe:10::/64   2
R3(config-ipv6-acl)#remark Permit PC3 telnet access to PC2
R3(config-ipv6-acl)#permit tcp host 2001:DB8:CAFE:30::12 host 2001:DB8:CA
R3(config-ipv6-acl)#remark Deny telnet access to PC2 for all other device
R3(config-ipv6-acl)#deny tcp any host 2001:db8:cafe:11::11 eq 23   4
R3(config-ipv6-acl)#remark Permit access to everything else
R3(config-ipv6-acl)#permit ipv6 any any   5
R3(config-ipv6-acl)#exit
R3(config)#interface g0/0
R3(config-if)#ipv6 traffic-filter RESTRICTED-ACCESS in   6
R3(config-if)#
```

Weryfikacja list ACL IPv6

```
R3#show ipv6 interface g0/0
GigabitEthernet0/0 is up, line protocol is up
  Global unicast address(es):
    2001:DB8:CAFE:30::1, subnet is 2001:DB8:CAFE:30::/64
  Input features: Access List
  Inbound access list RESTRICTED-ACCESS
```

<some output omitted for brevity>

```
R3#show access-lists
IPv6 access list RESTRICTED-ACCESS
    permit tcp any host 2001:DB8:CAFE:10::10 eq www sequence 20
    permit tcp any host 2001:DB8:CAFE:10::10 eq 443 sequence 30
    deny ipv6 any 2001:DB8:CAFE:10::/64 sequence 50
    permit tcp host 2001:DB8:CAFE:30::12 host 2001:DB8:CAFE:11::11 eq
    telnet sequence 70
    deny tcp any host 2001:DB8:CAFE:11::11 eq telnet sequence 90
    permit ipv6 any any sequence 110
R3#
```

Wykład 1: Podsumowanie

- W domyślnej konfiguracji router nie przeprowadza filtrowania ruchu. Ruch przychodzący do routera jest kierowany wyłącznie w oparciu o informacje w tablicy routingu.
- Filtrowanie pakietów zapewnia kontrolę dostępu do sieci poprzez analizę pakietów wchodzących i wychodzących oraz przepuszczanie lub blokowanie ich na podstawie zadanych kryteriów, takich jak np. adres źródłowy IP, docelowy adres IP i protokół powiązany z pakietem.
- Router, pełniący rolę filtra pakietów, korzysta z tzw. reguł filtrowania, aby określić, czy dany ruch należy przepuścić czy też odrzucić. Reguły te mogą obejmować nie tylko protokoły warstwy trzeciej, ale i czwartej (transportowej).
- Lista ACL jest sekwencyjną listą składającą się z instrukcji zezwoleń (permit) lub blokad (deny).

Wykład 1 : Podsumowanie (cd.)

- Ostatnią deklaracją każdej listy ACL jest tzw. niejawne odrzucenie, blokujące cały ruch. Aby zapobiec niejawnemu odrzuceniu wszystkich pakietów, które występuje na końcu każdej ACL, należy dodać polecenie **permit ip any any**.
- Gdy dane przechodzą przez interfejs, do którego przypisano listę ACL, router porównuje informacje zawarte w pakiecie z poszczególnymi wpisami ACL w zadanej kolejności, aby określić, czy pakiet pasuje do jednego z nich. Jeśli takie dopasowanie zostało znalezione, pakiet jest odpowiednio przetwarzany.
- Poszczególne listy ACL można skonfigurować do obsługi ruchu przychodzącego do routera, lub wychodzącego z niego.

Wykład 1 : Podsumowanie (cd.)

- Standardowe listy ACL stosowane są do przepuszczania lub blokowania ruchu tylko na podstawie adresów źródłowych IPv4. Ten rodzaj list ACL nie umożliwia kontroli adresów docelowych ani portów w pakietach. Podstawową zasadą dotyczącą lokalizacji standardowej listy ACL jest umieszczenie jej jak najbliżej sieci docelowej.
- Rozszerzone listy ACL zapewniają filtrowanie pakietów na podstawie takich atrybutów jak: typ protokołu, źródłowy i/lub docelowy adres IP, a także źródłowy i/lub docelowy port. Podstawową zasadą co do lokalizacji rozszerzonej listy ACL jest umieszczenie jej tak blisko źródła, jak to tylko możliwe.

Wykład 1 : Podsumowanie (cd.)

- Polecenie konfiguracji globalnej **access-list** definiuje standardową listę ACL numerem w zakresie od 1 do 99, lub rozszerzoną listę ACL numerem w zakresie od 100 do 199 i numerem w zakresie od 2000 do 2699. Standardowe i rozszerzone listy ACL mogą być również nazywane.
- Polecenie **ip access-list standard *nazwa*** jest używane do tworzenia nazywanej standardowej listy ACL, podczas gdy polecenie **ip access-list extended *nazwa*** do tworzenia nazywanej rozszerzonej listy ACL. W listach ACL IPv6 nie stosuje się masek blankietowych.
- Gdy skonfigurowana jest lista ACL, jest ona przypisywana do interfejsu za pomocą polecenia **ip access-group** w trybie konfiguracji interfejsu.

Wykład 1 : Podsumowanie (cd.)

- Należy pamiętać, że obowiązuje zasada trzy razy N: jedna lista ACL na protokół, jedna na kierunek, jedna na interfejs.
- Aby usunąć listę ACL z interfejsu, należy najpierw wpisać polecenie **no ip access-group** na interfejsie, a następnie polecenie w trybie konfiguracji globalnej **no access-list** w celu usunięcia całej listy ACL.
- Polecenia **show running-config** i **show access-lists** są stosowane do sprawdzenia konfiguracji listy ACL. Polecenie **show ip interface** służy do sprawdzenia listy ACL na interfejsie i kierunku, w którym został zastosowany.

Wykład 1 : Podsumowanie (cd.)

- Polecenie **access-class** skonfigurowane w trybie konfiguracji linii ogranicza przychodzące i wychodzące połączenia pomiędzy danymi VTY i adresów w liście dostępu.
- Podobnie jak w przypadku nazywanych list ACL IPv4, nazwy list IPv6 muszą zawierać znaki alfanumeryczne oraz być unikatowe, rozróżniana jest także wielkość liter. W odróżnieniu od IPv4, nie ma potrzeby podawania opcji standard lub extended.
- Z trybu konfiguracji globalnej należy użyć polecenia **ipv6 access-list *nazwa***, aby utworzyć listę ACL IPv6. Używana jest długość prefiksu, która określa, w jakiej części adres źródłowy lub docelowy IPv6 będzie dopasowany.
- Po konfiguracji listy ACL IPv6 jest ona połączona z interfejsem za pomocą polecenia **ipv6 traffic-filter**.