Sítě - návod

VLAN

Na obou switchích

```
Switch(config)# vlan <cislo_vlan>
SW2(config-vlan)# name <jmeno_vlan>
! Access mode (zařízení)
Switch(config)# int <port_klienta>
Switch(config-if)# switchport mode access
Switch(config-if)# switchport access vlan <cislo_vlan>
! Trunk mode (switch)
Switch(config)# int <port_switche>
Switch(config-if)# switchport mode trunk
Switch(config-if)# switchport trunk allowed vlan <cisla_vlan>
```

- Nastavují se na **switchích**
- Vytvoříme VLANy (každé dáme příslušné číslo a taky jméno)
- Na portu, který vede do zařízení (server, PC), nastavíme **access** a uvedeme zde číslo VLAN, ve které je
- Na portu, který vede do routeru, nastavíme **trunk** a uvedeme zde čísla všech VLAN oddělených čárkami

SUBINTERFACE

Na prvním portu routeru (vedoucí do switche)

```
Router(config)# int <nazev_int>.<cislo_vlan>
Router(config-subif)# encapsulation dot1q <cislo_vlan>
Router(config-subif)# ip address <dg_adresa> <maska>
```

- Nastavíme na klasickém interface, jen za něj dáme tečku, za kterou dáme číslo VLAN, jejíž DG nastavujeme
- Enkapsulace musí být u každé sítě, i když je jen jedna VLAN

STATICKÝ ROUTING

Na všech routerech

```
Router(config)#ip route <cilova_sit> <maska_cilove_site> <dalsi_port>
Router(config)# ip route 0.0.0.0 0.0.0.0 <next_hop>
! Default route
Router(config)#ip route 0.0.0.0 0.0.0.0 <ip_serveru>
```

- Jako cílovou síť nastavujeme síť, ke které router není připojen (síť je za hranicemi jiného routeru)
- Další port (next hop) je interface, který je připojený k jinému routeru směrem k nám
- Musíme nastavit vždy 2x, protože protože jsou zde 2 trasy, kterýma může packet projít
- Default route má samé nuly, nastavuje se na hraničním routeru a její next hop je ip adresa serveru

OSPF ROUTING

Na všech routerech

```
Router(config)#router ospf 1
Router(config-router)# network <blizka_sit> <wildcard> area 0
! Default routa se nastavuje na hraničním routeru
Router(config)# ip route 0.0.0.0 0.0.0.0 <dg_internetu>
Router(config-router)# default-information originate
```

- Zadáváme sítě, které má router KOLEM SEBE (opak statického routování)
- Do OSPF se nezahrnuje internetové rozhraní
- Default route má samé nuly, nastavuje se na hraničním routeru a její next hop je ip adresa serveru

DHCP Server

Na routeru (pokud je vzdálený, nastaví se i HA)

```
Router(config)# ip dhcp pool <nazev_poolu>
Router(dhcp-config)# network <adresa_site> <maska>
Router(dhcp-config)# default-router <ip_adresa_dg>
Router(dhcp-config)# dns-server 8.8.8.8
! Nastavuje se mimo interface
Router(config)# ip dhcp excluded-address <od_ip> <do_ip>
! Nastavujeme tam, kde jsme nastavovali subinterface
Router(config-subif)#ip helper-address <adresa_routeru>
```

- Helper-address nastavujeme na routeru, kde jsme nastavovali subinterface
- Jako helper-adress uvedeme adresu prvního portu routeru, na kterém nastavujeme DHCP
- Tato adresa se musí nastavit 2x, tj. na každý port, který vede od DHCP routeru
- Rozsah vyhrazených adres se nastavuje u excluded-address (např. pro DG)

NAT

Na hraničním routeru (vedoucí do internetu)

```
! Nastavíme VLAN, kterou chceme povolit
Router(config)# access-list 10 permit <vlan> <wildcard>
! Nastavíme VLAN, kterou chceme zakázat
Router(config)# access-list 10 deny <vlan> <wildcard>
! Jako interface uvedeme port, který míří do internetu (kde je nastavena DG)
Router(config)# ip nat inside source list 10 interface <port> overload
! Do všech vnitřních portů
Router(config-if)# ip nat inside
! Do DG portu
Router(config-if)# ip nat outside
```

- overload se nastavuje na portu, který vede z hraničního routeru do internetu (je na něm nastavena DG internetu)

PORT FORWARDING

Na hraničním routeru (vedoucí do internetu)

```
Router(config)# ip access-list extended <jmeno_acl>
Router(config)# ip nat inside source static tcp <ip_dmz_serveru> 21 <internet_dg> 21
! Nastavíme na každou službu zvlášť (pro 443, 21 i 20 dáme jako <port>)
Router(config-ext-nacl)#permit tcp any host <dg_internetu> eq <port>
Router(config-ext-nacl)#deny ip any any
! Nastavíme na každou službu zvlášť (pro 443, 21 i 20 dáme jako <port>)
Router(config)#ip nat inside source static tcp <ip_dmz_serveru> <port> <dg_internetu
    > <port>
! Nastavujeme na outside rozhraní (to, kde je nastavena DG internetu)
Router(config-if)#ip access-group <jmeno_acl> in
```

- Jméno pro access-list - <jmeno_acl>
- Default Gateway internetu (veřejná IP adresa na routeru) - <dg_internetu>

ACL

Na pravém routeru (vedoucí k VLANam)

```
Router(config)#ip access-list extended <jmeno_acl>
R3(config-ext-nacl)#permit tcp <sit> <wildcard> host <dmz_server> eq 443
R3(config-ext-nacl)#permit ip any any
! Musí se nastavit na VLAN interface
R3(config)#int vlan 10
R3(config-if)#ip access-group <jmeno_acl> in
! Musí se nastavit na VLAN interface
R3(config)#int vlan 20
R3(config-if)#ip access-group <jmeno_acl> in
```

- Jméno pro access-list - <jmeno_acl>
- Access list musí být extended