Šolski center Novo mesto  
Srednja elektro šola in tehniška gimnazija  
Šegova ulica 112  
8000 Novo mesto

**POSTAVITEV OMREŽJA V PODJETJU**(Seminarska naloga)

Predmet: Računalniški sistemi in omrežja  
  
Avtor: Nik Jenič, T4b  
Mentor: Gregor Mede, univ. dipl. inž. rač. in inf.

Novo mesto, maj 2022

**POVZETEK IN KLJUČNE BESEDE**

V seminarski nalogi predstavim osnovne sestavne dele omrežja, kako delujejo in zakaj so uporabni. Predstavim tudi mnogo znanj, ki je potrebnih, za učinkovito rabo teh naprav. Poleg tega predstavim tudi pojme in nastavitve, ki jih potrebujemo, za postavitev takega omrežja. Zraven teorije je pa tudi priložena simulacija omrežja, ki omogoča praktično predstavo take postavitve. Uporabil sem tudi slike omrežja in naprav, da si lahko bralci lažje predstavljajo opisane pojme, poglobil sem se v teoretične pojme postavljanja omrežij in dodal sem tabele, da so naslovi omrežij bolj razumljivo predstavljeni.

V seminarski sem se poglobil v naslavljanje znotraj omrežja, zagotavljanje varnosti znotraj tega, omejevanje dostopa določenih naslovov, posodabljanje omrežja na novejše standarde ter tudi omogočanje upravljanja nastavitev na daljavo.

Ključne besede:

* VLAN
* Omrežje
* Podomrežje
* Vmesnik
* Usmerjevalnik
* Stikalo
* IP
* Maska

**KAZALA**

**KAZALO VSEBINE**

[1 UVOD 1](#_Toc102353158)

[2 POSTAVITEV OMREŽJA V PODJETJU 2](#_Toc102353159)

[2.1 NAPRAVE IN POJMI PRI POSTAVITVI OMREŽJA 2](#_Toc102353160)

[2.1.1 USMERJEVALNIK 3](#_Toc102353161)

[2.1.2 STIKALO 4](#_Toc102353162)

[2.1.3 KONČNE NAPRAVE 5](#_Toc102353163)

[2.1.4 CLI 5](#_Toc102353164)

[2.1.5 VODNIKI 7](#_Toc102353165)

[2.2 POSTAVITEV OMREŽJA 9](#_Toc102353166)

[2.2.1 IMENA NAPRAV 10](#_Toc102353167)

[2.2.2 VSTOPNO SPOROČILO 11](#_Toc102353168)

[2.2.3 Geslo za prehod v priviligiran način 12](#_Toc102353169)

[2.2.4 GESLO NA KONZOLNI VHOD 13](#_Toc102353170)

[2.2.5 SSH dostop na VTY 14](#_Toc102353171)

[2.2.6 Naslov IPv4 za SVI 15](#_Toc102353172)

[2.2.7 Varnost na stikalih – izklopite neuporabljena vrata 16](#_Toc102353173)

[2.2.8 Nastavitev VLAN-ov na S1 17](#_Toc102353174)

[2.2.9 Vrata F0/24 povezava do usmerjevalnika 18](#_Toc102353175)

[2.2.10 SVI v VLAN Uprava 18](#_Toc102353176)

[2.2.11 Naslavljanje IPv4, DHCPv4 v omrežju z VLANi 19](#_Toc102353177)

[2.2.12 Usmerjanje OSPF 26](#_Toc102353178)

[2.2.13 Privzeta pot v WAN na usmerjevalniku, ki je povezan v WAN (kaže naj na ISP WAN), oglaševanje privzete poti ostalim usmerjevalnikom. 27](#_Toc102353179)

[2.2.14 IPv6 naslove v LAN Razvoj, DHCPv6 na omrežnem prehodu proti WAN, privzeta pot IPv6 v WAN. 28](#_Toc102353180)

[2.2.15 ACL 31](#_Toc102353181)

[2.2.16 NAT (PAT) 33](#_Toc102353182)

[2.3 TESTIRANJE OMREŽJA 34](#_Toc102353183)

[3 ZAKLJUČEK 35](#_Toc102353184)

[4 VIRI IN LITERATURA 36](#_Toc102353185)

[5 STVARNO KAZALO 40](#_Toc102353186)

[6 PRILOGE 41](#_Toc102353187)

**KAZALO SLIK**

[Slika 1: Priložena skica omrežja 2](#_Toc102353188)

[Slika 2: Usmerjevalnik Linksys E5350 (1) 3](#_Toc102353189)

[Slika 3: Stikalo TP-LINK TL-SG1024D (5) 4](#_Toc102353190)

[Slika 4: CLI pogled 5](#_Toc102353191)

[Slika 5: Logotip Cisco (10) 6](#_Toc102353192)

[Slika 6: Cisco Packet tracer (11) 6](#_Toc102353193)

[Slika 7: Kabel spisani par 7](#_Toc102353194)

[Slika 8: Razlika med navadnim in križnim kablom (12) 8](#_Toc102353195)

[Slika 9: Navodila za postavitev 9](#_Toc102353196)

[Slika 10: Postavitev omrežja in vse oznake 21](#_Toc102353197)

[Slika 11: Konfiguracija IP na končni napravi 23](#_Toc102353198)

[Slika 12: DHCP določen IP na končni napravi 25](#_Toc102353199)

[Slika 13: DHCPv6 nastavljen IPv6 29](#_Toc102353200)

[Slika 14: Testiranje s paketi 34](#_Toc102353201)

**KAZALO TABEL**

[Tabela 1: IPv4 razdelitev 20](#_Toc102353202)

[Tabela 2: Vsi IP naslovi na vmesnikih 24](#_Toc102353203)

# UVOD

Da lahko podjetja neprekinjeno in učinkovito opravljajo svoje delo potrebujejo kvalitetno postavljeno omrežje, ki ima možnosti nadgradnje, če kasneje priključimo dodatne naprave, ter ustreza vsem zahtevam. Postavitev omrežja lahko v naprej testiramo s programom Cisco Packet tracer. Da bi preizkusil postavljanje omrežja znotraj podjetja bom uporabil ta program, da se lahko pripravim za delo v prihodnosti.

Poleg učinkovitosti pa moramo v omrežju tudi zagotoviti varnost, zato bom v seminarski nalogi, po priloženih navodilih, postavil omrežje, ki ima potrebne varnostne funkcije.

# POSTAVITEV OMREŽJA V PODJETJU

Za postavitev omrežja smo pri pouku dobili navodila ter priloženo skico. To skico lahko vidite na sliki 1.

Diagram

Description automatically generated

Slika : Priložena skica omrežja

Na sliki 1 lahko vidite več različnih naprav ter povezave med njimi.

## NAPRAVE IN POJMI PRI POSTAVITVI OMREŽJA

Če želimo postaviti učinkovito omrežje, rabimo vedeti kaj posamezne naprave delajo znotraj tega ter kako lahko sploh te naprave nastavimo. Pri omrežju sem uporabil 4 usmerjevalnike, 3 stikala in več računalnikov.

### USMERJEVALNIK

Usmerjevalnik (ang. Router) nam omogoča komunikacijo med različnimi omrežji. Redko nam ob v podjetniškem okolju zadostovalo samo eno omrežje, še posebej, če želimo preprečiti komunikacijo med različnimi sklopi, kot na primer, ne želimo da lahko nekdo iz proizvodnje komunicira z računalniki iz administracije.

Poleg povezovanja omrežij nam te tudi omogočajo usmerjanje paketov po različnih omrežjih. Tudi v privatnih domačih omrežjih je to pomembno, saj če želimo dostop do spletnih omrežij, rabi naš paket nekako priti do strežnikov na katerih so te aplikacije.

(1)

Ker usmerjevalnik povezuje različna omrežja moramo nastaviti vsakemu vmesniku (ang. Interface) svoj naslov znotraj različnega omrežja. Vsak vmesnik lahko tudi razdelimo na pod-vmesnike (ang. Subinterface) da ustvarimo tako imenovan usmerjevalnik na palici (ang. Router on a stick). (2)

Izgled usmerjevalnika lahko vidite na sliki 2.



Slika : Usmerjevalnik Linksys E5350 (3)

### STIKALO

Usmerjevalniki imajo omejeno število vhodov. Hkrati obstaja velika verjetnost, da želimo imeti več naprav na istem omrežju. Pri temu nam pomagajo stikala (ang. Switch). Ta nam omogočajo povezovanje mnogo naprav na en usmerjevalnik pod istim omrežjem. Stikala so nadgradnja starejših razdelilnikov (ang. Hub). Stikala vejo, kje se nahajajo posamezne naprave in omrežja, zato lahko pošiljajo pakete samo določeni napravi, ne pa vsem v omrežju in s tem omrežje manj obremenjujejo. (4)

Stikalo lahko vidite na sliki 3:



Slika : Stikalo TP-LINK TL-SG1024D (5)

### KONČNE NAPRAVE

Celotno omrežje nič ne pomeni, če na njega niso priključene neke končne naprave. Te naprave raztezajo od osebnih računalnikov in telefonov vse do strežnikov. Te naprave imajo znotraj točno določen naslov (ang. Address). Če naprave želijo med seboj komunicirati rabijo vedeti kateremu naslovu pošiljajo podatke, tako lahko rečemo, da je IP naslov vsake naprave kot njen identifikator. (6)

Na končnih napravah rabimo poleg IP naslova nastaviti tudi privzeti prehod (ang. Default gateway), da vejo na kateri naslov pošiljati pakete, da pridejo do usmerjevalnika, ki jih nato pošlje dalje. (7)

### CLI

CLI ali Cisco command line je način nastavljanja naprav znotraj Cisco omrežja. Preko ukazov lahko nastavimo vse nastavitve na preprost način. Moje razlage bodo tudi predstavljene znotraj tega okolja. Na sliki 4 lahko vidite izgled CLI-ja. (8)

Graphical user interface, text, application

Description automatically generated

Slika : CLI pogled

Cisco je ameriško podjetje za omrežja. Poleg naprav imajo na ponudbo tudi svoj simulator Cisco Packet tracer, znotraj katerega bom tudi postavil svoje omrežje. (9)

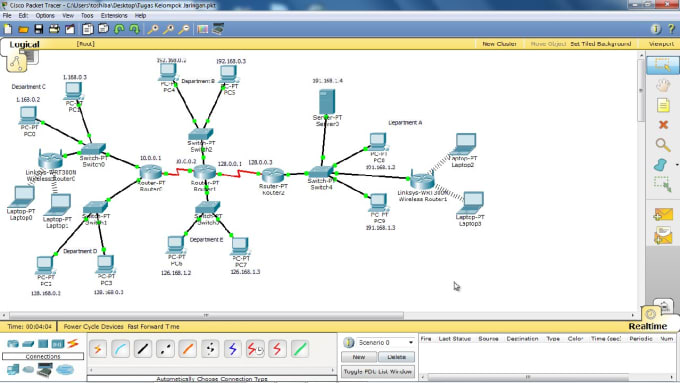
Na sliki 5 lahko vidite logotip podjetja Cisco.

Icon

Description automatically generated

Slika : Logotip Cisco (10)

Na sliki 6 lahko vidite kako izgleda program Cisco Packet tracer.



Slika : Cisco Packet tracer (11)

### VODNIKI

V omrežju uporabljamo različne vodnike za različne povezave. V moji seminarski sem rabil uporabiti samo dva različna vodnika.

**Navadni kabel ali kabel z dvema paricama (ang. Twisted-pair cables)**

To so standardni ethernet kabli. Te so namenjeni povezavi dveh naprav na različnem nivoju, kot sta stikalo in usmerjevalnik ali stikalo in končna naprava.

Primer takega kabla, ki ima tudi nameščen konektor, lahko vidite na sliki 7.

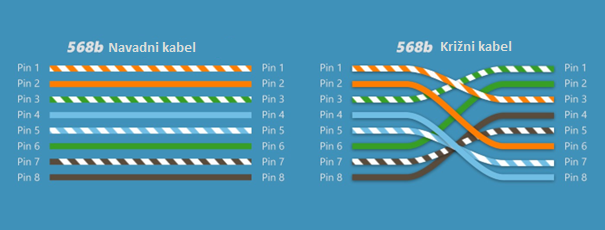
A picture containing indoor

Description automatically generated

Slika : Kabel spisani par

**Križni kabel (ang. Crossover cable)**

Križni kabli so standardni kabli, samo da v njih zamenjamo pozicije nekaterih žic znotraj kabla. Te razlike lahko vidimo na sliki 8.



Slika : Razlika med navadnim in križnim kablom (12)

(13)

## POSTAVITEV OMREŽJA

Poleg skice, ki jo lahko vidite na sliki 1, sem pri nalogi dobil tudi navodila, ki jih lahko vidite na sliki 9.

Graphical user interface, text, application

Description automatically generated

Slika : Navodila za postavitev

Na sliki 9 lahko vidimo, da je postopkov precej veliko, zato sem šel čez vsakega posebej, ena po ena točka. Na ta način bom navodila tudi razložil.

### IMENA NAPRAV

Vsem mrežnim napravam, torej stikalom in usmerjevalnikom, lahko nastavimo ime, ki ga bo ta naprava imela znotraj CLI pogleda.

Da lahko napravam spreminjamo nastavitve moramo za začetek priti v terminal za konfiguracije (ang. Configuration terminal). Do tega dostopamo z naslednjimi ukazi:

Router>enable

Router#configure terminal

Router(config)#

Ko vidimo, da znotraj oklepajev piše (config) vemo, da smo znotraj načina nastavljanja globalnih nastavitev.

Sedaj lahko napravimo spremenimo ime. To naredimo z naslednjim ukazom:

Router(config)#hostname »ime«

Po izvršitvi ukaza bo naš CLI prevzel določeno ime in bo zgledalo tako:

»ime«(config)#

(14) (15)

### VSTOPNO SPOROČILO

Če želimo imeti bolj personalizirane nastavitve ali podatki kakšno opozorilo lahko to storimo s sporočilom. Omrežne naprave imajo več različnih sporočil. Mi nastavljamo sporočilo »Message of the day« ali sporočilo dneva. To sporočilo se prikaže vsakič, ko kdorkoli dostopa do naprave.

Message of the day nastavimo preko naslednjih ukazov:

Router(config)# banner motd #

Nepoblascenim dostop prepovedan!#

V prvem ukazu je tretja beseda naš željeni končni simbol. V tem primeru sem izbral simbol #, saj tega nisem nameraval uporabiti v svojem sporočilu. Ko izvršimo prvi ukaz nas CLI prosi za sporočilo. To vpišemo in na koncu vpišemo še izbrani simbol. Sporočilo, ki ga bo izpisal program nato ni »Nepoblascenim dostop prepovedan!#«, ampak »Nepoblascenim dostop prepovedan!« brez #.

(16)

### Geslo za prehod v priviligiran način

V priviligiran način vstopimo preko prej omenjenega ukaza »enable«. S tem omogočimo vpogled v nastavitve in spreminjanje le teh. Da do teh nastavitev ne bi prišel kar vsak uporabnik jih zavarujemo z geslom. Nastavitev gesla lahko storimo preko dveh podobnih ukazov:

Router(config)#enable password “geslo”

In

Router(config)#enable secret “geslo”

Vidimo lahko, da sta ukaza zelo podobna. Edina razlika je v drugi besedi. Ta beseda določa kakšno varnost želimo. Če uporabimo ukaz »password«, bo naše geslo shranjeno v preprosti tekstovni obliki brez enkripcije in zaradi tega lahko izobraženi uporabniki preprosto vdrejo v naše omrežje. Če uporabimo ukaz »secret« je naše geslo shranjeno v enkriptirani obliki in je zaradi tega veliko bolj varno. Po navodilu sem nastavil geslo na »cisco«.

Za tem, ko nastavimo kaj bo naše geslo, moramo omenjeno enkripcijo samo še vključiti preko tega ukaza:

Router(config)#service password-encryption

(14)

### GESLO NA KONZOLNI VHOD

V realnem svetu je pogosto, da nastavljamo usmerjevalnike in stikala z uporabo drugega računalnika. Ta računalnik priključimo na naše omrežne naprave preko vmesnika imenovanega konzolni vhod (ang. Line). To nastavimo s preprostimi ukazi:

Router(config)#line console 0

Router(config-line)#password “geslo”

Router(config-line)#login

V prvi vrstici določimo na katerem vmesniku želimo spreminjati nastavitve. To je normalno vmesnik 0 in druga števila ne delujejo.

V drugi vrstici nato nastavimo naše geslo. Kot zahteva navodilo sem tega nastavil na »cisco«.

V zadnji vrstici še določimo, da nas prosi za to geslo vsakič, ko se želimo prijaviti.

(17)

### SSH dostop na VTY

Poleg dostopa preko konzolnega vhoda pa je možno, da želimo naprave upravljati preko normalnih povezav. Temu v namen nastavimo virtualni terminal (ang. Virtual Terminal). Tega nastavimo z naslednjimi ukazi:

Router(config)#line vty 0 15

Router(config-line)#password “geslo”

Router(config-line)#login

Router(config)#username “ime” secret “geslo”

Ukaz »line vty 0 15« določi, da želimo omogočiti virtualni dostop 16 napravam hkrati. Drugo števila določa koliko jih želimo. V tem primeru sem dal kar maksimum.

Druga vrstica, »password X« nam omogoča nastaviti geslo za te virtualne linije.

Tretja vrstica, »login« deluje enako kot pri prejšnji nastavitvi in sicer vključi potrebo po geslu ob prijavi.

Zadnja vrstica, »username X secret Y« vklopi uporabniško ime in geslo za naše omrežje. Po zahtevi navodila sem te nastavil na »admin« in »cisco«.

(18)

### Naslov IPv4 za SVI

Stikala lahko upravljamo tudi preko omrežne povezave, vendar za to potrebujemo SVI nastavitve. Da bi to omogočili, stikalu vključimo virtualni vmesnik, ki bo povezan preko VLANa in mu dodelimo IP.

Switch(config)#Interface vlan »št. VLANa«

Switch(config-if)#ip address “ipv4” “subnet maska”

Switch(config-if)#no shutdown

Prva vrstica izbere virtualni vmesnik, odvisno od VLANa na katerem želimo, da imajo uporabniki dostop do tega stikala. Privzeto to pustimo na številu 1.

V drugi vrstici temu vhodu določimo zadnji IPv4 v omrežju, kot zahteva naloga, ter tudi subnet masko tega naslova.

Zadnja vrstica uporabi ukaz »no«. Ta določi, da želimo nasprotni učinek od dalje napisanega ukaza. V tem primeru je nadaljni ukaz »shutdown«. Ta normalno izključi vmesnik, vendar v našem primeru, ker smo uporabili ukaz »no«, ta vmesnik vključi.

(19)

### Varnost na stikalih – izklopite neuporabljena vrata

V prejšnjem postopku smo že videli kako se vključi vmesnike. Sedaj pa bomo neuporabljene vmesnike izključili. To naredimo s tema ukazoma:

Switch(config)#interface range Fa0/X-Y

Switch(config-if-range)#shutdown

Ukaz »interface« nam da dostop do nastavitev za en vmesnik. Ker pa bi bilo izklapljanje vsakega vmesnika posebej zamudno dodamo še opcijo »range«. To nam omogoči spreminjanje nastavitev na več vmesnikih hkrati. Kot zadnji parameter določimo obseg vmesnikov, ki jih želimo spreminjati.

Drug ukaz je pa ukaz »shutdown«, ki izključi delovanje vmesnika.

(20) (21)

### Nastavitev VLAN-ov na S1

Da lahko ločimo različna omrežja jih rabimo razdeliti v virtualna omrežja ali tako imenovane VLANe. Na skici na sliki 1 lahko vidimo, da je stikalo S1 povezano v dve omrežji. Prvo omrežje je nastavljeno na VLAN 10, drugo pa na VLAN 20. Vsi vmesniki imajo privzeto nastavljen VLAN 1. To uredimo z naslednjimi ukazi:

S1(config)# vlan “št. VLANa”

S1(config-vlan)# name “ime VLANa”

S1(config)# interface range “vmesniki, ki jim želimo dodeliti VLAN”

S1(config-if-range)# switchport access vlan “št. VLANa”

Prva dva ukaza določita, da želimo ustvariti nov VLAN z določenim številom in kako želimo, da se ta VLAN imenuje.

Naslednji sklop ukazov vmesnikom nastavi filter, katere VLANe prepuščajo. Da ne nastavljamo vsakega vmesnika posebej si ponovno pomagamo z ukazom »interface range«.

Kot zahteva navodilo, sem vmesnikom F0/1-15 nastavil VLAN 10 in vmesnikom F0/16-20 nastavil VLAN 20.

(22)

### Vrata F0/24 povezava do usmerjevalnika

V prejšnjem sklopu smo opazili, da lahko vsakemu vmesniku nastavimo le en VLAN, vendar na povezavi do usmerjevalnika želimo prepuščati skozi vse VLANe. To popravimo tako, da vmesnik spremenimo v »trunk« način delovanja. Ta prepušča skozi vse VLANe.

Switch(config)#interface “vmesnik”

Switch(config-if)#switchport mode trunk

Izberemo naš vmesnik, ki je povezan z usmerjevalnikom in mu spremenimo način delovanja na »trunk«.

(23)

### SVI v VLAN Uprava

SVI smo nastavljali že v sklopu 2.2.6. Delovali smo po naslednjih ukazih:

Switch(config)#Interface vlan »št. VLANa«

Switch(config-if)#ip address “ipv4” “subnet maska”

Switch(config-if)#no shutdown

V tem primeru je razlika samo, da namesto števila VLANa 1 napišemo števili 10 in 20.

(19)

### Naslavljanje IPv4, DHCPv4 v omrežju z VLANi

Vsem usmerjevalnikom in končnim napravam je treba dodeliti svoj IP naslov, saj ta deluje kot njihov identifikator in jim omogoča komunikacijo med njimi.

**Naslavljanje IPv4**

Naloga zahteva, da naredimo omrežje v naslovnem prostoru 162.20.1.0/25. Da razumemo kaj to pomeni, moramo prvo razumeti »subnet« masko in kako je sestavljen IPv4.

IPv4 je sestavljen iz 32 bitov ter razdeljen je na 4 sklope:

00000000.00000000.00000000.00000000

Če te vse spremenimo v 1 in jih pretvorimo v desetiški sistem dobimo:

255.255.255.255

To je najvišje število, kar ga lahko po temu sistemu dosežemo. Vse te naslove pa delimo na naslove za posamezne naprave ter na omrežja. Da nam to uspe uporabimo »subnet« masko ali masko podomrežja. Ta je tudi sestavljena iz 32 bitov. Iz leve proti desni lahko spreminjamo bite v 1, te ne moremo pomešati. Če nato poravnamo IPv4 in njegovo masko podomrežja, lahko določimo kateri biti bodo uporabljeni za podomrežje ter kateri bodo uporabljeni za naprave znotraj omrežja. Npr.:

IPv4: 10101001.10010000.10100101.01000101

Maska podomrežja: 11111111.11111111.11110000.00000000

V temu primeru lahko vidimo, da je prvih 20 bitov uporabljenih za omrežje, torej imamo omrežje 10101001.10010000.10100000 kar je v desetiškem sistemu 169.144.160.0. Vsi ostali biti bodo samo naprave znotraj tega omrežja. Če želimo dobiti število vseh naprav uporabimo preprost izračun 2^(št. Bitov 0) - 2. V tem primeru je to 2^12 – 2 in dobimo 4094 naprav. Vsem napravam moramo odšteti 2, saj je prvi naslov v omrežju vedno rezerviran za identifikacijo omrežja, zadnji naslov pa je rezerviran kot »broadcast« naslov in nam omogoča pošiljanje paketa vsem napravam znotraj omrežja.

Zdaj, ko vemo kako deluje IPv4, lahko razumemo kaj pomeni naš začetni naslovni prostor. Maska /25 nam pove, da bomo uporabili samo zadnjih 7 bitov za naprave, torej imamo na razpolago samo 128 naslovov. Poleg tega rabimo te dalje razdeliti na podomrežja. Ker je naš naslovni prostor 162.20.1.0 pomeni, da bomo uporabljali naslove med 162.20.1.0 in 162.20.1.127.

(24)

Zaradi načina delovanja IPv4 bomo naslove za podomrežja dodeljevali najprej največjemu podomrežju. Da bi lažje nadaljeval z delom sem za začetek ustvaril tabelo 1.

Tabela : IPv4 razdelitev

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Oznaka**  **podomrežja** | **Maska podomrežja (v obliki /x in v desetiški obliki)** | **Št. uporabnih** | **IP naslov podomrežja (omrežni IP)** | **Broadcast naslov** | **Obseg naslovov za naprave** |
| ISP WAN | /29; 255.255.255.248 | 6 | 24.20.1.160 | 24.20.1.167 | .161-.166 |
| ProizvodnjaA1 | /26; 255.255.255.192 | 62 | 162.20.1.0 | 162.20.1.63 | .1-.62 |
| Proizvodnja B1 | /28; 255.255.255.240 | 14 | 162.20.1.64 | 162.20.1.79 | .65-.78 |
| Uprava | /28; 255.255.255.240 | 14 | 162.20.1.80 | 162.20.1.95 | .81-.94 |
| Razvoj | /29; 255.255.255.248 | 6 | 162.20.1.96 | 162.20.1.103 | .97-.102 |
| R1-R2 | /30; 255.255.255.252 | 2 | 162.20.1.104 | 162.20.1.107 | .105-.106 |
| R1-R3 | /30; 255.255.255.252 | 2 | 162.20.1.108 | 162.20.1.111 | .109-.110 |
| R2-R3 | /30; 255.255.255.252 | 2 | 162.20.1.112 | 162.20.1.115 | .113-.114 |

Hkrati sem si tudi dopisal vse naslove na svoj projekt, kakor se vidi na sliki 10.

Diagram

Description automatically generated

Slika : Postavitev omrežja in vse oznake

Ko smo določili katere IP naslove bodo imele vse naprave jim moramo te naslove še dodeliti.

Stikala IP naslovov ne potrebujejo, saj so ta namenjena samo povezovanju naprav s temi IP naslovi.

Na usmerjevalnikih nastavimo vsakemu vmesniku posebej IP naslov. To naredimo z naslednjimi ukazi:

Router(config)#interface “vmesnik”

Router(config-if)#ip address “IP” “maska”

Router(config-if)#no shutdown

S prvim ukazom izberemo vmesnik.

Z drugim ukazom nastavimo IP in masko. Vmesnikom normalno dodelimo prvi IP v omrežju, razen ko to ni mogoče, npr. če sta v omrežju dva usmerjevalnika.

Z zadnjim ukazom, ki je pa že znan, pa vključimo vmesnik.

(10)

Na problem naletimo, ko probamo dodeliti IP naslov vmesniku, ki je povezan na VLANe, saj je ta vmesnik povezan na dve podomrežji in mora zato imeti dva IP naslova. To storimo z podvmesniki in tako imenovanim »router on a stick« sistemom. Usposabljanje tega je zelo preprosto. Na ime vmesnika, ki ga želimo razdeliti na podvmesnike, samo dodamo decimalke, npr. F0/0.1. Takrat moramo pa tudi poskrbeti da temu podvmesniku nastavimo pravilen VLAN. Za to uporabimo naslednje ukaze:

Router(config)#interface “vmesnik”.”pod št.”

Router(config-subif)#encapsulation dot1Q “št. VLANa”

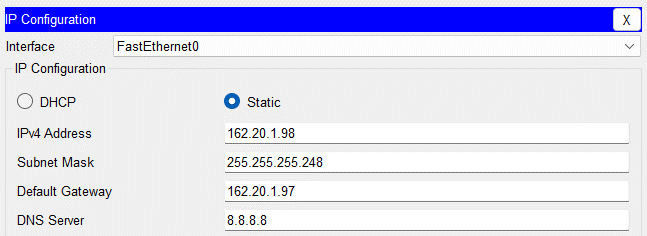
Router(config-subif)#ip address “IP” “maska”

Ukaz v drugi vrstici temu podvmesniku določi VLAN.

Ko pa vsem podvmesnikom določimo naslove in VLANe pa ne smemo pozabiti celoten vmesniku tudi vključiti z ukazom »no shutdown«.

(25)

Da dodelimo IP naslov končnim napravam, v našem primeru računalnikom, samo uporabimo njihovo namizje in to nastavimo tam. Za IP uporabimo prosti naslov, masko nastavimo takšno, kot jo ima podomrežje, za privzeti prehod uporabimo naslov vmesnika na usmerjevalniku, ki je povezan v omrežje, za DNS strežnik pa uporabimo en izmed mnogih razpoložljivih DNS strežnikov. Najbolj popularen DNS strežnik je ta od Googla, ki se glasi 8.8.8.8. Kako izgledajo nastavitve vidimo na sliki 11.



Slika : Konfiguracija IP na končni napravi

(26)

V tabeli 2 so prikazani vsi IP naslovi na posamezne vmesniku vseh naprav poleg stikal.

Tabela : Vsi IP naslovi na vmesnikih

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Naprava | Vmesnik | Naslov IP | Maska | Privzeti prehod |
| ISP WAN | Fa0/1 | 24.20.1.161 | 255.255.255.248 | / |
| R3 | Fa0/1 | 24.20.1.162 | 255.255.255.248 | / |
| R3 | Eth0/1/0 | 162.20.1.97 | 255.255.255.248 | / |
| R3 | Eth0/0/0 | 162.20.1.114 | 255.255.255.252 | / |
| R3 | Fa0/0 | 162.20.1.110 | 255.255.255.252 | / |
| R1 | Fa0/0 | 162.20.1.109 | 255.255.255.252 | / |
| R1 | Fa0/1 | 162.20.1.105 | 255.255.255.252 | / |
| R1 | Eth0/0/0 | 10.20.1.65 | 255.255.255.240 | / |
| R2 | Fa0/1 | 162.20.1.106 | 255.255.255.252 | / |
| R2 | Eth0/0/0 | 162.20.1.113 | 255.255.255.252 | / |
| R2 | Fa0/0.1 | 162.20.1.1 | 255.255.255.192 | / |
| R2 | Fa0/0.2 | 162.20.1.81 | 255.255.255.240 | / |
| PC2 | Fa0 | 10.20.1.66 | 255.255.255.240 | 10.20.1.65 |
| PC20 | Fa0 | 162.20.1.82 | 255.255.255.240 | 162.20.1.81 |
| PC21 | Fa0 | 162.20.1.83 | 255.255.255.240 | 162.20.1.81 |
| PC22 | Fa0 | 162.20.1.84 | 255.255.255.240 | 162.20.1.81 |
| PC10 | Fa0 | 162.20.1.2 | 255.255.255.192 | 162.20.1.1 |
| PC11 | Fa0 | 162.20.1.3 | 255.255.255.192 | 162.20.1.1 |
| PC12 | Fa0 | 162.20.1.4 | 255.255.255.192 | 162.20.1.1 |
| Pisarna | Fa0 | 162.20.1. | 255.255.255.248 | 162.20.1.97 |

V tabeli 2 lahko tudi vidimo, da na usmerjevalnikih nisem nastavil privzetih prehodov. To je zaradi tega, saj privzeti prehod nastavimo samo na končnih naprav in je enak IP naslovu vmesnika na usmerjevalniku.

(27)

**DHCPv4**

Končnim napravam lahko statično/ročno nastavimo naslove, ampak to postane zelo naporno, ko je teh naprav več. Temu v pomoč uporabimo DHCP. Ta avtomatsko napravam znotraj določenega omrežja dodeli njihove IP naslove. Naloga zahteva, da ta sistem uporabimo le na omrežjih z VLANi, torej na usmerjevalniku R2. Da ustvarimo DHCP strežnik uporabimo naslednje ukaze:

R2(config)#ip dhcp pool “ime strežnika” (npr. ProizvodnjaA1)

R2(dhcp-config)#network “IP” “maska”

R2(dhcp-config)#default-router “IP tega usmerjevalnika”

R2(dhcp-config)#dns-server 8.8.8.8

S prvim ukazom ustvarimo DHCP strežnik, ki bo dodeljeval IP naslove končnim napravam in ga tudi poimenujemo.

Z drugim ukazom določimo v katerem omrežju se nahaja ta DHCP strežnik.

Tretji ukaz določi privzeti prehod torej nanj nastavimo IP trenutnega usmerjevalnika.

Zadnji ukaz določi kater DNS strežnik bomo podeljevali, zato ga nastavimo kar na 8.8.8.8.

Ko smo ustvarili DHCP strežnik rabimo samo še na končnih napravam določiti, da prejemajo DHCP naslov in ne statičen/ročen naslov, počakamo nekaj trenutkov in kmalu dobimo avtomatski IP.

Graphical user interface, text, application

Description automatically generated

Slika : DHCP določen IP na končni napravi

(28)

### Usmerjanje OSPF

Usmerjevalniki privzeto ne vejo kje se nahajajo vsa ostala omrežja, zato ne znajo pošiljati paketov po verigi usmerjevalnikov. Ta problem lahko rešimo tako, da vsem usmerjevalnikom povemo kako priti do vsakega podomrežja v našem omrežju, vendar to je zelo časovno potratno in vedno, ko bi želeli dodati omrežju nov usmerjevalnik ali novo podomrežje, bi ponovno vse usmerjevalnike rabili naučiti nove poti.

Da se vsemu temu izognemo uporabimo dinamično usmerjanje. Ponovno lahko to naredimo na dva načina, preko RIP usmerjanja ali preko OSPF usmerjanja. RIP usmerjanje je starejše in v verziji 1 ne podpira podomrežji, ne omogoča ločevanje različnih področji itd. Zato uporabimo usmerjanje OSPF.

Na vsakemu stikalu omogočimo OSPF usmerjanje ter tudi povemo na katero omrežje je povezan. Usmerjevalnik bo nato vsem ostalim usmerjevalnikom oglaševal na katera omrežja je povezan in tako bodo ugotovili kje se nahajajo posamezni IP naslovi.

R1(config)#router ospf 1

R1(config-router)#router-id X.X.X.X

R1(config-router)#network “network, v katerega je povezan usmerjevalnik” “wildcard maska« area »št. področja«

S prvim ukazom določimo, da želimo uporabljati OSPF usmerjanje. Poleg tega napišemo identifikacijsko število OSPFja. To pustimo na 1.

Z drugim ukazom določimo identifikacijsko število usmerjevalnika. Za to samo uporabimo število usmerjevalnika, v podanem primeru je to 1, in ga štirikrat ponovimo. V tem primeru dobiš 1.1.1.1.

S tretjim ukazom določimo na katero omrežje je usmerjevalnik povezan. Ta ukaz izvedemo za vsa omrežja posebej. Usmerjevalniku bi tudi lahko samo rekli naj komunicira z vsemi omrežji, vendar to ni po načelu najboljše prakse. Poleg IP naslova pa dodamo tudi wildcard masko. Ta je ravno obratna od maske podomrežja, torej od števila 255 odštejemo vrednost posameznega okteta, npr. 255.255.192.0 se spremeni v 0.0.63.255. Na koncu tudi izberemo v katerem področju naj vmesnik deluje. Ker imamo vse kot eno omrežje kar pustimo področje 0.

(29) (10)

### Privzeta pot v WAN na usmerjevalniku, ki je povezan v WAN (kaže naj na ISP WAN), oglaševanje privzete poti ostalim usmerjevalnikom.

Na enak način kot ostale usmerjevalnike tudi povežemo usmerjevalnika ISP WAN in R3.

Ko to storimo na usmerjevalniku R3 vnesemo še naslednje ukaze:

R3(config)# ip route 0.0.0.0 0.0.0.0 “ip WAN usmerjevalnika”

R3(config)#default-information originate

S temi ukazi smo vključili privzeto pot. Ta usmerja pakete, ki jih noben usmerjevalnik znotraj omrežja ne prepozna. To naj bi sicer nastavili na vsakem usmerjevalniku posebej, vendar bi bilo to naporno, zato smo uporabili OSPF. Naslov privzete poti je 0.0.0.0.

(10)

### IPv6 naslove v LAN Razvoj, DHCPv6 na omrežnem prehodu proti WAN, privzeta pot IPv6 v WAN.

Vzporedno z IPv4 sistemom dandanes uporabljamo tudi sistem IPv6. Da tega nastavimo ne rabimo spremeniti nobene nastavitve, ki smo jih že nastavili.

**Naslavljanje IPv6**

IPv6 ima kar 128 bitov. Te so tudi razdeljeni v oktete. Ker pa so števila tako velika jih zapisujemo kar v šestnajstiškem sistemu. Največji naslov IPv6 je po temu sistemu FFFF:FFFF:FFFF:FFFF:FFFF:FFFF:FFFF. Opazimo, da oktete delimo z dvopičji namesto pikami. Pri IPv6 imamo tudi maske, ki delujejo na enak način kot pri IPv4, torej nam maska /64, kar je točno polovica od 128, pove, da bomo uporabljali v našem naslovnem prostoru naslove od 2020:0020:0021:00CF:0000:0000:0000:0000 do 2020:0020:0021:00CF:FFFF:FFFF:FFFF:FFFF. Hitro pa lahko opazimo, da je te naslove zaradi njihove dolžine zelo naporno pisati. Temu se izognemo tako, da vse ničle, ki so na začetku posameznega okteta kar spustimo ter oktete, ki so polni samih ničel tudi kar spustimo in jih nadomestimo z dvojnim dvopičjem ::. Na koncu pridemo iz naslova 2020:0020:0021:00CF:0000:0000:0000:0000 v naslov 2020:20:21:CF::, kar je mnogo bolj pregledno.

IPv6 nastavimo s tem ukazom:

Router(config-if)#ipv6 address “IPv6”/”velikost maske”

Enako naredimo tudi na ISP WAN usmerjevalniku in vmesnikom na usmerjevalniku R3, ki je povezan na WAN.

(30) (10)

**DHCP IPv6**

Omenil sem, da je zelo naporno pisati IPv6 naslove, zato se tega želimo čim bolj izogniti. Podobno kot pri IPv4 ustvarimo DHCP strežnik za IPv6 v podomrežju »Razvoj«.

R3(config)# ipv6 dhcp pool “ime DHCP strežnika”

R3(config-dhcpv6)#dns-server 2001:4860:4860::8888

R3(config)# interface “vmesnik”

R3(config-if)# ipv6 address “ipv6”/”velikost maske”

R3(config-if)# ipv6 dhcp server Razvoj

Prvi ukaz ustvari in poimenuje DHCP strežnik.

Drugi ukaz določe DNS strežnik tega. Ponovno sem uporabil DNS strežnik od Google, vendar tega za IPv6.

S tretjim ukazom določimo vmesnik, ki povezuje naprave katerim želimo dodeljevati IPv6 naslove.

Četrti ukaz določi IP in masko tega omrežja.

Zadnji ukaz določi kateri DHCP strežnik želimo uporabiti na temu vmesniku.

Ko smo ustvarili DHCPv6 strežnik gremo ponovno do naše končne naprave in za IPv6 naslavljanje določimo DHCP.

Graphical user interface, text, application

Description automatically generated

Slika : DHCPv6 nastavljen IPv6

(10)

**Privzeta pot**

Ko imamo določene IPv6 naslove, rabimo samo še nastaviti privzeto pot. Tudi to naredimo na podoben način kot pri IPv4.

Router(config)#ipv6 route ::/0 “IPv6 ISPja”

Ta ukaz izvršimo samo na usmerjevalniku, ki je povezan na ISP WAN usmerjevalnik. Tu lahko tudi vidimo, da smo uporabili ::/0, kar je naslov za privzeto pot.

(31)

### ACL

Pri omrežju ne želimo, da računalniki v proizvodnji dostopajo do računalnikov znotraj Uprave. Da bi to preprečili uporabimo ACL ali Access List (slo. Seznam dostopa). Ta nam omogoča, da določimo katere IPje želimo sprejemati na posameznem vmesniku.

Samo ACL pa ni dovolj, da bi preprečili komunikacijo med ProzvodnjaA1 in Uprava, saj bi te lahko pakete pošiljali kar preko stikala. Zato smo te tudi razdelili na VLANe. Ker te niso na istem VLANu stikalo ne pošilja paketov med njimi. Samo zato, ker pa stikalo ne pošilja paketov med VLANi, pa ne pomeni, da tega ne bo delal usmerjevalnik. Zato še zmeraj potrebujemo ACL.

ACL nastavitve naredimo v dveh postopkih. Najprej ACL ustvarimo, nato ga pa nastavimo. Da ACL ustvarimo uporabimo naslednje ukaze:

Router(config)#no access-list “št ACL”

Router(config)#access-list “št. ACL” deny/permit “IP naslov” “wildcard maska”

Router(config)#access-list deny/permit any <- omogoči dostop vsem razen tistemu, ki si ga napisal v prejšnjem ukazu. Ta ukaz mora biti zadnji, drugače ne dela pravilno

S prvim ukazom za vsak slučaj pobrišemo vse nastavitve iz izbranega ACL. Ker uporabljam samo enega sem njegovo število za udobje pustil kar na 1.

Z drugim ukazom določimo katere IP naslove želimo blokirati ali prepuščati skozi. Ker želimo preprečiti komunikacijo samo s proizvodnjo uporabljam blokiranje, torej »deny«. Ta ukaz lahko ponovimo večkrat za več naslovov. Ker imamo poleg ProizvodnjaA1 tudi ProizvodnjaB1 sem blokiral dva naslova.

Zadnji ukaz določi, da želimo blokirati ali prepuščati vse naslove poleg teh, ki smo jih nastavili s prejšnjim ukazom. V mojem primeru sem uporabil »permit any«, saj želim omogočiti dostop vsem naslovom, ki niso iz proizvodnje. Ta ukaz mora biti na koncu, drugače ACL ne bo deloval pravilno.

Ko smo ustvarili ACL ga pa rabimo samo še dodati na vmesnik, kjer želimo, da ta deluje.

Router(config)#interface “vmesnik”

Router(config-if)#ip access-group “št. ACL” in/out

Ko izberemo naš vmesnik določimo z ukazom ali želimo, da naš ACL velja za pakete, ki prihajajo v omrežje ali izven tega.

(32)

### NAT (PAT)

Če želimo znotraj omrežja uporabljati zasebna podomrežja rabimo uporabiti PAT.

Da pa lahko uporabimo PAT, prvo potrebujemo zasebno omrežje ustvariti. To naredimo tako, da preprosto zamenjamo prvo število v omrežju z 10. Tako sem spremenil omrežje za ProdukcijaB1 iz 162.20.1.64 v 10.20.1.64.

Ko imamo zasebno omrežje, izvedemo na usmerjevalniku, ki je povezan na ISP WAN, naslednje ukaze:

Router(config)#access-list “št. Access lista” permit “IP 10.x.x.x” “wildcard maska”

Omogočimo komunikacijo z zasebnim omrežjem. Ker je to na drugem usmerjevalniku kot prej, lahko ponovno uporabimo število 1 za ACL.

Router(config)#interface “vmesnik povezan na WAN”

Router(config-if)#ip nat outside

Izberemo vmesnik, ki je povezan na WAN in ga nastavimo kot zunanji NAT.

Router(config)#interface “ostali vmesniki”

Router(config-if)#ip nat inside

Vse ostale vmesnike, ki se povezujejo do tega zasebnega omrežja, nastavimo kot notranjost omrežja.

Router(config)#ip nat inside source list “št. Prej nastavljenega access lista” interface “vmesnik povezan na WAN” overload

S tem ukazom vključimo PAT.

(33)

## TESTIRANJE OMREŽJA

Omrežje lahko preprosto testiramo tako, da poskušamo pošiljati pakete med napravami. Poslal sem 3 pakete, kot je razvidno na sliki 14.

Graphical user interface, text, application, table

Description automatically generated

Slika : Testiranje s paketi

Na sliki 14 lahko vidimo, da je paket uspešno bil poslan iz ProizvodnjaB1 v Razvoj.

Uspešno je bil poslan tudi paket iz Razvoj v Uprava.

Paket iz Uprava v ProizvodnjaA1 pa ni bil uspešen, saj smo z ACL blokirali komunikacijo med tema omrežjema.

Vse deluje kot pričakovano.

# ZAKLJUČEK

Tekom seminarske sem uspešno postavil omrežje, ki bi lahko bilo implementirano tudi v podjetjih. Projekt sledi vsem zahtevanim navodilom in uspešno tudi deluje znotraj simulacije.

Poleg tega sem v seminarski natančno predstavil kako sem opravil posamezen postopek znotraj omrežja in s tem omogočil bralcem, da lahko tudi sami postavijo tako omrežje, če to želijo.

Z ustvarjanjem te seminarske sem lahko močno utrdil znanje, ki smo ga pridobili pri pouku in lahko sem doživel mnoge napake, ki jih lahko naredimo na poti pri postavljanju takega omrežja.

# VIRI IN LITERATURA

1. **Cloudflare.** What is a router? *Cloudflare.* [Online] 2022. https://www.cloudflare.com/learning/network-layer/what-is-a-router/.

2. **saurabhsharma56.** Configuration of Router on a stick. *GeeksForGeeks.* [Online] oktrober 25, 2021. https://www.geeksforgeeks.org/configuration-of-router-on-a-stick/.

3. **Mimovrste.** Linksys E5350, AC1000 brezžični WiFi usmerjevalnik. *Mimovrste.* [Online] https://www.mimovrste.com/usmerjevalniki-routerji/linksys-e5350-ac1000-brezzicni-wifi-usmerjevalnik.

4. **Williams, Lawrence.** Hub vs Switch: What’s the Difference? *Guru99.* [Online] april 30, 2022. https://www.guru99.com/hub-vs-switch.html#:~:text=KEY%20DIFFERENCES-,A%20Hub%20is%20a%20networking%20device%20that%20allows%20you%20to,on%20the%20data%20link%20layer..

5. **currys.** TP-LINK TL-SG1024D Network Switch - 24 port. *currys.* [Online] maj 1, 2022. https://www.currys.co.uk/products/tplink-tlsg1024d-network-switch-24-port-21429266.html.

6. **OpenLearn.** Internet of everything. *OpenLearn.* [Online] november 13, 2019. https://www.open.edu/openlearn/mod/oucontent/view.php?id=48444&section=3.3.

7. **Walker, Dale.** What is a default gateway? *ITPro.* [Online] februar 10, 2022. https://www.itpro.co.uk/network-internet/30327/what-is-a-default-gateway.

8. **NetworkLessons .** Introduction to Cisco IOS CLI (Command-Line Interface). *NetworkLessons.* [Online] https://networklessons.com/cisco/ccna-routing-switching-icnd1-100-105/introduction-cisco-ios-cli-command-line-interface#:~:text=Most%20Cisco%20devices%20(including%20routers,from%20the%20router%20or%20switch..

9. **Wikipedia.** Cisco. *Wikipedia.* [Online] april 18, 2022. https://en.wikipedia.org/wiki/Cisco.

10. **Cisco.** Cisco. *Cisco.* [Online] https://www.cisco.com/.

11. **karimatiki.** I will configure your cisco packet tracer problems. *fiverr.* [Online] https://www.fiverr.com/karimatiki/solve-your-cisco-packet-tracer-problems.

12. **ComputerCableStore.** What are Ethernet Crossover Cables? *ComputerCableStore.* [Online] https://www.computercablestore.com/what-are-ethernet-crossover-cables.

13. **Mitchell, Bradley.** Uvod v omrežne kable. *eYewated.* [Online] https://sl.eyewated.com/uvod-v-omrezne-kable/.

14. **Davis294, David.** Cisco administration 101: Learn 10 commands to configure on a new router. *TechRepublic.* [Online] oktober 13, 2005. https://www.techrepublic.com/article/cisco-administration-101-learn-10-commands-to-configure-on-a-new-router/.

15. **Cisco.** Using the Command-Line Interface. *Cisco.* [Online] https://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst3560/software/release/12-2\_46\_se/command/reference/cr1/intro.pdf.

16. **NetworkLessons.** How to configure Cisco IOS Banners. *NetworkLessons.* [Online] 2022. https://networklessons.com/cisco/ccie-routing-switching/how-to-configure-cisco-ios-banners.

17. **Cisco.** Configure Telnet, Console and AUX Port Passwords on Routers. *Cisco.* [Online] december 17, 2019. https://www.cisco.com/c/en/us/support/docs/ios-nx-os-software/ios-software-releases-110/45843-configpasswords.html#pw-line.

18. **Bhardwaj, Rashmi.** Meaning of line vty 0 4 in configuration of Cisco Router or Switch. *IPWithEase.* [Online] https://ipwithease.com/what-is-meaning-of-line-vty-0-4-in-configuration-of-cisco-router-or-switch/.

19. **IT\_NEWS.** how to configure a switch virtual interface. *YouTube.* [Online] june 21, 2021. https://www.youtube.com/watch?v=sjOg65wIVpQ.

20. **study-ccna.** Interface range command. *study-ccna.* [Online] https://study-ccna.com/interface-range-command/.

21. **KnowledgeBase.** HowTo : Enable/Disable Interface on CISCO - Shutdown Command. *KnowledgeBase.* [Online] https://answers.mak.ac.ug/network-connectivity/howto-enabledisable-interface-cisco-shutdown-command.

22. **Bialy, Marcin.** How to configure VLAN on Cisco. *Grandmetric.* [Online] https://www.grandmetric.com/knowledge-base/design\_and\_configure/how-to-configure-vlan-cisco/.

23. **cisco.** Cisco Networking Academy's Introduction to VLANs. *cisco.* [Online] april 7, 2014. https://www.ciscopress.com/articles/article.asp?p=2181837.

24. **Wikipedia.** Subnetwork. *Wikipedia.* [Online] april 19, 2022. https://en.wikipedia.org/wiki/Subnetwork.

25. **IT Exam Answers.** Encapsulation Dot1Q Command on CISCO Router/Switch. *IT Exam Answers.* [Online] april 24, 2018. https://itexamanswers.net/encapsulation-dot1q-command-on-cisco-router-switch.html.

26. **Sciker.** How to set IP Address to PC in Cisco Packet Tracer - Packet Tracer Sinhala Tutorial (Part 4). *YouTube.* [Online] marec 6, 2019. https://www.youtube.com/watch?v=dNi-dJK2PBA.

27. **Wikipedia.** IPv4. *Wikipedia.* [Online] april 26, 2022. https://en.wikipedia.org/wiki/IPv4.

28. **Gorman, Hunter.** Cisco IOS DHCP Server Configuration. *PIV IT.* [Online] maj 22, 2020. https://info.pivitglobal.com/resources/cisco-ios-dhcp-server-configuration.

29. **Maggio, Alessandro.** Cisco OSPF Configuration according to best practices. [Online] oktober 4, 2018. https://www.ictshore.com/advanced-networking/cisco-ospf-configuration/.

30. **Wikipedia.** IPv6. *Wikipedia.* [Online] april 2, 2022. https://en.wikipedia.org/wiki/IPv6.

31. **Hewlett Packard Enterprise.** Configuring the IPv6 default route. *Hewlett Packard Enterprise.* [Online] https://techhub.hpe.com/eginfolib/networking/docs/switches/K-KA-KB/16-01/5200-0133\_ipv6\_config\_k/content/ch06s07.html.

32. **ComputerNetworkingNotes.** Configure Standard Access Control List Step by Step Guide. *ComputerNetworkingNotes.* [Online] december 2, 2021. https://www.computernetworkingnotes.com/ccna-study-guide/configure-standard-access-control-list-step-by-step-guide.html.

33. **ManageEngine.** Configuring Port Address Translation (PAT) on Cisco devices. *ManageEngine.* [Online] https://www.manageengine.com/network-configuration-manager/configlets/configuring-pat-cisco.html.

# STVARNO KAZALO

DHCP, 19, 25, 28, 29

IP, 4, 5, 15, 19, 20, 22, 23, 24, 25, 26, 28, 29, 30, 31, 33

naprava, 5, 10, 14, 19, 23, 25, 34

omrežje, 1, 4, 1, 2, 3, 4, 5, 6, 7, 12, 14, 15, 17, 19, 21, 22, 23, 25, 26, 27, 29, 31, 32, 33, 35

OSPF, 26, 27

podomrežje, 19, 20, 26, 29, 33

stikalo, 2, 4, 7, 13, 15, 17, 24, 26, 31

strežnik, 3, 5, 23, 25, 29

usmerjevalnik, 4, 3, 4, 5, 7, 18, 22, 23, 24, 25, 26, 27, 28, 30, 31, 33

VLAN, 4, 15, 17, 18, 19, 22, 25, 31

vmesnik, 3, 13, 15, 16, 17, 18, 22, 23, 24, 26, 29, 31, 32, 33

WAN, 20, 24, 27, 28, 30, 33

# PRILOGE

Priloga 1 – Word dokument ter datoteka Packet tracer

<https://github.com/nik1178/RSO-final-seminar>