

svi svicevi van mreze ne ucestvuju u STP

1. biranje root bridga

- 1.1. najnizi konfigurisan prioritet
- 1.2. najnizu MAC adresu

prioritet po def. isti

2. root portovi

svaki svic koji nije root bridge (n-1 root portova)  
'kako najbrze doci do root bridga'

10Mb	100	100
100Mb	10	19
1000Mb	1	4
10Gb	1	2

root port se stavlja (kruzic) na link koji je najblizi root bridgu

3. designated portovi

portovi koji sigurno nece biti blokirani na kraju

- 3.1. svi na root bridgu, ne smiju biti blokirani
- 3.2. svi nasuprot root porta

[rezultujuce stablo]

4. blokirani portovi

kod linkova koji nemaju ni RP ni DP, gleda se koji svic je blizi root portu, [ D je jaci/blizi, pa se port na E blokira],  
zatim prioritet pa MAC adresa



2. primjer

3. primjer

izbor najkrece rute preko atributa, ruter redom prolazi kroz te attribute i dok ne nadje prvi mismatch, prolazi kroz attribute, atributi su rangirani po nekoj jacini

za nas u zadacima bitni Local Preference, AS Path, MED vrijednost (ovim redom sortirane jacine)

kod BGP nema load balancinga

mi smo uglavnom administratori na jednom autonomnom sistemu

jedan od dva nacina, sa LP ili sa AS Path,

ako ne uradimo nista. ruteri uglavnom koriste AS Path atribut, bira putanju sa kracim AS path (manji broj Autonomnih Sistema)

na odlazni saobracaj se utice manipulacijom dolaznih ruta

LP je bolji sto je veci, def vr je 100, lp je poznat cijelom autonomnom sistemu

drugi nacin, sa AS path, as path prepending (laziranje), upisivanje(ponavljanje) nekog autonomnog sistema u as pathu da bi as path izledao duzi,

nema potrebe i za LP i za AS Path

LP utice na odlazni saobracaj,  
AS Path utice i na dolazni i na odlazni  
MED utice na dolazni saobracaj

na dolazni saobracaj se utice manipulacijom odlaznih ruta

ovo na dva nacina, AS Path prepending i MED

MED je bolji sto je manji, popularno se naziva i metrika, Multiple Exit Discriminator

problem sa MEDom je sto je nizak, tj ako je na drugoj strani radjeno sa LP ili AS P za odlazni saobracaj, do meda se nece ni doci

cesto je kod bgp saobracaj asimetrican, od X-Y mreze nije isti put kao Y-X

AS1 {R1} dvije putanje AS2 {R2, R3} --- r3 daje LP vr 10 za sve rute koje dobije od r5, a LP vr 200 za sve rute koje dobije od r1->> sav saobracaj is AS2 u AS1 ce ici donjom putanjom, tj R3->R1, cak i kad r2 dobije paket sa r1, ovaj ga salje na r3 da bi ga ovaj proslijedio na r1

[CAKA] ako je LP postavljen, na bilo kakav nacin, MED se nece ni gledati

AS2 i AS3, putanja od as3 do as2 gdje nista nije uradjeno(ni LP ni AS ni MED), gleda se zadnji kriterijum, tj ruta koja je prva naucena??? u primjeru se uzima R12-R10 umjesto R12-R11 jer je index r10 manji od r11 [TESTIRATI ]

unutar AS2 je ospf sa admin dist 110, a interni bgp (koji vjerovatno postoji) ima admin distancu 200 -> ospf bira kako ce saobracaj proci kroz autonomni sistem, jer je jaci od internog bgp

next hop kod bgp ne funkcionise isto kao kod internih protokola rutiranja, to nije sljedeci ruter kojem se salje poruka, nego sljedeci ruter u drugom AS kojem se salje poruka

pitanje 22 sa prezentacije. u ovoj situaciji se ne moze koristiti MED jer nem ozemo iz AS2 slati MED u dva razlicita ASistema,

MED ima smisla samo ako se salje ka ruterima koji su u istom Autonomnom Sistemu

kod pitanja obratiti paznju sta pise, tacnije, koji se atribut postavlja, gdje, za kakve rute i kako je postavljen

LP i AS Path

na odlazni saobraćaj se utice manipulacijom dolaznih ruta

AS Path i MED

na dolazni saobraćaj se utice manipulacijom odlaznih ruta

spanning tree po defoltu upaljen kod switcheva

#show spanning-tree ( u privilegovanom modu)

root id - info o root bridgu

bridge id - trenutni switch

lista i stanje interfejsa

po def switcevi imaju prioritet 32768

+1 sabiranje sa vlanom [TESTIRATI kad je vlan razlicit od jedan koliki je zbir]

ako ne kreiramo nijedan vlan, znamo da je podesen na vlan1

status [FWD, BLK]

#spanning-tree vlan 1 priority [ manji od postojeceg]

alternativa

#spanning-tree vlan 1 root primary -- automatski bira prioritet i postaje root bridge

#spanning-tree 1 root secondary -- zamjenik root bridga

tajmeri - oko 50 sekundi, kad prodje tajmer tad se bira da li ce port da prosljedjuje podatke ili ne

ako se pc poveze na svic, bez petlje, moze se natjerati svic da taj port odmah postavi kao prosljedjujuci --

# komanda na interfejsu

# spanning-tre portfast

dobijamo upozorenje - ni u kom slucaju nakon ove komande na taj port ne smijemo prikljuciti drugi svic, jer se moze desiti da nastane petlja i da taj port bude blokiran -- preporuka

# spanning-tre portfast

# spanning-tree bpduguard enable -- ako se na ovom portu ikad prikaze BPDU poruka (a nju salje samo svic, nikad racunar), onda ce taj port automatski ugasiti (bolje ugasen nego petlja)

-- ako imamo 2 svica povezana preko 2 kabla -> petlja -> svi dodatni kablovi su blokirani (ima komanda etherchannel - kasnije)

treći kriterijum - bira port koji sa druge strane ima port sa nizim indeksom

-> ako to ne zelimo, podesavamo:

#show spanning-tree

ovdje gledamo priority.number

128 je prioritet porta

.1 i .2 su indexi porta

[ sw 4 i sw 5, sw4 je root port, znaci blokira se jedan port kod sw 5, isti switcevi, isti , switch 5 gleda kolonu u sw 4]

u sw4 # spanning-tree vlan 1 port-priority [k\*16]

vlan mozemo poistovijetiti sa pojmom brotkast domen ili mreza, omogucava da napravimmo razlicite brotkast domene na nivou svica kao l2 uredjaja -- na jedan svic povezati vise racunara koji ne pripadaju jednoj vec mogu i razlicitim mreza

mora postojati uredjaj 3 sloja da bi se omogucila komunikacija uredjaja u razlicitim vlanovima

tehnika sa ruterima

[ po defoltu racunari nece moci razgovaratu jer su u razlicitim mreza, tako konfigurisani, a svicevi se ponasaju kao da su svi uredjaji u istoj mrezi]

vlaanovi transparentni za racunari, njima pojam vlan nije poznat, sve se podesava, na svicu

svaki svicevi imaju vlan 1 po defoltu, i svi portovi se nalaze u vlanu 1

wsitch#show vlan brief

imamo predefinisane 1002 - 1005 vlanove, -legacy

ostali vlanovi se eksplicitno kreiraju

```
(config) #vlan 10
(config-vlan) #name Studenti
```

```
(config) #vlan 20
(config-vlan) #name Profesori
```

ovo se mora uraditi na svim ostalim svicovima, bez obzira da li imaju hostove u tim vlanovima, jer moraju znati gdje da salju saobracaj [TESTIRATI sta ako nisu postavljeni vlanovi na svim svicovima, kakva je komunikacija tu moguca]

na osnovu porta se stavlja racunar u neki vlan

```
config # int fasteternet 0/3
switch(cofnig-int)#switchport mode access
-- moze bit access ili trunk
access znaci da se tu nalazi pc
```

switch(cofnig-int)#switchport access vlan 10 -- ovo podesava koji je vlan na tom interfejsu [TESTIRATI ima li komanda switchport trunk vlan 10]

```
switch(cofnig-int)#
```

ako je svic u vlan1 onda moze slati samo saobracaj sa vlan1, sto je u ovom primjeru nikakav sadrzaj [TESTIRATI]

svi portovi izmedju sviceva su u trunk modu, trunk znaci da ce se preko tog porta slati saobracaj izmedju svih vlanova, ali se moraju tagovati tj - jedan svic govori drugom iz kog to vlana dolazi frejm

```
SW(config)# interface range f0/1-2
SW(config-if-range)# switchport mode trunk
```

[CAKA] -- provjeriti access/trunk ako je na portu pc ili svic

do sad moze onda komunikacija medju istim vlanovima, za druge vlanove treba ruter

moze koliko vlanova toliko kablova ruter-svic, ovo nije skalabilno rjesenje npr za 100 vlanova

KONCEPT PODINTERFEJS = na jednom fizickom portu rutera kreiramo vise logickih podinterfejsa, a ruter svake od njih smatra kao zasebne interfejsse -> ruter i svic povezani samo sa jednim kablom, a na portu rutera pravimo (broj vlanova) podinterfejsa

[TESTIRATI dvije linije ispod, da li valja u zagradama, tj mod u ruteru]

```
ruter(config-if)#no shutdown
```

```
ruter(config)# interface g0/0.brojPodinterfejsa {dobra praksa broj vlana, ne mora} --ovo ulazi u mod subinterfejsa
```

kljucna komanda

```
ruter(config-subif)# encapsulation dot1Q 10 {ovaj broj mora se podudarati sa brojem vlana}
```

```
ruter(config-subif)#ip address 192.168.10.254 255,255,255,0 -- ovo je defaultni gejtvej za racunare sa vlana 10
```

[CAKA] ----- OBAVEZAN REDOSLIJED-----

```
encapsulation dot1Q ponistava ip adresu ako postoji
```

isto i za drugi subinterfejs i vlan 20

-- postaviti na racunarima gejtvej

frejm sa pca izgleda normalno, kao i kod obicne komunikacije sa racunarima van svoje mreze, jedino mu je potrebna mac adresa defaultnog gejtveja, poruka dolazi do svica, koji mora obavjestiti naredni svic da taj paket dolazi sa nekog vlana, to je tgovanje, tag je posebno polje koje govori iz kog vlana dolazi ta poruka, to su polja nakon source adrese, u njima je identifikator za vlan, ima 12 bita.

taj se protokol naziva 800.1q pa odatle i ime dot1Q.

na ruteru se mijenja tag u npr sa 10 na 20. zadnji svic skida taj tag kad ga salje racunaru, jer ovaj ne razumije koncept tagovanja

svaka mreza preko vlana i podinterfejsa rutera predstavlja posebnu direktnu vezu na ruteru u tabeli rutiranja

spanning tree se moze napraviti posebno za svaki vlan

spanning tree pravi stablo za svaki vlan, ako se ne podesi drugacije, stablo ce izgledati isto za svaki vlan

prvo svi svicevi tj portovi u trunk mod

optimizacija linkova :npr switch0 root brid za vlan1, sw1 za vlan10, sw2 za vlan20

etherchannel -- ako su swicevi povezani sa dva linka, kada se etherchannel konfigurise ispravno, onda se dva linka posmatraju kao jedan logicki, pa ga onda spanning tree neće blokirati, može do 8 linkova u jedan etherchannel

```
switch(config)# int range fa0/1-2
switch(config-if-range)#channel-group [broj etherchanela] mode [5 opcija, on znaci da linkovi bezuslovno odu u etherchannel]
```

[CAKA]'ove ostale opcije mozete sami istraziti, nije toliko bitno'

mora na oba svica

u etherchannel moraju linkovi istih brzina, npr ne može fast i gigab

switch#show etherchannel summary -- komanda za verifikaciju etherchanela  
-Po1(SU) - s znaci da su u etherchannelu na nivou 2, a u znaci da se koriste [TESTIRATI ]

HWIC-2T -- za serijski link [TESTIRATI sta je ovo]

napomena -- ruter -> copy running startup

def protokol na serijskim linkovima nije ethernet vec HDLC, nije najjace rjesenje bolji je PPP

PPP može sve sto i HDLC, a i dodatne bitne 4, jedna od njih je autentikacija

```
r1(config-if)# encapsulation ppp
```

ovo mora na oba rutera, jer nisu kompatibilni

no encapsulation ppp vraća na def

konfiguracija ppp autentikacije -- ruteri moraju razmijeniti neku zajednicku sifru da bi link postao aktivan

podesavanje sifre --

```
R1(config)# username [R2 - ovdje ide hostname rutera sa kojim se treba izvesti autentikacija, ruter sa druge strane]
password lozinka
R2(config)#username R1 password lozinka
```

aktivacija autentikacije --

na interfejsu

```
#int s0/0/1 ; #ppp authentication chap [TESTIRATI sta je chap]
```

----- wlan

svaki wireless ruter po def ima 5 portova, 1 od njih je internet port koji služi za povezivanje na neku mrežnu infrastrukturu, na ostala 4 se povezujemo kao na swic, + on je i ACCESS POINT

ruter na wireless ruter se povezuje sa 'Internet' portom

svaki wireless ruter ima dvije mreže, jedna prema infrastrukturi, druga prema mreži u kojoj funkcioniše i kao dhcp server

wireless -- podesava se preko gui-ja

setup -- podesavanje one dvije mreže, internet i network

def gateway kod wireless rutera je ruter na koji je on povezan, ovo je za internet mrežu

drugi korak - karakteristike wireless mreže

ssid - ime mreže

wireless security - za lozinku, min 8 karaktera, po defaultu nema sigurnosti

wpa2 personal - za kucu i obicne korisnike

wpa2 enterprise - za servere

administration -

\*\*\*\*\* - admin

\*\*\*\*\* - admin

laptopi u packet traceru nemaju wireless karticu, mora se dodati wpc300n

svaki wireless ruter pri slanju paketa radi NATiranje, tj skida source ip adresu hosta u tom networku i stavlja source svoju ip adresu od svog interfejsa,

situacija R2 - WIRELESS - NETWORK -> za r2 ne treba staticka ruta ka NETWORK, bas zbog natiranja, jer je onda njemu udaljena mreza u sustini direktno povezana

NETWORK je nevidljiv za ostatak mreže

svaki wireless ruter ima samo jednu def rutu, jer je uvijek rubni ruter, pa se ne treba nista konfigurirati

[TESTIRATI] sta se nalazi u nat tabeli



umjesto da gasimo portove, koristimo ovo

natjeramo svic da nauci koje su mak adrese na njegovim portovima, pa ako se pojavi neka druga, on odbije tog hosta

konfigurise se na portovima svica

```
sw1(config)# int range fo/1-2
```

```
sw1(config-if-range)# [TESTIRATI sta fali ovjde]
```

kljucna komanda

```
sw1(config-if-range)# switchport port-security
```

postavljanje max 1 mak adrese za dati port -- sw1(config-if-range)# switchport port-security maximum 1 [1 je def]

komanda koja omogucava svicu da dinamicki nauci mak adresu na portu i da je stavi u radnu konfiguraciju, nakon restartovanja svica on ce na odredjenom portu dozvoliti samo tu mak adresu --sw1(config-if-range)# switchport port-security mac-address sticky

mod pri nezeljenom pristupu

```
sw1(config-if-range)# switchport port-security violation [protect - bez informacija, restrict - kod ove imaju neke informacije,shutdown - def]
```

ostale portove po preporuci ugasiti

```
s1#show port security int f0/2 -- ovo je za ispis
```

ako je na portu ukljucen violation shutdown, i on se poveze na ispravni host sa mac adresom iz konfiguracije, mora se izvorsiti intervencija, tad je port u error-disabled, zbog ovog stanja mora prvo #shutdown pa onda #no shutdown

RIP - prvi protokol, prvi uveo dinamičko rutiranje, verzija 2 u upotrebi, koncepti vaze i za ostale protokole rutiranja

ideja kod ripa, skroz obrnuta od statičkog rutiranja gdje se konfigurisu udaljene mreže, kod ripa se podesava da ono oglašava svoje direktno povezane mreže

ključna riječ router

```
R1(config)# router [konfiguracija za neki od protokola rutiranja ]  
#router rip
```

glavna komanda network

```
r1 (config-router)# network [direktno povezane mreže-oglašava dir pov mreže, te aktivira interfejs da aktivno  
učestvuju u slanju i primanju routing-update poruka ]
```

kod ripa se mreže unose bez maske i rip 1 razumije samo classful mreže [A,B,C]

mora se podesiti na svim ruterima

rip je protokol sa generalno sporom konvergencijom, treba više vremena da se uspostavi tabela rutiranja za sve rutere, AD == 120 metrika

u slučaju da udaljena mreža ima metriku istu za 2 ili više putanja, sve te putanje će se nalaziti u jednom zapisu ruting tabele i vrsice se load balancing

[TESTIRATI može li RIP i statičke putanje]

danas nije moguće upotrebiti verziju 1,

diskontinuirana mreža -- to su podmreže koje su nastale iz istog klasnog opsega [npr B], ali nisu direktno povezane nego su razdvojene nekim drugim klasnim opsegom, [npr A], rip 1 ne može da radi ako imamo diskontinuirane mreže, danas uvijek tako jer imamo svuda VLSM

kod ripa se uvijek u komandi #network [adresa] uvijek unosi klasna adresa [npr 172.16.0.0]

apdejtiti se kor RIP 1 mogu slati samo kao klasne adrese, tu nastaje problem npr ako se udaljene mreže nalaze isti broj hopova od R2, a on dobija istu adresu, tj. adresu klase, onda u ruting tabelu upisuje tu adresu klase sa 2 interfejsa, odnosno radi pomenuti load balancing i nastaje haos

za 2 mreže sa istom metrikom, kod pinga prolazi svaka druga poruka, a ostale su unreachable

rip verzija 2 ima prednost jer može da pošalje masku u apdejtu, pa može da šalje tačnu mrežu a ne klasnu adresu

```
R1(config-router)# version 2
```

ovo nije dovoljno, verzija 2 iz nekih legacy razloga vrsi automatsku sumarizaciju, odnosno isto sto i rip1

```
R1(config-router)#no auto-summary
```

network komande se ne mijenjaju,

nakon 'no auto-summary' automatski se prepoznaje koja mreža se šalje u apdejtu, tj prepoznaje masku

ako je neka veka topologija, preporuka je da se predje na ospf jer ima brzu konvergenciju

svaki ruter, svakih 30 sekundi, uzima svoju ruting tabelu i šalje je na 'sve ripom aktivirane interfejse' [TESTIRATI da li se šalju apdejtiti na direktno povezane mreže, ili samo na ove unesene preko 'network {address}']

nepotrebno, ruter šalje i na mreže na kojima nema drugih rutera -- optimizacija > treba je izvršiti na svim interfejsima

gdje su svicevi i racunari - onemogucava ruter da salje apdejt na lokalnu mrezu  
komanda R1(config-router)#passive-interface fa0/0

za ipv6 'RIP next generation'

za razliku od telnet, ssh omogućava sigurno remote pristupanje udaljenim uređajima

1. spreciti ios da razrijesi pogresno unesene komande -- r1(config)#no ip domain-lookup

hostname mora biti isti na topologiji da bi se bodovao

r1(config)#security passwords min-length 10

r1(config)#exec-timeout 7 -- ako smo neaktivni ovoliko minuta, onda nas ruter izbací iz modova i moramo se ponovo ulogovati

moramo dodati korisnika i sifru njegovu, ovo nema kod telnet  
config#username ime secret sifra

preduslov za ssh he da se ruter nalazi u nekom domeni -- r1(config)#ip domain-name [neki domen npr securiti.com, ne znaci nista ali mora biti konfigurisan]

generisanje kljuceva koji se koriste pri ssh komunikaciji --  
r1(config)#crypto key generate rsa

da se omoguci [valjda razmjena kljuceva] mora se uci u line vty 0 4

r1(config)#line vty 0 4

r1(config-line)#transport input [all,ssh,none,telnet - defaultni]

r1(config-line)# login local -- pozivamo se na lokalnu bazu koja je definisana pri definisanju korisnika preko username komande

blokiranje bruteforse logovanja -- r1(config)#login block-for 45 attempts 3 within 100 (45,100 sekunde)

kod svica, dobra praksa da se ugase svi portovi koji se ne koriste, ako se napadaz nakaci na neki od portova, ne moze nita uraditi jer je ugasen port

sw1(config)# interface range fa0/1, fa0/3-9, fa0/11-24, go/2

sw1(config-if-range)# shutdown

ip adresa na switчу da mu se moze pristupiti [TESTIRATI kako se postavlja]

kod svica, ip adresa se stavlja na vlan1 a defaultni gejtvej u config#ip default-gateway

sw1(config)# ip domain-name security.com

sw1(config)# crypto key generate rsa

#transport input ssh

#login local

verifikacija ssh -- u cmd# ssh -l nazivKorisnika adresaNaKojuIdeSSH [TESTIRATI u kojem cmd]  
zatim password

preduslov za ssh i telnet je da se ukljuci #enable password secret

kod svica, ip adresa se stavlja na vlan1 a defaultni gejtvej u config#ip default-gateway

open shortest path first  
classless protokol  
slicno kao kod ripa, oglasavanje pobezanih mreza

konfigurise se u config modu

```
R1(config)#router ospf [broj procesa na ovom ospf ruteru, lokalna uloga, omogucava da se pokrene vise ospf instanci]  
R1(config)#router ospf 1  
R1(config-router)#network 162.168.1.0 [wildcard mask] area [oblast kojoj pripada interfejs, po def je backbone oblast,  
tj == 0]
```

wildcard maska, inverz obicne maske, kad se u maski obrnu jedinice i nule,  
npr

```
255.255.255.0 -- 0.0.0.255  
0. 0. 0.255 - racunanje, zbir po oktetima, kolonama mora da bude 255
```

2 rutera su susjedi ako im se poklapa vrijednost area

kad ruteri postanu susjedi, treba da dodje poruka u konzoli

AD == 110, jaci od ripa

metrika, racuna se : sabira cost-ove do neke udaljene mreze, uzima u obzir bandwidth,  $10^8/\text{bandwidth}$  -- formula

serijski ling - 1.5Mb >> cost je 64  
fasteternet -  $10^8$  Mb >> cost je 1

loopback interface na nekom ruteru -- logicki/softverski interfejs, u odnosu na fizicki interface ne moze biti u stanju down(ovo je prednost), ospf ga koristi za kreiranje nekih identifikatora, ne zavisi da li je u njega kabl ustekan, moze se simulirati da postoji neka mreza na tom interfejsu, npr simulira vezu ka internetu, nalazi se u tabeli rutiranja kao i svaki drugi interfejs

```
R1(config)#interface loopback 0  
R1(config-if)#ip address 209.165.200.1 255.255.255.0
```

```
R1(config)#ip route 0.0.0.0 0.0.0.0 loopback 0 -- def staticka ruta
```

pomocu loopback rute i ospf, ospf se moze natjerati da spusti def rutu na sve ostale rutere:

```
R1(config-if)#default-information originate -- govori ruteru r1 da posalje info o def ruti svim ostalim ruterima, efekat  
se provjerava na ostalim ruterima,  $O^*E2$  u tabeli rutiranja kod r2, ad. ustanca 110 umjesto 1, metrika 1????
```

ako se nesto mijenja na ruteru, samo ruteri u istoj oblasti ce vristi ospf izracunavanja

area se definise na nivou interfejsa, area border router - ruter koji dijeli oblasti,

O IA - ia je interarea, oznacava da ruter na kom se gleda tabela nije u istoj oblasti kao ruteri koji su dobijeni preko ospf,

tipovi LSA porukua koje razmjenjuju ospf ruteri? za rutere van svoje oblasti, ruter je dobio informaciju preko LSA tipova 3 i 4, a za eksterne rute preko LSA tipa 5,  
LSA 1,2 IntraArea- unutar svoje oblasti

[TESTIRATI sta ako se umjesto loopbeka stavi internet na taj port]

sumarizacija kod ospf se vrsi na nivou oblasti, [ npr za loopback 1 sumarna ruta je 172.16.0.0/22 ]:

```
r3(config)#router ospf 1  
r3(config)#area 1 range 172.16.0.0 255.255.255.0
```

multiaccess mreza - npr 3 rutera preko svica povezani, vise rutera dijele istu mrezu, kod ospf nisu svi medjusobno susjedi, vec se postavlja glavni(designated router DR) ruter i svi su njemu susjedi (skalabilno), postoji i zamjenik, backup designated ruter BDR( da ne bude jedan ruter usko grlo), algoritam biranja(ako nije rucno postavljeno koji ce biti glavni): 1. router-id> bilo kakav 32b podatak u dot dec formatu  
2. najveći loopback interfejs (npr 192.168 > 172.16)  
3. najveći fizicki interfejs (10.10.10.1 < 10.10.10.2 < 10.10.10.3)

ako outer 2 ( 10.10.10.3) ima i neki drugi interfejs veci od 10.10.10.3, npr 192.168, on ce taj interfejs uzeti za id

router# show ip ospf neighbor -- prikaz susjednih rutera, bitna kolona state, FULL - puno susjedstvo sa stranim ruterom  
FULL/DROTHER i FULL/BDR ??? [TESTIRATI ]

rucno: postavlja se prioritet na nivou interfejsa : router(config)#int g0/0; (config-if)#ip ospf priority <1-255> {1 je default  
, ova komanda se ne tretira odmah, 'nema taj tzv preemptive karakter', mora se ponovo pokrenuti mreza,  
najjednostavnije na switchu interfejs range shutdown pa no shutdown  
[TESTIRATI da li se mijenja 'komsiluk' kad se dodaju interfejsi na rutere dalje od svica ]

kad se doda novi ruter, nije povezan sa FULL/DROTHER, vec 2WAY/DROTHER, sto je i poenta jer se komunikacija odvija preko designated rutera

podesavanje R2 da bude dhcp server, treba podesiti onoliko poolova koliko ima mreza

dhcp pool ima vise adresa, neke se moraju iskljuciti, npr zauzete

```
r2(config)#ip dhcp excluded-address 192.168.10.1 192.168.10.10 -- iskljucene sve adrese izmedju 1 i 10
```

```
r2(config)#ip dhcp pool R1-LAN
```

```
r2(dhcp-config)#network 192.168.10.0 255.255.255.0 -- ovo je adresa mreze iz koje se dodjeljuju adrese, [TESTIRATI adrese u kojoj se pool nalazi]
```

```
r2(dhcp-config)#default-router 192.168.10.1 -- [CAKA ovdje nije default gateway nego default router]
```

```
r2(dhcp-config)#dns-server 192.168.20.254
```

kad host trazi dhcp adresu, salje brodcast poruku, a ona nece moci proci dalje od rutera na kom je nakace host, mora se podesiti interfejs na kome se nalazi host

```
R1(config)#int g0/0
```

```
R1(config-if)#ip helper-address 10.1.1.2 -- ovo govori ruteru da kad primi brodcast poruku, pretvori je u unicast i salje je na adresu 10.1.1.2
```

u slucaju da neki od parametara ne dodje sa dhcp odgovorom, moze se pozvati iz cmdPc2#ipconfig /renew

za ruter koji treba biti dhcp klijent, npr ruter da dobije adresu sa interneta:

```
r2(config)# int g0/1
```

```
r2(config-if)#ip address dhcp
```

```
r2(config-if)#no shutdown
```

```
r2#show ip int brief
```

network address translation

staticki, dinamicki, pat

staticki nat - prevodjenje adresa 1 prema 1, 1 privatna adresa u 1 javnu, scenario zelimo da dozvolimo pristup nekom nasem serveru koji ima privatnu adresu s vana, tu privantu adresu prevedemo u javnu i damo je kome treba

server je nat-transparentan, ne zna da ce njegova adresa da bude prepisana

natovanje se radi na ruteru, tj sva konfiguracija

2 nacina, npr [internet -- r1 -- sv1 -- server]

1. mozemo serversku adresu zamijeniti sa nekom adresom iz mreze [internet -- r1 ]

2. zamijenimo bilo kojom adresom, ali je bitno da ruteri znaju doci do njega

inside -- outside adrese

staticko rutiranje u jednoj komandi

```
r1(config)# ip nat inside source static 172.16.16.1 64.100.50.1
```

dodatno, mora se podesiti na ruteru svi interfejsi koji ucestvuju u natovanju, oni na koje dolaze privatne adrese i one na koje izlaze javne, inside i outside interfejs,

```
r1(config)#int g0/0
```

```
r1(config-if)#nat inside
```

```
r1(config)#int s0/0/0
```

```
r1(config-if)#nat outside
```

sad se pinga javna adresa, a ne privatna

kad nat poruka [TESTIRATI koja tacno poruka] dodje do rutera koji vrsi natovanje, destination ip se mijenja, inbound je javna, 64.x.x.x a outbound je 172.x.x.x

kad server salje odgovor, onda se mijenja source ip adresa

```
r1#show ip nat translations -- prikaz natovanja
```

dinamicki nat

ovdje se vise adresa prevodi u vise adresa, problem ako ja [TESTIRATI ruter valjda] imam 5 javnih adresa, onda mogu natirati samo 5 racunara iz mreze

ruter za natovanje je ruter koji je granica javnog i privatnog opsega

prvo se definisu privatne adrese, pa javne, pa se ta dva skupa povezu

standardna kontrol lista -- jednostavan zapis kojim se obuhvataju sve adrese sumarno, access lista

```
r2(config)# access-list 1 permit 172.16.0.0 [wildcard maska - 0.0.255.255] -- konfigurisanje access liste jedan
```

sad se obuhvataju javne adrese --

```
r2(config)# ip nat pool nazivPoola prvaAdresa zadnjaAdresa netmaska adresaMaske
```



r2(config)# ip nat pool POOL 209.165.200.229 209.165.200.230 netmask 255.255.255.224 -- ovjde imaju dvije javne adrese, .29 i .30

povezivanje access liste i poola --

r2(config)# ip nat inside source list 1 pool POOL

u primjeru, 3 racunara i 2 javne adrese, kada se prva dva racunara povezu na internet, treci nece moci izaci na internet

po dinamickom natu moze se izvesti onoliko racunara koliko ima slobodnih (javnih) adresa

verzija nata, PAT, izvodjenje vise racunara preko cak jedne adrese

Port Address translation

pat se naziva i Dinamicki NAT sa Overload-om

ralika u odnosu na dinamicki nat:

r1(config)# ip nat inside source list 1 pool ANY\_POOL\_NAME overload -- govori ruteru da ubaci portove u pricu, da preko tih portova prepozna odgovor, i preko tih portova izabere kojem hostu ce proslijediti odgovor

ako se privatne adrese mapiraju u jednu javnu, tj javnu adresu rutera, onda ne treba pool izlaznih adresa, vec samo access lista privatnih i komanda:

r2(config)#ip nat inside source list 2 interface s0/1/1 overload

port nije kao obicni port vec vise je identifikator po kojem ce ruter razlikovati kome treba poslati odgovor

svaki interfejs koji radi sa ipv6 adresama ima dvije adrese, tacnije jednu mora da ima, drugu moze da ima

svaki interfejs mora da ima link lokal adresu, one pocinju sa fe80, ako je mi ne zadamo, interfejs ce je sam kreirati

druga vrsta (tacnije prva) su globalne unicast ipv6 adrese, ekvivalent javnim ipv4 adresama

za sad se koristi samo 1/8 adresa, prepoznajemo ih kako pocinju sa 2001: nestodrugog

R1(cpnfig)#ipv6 unicast-routing --- bitna komanda, omogucava da kroz interfejse rutera prolazi ipv6 komunikacija

R1(cpnfig)#int g0/0

R1(cpnfig-if)#ipv6 address 2001:db8:1:1::1/64 --- sve komande iste kao kod ipv4, samo se koristi ipv6 prva kljucna rijec, subnet maska ne postoji kao takova, vec se kuca sa '/brojMaske'

R1(cpnfig-if)#ipv6 address fe80::1 link-local -- interfejs bi je svakako kreirao, ali bi bila dugacka i teska za prekucavanje, ovo je dobra praksa jer se preko ove adrese postavlja def gejtvaj

'cetvrti hekstet'

link lokal adresa ima iskljucivo lokalno znacenje, (slicno MAC adresi) pa nije problem da se ista link lokal adresa koristi u razlicitim mrezama, jer ne izlazi iz mreze -> svi hostovi imaju istu adresu def gejtvaja, ali on zapravo nije isti

link lokal adresa se ne dodaje na racunaru, on ce je sam dodati

podmrezavanje ipv6

podmrezavanje kod ipv6 se uvijek radi mijenjanjem cetvrtog heksteta, jer ako je maska /64 i ako je taj hekstet razlicit onda ce i mreze biti razlicite

ipv6 nisu case-sensitiv adrese

ne mogu biti dvije iste link lokal adrese u jednoj mrezi, doslo bi do kolizije, npr serijski link izmedju dva rutera

gui64

hostovi mogu dobiti adresu automatski preko autoconfiga, : dobije prefiks od rutera, a onda sam sebi kreira host id (adresu) koristeći gui64 pravilo -- unapredjenje u odnosu na ipv4, a ipv6 moze koristiti i dhcp

-----A1spanningTree

-----A6BGP

-----L1stp

```
#show spanning-tree ( u privilegovanom modu)
#spanning-tree vlan 1 priority [ manji od postojećeg]
#spanning-tree vlan 1 root primary -- automatski bira prioritet i postaje root bridge
#spanning-tree 1 root secondary -- zamjenik root bridga
# komanda na interfejsu
# spanning-tree portfast
# spanning-tree portfast
# spanning-tree bpduguard enable -- ako se na ovom portu ikad prikaze BPDU poruka (a nju salje samo svic, nikad
racunar), onda ce taj port automatski ugasiti (bolje ugasen nego petlja)
  #show spanning-tree
  u sw4 # spanning-tree vlan 1 port-priority [k*16]
```

-----L2VLAN

```
wsitch#show vlan brief
(config) #vlan 10
(config-vlan) #name Studenti
(config) #vlan 20
(config-vlan) #name Profesori
config # int fastEthernet 0/3
switch(config-int)#switchport mode access
switch(config-int)#switchport access vlan 10 -- ovo podesava koji je vlan na tom interfejsu [TESTIRATI ima li
komanda switchport trunk vlan 10]
switch(config-int)#
SW(config)# interface range f0/1-2
SW(config-if-range)# switchport mode trunk
ruter(config-in)#no shutdown
ruter(config)# interface g0/0.brojPodinterfejsa {dobra praksa broj vlana, ne mora} --ovo ulazi u mod subinterfejsa
ruter(config-subint)# encapsulation dot1Q 10 {ovaj broj mora se podudarati sa brojem vlana}
ruter(config-subint)#ip address 192.168.10.254 255,255,255,0 -- ovo je defaultni gejtvej za racunare sa vlana 10
```

-----L3etherchannelWanWlan

```
switch(config)# int range fa0/1-2
switch(config-if-range)#channel-group [broj etherchanela] mode [5 opcija, on znaci da linkovi bezuslovno odu u
etherchannel]
switch#show etherchannel summary -- komanda za verifikaciju etherchanela
r1(config-if)# encapsulation ppp
R1(config)# username [R2 - ovdje ide hostname rutera sa kojim se treba izvrsti autentikacija, ruter sa druge strane]
password lozinka
R2(config)#username R1 password lozinka
#int s0/0/1 ; #ppp authentication chap [TESTIRATI sta je chap]
```

-----L4portSecurity

```
sw1(config)# int range fo/1-2
```

```
sw1(config-if-range)# [TESTIRATI sta fali ovjde]
sw1(config-if-range)# switchport port-security
postavljanje max 1 mak adrese za dati port -- sw1(config-if-range)# switchport port-security maximum 1 [1 je def]
komanda koja omogucava svicu da dinamički nauči mak adresu na portu i da je stavi u radnu konfiguraciju, nakon
restartovanja svica on će na određenom portu dozvoliti samo tu mak adresu --sw1(config-if-range)# switchport port-
security mac-address sticky
sw1(config-if-range)# switchport port-security violation [protect - bez informacija, restrict - kod ove imaju neke
informacije,shutdown - def]
s1#show port security int f0/2 -- ovo je za ispis
ako je na portu uključen violation shutdown, i on se poveže na ispravan host sa mac adresom iz konfiguracije, mora se
izvršiti intervencija, tad je port u error-disabled, zbog ovog stanja mora prvo #shutdown pa onda #no shutdown
```

#### -----L4RIP

```
R1(config)# router [konfiguracija za neki od protokola rutiranja ]
#router rip
r1 (config-router)# network [direktno povezane mreže-oglašava dir pov mreže, te aktivira interfejs da aktivno
učestvuju u slanju i primanju routing-update poruka ]
kod ripa se uvijek u komandi #network [adresa] uvijek unosi klasna adresa [npr 172.16.0.0]
R1(config-router)# version 2
R1(config-router)#no auto-summary
komanda R1(config-router)#passive-interface fa0/0
```

#### -----L4ssh

```
1. spreciti ios da razrijesi pogresno unesene komande -- r1(config)#no ip domain-lookup
r1(config)#security passwords min-length 10
r1(config)#exec-timeout 7 -- ako smo neaktivni ovoliko minuta, onda nas ruter izbaci iz modova i moramo se ponovo
ulogovati
config#username ime secret sifra
preduslov za ssh he da se ruter nalazi u nekom domeni -- r1(config)#ip domain-name [neki domen npr securiti.com, ne
znaci nista ali mora biti konfigurisan]
r1(config)#crypto key generate rsa
r1(config)#line vty 0 4
r1(config-line)#transport input [all,ssh,none,telnet - defaultni]
r1(config-line)# login local -- pozivamo se na lokalnu bazu koja je definisana pri definisanju korisnika preko username
komande
blokiranje bruteforse logovanja -- r1(config)#login block-for 45 attempts 3 within 100 (45,100 sekunde)
sw1(config)# interface range fa0/1, fa0/3-9, fa0/11-24, go/2
sw1(config-if-range)# shutdown
kod svica, ip adresa se stavlja na vlan1 a defaultni gejtvej u config#ip default-gateway
sw1(config)# ip domain-name security.com
sw1(config)# crypto key generate rsa
#transport input ssh
#login local
verifikacija ssh -- u cmd# ssh -l nazivKorisnika adresaNaKojuIdeSSH [TESTIRATI u kojem cmd]
preduslov za ssh i telnet je da se ukljuci #enable password secret
kod svica, ip adresa se stavlja na vlan1 a defaultni gejtvej u config#ip default-gateway
```

#### -----L5ospf

```
R1(config)#router ospf [broj procesa na ovom ospf ruteru,lokalna uloga, omogucava da se pokrene vise ospf instanci]
R1(config)#router ospf 1
R1(config-router)#network 162.168.1.0 [wildcard mask] area [oblast kojoj pripada interfejs, po def je backbone oblast,
```

```
tj == 0]
R1(config)#interface loopback 0
R1(config-if)#ip address 209.165.200.1 255.255.255.0
R1(config)#ip route 0.0.0.0 0.0.0.0 loopback 0 -- def staticka ruta
R1(config-if)#default-information originate -- govori ruteru r1 da posalje info o def ruti svim ostalim ruterima, efekat se provjerava na ostalim ruterima, O*E2 u tabeli rutiranja kod r2, ad. ustanca 110 umjesto 1, metrika 1????
r3(config)#router ospf 1
r3(config)#area 1 range 172.16.0.0 255.255.255.0
router# show ip ospf neighbor -- prikaz susjednih rutera, bitna kolona state, FULL - puno susjedstvo sa stranim ruterom
rucno: postavlja se prioritet na nivou interfejsa : router(config)#int g0/0; (config-if)#ip ospf priority <1-255> {1 je default
}, ova komanda se ne tretira odmah, 'nema taj tzv preemptive karakter', mora se ponovo pokrenuti mreza,
najjednostavnije na switchu interfejs range shutdown pa no shutdown
```

#### -----L6dhcp

```
r2(config)#ip dhcp excluded-address 192.168.10.1 192.168.10.10 -- iskljucene sve adrese izmedju 1 i 10
r2(config)#ip dhcp pool R1-LAN
r2(dhcp-config)#network 192.168.10.0 255.255.255.0 -- ovo je adresa mreze iz koje se dodjeljuju adrese, [TESTIRATI
adrese u kojoj se pool nalazi]
r2(dhcp-config)#default-router 192.168.10.1 -- [CAKA ovdje nije default gateway nego default router]
r2(dhcp-config)#dns-server 192.168.20.254
R1(config)#int g0/0
R1(config-if)#ip helper-address 10.1.1.2 -- ovo govori ruteru da kad primi brodcast poruku, pretvori je u unicast i salje
je na adresu 10.1.1.2
u slucaju da neki od parametara ne dodje sa dhcp odgovorom, moze se pozvati iz cmdPc2#ipconfig /renew
r2(config)# int g0/1
r2(config-if)#ip address dhcp
r2(config-if)#no shutdown
r2#show ip int brief
```

#### -----L6bnat

```
r1(config)# ip nat inside source static 172.16.16.1 64.100.50.1
r1(config)#int g0/0
r1(config-if)#nat inside
r1(config)#int s0/0/0
r1(config-if)#nat outside
r1#show ip nat translations -- prikaz natovanja
r2(config)# access-list 1 permit 172.16.0.0 [wildcard maska - 0.0.255.255] -- konfigurisanje access liste jedan
r2(config)# ip nat pool nazivPoola prvaAdresa zadnjaAdresa netmaska adresaMaske
r2(config)# ip nat pool POOL 209.165.200.229 209.165.200.230 netmask 255.255.255.224 -- ovjde imaju dvije javne
adrese, .29 i .30
r2(config)# ip nat inside source list 1 pool POOL
r1(config)# ip nat inside source list 1 pool ANY_POOL_NAME overload -- govori ruteru da ubaci portove u pricu, da
preko tih portova prepozna odgovor, i preko tih portova izabere kojem hostu ce proslijediti odgovor
r2(config)#ip nat inside source list 2 interface s0/1/1 overload
```

#### -----L7ipv6

```
R1(cpnfig)#ipv6 unicast-routing --- bitna komanda, omogucava da kroz interfejse rutera prolazi ipv6 komunikacija
R1(cpnfig)#int g0/0
R1(cpnfig-if)#ipv6 address 2001:db8:1:1::1/64 --- sve komande iste kao kod ipv4, samo se koristi ipv6 prva kljucna
rijec, subnet maska ne postoji kao takova, vec se kuca sa '/brojMaske'
R1(cpnfig-if)#ipv6 address fe80::1 link-local -- interfejs bi je svakako kreirao, ali bi bila dugacka i teska za
```

prekucavanje, ovo je dobra praksa jer se preko ove adrese postavlja def gejtvej

-----script.sh

#!/bin/bash

cat "\$i" | grep '#'>>komande

-----A1spanningTree

-----A6BGP

AS2 i AS3, putanja od as3 do as2 gdje nista nije uradjeno(ni LP ni AS ni MED), gleda se zadnji kriterijum, tj ruta koja je prva naucena??? u primjeru se uzima R12-R10 umjesto R12-R11 jer je index r10 manji od r11 [TESTIRATI ]

-----komande

switch(cofnig-int)#switchport access vlan 10 -- ovo podesava koji je vlan na tom interfejsu [TESTIRATI ima li komanda switchport trunk vlan 10]  
#int s0/0/1 ; #ppp authentication chap [TESTIRATI sta je chap]  
sw1(config-if-range)# [TESTIRATI sta fali ovjde]  
verifikacija ssh -- u cmd# ssh -l nazivKorisnika adresaNaKojuIdeSSH [TESTIRATI u kojem cmd]  
r2(dhcp-config)#network 192.168.10.0 255.255.255.0 -- ovo je adresa mreze iz koje se dodjeljuju adrese, [TESTIRATI adrese u kojoj se pool nalazi]

-----L1stp

+1 sabiranje sa vlanom [TESTIRATI kad je vlan razlicit od jedan koliki je zbir]

-----L2VLAN

ovo se mora uraditi na svim ostalim svicovima, bez obzira da li imaju hostove u tim vlanovima, jer moraju znati gdje da salju saobracaj [TESTIRATI sta ako nisu postavljeni vlanovi na svim svicovima, kakva je komunikacija tu moguca]  
switch(cofnig-int)#switchport access vlan 10 -- ovo podesava koji je vlan na tom interfejsu [TESTIRATI ima li komanda switchport trunk vlan 10]  
ako je svic u vlan1 onda moze slati samo saobracaj sa vlan1, sto je u ovom primjeru nikakav sadrzaj [TESTIRATI]  
[TESTIRATI dvije linije ispod, da li valja u zagradama, tj mod u ruteru]

-----L3etherchanelWanWlan

-Po1(SU) - s znaci da su u etherchanelu na nivou 2, a u znaci da se koriste [TESTIRATI ]  
HWIC-2T -- za serijski link [TESTIRATI sta je ovo]  
#int s0/0/1 ; #ppp authentication chap [TESTIRATI sta je chap]  
[TESTIRATI] sta se nalazi u nat tabeli

-----L4portSecurity

sw1(config-if-range)# [TESTIRATI sta fali ovjde]

-----L4RIP

[TESTIRATI moze li RIP i staticke putanje]  
svaki ruter, svakih 30 sekundi, uzima svoju ruting tabelu i salje je na 'sve ripom aktivirane interfejse' [TESTIRATI da li se salju apdejti na direktno povezane mreze, ili samo na ove unesene preko 'netwokr {address}']

-----L4ssh

ip adresa na swittchu da mu se moze pristupiti [TESTIRATI kako se postavlja]  
verifikacija ssh -- u cmd# ssh -l nazivKorisnika adresaNaKojuIdeSSH [TESTIRATI u kojem cmd]

-----L5ospf

[TESTIRATI sta ako se umjesto loopbeka stavi internet na taj port]

FULL/DROther i FULL/BDR ??? [TESTIRATI ]

[TESTIRATI da li se mijenja 'komsiluk' kad se dodaju interfejsi na rutere dalje od svica ]

-----L6dhcp

r2(dhcp-config)#network 192.168.10.0 255.255.255.0 -- ovo je adresa mreze iz koje se dodjeljuju adrese, [TESTIRATI adrese u kojoj se pool nalazi]

-----L6bnat

kad nat poruka [TESTIRATI koja tacno poruka] dodje do rutera koji vrsi natovanje, destination ip se mijenja, inbound je javna, 64.x.x.x a outbound je 172.x.x.x

ovdje se vise adresa prevodi u vise adresa, problem ako ja [TESTIRATI ruter valjda] imam 5 javnih adresa, onda mogu natirati samo 5 racunara iz mreze

-----L7ipv6

-----script.sh

cat "\$i" | grep 'TEST'>>test



-----A1spanningTree

-----A6BGP

[CAKA] ako je LP postavljen, na bilo kakav nacin, MED se nece ni gledati

-----cake

[CAKA] ako je LP postavljen, na bilo kakav nacin, MED se nece ni gledati

-----komande

r2(dhcp-config)#default-router 192.168.10.1 -- [CAKA ovdje nije default gateway nego default router]

-----L1stp

-----L2VLAN

[CAKA] -- provjeriti access/trunk ako je na portu pc ili svic

[CAKA] ----- OBAVEZAN REDOSLIJED-----

-----L3etherchannelWanWlan

[CAKA]'ove ostale opcije mozete sami istraziti, nije toliko bitno'

-----L4portSecurity

-----L4RIP

-----L4ssh

-----L5ospf

-----L6adhcp

r2(dhcp-config)#default-router 192.168.10.1 -- [CAKA ovdje nije default gateway nego default router]

-----L6bnat

-----L7ipv6

-----script.sh

cat "\$i" | grep 'CAK'>>cake

-----test