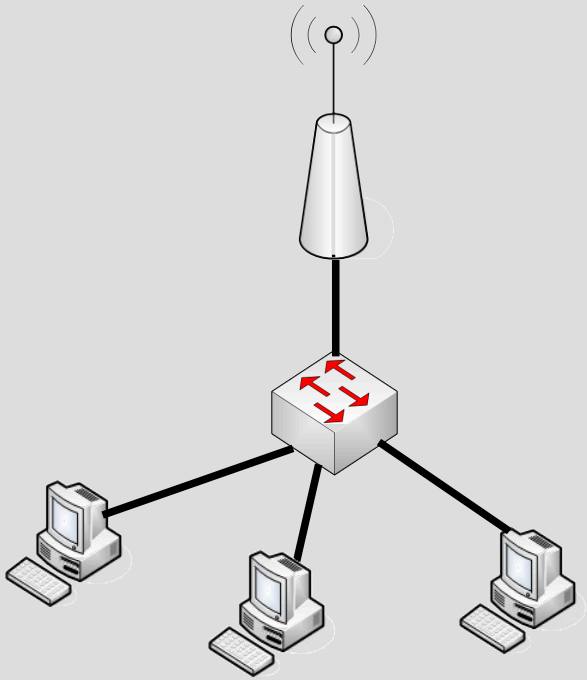
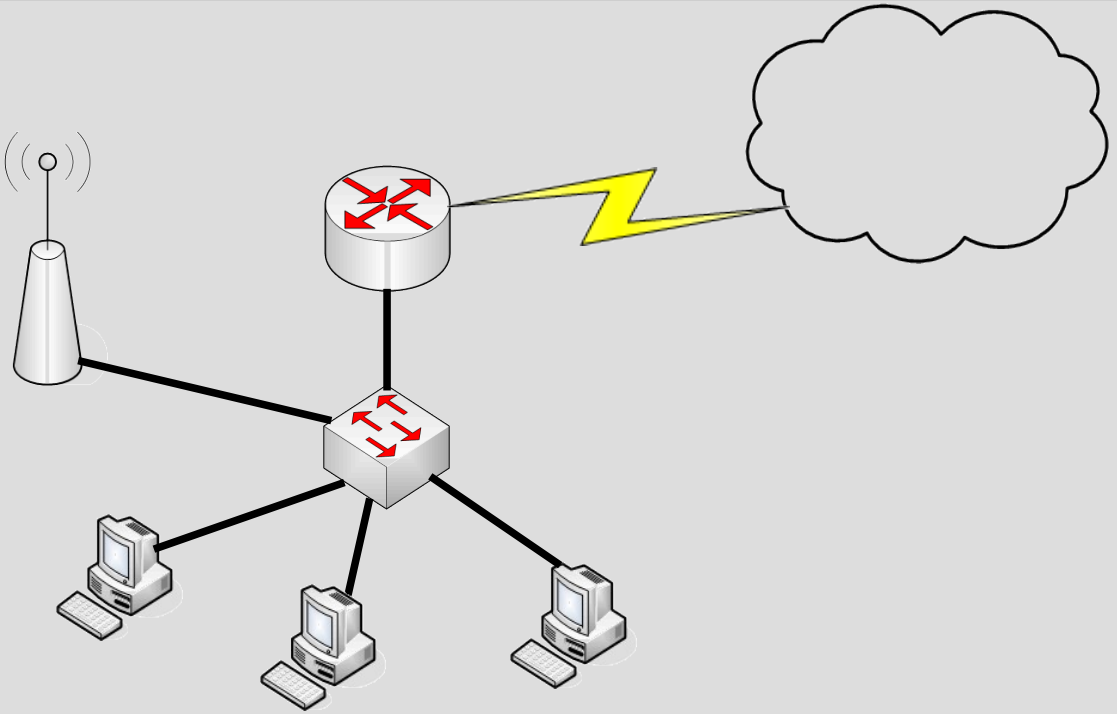
Y36PSI
Návrh sítě

Jednoduchá síť





Požadované služby

- připojení na Internet
  - www
  - ftp
  - mail
  - ssh
- lokální www server
- lokální ssh server
- vzdálené připojení k WinXP

Požadované služby

- připojení na Internet – IP adresy, směrování, DNS, NAT
  - www – firewall, http/https
  - ftp – firewall, aktivní/pasivní spojení
  - mail – firewall, způsob doručení/příjmu
  - ssh - firewall
- lokální www server – určení serveru, firewall, NAT
- lokální ssh server – určení serveru, firewall, NAT
- vzdálené připojení k WinXP – určení serveru, firewall, NAT

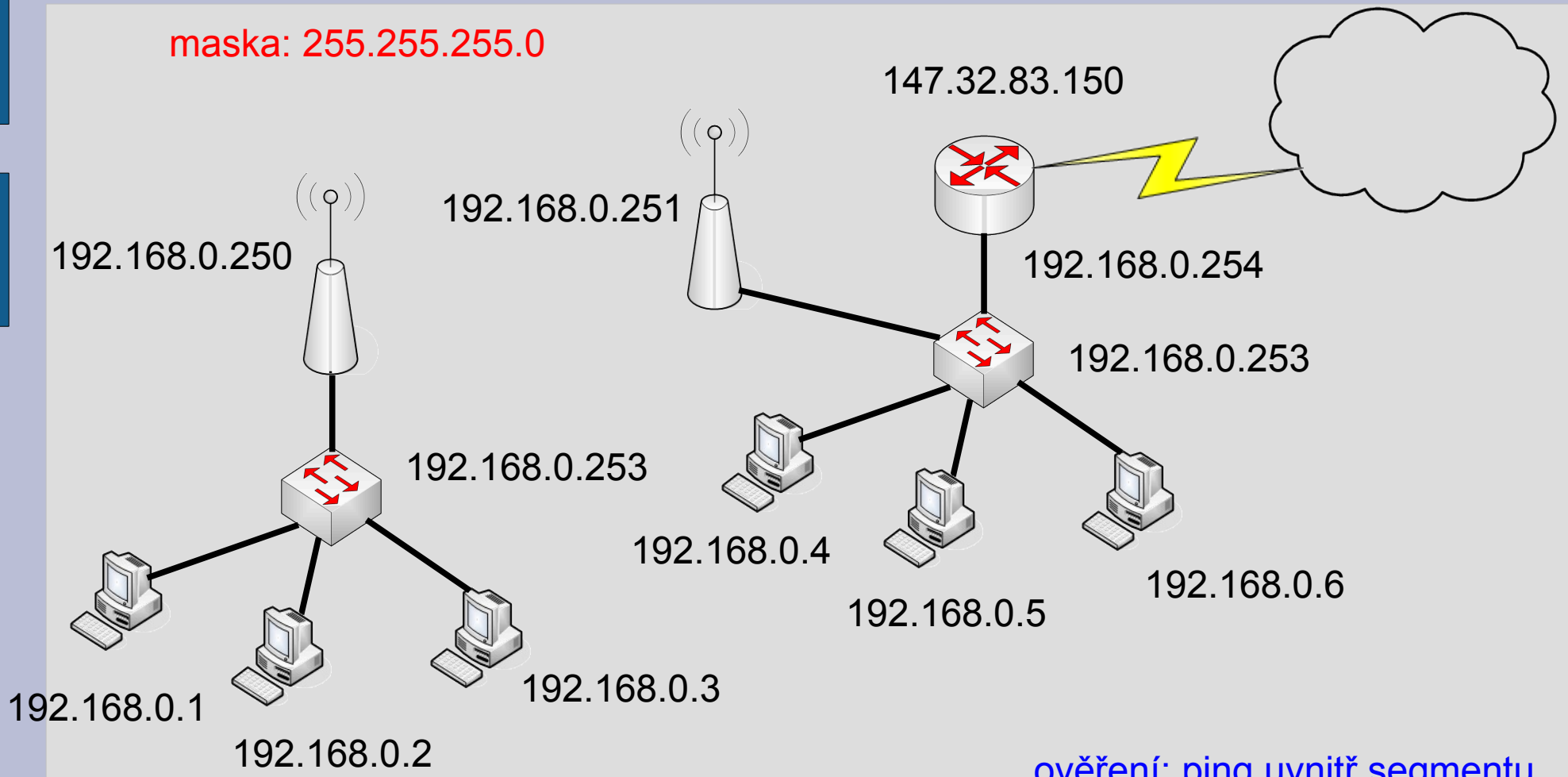
Nastavení

- Adresace
  - privátní/veřejný rozsah
- směrování
  - stačí default brána
- NAT
  - směr do Internetu – SNAT, masquerade
  - vnitřní služby – DNAT
- paketový filtr
  - povolené služby v Internetu
    - problematické služby
  - povolené služby ve vnitřní síti (nebo na směrovači)
  - běžná funkcionalita a útoky

Adresace

- libovolný privátní prostor
  - 192.168.0.0/16 – C
  - 172.16.0.0/12 – B
  - 10.0.0.0/8 - A
  - členění po 8 bitech adresy – doporučuji (netřeba šetřit)
- adresní prostor poskytovatele
  - použijte adresy s rozvahou
- adresy síťových prvků
  - pro správu
- nastavení DNS serveru a domény

Adresace

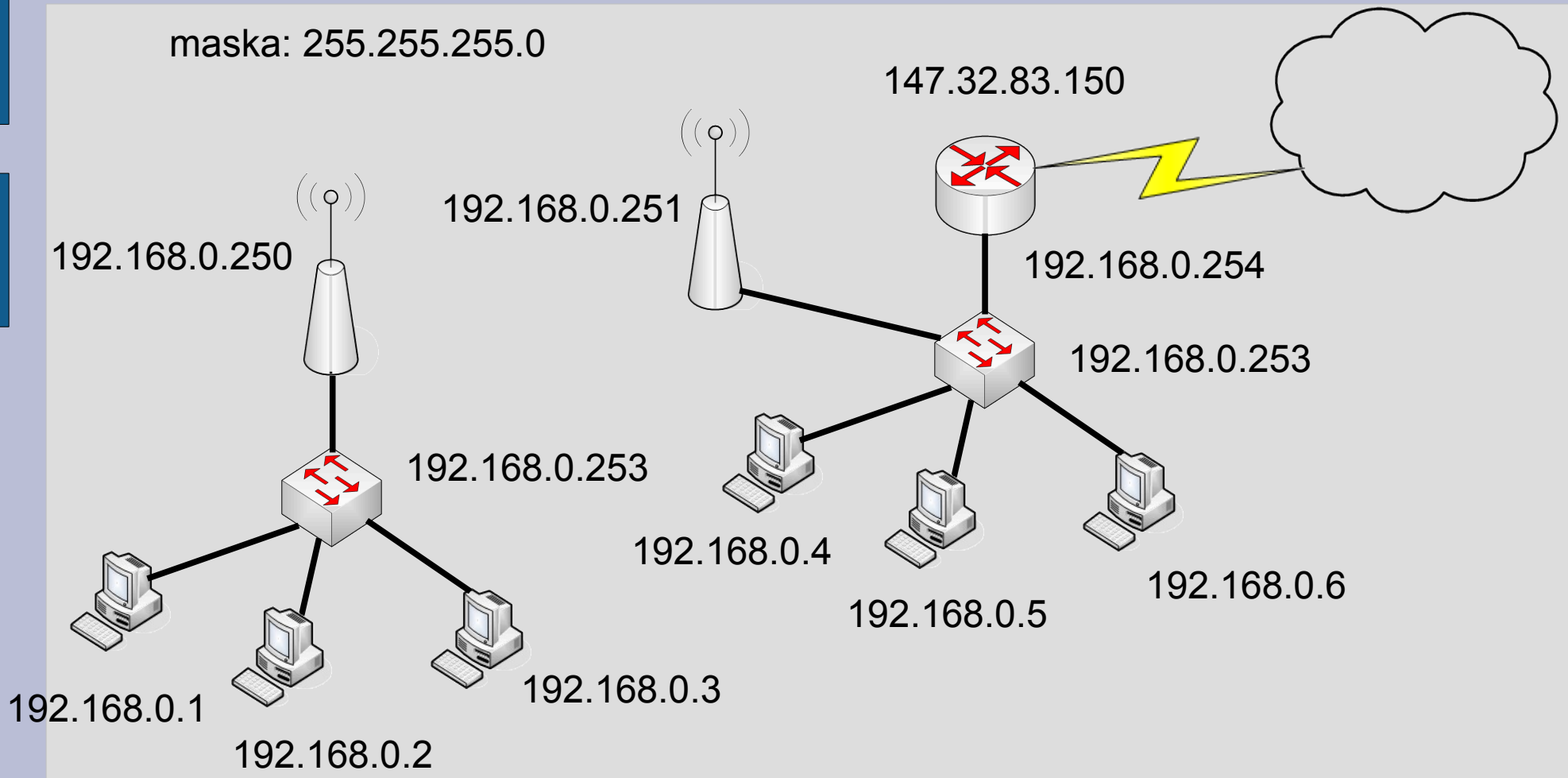


ověření: ping uvnitř segmentu
podle IP a jména

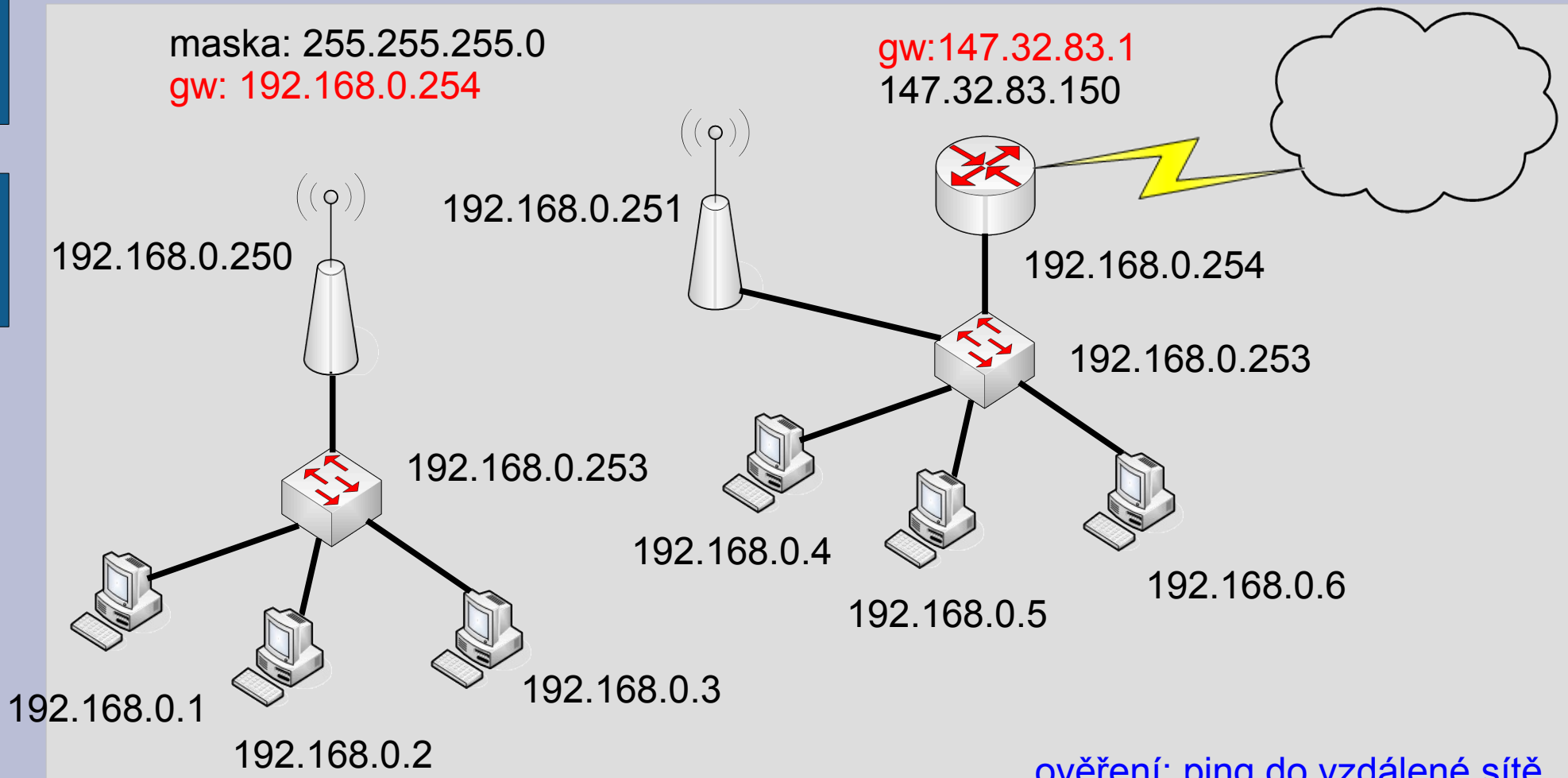
Směrování

- defaultní brána
  - směrem k Internetu
- vnitřní sítě (pokud je víc vnitřních sítí)
- implicitní směrování
  - vzniká automaticky
- PC směrovač
  - zapnout forwarding
- classless směrování
- dynamické směrování

Směrování


maska: 255.255.255.0
147.32.83.150
192.168.0.251
192.168.0.250
192.168.0.254
192.168.0.253
192.168.0.253
192.168.0.4
192.168.0.5
192.168.0.6
192.168.0.1
192.168.0.2
192.168.0.3

Směrování



ověření: ping do vzdálené sítě,
kontrola tabulek

NAT

- komunikace do Internetu
  - masquerade, SNAT
    - iptables -t nat -A POSTROUTING -o eth1 -j SNAT -- to 147.32.83.150
    - iptables -t nat -A POSTROUTING -o eth1 -j MASQUERADE
- vnitřní služby
  - NAT pro hraniční počítač není potřeba
  - DNAT
    - iptables -t nat -A PREROUTING -p tcp -d 147.32.83.150 --dport 22 -j DNAT --to 192.168.0.1:22
    - iptables -t nat -A PREROUTING -d 147.32.83.150 -j DNAT --to 192.168.0.1

Paketový filtr

- defaultní politika
  - všechno zakázat
  - všechno povolit
- povolení komunikace do Internetu
  - většinou to není bezpečnostní riziko
- povolení komunikace k vnitřním službám
  - bezpečnostní riziko
- ochrana hraničního směrovače

Paketový filtr

- defaultní politika
  - všechno zakázat
    - iptables -P INPUT DROP
    - iptables -P OUTPUT DROP
    - iptables -P FORWARD DROP
  - všechno povolit
    - ACCEPT
  - nežádoucí adresy
    - iptables -A FORWARD -i eth1 -s 192.168.0.0/16 -j DROP
- povolení komunikace do Internetu
  - většinou to není bezpečnostní riziko
    - iptables -A FORWARD -i eth0 -j ACCEPT

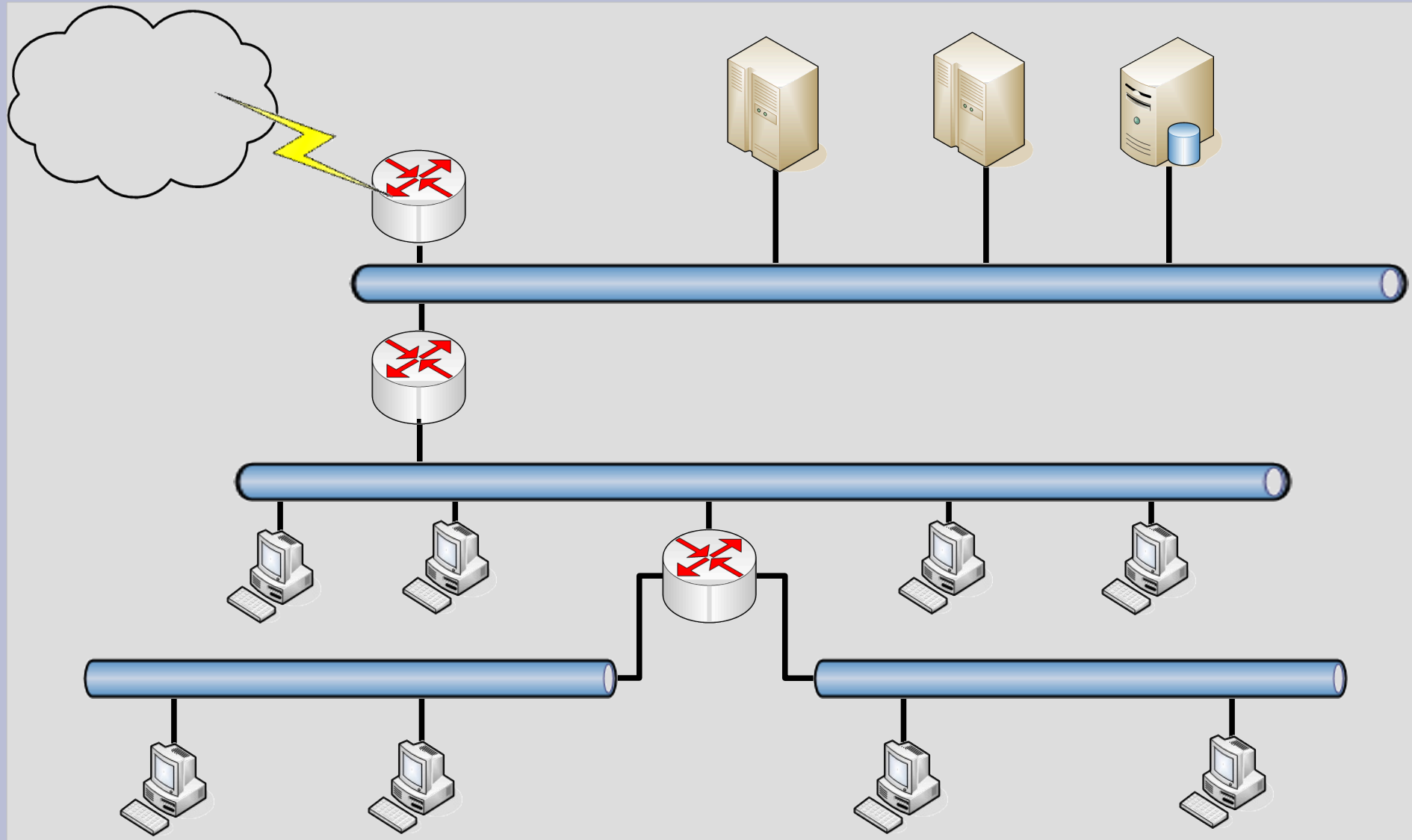
Paketový filtr

- povolení komunikace k vnitřním službám
  - bezpečnostní riziko
    - iptables -A FORWARD -i eth1 -o eth0 -m state --state ESTABLISHED,RELATED -j ACCEPT
    - iptales -A FORWARD -i eth1 -o eth0 -p tcp -d 192.168.0.1 --dport ssh -j ACCEPT

Paketový filtr

- ochrana hraničního směrovače
  - www, mail, ssh (80, 443, 25, 22)
    - iptables -A INPUT -i eth1 -p TCP --dport 22 --src 147.32.83.179 -j ACCEPT
    - iptables -A INPUT -i eth1 -p ICMP --icmp-type echo-request -j ACCEPT
    - iptables -A INPUT -d 147.32.83.150 -m state --state ESTABLISHED,RELATED -j ACCEPT
    - iptables -A INPUT -i lo -j ACCEPT
    - iptables -A INPUT -i eth0 -j ACCEPT
    - iptables -A OUTPUT -s 147.32.83.150 -j ACCEPT
    - iptables -A OUTPUT -s 192.168.0.254 -j ACCEPT

Složitější síť



vpn
správa
...