Opracował: Konrad Kawecki <cogi@pjwstk.edu.pl>

Tematyka

Listy kontroli dostępu.

ACL

Za pomocą list kontroli dostępu możemy klasyfikować ruch sieciowy. Poniżej mamy przykład ACL (polecenie wykonujemy w trybie konfiguracji).

```
access-list 100 deny udp 192.168.0.0 0.0.0.255 any eq domain
access-list 100 permit ip any any
```

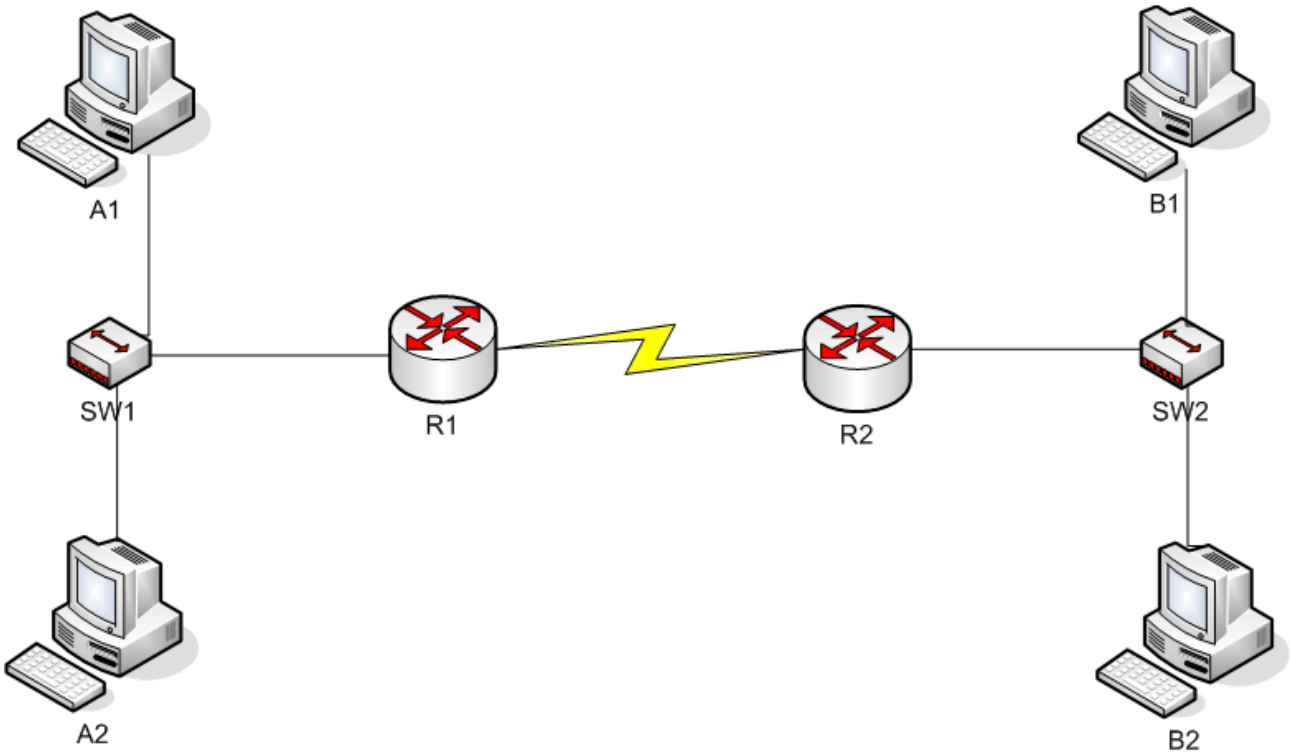
Za pomocą tej ACL blokujemy dostęp do usługi DNS wszystkich hostom z podsieci 192.168.0.0/24.

ACL musimy przypisać do interfejsu, wykonujemy to poniższym poleceniem (polecenie wykonujemy w trybie konfiguracji interfejsu).

```
ip access-group 100 in
```

W tym przypadku umieściliśmy listę w kierunku „do interfejsu”.

Dokładny opis składni polecenia możesz sprawdzić korzystając z systemu pomocy IOS.



Ćwiczenie 1

Zbuduj sieć jak na ilustracji 1.
A1 – 192.168.0.1/24
A2 – 192.168.0.128/24
R1 – 192.168.0.254/24

B1 – 192.168.1.1/24
B2 – 192.168.1.128/24
R2 – 192.168.1.254/24

Zablokuj możliwość korzystania z „ICMP – echo request”:
A1 do B2
B1 do A2

Ćwiczenie 2

Konfiguracja sieci jak w ćwiczeniu 1.

Zablokuj możliwość korzystania z „ICMP – echo request”:
Komputerom o adresach 192.168.0.1 - 192.168.0.127 do B2
Komputerom o adresach 192.168.1.128 – 192.168.1.254 do A2