Listy dostępu systemu Cisco IOS

Obsługa routera Cisco

Konsola zarządzania routera firmy Cisco pracującego pod kontrolą systemu operacyjnego IOS może pracować w **trybie zwykłym** lub **uprzywilejowanym**, sygnalizowanymi różnymi znakami zachęty konsoli routera.
Tryb zwykły: **`ROUTER>`**
Tryb uprzywilejowany: **`ROUTER#`**
Większość opisanych poniżej poleceń, wymaga trybu uprzywilejowanego (ilość poleceń w obu trybach można porównać, wykonując polecenie **`?`**, powodujące wypisanie wszystkich dostępnych poleceń).
Na przejście do trybu uprzywilejowanego pozwala polecenie: **`enable`**. Po jego wydaniu należy wprowadzić odpowiednie hasło.

Tryb uprzywilejowany udostępnia, między innymi, polecenie **`configure`**, które powoduje przejście do **trybu konfiguracji routera**. Na pytanie o sposób konfiguracji odpowiadamy **`terminal`**, lub, jeśli terminal jest wyświetlony jako opcja domyślna (w nawiasach kwadratowych), po prostu naciskając ENTER.
Tryb konfiguracji: **`ROUTER(config)#`**
Tryb ten udostępnia własny zestaw poleceń, dotyczących głównie zamiany ustawień routera.

W obrębie tego trybu można wchodzić do „pod-menu", na przykład w celu zmiany ustawień interfejsu (poleceniem np.: **`interface ethernet 1`** – konfiguracja interfejsu ethernetowego numer 1).
Przejście do takiego pod-menu, sygnalizowane jest zmianą znaku zachęty.
Pod-menu konfiguracji interfejsu sieciowego: **`ROUTER(config-if)#`**
Wyjście z pod-menu, do głównego menu konfiguracji, możliwe jest z użyciem polecenia **`exit`**.

Wyjście z trybu konfiguracji do trybu uprzywilejowanego, następuje po wydaniu polecenia **`end`** lub naciśnięciu **Ctrl+Z**.
Wprowadzone w ten sposób zmiany konfiguracji dotyczą, tak zwanej, konfiguracji bieżącej (running-config) i zostaną utracone po restarcie routera.

Mechanizm Help systemu IOS

System IOS jest wyposażony w rozbudowany system pomocy. Poniżej przedstawiono podstawowe sposoby jego wykorzystania.
Polecenie:
? – powoduje wypisanie listy wszystkich dostępnych w danym trybie poleceń.
***ciąg_znaków*?** – powoduje wypisanie wszystkich dostępnych poleceń rozpoczynających się od podanego ciągu znaków
***ciag_znaków*<TAB>** – powoduje uzupełnienie ciągu znaków do pełnego polecenia, o ile można to zrobić jednoznacznie
***polecenie* ?** – powoduje podanie opisu następnego argumentu którego wymaga polecenie. Ta możliwość jest szczególnie przydatna, gdyż pozwala nam stworzyć odpowiednie polecenie krok po kroku, dopisując kolejne parametry i wywołując po każdym pomoc dotyczącą następnego. Jeśli router wyświetla na liście możliwości **<cr>** można nakazać wykonanie polecenia, naciskając ENTER.

Konfiguracja IP interfejsów sieciowych

Do wyświetlenia aktualnej konfiguracji IP interfejsów sieciowych używamy polecenia:
`show ip interface [`*`interfejs`*`]`

Interfejs podajemy jako parę wartości: <*typ*> <*numer*>. Na przykład: ethernet 2.

Aby zmienić konfigurację interfejsu wchodzimy do trybu konfiguracji, a następnie do pod-menu danego interfejsu sieciowego używając polecenia:
`interface <typ interfejsu> <nr interfejsu>`
Gdzie:

- typ interfejsu – np: ethernet, fddi, serial itp.
- nr interfejsu – numer kolejny interfejsu w obrębie danego typu. Patrz rozdział „Numeracja interfejsów" poniżej.

W pod-menu mamy możliwość użycia następujących poleceń:
`ip address <adres IP> <maska>` - aby zmienić adres IP oraz maskę IP,
`shutdown` – aby wyłączyć interfejs,
`no shutdown` – aby włączyć interfejs.
Po dokonaniu zmian wychodzimy z trybu konfiguracyjnego.

Numeracja interfejsów

Interfejsy routerów Cisco numerowane są od 0, oddzielnie dla każdego z typów, np.: ethernet, fddi, serial… W obrębie jednego typu, niższe numery mają moduły zlokalizowane z prawej strony routera. W obrębie jednego modułu interfejsy opisane są numerami wskazującymi na kolejność ich liczenia. Na przykład jeśli nasz router ma 2 moduły Ethernetowe i jeden moduł FDDI to:
Ethernet 0 – port 0 z prawego modułu Ethernet,
Ethernet 1 – port 1 z prawego modułu Ethernet,
Ethernet 2 – port 0 z lewego modułu Ethernet,
Ethernet 3 – port 1 z lewego modułu Ethernet,
Fddi 0 – jedyny port FDDI.

ACL - Informacje ogólne

Aby skorzystać z mechanizmów filtrowania ruchu, opartych na listach dostępu (Access Control Lists – ACLs), należy:

- stworzyć listę ACL, dodając do niej reguły,
- przypisać listę ACL do interfejsu – jeden interfejs może obsługiwać tylko jedną listę ACL.

Router będzie, dla każdego pakietu przechodzącego przez interfejs, przeszukiwał nakazaną listę ACL do czasu napotkania pierwszej pasującej reguły. Jeśli znajdzie pasującą regułę, wykona zawarte w niej polecenie (**permit** lub **deny**) i zakończy przeszukiwanie listy. Jeśli żadna pasująca reguła nie zostanie odnaleziona, wobec pakietu zostanie zastosowanie działanie **deny**.
Listy ACL dotyczą wyłącznie ruchu przychodzącego z zewnątrz, a nie generowanego przez router.

Opisane poniżej polecenie **access-list**, pozwala na dodawanie reguł do list ACL. Lista do której chcemy dodać regułę nie musi być „tworzona" w jawny sposób – stanie się to automatycznie po dopisaniu do niej pierwszej reguły. Reguły dopisywane poleceniem **access-list** dodawane są zawsze na koniec danej listy ACL.
Nie ma możliwości edycji bądź usunięcia wybranej reguły z listy ACL. W takim przypadku należy usunąć całą listę poleceniem **no access-list <*nr listy*>** i stworzyć ją ponownie wprowadzając pożądane reguły.

Stworzoną listę ACL należy przypisać do interfejsu opisanym poniżej poleceniem **access-group**. Z chwilą przypisania zacznie być ona uwzględniana przy przetwarzaniu pakietów. Przypisanie nie istniejącej listy ACL lub skasowanie poleceniem **no access-list** listy ACL przypisanej aktualnie do interfejsu, spowoduje przekazywanie przez ten interfejs dowolnego ruchu, do czasu ponownego stworzenia tej listy ACL.

Wyświetlanie stworzonych list ACL i statystyk

`show access-list [`*`<nr listy>`*`]`

Jeśli podamy to polecenie bez parametru, to spowoduje to wyświetlenie zawartości wszystkich (podstawowych i rozszerzonych) list ACL danego routera.
Podanie parametru **<nr listy>** spowoduje wyświetlenie tylko listy ACL o podanym numerze.
W otrzymanej tabeli, w nawiasach podawana jest liczba pakietów przetworzonych z użyciem danej reguły, co może okazać się przydatne dla celów diagnostyki i usuwania błędów.

Dodawanie reguł

Listy podstawowe

`access-list` *`<nr listy 1-99>`* **`{permit | deny}`** *`<adres IP> [maska wzorca]`*

gdzie:

- **<nr listy>** - numer listy ACL którą modyfikujemy. Listy podstawowe IP mają numery 1-99.
- **{permit | deny}** – decyzja czy dany pakiet przepuścić (permit) czy odrzucić (deny).
- **<adres IP>** - adres IP który zostanie porównany z zawartym w nagłówku pakietu,
- **opcjonalnie: <maska wzorca>** – określa które bity adresu są porównywane. Jeśli dany bit jest ustawiony na 0 to musi on być zgodny z ustawionym w parametrze <*adres IP*>. Jeśli bit maski wzorca ma wartość 1 to jego wartość nie jest brana pod uwagę przy porównywaniu. Np: 0.0.255.255 oznacz, że porównywane są 2 pierwsze bajty.
  Brak parametru oznacza przyjęcie maski 0.0.0.0.

Przykłady:

`access-list 1 permit 192.168.1.1` – powoduje dopisanie do listy ALC nr 1, reguły nakazującej przepuszczenie ruchu od adresu 192.168.1.1

`access-list 1 permit 192.168.1.0 0.0.0.255` – powoduje dopisanie do listy ALC nr 1, reguły nakazującej przepuszczenie ruchu od adresów rozpoczynających się od 192.168.1, czyli od 192.168.1.0 do 192.168.1.254.

`access-list 1 deny 0.0.0.0 255.255.255.255` – powoduje dopisanie do listy ALC nr 1, reguły nakazującej zablokowanie ruchu ze wszystkich adresów IP.

Listy rozszerzone

`access-list` *`<nr listy 100-199>`* **`{permit | deny}`** *`<protokół>`*
`<definicja punktu źródłowego>`
`<definicja punktu docelowego>`
`[established] [log]`

gdzie:

- **<nr listy>** - numer listy ACL którą modyfikujemy. Listy rozszerzone IP mają numery 100-199.
- **{permit | deny}** – decyzja czy dany pakiet przepuścić (permit) czy odrzucić (deny).
- **<protokół>** - protokół którego dotyczy dana reguła. Możliwe wartości: ***ip, tcp, udp, icmp,*** lub ***numer protokołu ip.***
- **<definicja punktu źródłowego>** i **<definicja punktu docelowego>**
  Definiowane w ten sam sposób mają następującą składnię:
  `<adres IP> [maska wzorca]` **`[{eq|neq|gt|ln|range}`** *`<port(y)>`*`]`
  gdzie:
  - **<adres IP>** - jak w przypadku list prostych,
  - **opcjonalnie: [maska wzorca]** – jak w przypadku list prostych.
  - **{eq | neq| gt | ln | range} <port(y)>** - określa jakiego zbioru portów dotyczy reguła.
    - eq <port> – nr portu równy parametrowi <port>

        - neq <port> - nr portu różny od parametru <port>
        - gt <port> – nr portu większy od parametru <port>
        - ln <port> – nr portu mniejszy od parametru <port>
        - range <port1> <port2> – nr portu zawarty w przedziale od <port1> do <port2> (włącznie).
- **opcjonalnie: established** – opcja dostępna tylko dla protokołu TCP. Powoduje, że reguła dotyczy wszystkich pakietów już zestawionego połączenia TCP, niezależnie od portu docelowego i źródłowego (których nie podajemy). Np.: **access-list 101 permit tcp 192.168.1.1 any established** – nakazuje przepuszczać ruch należący do już zestawionych połączeń TCP pomiędzy adresem 192.168.1.1 a wszystkimi innymi.
- **opcjonalnie: log** – powoduje rejestrowanie pasujących do reguły pakietów w logu systemowym.

Przykłady:
access-list 100 permit tcp 10.1.1.1 0.0.0.0 gr 1023 0.0.0.0 255.255.255.255 eq 436
Powoduje dopisanie do listy nr 100, reguły przepuszczającej ruch TCP z adresu 10.1.1.1, z portów źródłowych większych od 1023, skierowany do dowolnych docelowych adresów IP na port 436.

access-list 100 permit udp 10.15.1.1 eq 123 192.168.5.0 0.0.0.255 range 1024 2048
Powoduje dopisanie do listy nr 100, reguły przepuszczającej ruch UDP z adresu 10.15.1.1, z portu 123, do docelowych adresów IP rozpoczynających się sekwencją 192.168.5 na porty od 1024 do 2048.

access-list 100 deny icmp 0.0.0.0 255.255.255.255 0.0.0.0 255.255.255.255 log
Powoduje dopisanie do listy nr 100, reguły blokującej ruch ICMP z dowolnego źródłowego adresu IP do dowolnego docelowego adresu IP i zapisywanie informacji o takich pakietach w logu systemowym.

Przypisanie listy do interfejsu

W trybie konfiguracyjnym wchodzimy do menu konfiguracyjnego określonego interfejsu z użyciem polecenia:
`interface {ethernet | fddi } <nr interfejsu>`
przypisujemy daną listę do interfejsu poleceniem:
`ip access-group <nr listy> {in | out}`
gdzie:

- <nr listy> – numer, stworzonej wcześniej, listy ACL, którą chcemy przypisać do interfejsu.
- {in | out} – decyzja, czy lista ACL ma dotyczyć ruchu odbieranego (in) czy wysyłanego (out) przez interfejs.

Usuwanie list ACL

Listy ACL usuwamy poleceniem:
`no access-list <nr listy>`
Usunięcie listy ACL nie powoduje likwidacji przypisania listy do interfejsu. Interfejs z przypisaną nieistniejącą listą przenosi dowolny ruch sieciowy.

Likwidacja przypisania listy do interfejsu

Przypisanie listy ACL do interfejsu likwidujemy z menu konfiguracyjnego danego interfejsu, z użyciem polecenia:
`no ip access-group <nr listy> {in | out}`
Likwiduje to przypisanie określonej listy do interfejsu.
Polecenie **`no ip access-group in`** likwiduje wszystkie przypisania ograniczające ruch odbierany na interfejsie, a **`no ip access-group out`** – wszystkie przypisania ograniczające ruch wysyłany

przez interfejs. Polecenie **`no ip access-gorup`** likwiduje wszystkie przypisania list ACL do interfejsu.

Inne przydatne polecenia

ping <adres> – wysyła, z routera, ping pod podany adres
connect <adres> – łączy się telnetem pod wskazany adres
write terminal – powoduje wyświetlenie skryptu konfiguracji routera, zawierającego jego obecnie aktywne ustawienia (running-config).

Inne uwagi

Przy podawaniu adresów IP i masek w regułach list ACL, można posłużyć się następującymi skrótami:
`any = 0.0.0.0 255.255.255.255`
`host <adres IP> = <adres IP> 0.0.0.0`
Przykładowo pozwoli to na zapisanie, wyżej przytoczonych przykładów reguł z rozszerzonej listy ACL w postaci:
Przykład 1:
access-list 100 permit tcp 10.1.1.1 0.0.0.0 gr 1023 0.0.0.0 255.255.255.255 eq 436
access-list 100 permit tcp host 10.1.1.1 gr 1023 any eq 436
Przykład 2:
access-list 100 deny 47 0.0.0.0 255.255.255.255 0.0.0.0 255.255.255.255 log
access-list 100 deny 47 any any log

Polecenie „nc" systemu Windows

Program narzędziowy netcat, wywoływany poleceniem nc, pozwala na:

- dokonywanie połączeń TCP i wysyłanie pakietów UDP pod wskazany adres i port,
- tworzenie procesów oczekujących na połączenia TCP lub pakiety UDP na określonych portach.

Domyślnie dane do wysłania wprowadzane są z klawiatury, a odbierane wyświetlane na ekranie. Aby zakończyć połączenie należy użyć **Ctrl+Z** lub **Ctrl+C**.
Pomoc dotyczącą składni polecenia można uzyskać wywołując je z opcją **-h**.

Polecenie to będzie nam przydatne do testowania dostępności usług funkcjonujących na innych komputerach.

Ogólna składnia:

Połączenia wychodzące:
`nc [opcje] <adres docelowy> <port docelowy>`
Opcje:
-p <port> – łącz/wysyłaj z podanego portu źródłowego,
-s <adres> – łącz/wysyłaj z podanego adresu źródłowego,
-u – użyj protokołu UDP (domyślnie TCP),
-v - podaje informacje o działaniach programu w trakcie ich wykonywania.
Na przykład polecenie **`nc -u -p 11254 200.0.0.1 17`** powoduje wysyłanie pakietów UDP pod adres 200.0.0.1 na port 17 z własnego portu 11254.

Tworzenie procesów oczekujących:
`nc -l -p <port> [opcje]`
Opcje:

-u – użyj protokołu UDP (domyślnie TCP),
-v - podaje informacje o działaniach programu w trakcie ich wykonywania.
Na przykład polecenie `nc -l -p 256` powoduje rozpoczęcie oczekiwania na połączenie na porcie TCP 256.
Program zakończy działanie po obsłużeniu 1 połączenia. Aby po jego zakończeniu czekał on na następne (do momentu aż zakończymy jego działanie przez Ctrl+C) należy użyć opcji **-L** w miejsce **-l**.

Lista portów wybranych usług IP

Port	Protokół	Usługa
7	TCP/UDP	Echo
13	TCP/UDP	Daytime
17	TCP/UDP	Quote of the day (qotd)
19	TCP/UDP	Chargen
23	TCP	Telnet