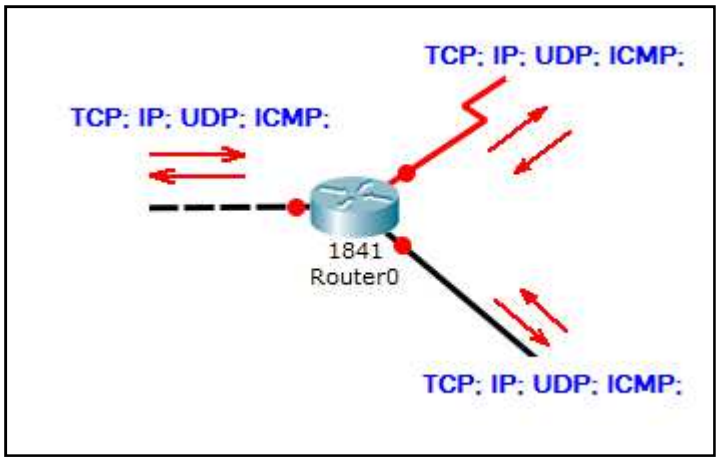
WSTĘP

Głównym celem stosowania **list kontroli dostępu** (*ACL – ang. Access Control List*) jest kontrola i ograniczenie ruchu sieciowego, przechodzącego poprzez routery. Poprzez ich zastosowanie możemy wpłynąć nie tylko na podniesienie poziomu bezpieczeństwa naszej sieci, ale również na poprawę jej wydajności. Kontrolowanie i filtrowanie ruchu sieciowego to bardzo odpowiedzialne zadanie każdego administratora, który decyduje jaki typ ruchu będzie przepuszczany przez router, a jaki blokowany. Dlatego w tym rozdziale książki skupimy się na omówieniu konfiguracji tego typu zagadnień.

Każdy router może mieć skonfigurowaną dużą liczbę **ACL**, nie wszystkie jednak muszą być aktywne, tzn. utworzona lista kontroli dostępu i zapisana w konfiguracji routera będzie działać dopiero wtedy, gdy przypisze się jej dany interfejs dla którego ma filtrować ruch oraz zdefiniuje kierunek działania, tzn. czy ACL ma filtrować pakiety wchodzące czy wychodzące do/z routera. Ponadto każdą ACL można zdefiniować dla danego protokołu sieciowego np. IP, TCP, UDP, ICMP, tak jak przedstawia to poniższy rysunek.



Rysunek 1. Możliwości rozmieszczenia list kontroli dostępu, kierunku ich działania oraz wybranych protokołów

Filtrowanie ruchu sieciowego pozwala na kontrolowanie co dzieje się w poszczególnych segmentach sieci. Jest to proces analizujący zawartość pakietów w celu podjęcia decyzji, czy pakiet ma być dopuszczony do pewnej strefy sieci czy też zablokowany.

Filtrowanie pakietów może odbywać się na podstawie:

- adresu źródłowego IP,
- adresu docelowego IP,
- protokołów (nazwy protokołów),
- typu aplikacji (numery portów).

Na podstawie materiałów CISCO opracował Jerzy Kluczewski

RODZAJE LIST ACL

1. Standardowe ACL

Cechy **standardowej** listy kontroli dostępu (**standard ACL**):

- numery ACL zawierają się w zakresie od **1 do 99** oraz od **1300 do 1999**
- filtruje ruch na podstawie adresu **źródłowego IP** pakietu
- zezwala (**permit**) lub blokuje (**deny**) na podstawie **całego protokołu** np. IP
- jeśli dany host jest zablokowany przez standardową ACL, to **wszystkie usługi wychodzące** z tego hosta są zablokowane

Składnia polecenia IOS tworzącego **standardową** listę:

access-list [*access-list-number*] [deny|permit] [*source address*] [*source-wildcard*][log]

Składnia polecenia IOS usuwającego **ACL**:

no access-list ***access-list-number***

Aby przypisać **ACL** do interfejsu, należy zastosować polecenie **ip access-group**. Każdy interfejs może mieć przypisane dwie listy (dla ruchu wchodzącego oraz wychodzącego). Jeśli przypisane są obie listy, muszą być tego samego typu.

Składnia polecenia IOS przypisującego **ACL** do interfejsu:

ip access-group ***access-list-number*** **{ in | out }**

2. Rozszerzone ACL

Cechy **rozszerzonej** listy kontroli dostępu (**extended ACL**):

- numery ACL zawierają się w zakresie od **100 do 199** oraz od **2000 do 2699**
- filtruje ruch na podstawie adresu **źródłowego IP** pakietu oraz na podstawie adresu **docelowego IP**
- filtruje ruch na podstawie rodzaju **protokołu,** numerów **portów**
- zezwala (**permit**) lub blokuje (**deny**) na podstawie **rodzaju protokołu** np. TCP lub **rodzaju aplikacji** (numeru portu)

Składnia polecenia IOS tworzącego **rozszerzoną** listę:

access-list *access-list-number* **{ deny | permit }** *protocol {source-address [source-mask] {destination-address [destination-mask] } operator service*

Różnice między listą standardową i listą rozszerzoną:

- Standardowa lista zezwala lub blokuje na podstawie adresu źródłowego IP.
- Rozszerzona lista zezwala lub blokuje dostęp bazując na adresach źródłowych IP, docelowych adresach IP, typie protokołu, numerach portu.

Na podstawie materiałów CISCO opracował Jerzy Kluczewski

3. Nazywane ACL

Właściwości **nazywanej** listy kontroli dostępu (**named ACL**):

- mogą być **standardowe lub rozszerzone**
- ACL jest **identyfikowana za pomocą nazwy** przypisanej do niej
- konfiguracja nazywanych list ACL używa trybu konfiguracji (**nacl**)

Począwszy od wersji systemu Cisco IOS 11.2 można tworzyć tzw. **Named ACL** (NACLs), czyli listy ACL posiadające nazwę zamiast numeru. Oferują one te same możliwości co listy standardowe i rozszerzone. Jedyną różnicą jest składnia.

Nazwa listy powinna być unikalna. Używając dużych liter w nazwach jest łatwiej je znaleźć w routerze.

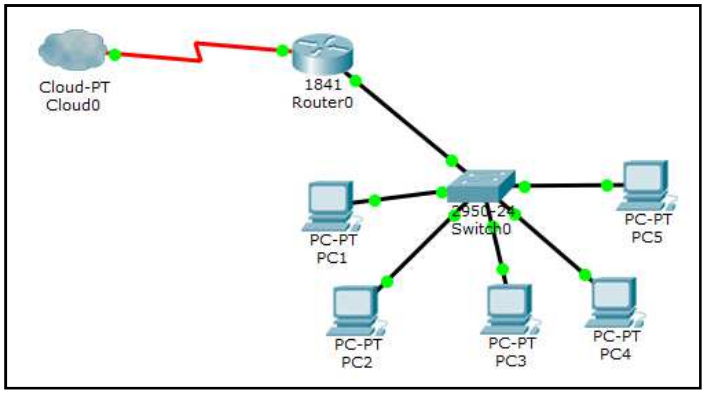
Składnia polecenia IOS tworzenia listy nazywanej (**named ACL**):

ip access-list {standard | extended} name

Po wykonaniu tego polecenia router przechodzi do podtrybu konfiguracji **nacl**.
W tym podtrybie należy wprowadzać polecenia **permit** lub **deny**.

ZASADY TWORZENIA LIST KONTROLI DOSTĘPU

Podczas tworzenia list kontroli dostępu, ogromne znaczenie ma kolejność zdefiniowanych reguł. To właśnie kolejność odgrywa ogromne znaczenie podczas analizy list przez system IOS. Dlatego musimy pamiętać o bardzo ważnej kwestii: system IOS pozwala na wprowadzenie tylko dwóch reguł: ZEZWALAJ (**permit**) oraz ODMÓW (**deny**). Jeżeli mamy sieć, w której router połączony jest przykładowo z pięcioma urządzeniami, tak jak przedstawia to poniższy rysunek, bez włączania jakichkolwiek ACL, router zachowuje się w taki sposób, że domyślnie przepuszcza cały ruch sieciowy we wszystkich kierunkach.



Rysunek 2. Przykładowa topologia do opisania zasad tworzenia ACL

Załóżmy taki przypadek, w którym chcemy udostępnić dostęp komputerom PC1 – PC5 do usług w sieci WAN, które będzie symbolizowała ikona chmury. W tym przypadku kolejność tworzenia ACL jest

bardzo ważna: najpierw należy zdefiniować reguły, w których ustawimy dostęp komputerów PC1 – PC5, a potem zezwolimy pozostałym na komunikację ze „światem”.

Pozostaje teraz tylko ostatnia czynność, która polegać będzie na wyborze interfejsu na którym ma ona działać i zdefiniowania kierunku.

PLANOWANIE LIST KONTROLI DOSTĘPU

Krok 1 – określ wymagania dotyczące filtrowania ruchu
Określ i zapisz wymagania dotyczące każdej podsieci. Wymagania te są prawdopodobnie oparte na potrzebach użytkowników, wymaganiach bezpieczeństwa odnośnie rodzaju ruchu sieciowego.

Krok 2 – wybierz typ ACL dopasowanej do wymagań
Podejmij decyzję, czy użyć standardowej ACL czy rozszerzonej ACL, zależnie od wymagań filtrowania. Wybierz typ ACL w zależności od jej elastyczności a także od wydajności routerów, sieci, pasma interfejsów.

Standardowe ACL są proste w tworzeniu, ale filtrują ruch jedynie na podstawie adresu źródłowego. Przy rutowaniu do wielu podsieci, **standardowe listy ACL powinieneś umieszczać jak najbliżej celu**, aby nie blokować ruchu nieobsługiwanego przez te listy.

Gdy filtrowanie ma być bardziej złożone, użyj **rozszerzonych ACL**. Pozwalają one na filtrowanie na podstawie **adresu źródłowego i docelowego oraz warstwy 3 i 4 oraz numeru portu**.

Umieszczaj rozszerzone listy ACL jak najbliżej adresów źródłowych. Pakiety wysyłane do sieci docelowych można blokować już zanim opuszczą router źródłowy, co pozwala obniżyć obciążenie łączy w sieci.

Krok 3 – wybierz router oraz jego interfejs dla ACL
ACL umieść w routerze i przypisz ją do interfejsu.

Krok 4 – wybierz kierunek ruchu do filtrowania
Staraj się przedstawić przebieg pakietów z perspektywy routera.

ACL umieść w routerze i przypisz ją do interfejsu jako wejściową (in) albo jako wyjściową (out).

Wejściowy ruch to ruch przychodzący z zewnątrz routera. Router najpierw sprawdza ten ruch, tj. porównuje go z listą, a potem szuka sieci docelowej w tablicy routingu.

Wyjściowy ruch znajduje się wewnątrz routera i jest już obsłużony przez tablicę routingu. Przed opuszczeniem interfejsu wyjściowego ruch jest sprawdzany (porównywany) z listą, jeśli wynik porównania jest pozytywny, to opuszcza interfejs.

Uwaga: w przypadku routerów firmy Cisco na końcu każdej listy ACL automatycznie dodawane jest niejawne i niewidoczne polecenie
- dla list standardowych: **deny any**
- dla list rozszerzonych: **deny ip any any**

Na podstawie materiałów CISCO opracował Jerzy Kluczewski

SKŁADNIA POLECEŃ

1. STANDARDOWE ACL

Tu znajduje się opis prostych, standardowych ACL. **Standardowa** ACL zezwala lub blokuje ruch sieciowy **tylko** na podstawie adresu **źródłowego** IP.

Składnia standardowych ACL

Poniższa składnia jest wzorem, który będzie stosowanym w ćwiczeniach i zadaniach.

access-list NR RODZAJ-ACL WARUNKI-ŹRÓDŁA

Legenda:

access-list – polecenie wpisywane w trybie globalnej konfiguracji;

NR – numer ACL, w przypadku list standardowych jest to liczba z zakresu 1-99;

RODZAJ-ACL – w tym miejscu może być wpisane jedno z dwóch dostępnych słów: permit – zezwól lub deny – zabroń;

WARUNKI-ŹRÓDŁA – w tym miejscu określamy, jakiego źródła ma dotyczyć ACL:

- WARUNEK1 – jeżeli chcemy odnieść ACL do jednego urządzenia w sieci, wpisujemy: host 1.2.3.4 (gdzie 1.2.3.4 – to adres IP urządzenia do którego chcemy się odwołać);
- WARUNEK2 – jeżeli chcemy zastosować ACL dla grupy urządzeń (przykładowo całej sieci lub podsieci) wówczas stosujemy tzw. maskę odwróconą (zwaną też maską blankietową); Przykładowo, jeżeli chcemy zastosować ACL dla wszystkich urządzeń w sieci: 192.168.1.0 o masce 255.255.255.0, możemy zastosować maskę odwróconą 0.0.0.255;
- WARUNEK 3 – jeżeli ACL ma mieć zastosowanie do wszystkich urządzeń w dowolnej sieci – wówczas wystarczy wpisać słowo: any;

Przykład

```
access-list 10 deny host 200.200.200.4
```

2. ROZSZERZONE ACL

Tu znajduje się opis **rozszerzonych** ACL, które zezwalają lub blokują dostęp bazując na adresach **źródłowych** IP, **docelowych** adresach IP, typie **protokołu**, **numerach portu**.

Składnia rozszerzonych ACL

Poniższa składnia jest wzorem, który będzie stosowanym w ćwiczeniach i zadaniach.

access-list NR RODZAJ-ACL TYP-PROTOKOŁU WARUNEK-ŹRÓDŁA WARUNEK-CELU [NR-PORTU]

Legenda:

access-list – polecenie wpisywane w trybie globalnej konfiguracji;
NR – numer ACL, w przypadku list rozszerzonych jest to liczba z zakresu 100-199;
RODZAJ-ACL – w tym miejscu może być wpisane jedno z dwóch dostępnych słów: permit – zezwól lub deny – zabroń;
TYP-PROTOKOŁU – w tym miejscu określamy dla jakiego protokołu będą stosowane warunki zawarte w ACL: ip, icmp, tcp, udp;

- WARUNEK-ŹRÓDŁA – w tym miejscu określamy, jakiego źródła ma dotyczyć ACL:
- WARUNEK-CELU – w tym miejscu określamy, jakiego miejsca docelowego ma dotyczyć ACL:
- WARUNEK1 – jeżeli chcemy odnieść ACL do pojedynczego urządzenia w sieci, to wpisujemy: host 1.2.3.4 (gdzie 1.2.3.4 – to adres IP urządzenia źródłowego);
- WARUNEK2 – jeżeli chcemy zastosować ACL dla grupy urządzeń (przykładowo całej sieci lub podsieci) wówczas stosujemy tzw. maskę odwróconą; Przykładowo, jeżeli chcemy zastosować ACL dla wszystkich urządzeń w sieci: 192.168.1.0 o masce 255.255.255.0, możemy zastosować maskę odwróconą (zwaną też maską blankietową) 0.0.0.255;
- WARUNEK 3 – jeżeli ACL ma mieć zastosowanie do wszystkich urządzeń z dowolnej sieci – wówczas wystarczy wpisać słowo: any;
- NR-PORTU – w tym miejscu określamy, warunek filtrowania bazujący na numerze portu (tylko jeśli wybraliśmy typ protokołu TCP lub UDP):
- Opcja NR-PORTU składa się z symbolu operatora oraz numeru lub nazwy portu – szczegółowy opis umieściliśmy w tabelach, znajdujących się w dalszej części podrozdziału;

Typy protokołów stosowane w rozszerzonych ACL:

- IP
- ICMP
- TCP
- UDP

Maska odwrotna (blankietowa) (*ang. wildcard mask*) – ciąg binarnych zer i jedynek, służących do filtrowania pojedynczych adresów IP lub ich grup. Zera oznaczają bity adresu IP, które mają zostać dopasowane, a jedynki wskazują bity które mają być ignorowane. Na przykład maska blankietowa **0.0.0.3** oznacza dopasowywanie pierwszych **30** bitów adresu IP.

Symbole operatorów dla opcji NR-PORTU stosowane w rozszerzonych ACL znają się w następującej tabeli.

Symbol operatora	***Przeznaczenie***
eq	równy
gt	większy od
lt	mniejszy od
neg	nie równy
range	zakres

Rodzaje operatorów dla protokołów TCP i UDP.

Numery (oraz nazwy) tzw. dobrze znanych portów dla opcji NR-PORTU stosowane w rozszerzonych ACL znajdują się w następującej tabeli.

Numer (nazwa) portu	***Przeznaczenie***
21 (ftp)	Protokół FTP
23 (telnet)	Usługa Telnet
25 (smtp)	Protokół SMTP
80 (www)	Protokół HTTP
110 (pop3)	Protokół POP wersja 3
0 – 65535	Dowolny port z podanego zakresu

Numery i nazwy portów dla protokołów TCP i UDP.

Przykład

```
access-list 100 deny tcp host 192.168.1.1
host 192.168.1.3 eq 80
```

3. NAZYWANE ACL

KONFIGUROWANIE NAZYWANYCH ACL wymaga podania następującego polecenia (określającego rodzaj ACL: **standard, extended**):

ip access-list

Konfigurowanie jest takie same jak w przypadku list przedstawionych wyżej, wymaga podania nazwy zamiast numeru listy.

ip access-list standard <nazwa-listy> **ip access-list extended <nazwa-listy>**

Przykład

```
ip access-list extended BLOCK_WWW
deny tcp any host 2.2.2.2 eq www
permit ip any any
```