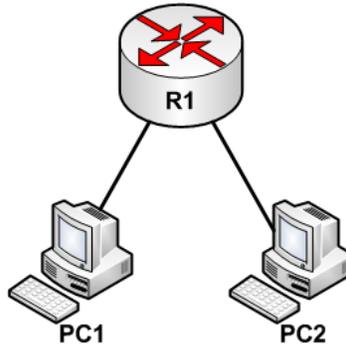


Filtrovanie komunikácie pomocou ACL



Zariadenie	Rozhranie	IP adresa	Maska podsiete
R1	Smerom k PC1	192.168.1.1	255.255.255.0
R1	Smerom k PC2	192.168.2.1	255.255.255.0
PC1	NIC	192.168.1.10	255.255.255.0
PC2	NIC	192.168.2.10	255.255.255.0

Úlohy:

1. Ubezpečte sa, že sú zariadenia čisté, prípadne ich vyčistite.
2. Nakonfigurujte pomenovanie (hostname), heslo na konzolu, heslo do privilegovaného režimu, heslo pre telnet pripojenie a pridajte výstižný popis (description) na jednotlivé rozhrania. Deaktivujte preklad domén a synchronizujte logovanie.
3. Nastavte zariadeniam IP adresy podľa zobrazenej tabuľky (nezabudnite na predvolenú bránu na PC).
4. Vytvorte rozšírený ACL, ktorý zabezpečí aby sa PC1 mohol pripojiť na HTTP server bežiaci na PC2, ale PC2 sa nemohol pripojiť na HTTP server bežiaci na PC1. Ostatná komunikácia má byť povolená.

```
Router(config)# access-list <100-199> {permit|deny} <protocol> <source-ip>  
<wildcard-mask> [<operator> <source-port>] <dest-ip> <wildcard-mask>  
[<operator> <dest-port>] [established]
```

5. Aplikujte tento ACL na vhodné rozhranie a zvolte smer, pri ktorom má byť komunikácia filtrovaná.

```
Router(config-if)# ip access-group <acl-number> {in | out}
```

6. Vytvorte štandardný ACL, ktorý povolí telnet pripojenie len zo siete PC1.

```
Router(config)# access-list <1-99> {permit|deny} <source-ip> <wildcard-mask>
```

7. Aplikujte tento ACL na všetky nakonfigurované kanály vzdialeného pripojenia (line vty).

```
Router(config-line)# access-class <acl-number> in
```

8. Overte správnosť konfigurácie a overte funkčnosť filtrovania.

```
Router# show access-lists
```

Command summary

```
Router(config)# access-list <num> {permit|deny} <source-ip> <wildcard-mask>  
Router(config)# access-list <num> {permit|deny} <protocol> <source-ip>  
<wildcard-mask> [<operator> <source-port>] <dest-ip> <wildcard-mask>  
[<operator> <dest-port>] [established]
```

```
Router(config)# ip access-list {standard|extended} <name>  
Router(config-ext-nacl)# {permit|deny} <protocol> <source-ip> <wildcard-mask>  
[<operator> <source-port>] <dest-ip> <wildcard-mask> [<operator> <dest-port>]  
[established]
```

```
Router(config-if)# ip access-group <acl-number> {in | out}  
Router(config-line)# access-class <acl-number> in  
Router(config-if)# no ip unreachable
```

```
Router# clear access-list counters [<acl-number>|<acl-name>]  
Router# show access-lists
```

ACL for IPv6

```
Router(config)# ipv6 access-list <name>  
Router(config-ipv6-acl)# {permit|deny} <protocol> <source-ipv6/prefix-length>  
[<operator> <source-port>] <dest-ipv6/prefix-length> [<operator> <dest-port>]  
[established] [sequence <value>]
```

```
Router(config-if)# ipv6 traffic-filter <acl-name> {in | out}  
Router(config-line)# access-class <acl-name> in
```

```
Router#show access-lists  
Router#show ipv6 access-list [<name>]
```