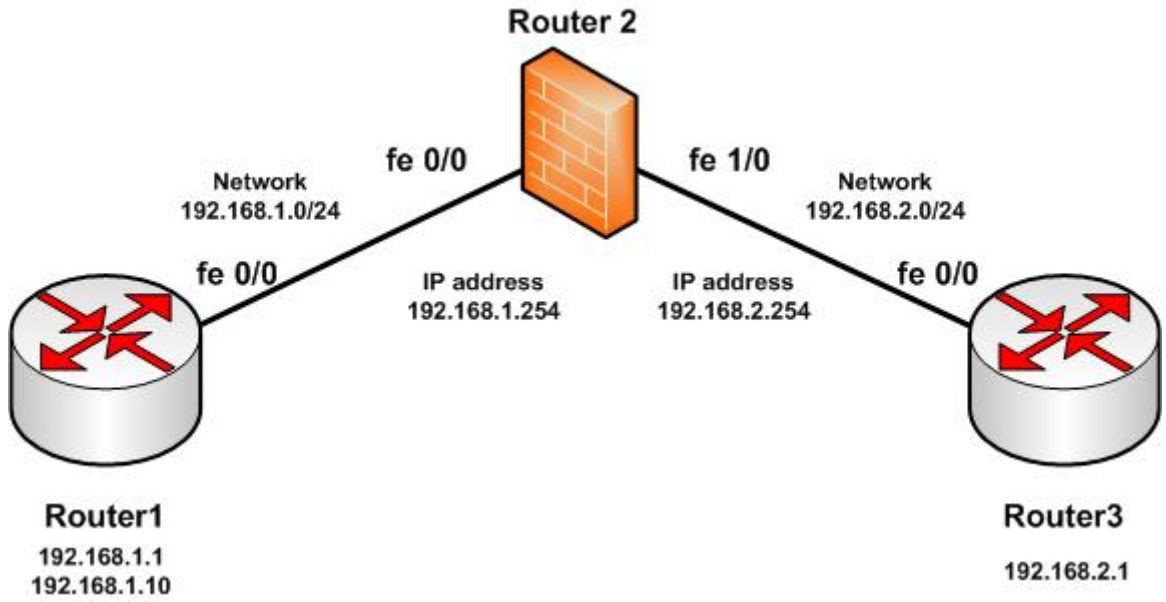
Úloha č. 4

Filtrování provozu v síti IP

Úkol:

a) použijte konfiguraci směrovačů z úlohy č. 2
b) na Router 1 přidejte další IP adresu 192.168.1.10
c) na Router 3 přidejte další IP adresu 192.168.2.10
d) vyzkoušejte funkci standardního ACL:
   nastavte Router 2 jako firewall mezi sítěmi zakažte veškerý odchozí provoz ze sítě 192.168.1.0/24, povolte výjimku pouze pro IP adresu 192.168.1.10
e) zrušte standardní ACL
f) vyzkoušejte funkci rozšířeného ACL:
   nastavte Router 2 firewall mezi sítěmi zakažte veškerý příchozí provoz do sítě 192.168.1.0/24 kromě protokolu ICMP. Nastavte ACL tak, aby fungovalo odchozí spojení do sítě 192.168.2.0/24.
g) Povolte ze sítě 192.168.2.0/24 připojení TELNET na IP adresu 192.168.1.10
h) ujistěte se, aby nastavení fungovalo i po restartu

Popis:



Propojení směrovačů v labu

Příkazy:

enable	přechod do privilegovaného režimu
show running-config	zobrazí aktuální konfiguraci
ip address <ip-adr> <mask> **secondary**	přidá další IP adresu k rozhraní
ping <ip-address>	příkaz ping
write memory	uloží konfiguraci
configure terminal	přechod do konfiguračního režimu
?	nápověda

Wildcard maska:

Při definici ACL se používají tzv. wildcard masky. Jedná se v podstatě o inverzní masku.
Pokud wildcard maska obsahuje bit 0 znamená to: kontroluj daný bit.
Pokud wildcard maska obsahuje bit 1 znamená to: ignoruj daný bit.

Příklad:

síť	**bitů/podsíť**	**maska**	**wildcard maska**
192.168.1.0	24	255.255.255.0	0.0.0.255
192.168.1.10	32	255.255.255.255	0.0.0.0
192.168.0.0	16	255.255.0.0	0.0.255.255

Standardní ACL:

- standardní ACL používají označení 1 .. 99
- je možné filtrovat pouze na základě zdrojové adresy
- po definici ACL je nutné jej přiřadit k některému rozhraní

access-list <ACL number> {permit | deny} <source> [mask]

ACL number – identifikuje ke kterému ACL záznam patří, 1..99
permit | deny – povolí nebo zakáže specifikovaný provoz
source – zdrojová IP adresa
source [mask] – identifikuje, které bity se mají testovat; výchozí wildcard maska je 0.0.0.0

Rozšířené (extended) ACL:

- rozšířené ACL používají označení 100..199
- je možné filtrovat na základě zdrojové i cílové IP adresy
- je možné specifikovat typ protokolu
- je možné specifikovat další podmínky (např. číslo portu)
- po definici ACL je nutné jej přiřadit k některému rozhraní

access-list <ACL number> {permit | deny} protocol <source> [mask] <destination> [mask] [operator] [established]

ACL number – identifikuje ke kterému ACL záznam patří, 100..199
permit | deny – povolí nebo zakáže specifikovaný provoz
protocol – specifikuje typ protokolu např. ICMP, IP nebo TCP/IP
source – zdrojová IP adresa
source [mask] – identifikuje, které bity se mají testovat; výchozí wildcard maska je 0.0.0.0
destination – cílová IP adresa
destination [mask] – identifikuje, které bity se mají testovat; výchozí maska je 0.0.0.0
operator – lt (less than), gt (greater than), eq (equal), neq (not equal) a následuje číslo portu
established – pro navázaná TCP spojení. Pro spojení, která mají nastavený ACK bit.

Přiřazení ACL k rozhraní:

Ke konkrétnímu rozhraní se definovaný ACL přiřadí příkazem:

ip access-group <ACL number> {in | out}

ACL number – identifikuje ACL
in | out – identifikuje zda-li se filtr aplikuje jako vstupní nebo jako výstupní

Nápověda:

- Použijte konfiguraci směrovačů z úlohy č.2.
- Místo wildcard masky 255.255.255.255 lze použít příkaz **any**.
- Každý ACL končí implicitním (neviditelným) příkazem **implicit deny all** !