

Obvladajmo lokalna omrežja – OLO

SIRIKT 2009

Potek delavnice z opisom vaj.

Matjaž Straus, Arnes

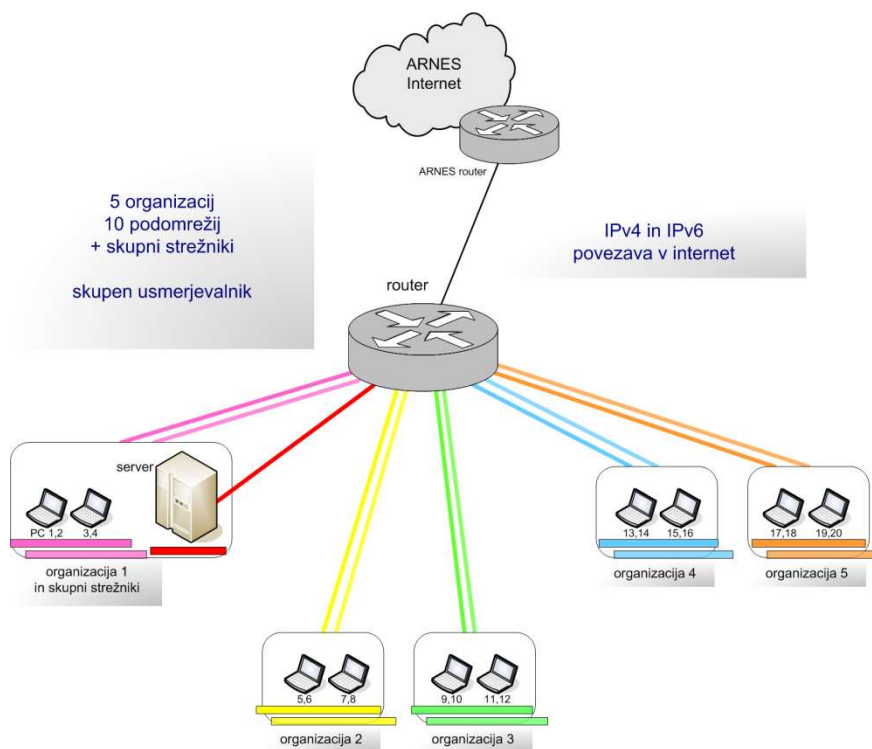
*Go beyond ::1
Pojdi onkraj ::1*

Uvod

V delavnici »Obvladajmo lokalna omrežja« - OLO – bomo z omrežno opremo proizvajalca Cisco zgradili 10 lokalnih omrežij, ki bodo razdeljena v 5 »organizacij«. Vsaka organizacija bo imela dve omrežji – administrativno in pedagoško. Ta omrežja bomo povezali s skupnim usmerjevalnikom, kamor bo povezano tudi omrežje za skupne strežnike. S tem usmerjevalnikom bomo omrežje v delavnici povezali z omrežjem ARNES in internetom.

V omrežju delavnice bomo poleg trenutno razširjenega IP-protokola različice 4 uporabljali tudi sodobnejšo različico – IPv6.

Končno omrežje delavnice – naš cilj – prikazuje slika 1.



Slika 1: Ciljna topologija IP-omrežij v delavnici. Prikazanih je 10 ločenih IP-podomrežij v 5 organizacijah in posebno omrežje za skupne strežnike.

V omrežje delavnice bomo povezali skupen strežnik. To bo naš DNS strežnik za domeno delavnica.arnes.si, DHCP strežnik za vse organizacije in spletni - HTTP (WWW) strežnik.

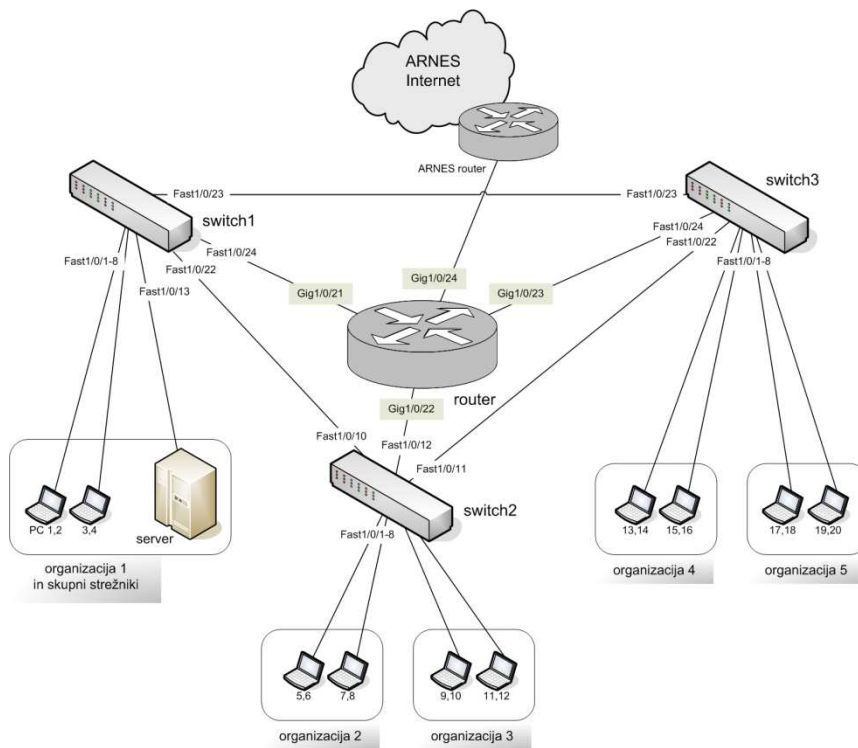
Zahtevnejši udeleženci bodo preverili zmogljivost (prepustnost) našega lokalnega omrežja in zmogljivost povezave z omrežjem ARNES/internet ter lokalno omrežje zaščitili s filtri na usmerjevalniku.

Oprema in ožičenje

Na sliki 2 je shema omrežne opreme in povezav v delavnici. Uporabili bomo 3 stikala (na sliki so označena z »switch1«, »switch2« in »switch3«) in en usmerjevalnik (»router«). Stikala in usmerjevalnik so že povezani z ustreznimi kabli. Udeleženci delavnice bodo povezali svoje prenosne računalnike na vmesnike stikal z zaporednimi številkami od 1 naprej (vmesniki na levi strani stikala). V delavnici se nahaja tudi strežnik, ki bo skupen vsem petim organizacijam.

Uporabili bomo naslednjo opremo:

- switch1: Cisco C3750-24TS
- switch2: Cisco C2950-12
- switch3: Cisco C2950-24
- router: Cisco C3750G-24TS, Advanced IP services IOS



Slika 2: Omrežna oprema in ožičenje v delavnici.

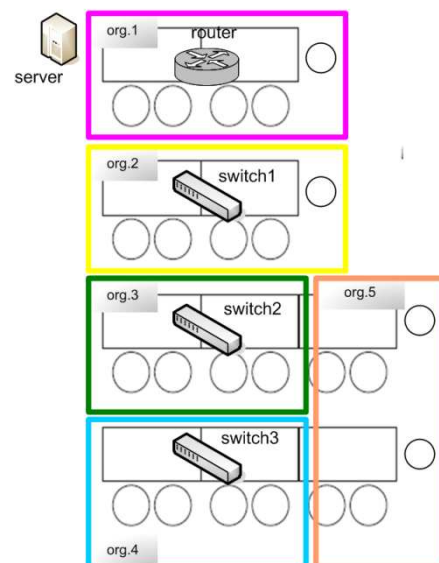
Opomba: zaradi večjega števila udeležencev in pomanjkanja priključkov na stikalo 2 se bodo udeleženci iz organizacije 2 povezali na stikalo 1 in ne na stikalo 2, tako kot je prikazano na sliki.

Razpored delovnih mest, organizacijska shema, dostop do opreme

Na delavnici je 24 udeležencev. Razporedili se bomo v 5 skupin – organizacij, tako kot prikazuje skica na desni.

Povezava prenosnih računalnikov udeležencev (glej tudi shemo povezav v prilogi):

Organizacija	Stikalo	Vmesniki
1	switch1	1 – 6
2	switch1	7 – 12
3	switch2	1 – 8
4	switch3	1 – 6
5	switch3	7 – 12



Vsak udeleženec naj med delom z omrežno opremo uporablja lastno uporabniško ime. Na strežniku bomo uporabljali administrativno uporabniško ime »root«. Uporabniška imena in podatki o navideznih omrežjih in IP-naslovih so v prilogi (tabela 1). Gesla za dostop do opreme bomo sporočili na delavnici.

Do opreme bomo dostopali preko IP-protokola s programoma **telnet** in/ali **ssh** in pri tem, tako kot v realnih IP-omrežjih, skrbno pazili, da ne onemogočimo dosegljivosti omrežne opreme. Za vsak primer so stikala in usmerjevalniki dosegljiva tudi preko konzolnih priključkov na strežniku.

Potrebna programska oprema

Na strežniku v delavnici (<http://153.5.188.5/tools/>) se nahaja vsa potrebna programska oprema, ki jo bodo potrebovali udeleženci delavnice z računalniki, ki imajo nameščen operacijski sistem Windows. Udeležence, ki uporabljajo Linux, MAC OS in druge UNIX-u podobne operacijske sisteme, prosimo, da na svoje računalnike predhodno namestijo:

- odjemalca telnet in ssh
- tcpdump, wireshark
- nmap
- iperf

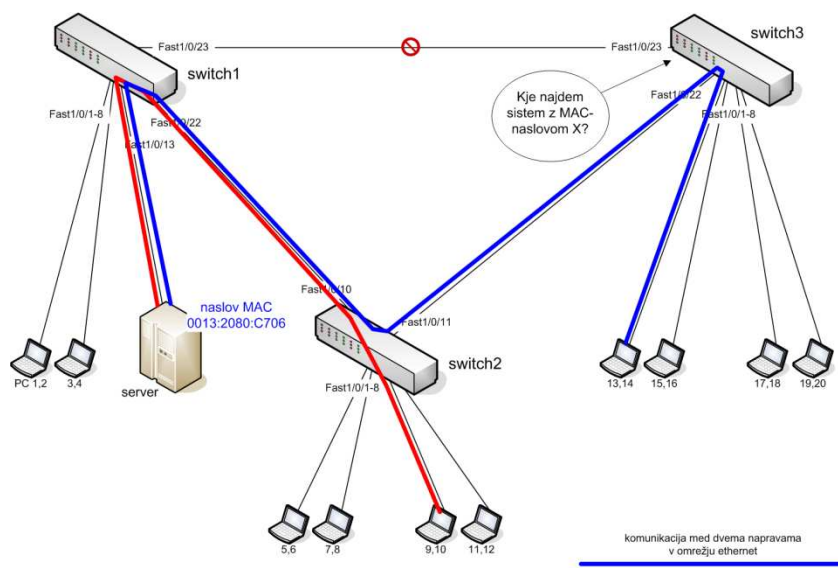
Dokumenti

Na strežniku v delavnici (<http://153.5.188.5/>) se nahajajo dokumenti, ki bodo v pomoč udeležencev, vključno s slikami iz tega priročnika v polni velikosti.

Ethernet

MAC-naslovi, broadcast naslov, ethernet stikala in »forwarding« tabele.

Naprave v omrežju ethernet komunicirajo s pomočjo naslovov MAC. Stikala imajo in dinamično posodablajo posebne »forwarding« tabele, kjer je za vsak znan naslov MAC zapisan vmesnik, preko katerega je dosegljiv sistem s tem naslovom. Na spodnji sliki je prikazana komunikacija dveh računalnikov s strežnikom.



Slika 3: Komunikacija med napravami v omrežju ethernet. Eno od povezav smo namenoma prekinili, tako da med stikali ne redondančnih poti.

Vaja 1: Ugotovi MAC-naslov svojega računalnika. **Ping** stikala. Poišči svoj MAC in vmesnik na stikalu. Označi »svoj« vmesnik. Ping strežnika. Poišči MAC strežnika in vmesnik na stikalu, kamor je povezan strežnik.

Primer:

```
# ifconfig eth2 153.5.188.55/26
```

Moj MAC-naslov?

```
# ifconfig eth2
eth2      Link encap:Ethernet  HWaddr 00:11:95:5C:EC:AA
          inet addr:153.5.188.55  Bcast:153.5.188.63  Mask:255.255.255.192
```

Ping strežnika:

```
# ping 153.5.188.5
PING 153.5.188.5 (153.5.188.5) 56(84) bytes of data.
```

```
64 bytes from 153.5.188.5: icmp_seq=0 ttl=64 time=2.48 ms
64 bytes from 153.5.188.5: icmp_seq=1 ttl=64 time=1.13 ms
64 bytes from 153.5.188.5: icmp_seq=2 ttl=64 time=1.13 ms
...
```

Kje je moj PC?

```
switch2>show mac-address-table
      Mac Address Table
```

```
-----
Vlan    Mac Address      Type    Ports
-----
All     000d.bce6.9b80    STATIC  CPU
All     0100.0ccc.cccc    STATIC  CPU
All     0100.0ccc.cccd    STATIC  CPU
All     0100.0cdd.dddd    STATIC  CPU
1       000d.bde1.d398    DYNAMIC Fa0/10
1       000d.bde1.d3c0    DYNAMIC Fa0/10
1       000f.f75c.0b40    DYNAMIC Fa0/11
1       000f.f75c.0b56    DYNAMIC Fa0/11
1       0011.955c.ecaa    DYNAMIC Fa0/9
1       0013.2080.c706    DYNAMIC Fa0/10
Total Mac Addresses for this criterion: 10
```

```
switch2>show mac-address-table | inc ecaa
1       0011.955c.ecaa    DYNAMIC  Fa0/9
```

Opis vmesnika:

```
interface FastEthernet0/9
description --- predavatelj ---
switchport mode access
no ip address
```

Kje je strežnik (MAC-naslov 0013:2080:C706)?

```
switch2#sh mac-address-table | inc c706
1       0013.2080.c706    DYNAMIC  Fa0/10
```

```
switch2#sh run int fast0/10
!
interface FastEthernet0/10
description --- switch1, Fast1/0/22 ---
```

Strežnik je priklopljen na stikalo switch1.

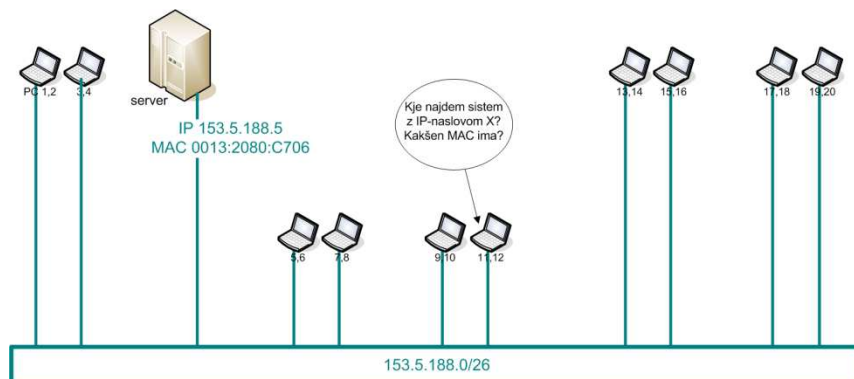
```
switch1>sh mac-address-table | inc c706
1       0013.2080.c706    DYNAMIC  Fa1/0/13
```

Strežnik je na vmesniku Fa1/0/13 stikala switch1.

Ethernet in IPv4

ARP

Protokol ARP omogoča povezovanje IPv4 naprav v ethernet-omrežju. Z ARP-poizvedbami IPv4-naprava izve MAC-naslov druge naprave v istem omrežju.



Slika 4: IP-sistem uporabi mehanizem ARP, s katerim izve MAC-naslov naprave v ethernet-omrežju, s katero bo komuniciral po protokolu IPv4.

Vaja 2: Preglej ARP tabelo na svojem računalniku. S pomočjo **tcpdump** preveri, kaj se zgodi ob ping-u drugega sistema v istem ethernet-omrežju.

Primer:

Ping stikala 3:

```
# ping 153.5.188.3

PING 153.5.188.3 (153.5.188.3) 56(84) bytes of data.
64 bytes from 153.5.188.3: icmp_seq=1 ttl=255 time=1.50 ms
64 bytes from 153.5.188.3: icmp_seq=2 ttl=255 time=1.49 ms
64 bytes from 153.5.188.3: icmp_seq=3 ttl=255 time=1.47 ms

# arp -a
? (153.5.188.3) at 00:0F:F7:5C:0B:40 [ether] on eth2

# tcpdump -i eth2 -vv -nn
15:50:13.210365 arp who-has 153.5.188.3 tell 153.5.188.55
15:50:13.211597 arp reply 153.5.188.3 is-at 00:0f:f7:5c:0b:40
15:50:13.211610 IP (tos 0x0, ttl 64, id 0, offset 0, flags [DF], proto 1, length: 84) 153.5.188.55 > 153.5.188.3: icmp 64: echo request seq 0
15:50:13.213123 arp who-has 153.5.188.55 tell 153.5.188.3
15:50:13.213152 arp reply 153.5.188.55 is-at 00:11:95:5c:ec:aa
15:50:14.209270 IP (tos 0x0, ttl 64, id 0, offset 0, flags [DF], proto 1, length: 84) 153.5.188.55 > 153.5.188.3: icmp 64: echo request seq 1
15:50:14.210739 IP (tos 0x0, ttl 255, id 0, offset 0, flags [DF], proto 1, length: 84) 153.5.188.3 > 153.5.188.55: icmp 64: echo reply seq 1
15:50:15.210132 IP (tos 0x0, ttl 64, id 0, offset 0, flags [DF], proto 1, length: 84) 153.5.188.55 > 153.5.188.3: icmp 64: echo request seq 2
15:50:15.211595 IP (tos 0x0, ttl 255, id 0, offset 0, flags [DF], proto 1, length: 84) 153.5.188.3 > 153.5.188.55: icmp 64: echo reply seq 2
15:50:16.211547 IP (tos 0x0, ttl 64, id 0, offset 0, flags [DF], proto 1, length: 84) 153.5.188.55 > 153.5.188.3: icmp 64: echo request seq 3
15:50:16.212992 IP (tos 0x0, ttl 255, id 0, offset 0, flags [DF], proto 1, length: 84) 153.5.188.3 > 153.5.188.55: icmp 64: echo reply seq 3
...
```

IPv4 in IPv6

IPv4 in IPv6 naslov, tipi IPv6 naslovov, IP-podomrežja.

IPv4 in IPv6 header. ICMP in ICMPv6.

IPv4 naslov je dolg 32 bitov. Zapišemo ga s štirimi decimalnimi števili (po 8 bitov skupaj), ločenimi s pikami. Primer: **153.5.188.5**. IPv6 naslov je dolg 128 bitov. Zapišemo ga z največ 8 šestnajstimi števili (po 16 bitov skupaj), ločenimi z dvopičji. Primer: **2001:1470:fac0::5**. Vodilne ničle v 16-bitnih besedah lahko opustimo – namesto **0db8** zapišemo **db8**. Prav tako lahko opustimo zaporedne ničelne 16-bitne besede v zapisu IPv6 naslova in jih nadomestimo z dvema dvopičjema »:«. V naslovu **2001:1470:fac0::5**, na primer, smo z dvema dvopičjema nadomestili vse zaporedne ničle med »fac0« in končno 5. Sicer bi ta naslov morali zapisati v celoti kot **2001:1470:fac0:0000:0000:0000:0005**.

Primer – naslednji zapisi predstavljajo isti IPv6 naslov:

```
2001:0db8:0000:0000:0001:0000:0000:0001
2001:0db8:0:0:1:0:0:1
2001:db8:0:0:1:0:0:1
2001:db8::1:0:0:1
2001:db8::0:1:0:0:1
2001:0db8::1:0:0:1
2001:db8:0:0:1::1
2001:db8:0000:0:1::1
2001:DB8:0:0:1::1
2001:dB8:0:0:1::1
```

IPv6-naslovi so lahko (navajamo le najpomembnejše tipe):

- globalni (»global unicast«)
- lokalni znotraj omrežja (»link-local unicast«)
- multicast (»all local«, »solicited-node«)

Globalne naslove prepoznamo, ker imajo 2 ali 3 na začetku naslova (trenutno se uporabljajo le globalni naslovi, ki so del IPv6-omrežja 2000::/3, torej od 2000:: do 3fff::). To so naslovi, ki se uporabljajo za komunikacijo v internetu. Lokalni naslovi se začnejo z **fe80**. Lokalni naslovi so uporabni le v skupnem omrežju. Vsak IPv6-vmesnik, ki je povezan v ethernet-omrežje, ima svoj unikatni lokalni IPv6 naslov, ki je zgrajen iz fe80::/10 in ethernet naslova v zapisu EUI-64 – npr.:

```
# ifconfig eth1
eth1      Link encap:Ethernet  HWaddr 00:12:F0:4B:B9:37
          inet6 addr:  2001:1470:8000:566:212:f0ff:fe4b:b937/64 Scope:Global
          inet6 addr:  fe80::212:f0ff:fe4b:b937/64 Scope:Link
```

Multicast naslovi se začnejo z **ff**, npr. naslov ff02::2 je naslov vseh usmerjevalnikov v lokalnem omrežju (»all routers«).

IP-naslovi so del IP-podomrežij. Vsi naslovi, ki imajo enako zaporedje začetnih n bitov, so del istega IP-podomrežja z »dolžino prefiksa« n . Dolžino prefiksa zapišemo za poševnico - / n . Celoten IP-naslovni prostor zapišemo z dolžino prefiksa $n = 0$ – 0.0.0.0/0. To velja tako za IPv4 kot za IPv6.

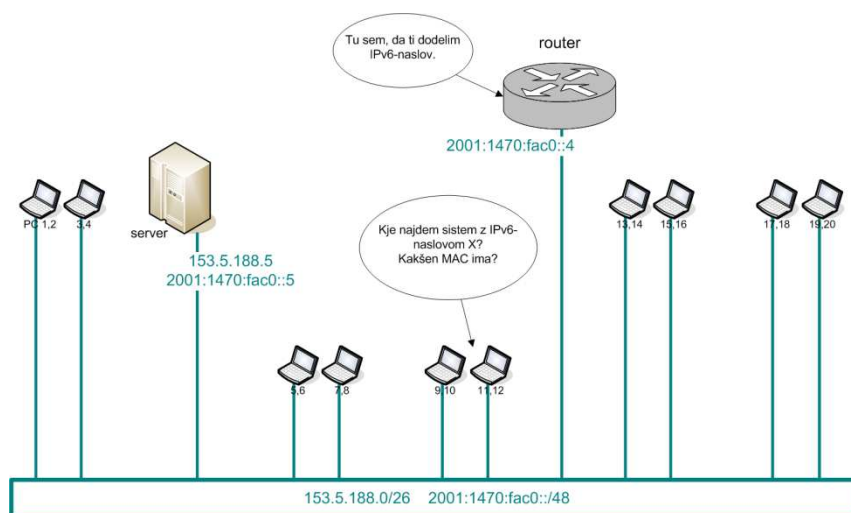
Vaja 3: Z X označi omrežja, v katerih je IP-naslov iz prvega stolpca na levi:

IP-naslov/omrežje	0.0.0.0/0	153.5.184.0/22	153.5.188.160/28	::/0	2001:1470:fac0::/45	2001:1470:fac3::/48
primer: 153.5.185.88	X	X	-	-	-	-
153.5.188.5						
153.5.188.175						
0.0.0.0						
2001:1470:fac3:1::1						
2001:1470:fac0::5						
2001:1470:fac8::8						
::						

Ethernet in IPv6

IPv6 ND (»neighbour discovery«), IPv6 samodejna konfiguracija (»stateless autoconfig«).

Na računalnikih bomo omogočili protokol IPv6. IPv6 naslov nam bo dodelil usmerjevalnik. V IPv6 omrežjih se namesto mehanizma ARP uporablja protokol IPv6 ND – »neighbour discovery«. IPv6 sistemi si izmenjujejo posebna ICMPv6 sporočila, s katerimi ugotavljajo IPv6-naslove in MAC naslove sistemov v istem ethernet-omrežju (»neighbour solicitation«). Z ICMPv6 sporočili protokola ND se sporoča tudi podatke za privzeti prehod (RA ali »router advertisement«). ND skrbi tudi za preprečevanje podvajanja IPv6-naslovov (DAD ali »duplicate addresss detection«).



Slika 5: IP-sistem uporabi mehanizem ND, s katerim izve MAC-naslov naprave v ethernet-omrežju, s katero bo komuniciral po protokolu IPv6.

Vaja 4: Vkllop usmerjevalnika. Ali je usmerjevalnik dosegljiv preko IPv4? Na računalnikih omogočimo IPv6 in samodejno konfiguracijo. Ali imamo IPv6-naslov na vmesniku računalnika? Kako smo dobili ta naslov? Uporabi **tcpdump** in pogledj, kako poteka samodejna konfiguracija IPv6-naslova. Preveri, ali je usmerjevalnik dosegljiv preko IPv6?

Primer: Usmerjevalnik je računalniku dodelil IPv6-naslov 2001:1470:fac0:0:211:95ff:fe5c:ecaa. Ping strežnika na naslovu 2001:1470:fac0::5.

IPv6 »router advertisement« - ciljni naslov je »multicast - all nodes on the link«:

```
# tcpdump -i eth2 -vv -nn
08:47:24.421494 fe80::20e:38ff:fe5c:ecaa > ff02::1: icmp6: router advertisement(chlim=64, pref=medium, router_ltime=1800, reachable_time=0,
retrans_time=0)(src lladdr: 00:0e:38:f4:65:c0)(mtu: mtu=1500)[ndp opt] [class 0xe0] (len 64, hlim 255)
08:47:24.534160 :: > ff02::1:ff5c:ecaa: [icmp6 sum ok] icmp6: neighbor sol: who has 2001:1470:fac0:0:211:95ff:fe5c:ecaa (len 24, hlim 255)

# ifconfig eth2
eth2      Link encap:Ethernet  HWaddr 00:11:95:5C:EC:AA
          inet6 addr:  2001:1470:fac0:0:211:95ff:fe5c:ecaa/64  Scope:Global
          inet6 addr:  fe80::211:95ff:fe5c:ecaa/64  Scope:Link
```

Ping strežnika in IPv6 »neighbour solicitation« - uporabi se »multicast – solicited-node«:

```
# ping6 2001:1470:fac0::5
PING 2001:1470:fac0::5(2001:1470:fac0::5) 56 data bytes
64 bytes from 2001:1470:fac0::5: icmp_seq=0 ttl=64 time=2.82 ms
64 bytes from 2001:1470:fac0::5: icmp_seq=1 ttl=64 time=1.14 ms
64 bytes from 2001:1470:fac0::5: icmp_seq=2 ttl=64 time=1.14 ms

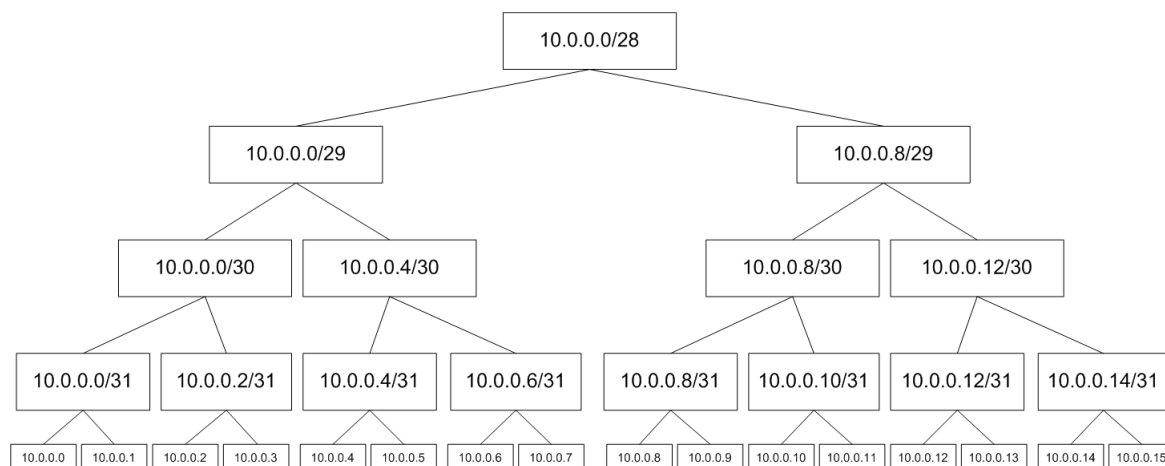
# tcpdump -i eth2 -vv -nn
08:48:48.261956 2001:1470:fac0:0:211:95ff:fe5c:ecaa > ff02::1:ff00:5: [icmp6 sum ok] icmp6: neighbor sol: who has 2001:1470:fac0::5(src lladdr:
00:11:95:5c:ec:aa) (len 32, hlim 255)
08:48:48.263079 2001:1470:fac0:0:211:95ff:fe5c:ecaa: [icmp6 sum ok] icmp6: neighbor adv: tgt is 2001:1470:fac0::5(SO)(tgt
lladdr: 00:13:20:80:c7:06) (len 32, hlim 255)
08:48:48.263100 2001:1470:fac0:0:211:95ff:fe5c:ecaa > 2001:1470:fac0::5: icmp6: echo request seq 0 (len 64, hlim 64)
08:48:48.264085 2001:1470:fac0::5 > 2001:1470:fac0:0:211:95ff:fe5c:ecaa: icmp6: echo reply seq 0 (len 64, hlim 64)
08:48:49.261848 2001:1470:fac0:0:211:95ff:fe5c:ecaa > 2001:1470:fac0::5: icmp6: echo request seq 1 (len 64, hlim 64)
08:48:49.262964 2001:1470:fac0::5 > 2001:1470:fac0:0:211:95ff:fe5c:ecaa: icmp6: echo reply seq 1 (len 64, hlim 64)
08:48:50.262712 2001:1470:fac0:0:211:95ff:fe5c:ecaa > 2001:1470:fac0::5: icmp6: echo request seq 2 (len 64, hlim 64)
08:48:50.263829 2001:1470:fac0::5 > 2001:1470:fac0:0:211:95ff:fe5c:ecaa: icmp6: echo reply seq 2 (len 64, hlim 64)
```

Primer konfiguracije usmerjevalnika:

```
interface Vlan51
description --- org.5/admin ---
ipv6 address 2001:1470:FAC5:1::1/64
ipv6 nd prefix 2001:1470:FAC5:1::/64
!
router#show ipv6 interface vlan 51
Vlan51 is up, line protocol is up
IPv6 is enabled, link-local address is FE80::20E:38FF:FEF4:65C2
Description: --- org.5/admin ---
Global unicast address(es):
  2001:1470:FAC5:1::1, subnet is 2001:1470:FAC5:1::/64
Joined group address(es):
  FF02::1          ← multicast all nodes
  FF02::2          ← multicast all routers
  FF02::1:FF00:1   ← multicast solicited-node za global unicast
  FF02::1:FFF4:65C2 ← multicast solicited-node za link-local
MTU is 1500 bytes
ICMP error messages limited to one every 100 milliseconds
ICMP redirects are enabled
ND DAD is enabled, number of DAD attempts: 1
ND reachable time is 30000 milliseconds
ND advertised reachable time is 0 milliseconds
ND advertised retransmit interval is 0 milliseconds
ND router advertisements are sent every 200 seconds
ND router advertisements live for 1800 seconds
Hosts use stateless autoconfig for addresses.
```

Delitev IP-omrežij (»IP subneting«)

IP-omrežje lahko delimo na več manjših podomrežij. Delitev predstavimo z drevesno strukturo:



Slika 6: Delitev IP-omrežja 10.0.0.0/28. V listih drevesa so vsi IPv4-naslovi, ki so v podomrežju 10.0.0.0/28. Določen IPv4-naslov se nahaja v vseh omrežjih, ki so na poti od ustreznega lista proti korenu drevesa. Npr., 10.0.0.11 je v omrežjih 10.0.0.10/31, 10.0.0.8/30, 10.0.0.8/29, 10.0.0.0/28 itd.

Mimogrede – višina drevesa na sliki je 4. V drevesu je (skupaj z $2^4 = 16$ IPv4-naslovi (omrežja /32)), $2^5 - 1 = 31$ IPv4-omrežij. Koliko je IPv4-naslovov in koliko je IPv4-omrežij v celotnem naslovnem prostoru IPv4 interneta 0.0.0.0/0?

Vaja 5: Predlagaj delitev IPv4-naslovnega prostora 153.5.188.0/24 na 5 organizacij s skupaj 10 lokalnimi omrežji in s skupnim strežniškim omrežjem. Strežniško omrežje naj bo dovolj veliko za priklop vsaj 50 računalnikov. Skiciraj delitev v drevesu, kjer je koren omrežje 153.5.188.0/24 (glej priloge). Dodatno: Skiciraj drevo celotnega naslovnega prostora IPv4 od korena 0.0.0.0/0 do vej z omrežji /4.

Primer uporabe Arnesovega programa »netcalc«:

```
# netcalc 153.5.188.96 - 255
```

```
153.5.188.96/27      (9905bc60, 10011001.00000101.10111100.01100000)
```

```
-----
network mask for /27: 255.255.255.224      (ffffffe0)
Cisco ACL mask:      0.0.0.31      (0000001f)
network address:      153.5.188.96      (9905bc60)
broadcast address:     153.5.188.127      (9905bc7f)
number of hosts:       32      (including net and bcast address)
```

```
153.5.188.128/25     (9905bc80, 10011001.00000101.10111100.10000000)
```

```
-----
network mask for /25: 255.255.255.128      (ffffff80)
Cisco ACL mask:      0.0.0.127      (0000007f)
network address:      153.5.188.128      (9905bc80)
broadcast address:     153.5.188.255      (9905bcff)
number of hosts:       128      (including net and bcast address)
```

153.5.188.96 - 153.5.188.255 consists of 2 subnet(s) as follows:

153.5.188.96/27

153.5.188.128/25

Navidezna omrežja (802.1q VLAN)

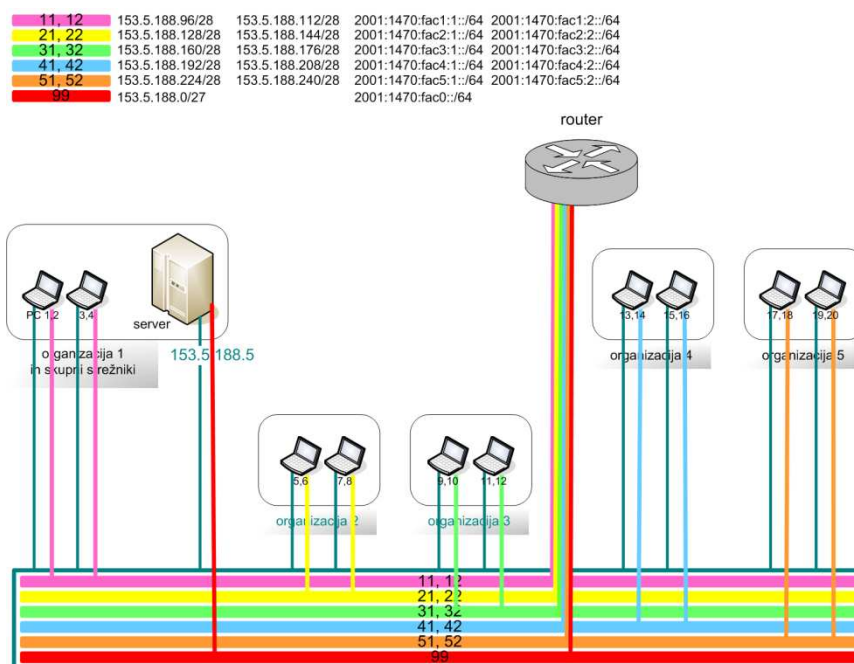
Razločevanje med ethernet-okvirji, ki so v različnih navideznih omrežjih (802.1q VLAN »tag«). »Trunk« in »access« vmesniki.

Tehnologija 802.1q omogoča ločevanje med ethernet-okvirji v istem ethernet-omrežju. Okvirji so označeni z 12-bitno »značko« - 802.1q »VLAN tag«. V delavnici bomo tej oznaki poenostavljeno rekli »barva«. Okvirji enake barve so v skupnem navideznem ethernet-omrežju – slika 7. Skupen ethernet »razpade« na več navidezno ločenih ethernet-omrežij, v katerih delujejo enaki mehanizmi kot v običajnem ethernetu – učenje MAC-naslovov, ARP, IPv6 ND ipd.

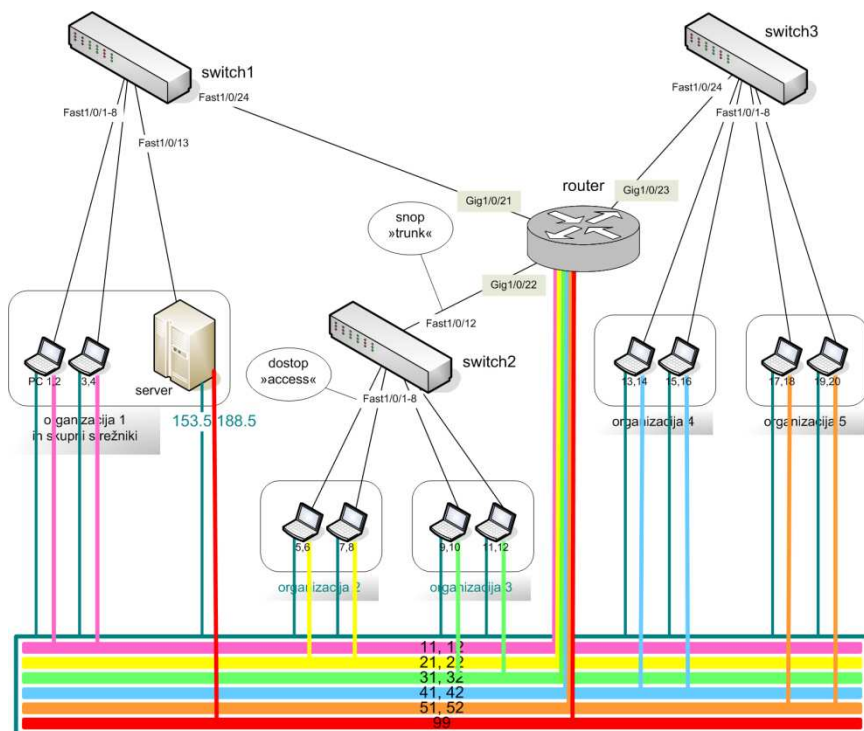
Stikala prepoznajo barve okvirjev in okvirje določene barve posredujejo le na tiste vmesnike, ki so nastavljeni za posredovanje okvirjev te barve. Vmesniki, preko katerih se posredujejo barvni okvirji, so v načinu snopa (»trunk«). Na vmesniku tipa »trunk« lahko nastavimo dovoljene barve.

Običajno računalniki v ethernet-omrežju ne prepoznajo barv – ti sprejemajo in oddajajo povsem običajne ethernet-okvirje – brez barve. Vmesniki stikal, kamor so priključeni računalniki, so v dostopnem način (»access«). Stikala pobarvajo okvir, ko ga prejmejo na »access« vmesniku in sicer s tisto barvo, ki je določena za ta vmesnik. Stikala razbarvajo okvirje, ko jih posredujejo na »access« vmesnike proti računalnikom.

Stikala poznajo tudi poseben VLAN, v katerem so ethernet-okvirji brez barvnih oznak. Temu VLAN-u pravimo »untagged native« VLAN. V delavnici je to VLAN z oznako 1. Uporabljali smo ga vse do sedaj. V eni od vaj v nadaljevanju bomo ta VLAN ukinili.



Slika 7: 802.1q VLAN-i v delavnici s pripadajočimi IP-podomrežji.



Slika 8: Razvod VLAN-ov preko stikal. Vmesniki med stikali in usmerjevalniku so v načinu »trunk«, vmesniki, kamor so povezani računalniki, pa so v dostopnem načinu (»access«).

Vaja 6 (**zahtevno!**): Prekonfiguracija enotnega omrežja z »native« VLAN-om v omrežje z 11 VLAN-i.

Prekonfiguracije se bomo lotili v več korakih. Vsaka organizacija poskrbi za svoje VLAN-e. Udeleženci se dogovorijo, kdo bo konfiguriral opremo – v izogib težavam naj določen vmesnik konfigurira en sam udeleženec.

1. Povežimo se na usmerjevalnik – uporabimo management IPv4-naslov. Vmesnik proti stikalu bomo nastavili v način »trunk«. V snopu bomo sprva omogočili vse VLAN-e. Definiramo VLAN:

```
vlan 51
 name org5admin
!
```

Vmesnik postavimo v »trunk«. Ali bomo pri tem izgubili povezavo do usmerjevalnika? Da. Vmesnik na eni strani je »trunk«, na drugi (na stikalu) pa ne.

```
interface GigabitEthernet1/0/22
 switchport trunk encapsulation dot1q
 switchport mode trunk
```

2. Povežimo se na stikalo in tam nastavimo vmesnik proti usmerjevalniku. Na stikalu je vmesnik v stanju BKN (broken):

```
switch2#sh spanning-tree vlan 1
Interface      Role Sts Cost      Prio.Nbr Type
-----
Fa0/9          Desg FWD 19        128.9    P2p
Fa0/12         Desg BKN*19 128.12    P2p *TYPE_Inc
```

Popravimo to in nastavimo vmesnik kot »trunk«:

```
interface FastEthernet0/12
 description --- router, Gig1/0/22 ---
 switchport mode trunk
!
```

3. Sedaj se bomo lahko ponovno povezali na usmerjevalnik. Na usmerjevalniku za vsak »naš« VLAN nastavimo vmesnik z ustreznim IPv4-naslovom. Ta vmesnik bo naš »gateway«. V snopu sedaj omejimo VLAN-e – dovolimo le tiste, ki jih bomo uporabljali v organizaciji in »untagged native« VLAN 1, ki ga – ne pozabimo - še vedno uporabljamo za dostop do opreme:

```
interface Vlan51
 description --- org.5/admin ---
 ip address 153.5.188.225 255.255.255.240
!
interface GigabitEthernet1/0/22
 description --- switch2, Fast0/12 ---
```

```

switchport trunk encapsulation dot1q
switchport trunk allowed vlan 1,51,52
!

```

... in podobno na stikalu:

```

interface FastEthernet0/12
switchport trunk allowed vlan 1,51,52
!

```

4. Nastavimo se "access" vmesnik, kamor je priključen naš prenosnik:

```

interface FastEthernet0/9
switchport access vlan 51
!

```

Pri tem bomo ponovno izgubili povezavo do usmerjevalnika. Na prenosniku moramo zamenjati IPv4-naslov in s tem lahko dostopamo do usmerjevalnika neposredno iz svojega VLAN-a:

```

# ifconfig eth2 153.5.188.226 netmask 255.255.255.240

# ping 153.5.188.225
PING 153.5.188.225 (153.5.188.225) 56(84) bytes of data.
64 bytes from 153.5.188.225: icmp_seq=0 ttl=255 time=0.535 ms
64 bytes from 153.5.188.225: icmp_seq=1 ttl=255 time=0.531 ms
64 bytes from 153.5.188.225: icmp_seq=2 ttl=255 time=0.520 ms
...

```

5. Nastavimo še IPv6:

```

interface Vlan51
description --- org.5/admin ---
ip address 153.5.188.225 255.255.255.240
no ip redirects
ipv6 address 2001:1470:FAC5:1::1/64
ipv6 nd prefix 2001:1470:FAC5:1::/64
no ipv6 redirects
!

```

Preverimo, ali ima naš računalnik pravi IPv6-naslov in »default gateway«:

```

# ifconfig eth2
eth2      Link encap:Ethernet  HWaddr 00:11:95:5C:EC:AA
          inet addr:153.5.188.226  Bcast:153.5.188.239  Mask:255.255.255.240
          inet6 addr: 2001:1470:fac5:1:211:95ff:fe5c:ecaa/64  Scope:Global

# route -n -A inet6
Kernel IPv6 routing table

```

Destination	Next Hop	Flags	Metric	Ref	Use	Iface
2001:1470:fac5:1::/64	::	UA	256	0	0	eth2
::/0	fe80::20e:38ff:fef4:65c2	UGDA	1024	1	0	eth2

```

# ip -6 addr
# ip -6 route

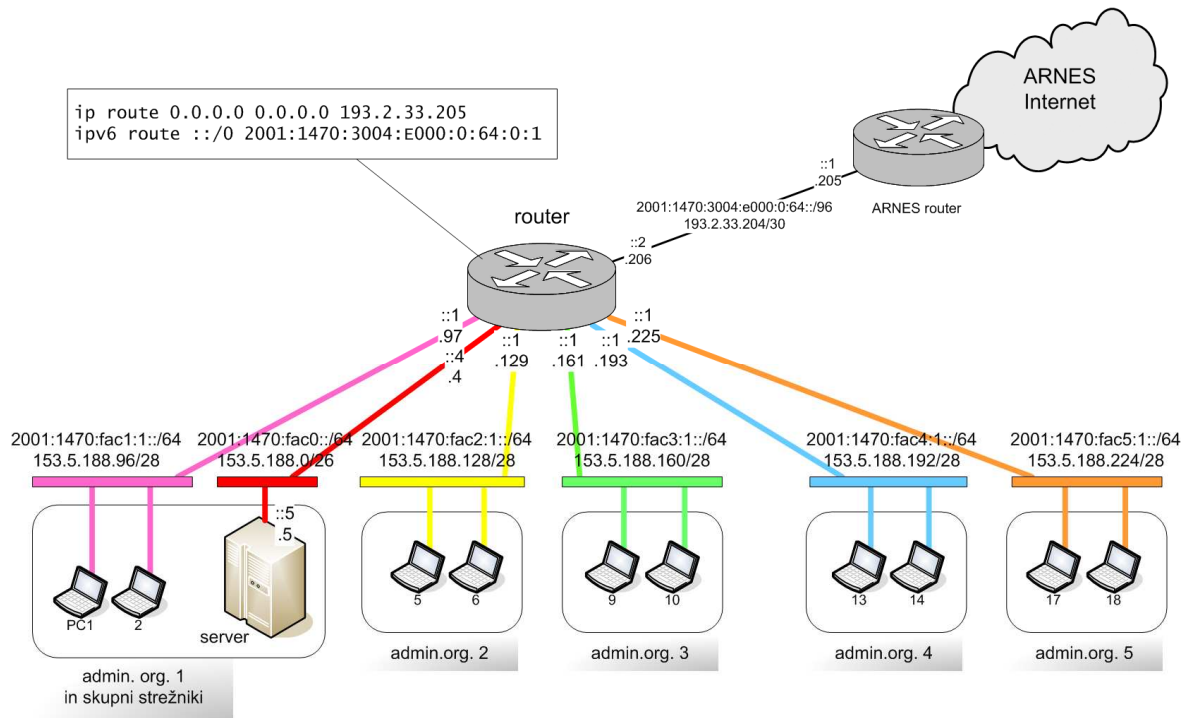
```

Statično usmerjanje IP-prometa

Priključena (»connected«) omrežja in statično usmerjanje.

Usmerjevalniki posredujejo IP-pakete glede na informacije, ki jih imajo v posebnih »routing« tabelah. Usmerjevalnik pregleda ciljni IP-naslov, nato preveri »routing« tabelo in ugotovi, na kateri vmesnik mora posredovati paket, da bo le-ta lahko posredovan do ciljnega IP-naslova. Če tega podatka nima, potem za posredovanje paketa uporabi poseben zapis iz routing tabele, kjer je zabeleženo preko katerega vmesnika je dosegljivo celotno internetno omrežje – vse, za kar v routing tabeli ni bolj natančnega - specifičnega - zapisa. Temu zapisu pravimo »default route« – za IPv4 je to zapis za omrežje 0.0.0.0/0, za IPv6 pa ::/0.

Routing tabelo v usmerjevalniku lahko zapišemo ročno – statično, lahko pa za te vpise skrbijo posebni – dinamični – routing protokoli. V delavnici imamo en sam usmerjevalnik s statično routing tabelo. V njej so zapisani podatki o omrežjih, ki so priključena neposredno na usmerjevalni (»connected subnets«) in »default route« proti omrežju ARNES.



Slika 9: Statično usmerjanje IP-prometa proti omrežju ARNES/internetu.

Vaja 7: Preglej usmerjevalno tabelo na usmerjevalniku. Preveri »default route«. Izvedi »traceroute 153.5.188.64«. Kaj se zgodi in zakaj? Dodatno: Kaj izpiše ukaz »show ipv6 route ::« in kaj »show ipv6 route ::/0«? Od kod razlika?

Primer:

```
router#show ip route
Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route
```

Gateway of last resort is 193.2.33.205 to network 0.0.0.0

```
153.5.0.0/16 is variably subnetted, 2 subnets, 2 masks
C      153.5.188.0/26 is directly connected, Vlan1
C      153.5.188.224/28 is directly connected, Vlan51
193.2.33.0/30 is subnetted, 1 subnets
C      193.2.33.204 is directly connected, GigabitEthernet1/0/24
S*    0.0.0.0/0 [1/0] via 193.2.33.205
```

```
router#show ipv6 route
IPv6 Routing Table - 10 entries
Codes: C - Connected, L - Local, S - Static, U - Per-user Static route
       R - RIP
       O - OSPF Intra, OI - OSPF Inter, OE1 - OSPF ext 1, OE2 - OSPF ext 2
       ON1 - OSPF NSSA ext 1, ON2 - OSPF NSSA ext 2
```

```

S   ::/0 [1/0]
    via 2001:1470:3004:E000:0:64:0:1
C   2001:1470:3004:E000:0:64::/96 [0/0]
    via ::, GigabitEthernet1/0/24
L   2001:1470:3004:E000:0:64:0:2/128 [0/0]
    via ::, GigabitEthernet1/0/24
C   2001:1470:FAC0::/64 [0/0]
    via ::, Vlan1
L   2001:1470:FAC0::4/128 [0/0]
    via ::, Vlan1
C   2001:1470:FAC5:1::/64 [0/0]
    via ::, Vlan51
L   2001:1470:FAC5:1::1/128 [0/0]
    via ::, Vlan51
L   FF00::/8 [0/0]
    via ::, Null0

```

Statično usmerjanje IPv6-prometa.

OPOMBA: Pri statičnem usmerjanju IPv6-prometa nekateri priporočajo uporabo link-local naslovov (vzrok za ta predlog vam bo raje zamolčal ☺). V praksi v omrežju ARNES tega ne počnemo in uporabljamo globalne naslove. Tako je pregledneje in manj možnosti za napako.

Primer: Namesto »`ipv6 route ::/0 2001:1470:3004:E000:0:64:0:1`« bi lahko zapisali

```
ipv6 route ::/0 Gi1/0/24 FE80::222:56FF:FEBA:21BF
```

FE80::222:56FF:FEBA:21BF je namreč link-local naslov Arnesovega usmerjevalnika na SIRIKT.

```

router#sh ipv6 neighbors
IPv6 Address                               Age Link-layer Addr State Interface
2001:1470:3004:E000:0:64:0:1               14 0022.56ba.21bf STALE Gi1/0/24
FE80::222:56FF:FEBA:21BF                   14 0022.56ba.21bf STALE Gi1/0/24

```

Nadzorno podomrežje («management VLAN»)

Uporaba datotek s konfiguracijami. TFTP.

»Untagged native« VLAN 1 bomo ukinili in nadomestili z VLAN-om 99 za upravljanje in nadzor naprav. V tem VLAN-u bo zaradi poenostavitve (izjemoma!) tudi strežnik 153.5.188.5/2001:1470:fac0::5. Ker VLAN 1 uporabljamo za terminalski («telnet») dostop do naprav, bo z ukinitvijo tega VLAN-a prekinjen dostop do opreme. Pomagali si bomo z naslednjo metodo:

- Pripravili bomo ukaze za prekonfiguracijo stikala. Ukaz bomo shranili v datoteko na TFTP-strežniku.
- Datoteko z ukazi bomo prenesli na stikalo.
- Na stikalu bomo izvedli ukaze iz datoteke.

Če bi ukaze za prekonfiguracijo izvajali »ročno«, bi se naša TCP/IP povezava s stikalom prekinila in do stikala ne bi več mogli dostopati. Uporabiti bi morali dostop preko konzolnega priključka.

S prekonfiguracijo usmerjevalnika ne bo tovrstnih težav, saj ima usmerjevalnik več IP-vmesnikov («gateway«-ev), preko katerih lahko dostopamo do njega in tako lahko brez prekinitve spremenimo nastavitve management vmesnika.

Vaja 8 (zahtevno!): Skupen »native« VLAN 1 nadomesti z posebnim VLAN-om za upravljanje in nadzor.

1. Začnimo tako, da v vse »trunk«-e poleg VLAN-a 1 dodamo še nov management VLAN 99.

Primer:

```

[router]
interface GigabitEthernet1/0/21
description --- switch1, Fast1/0/24 ---
switchport trunk encapsulation dot1q
switchport mode trunk
switchport trunk allowed vlan 1,11,12,21,22,99

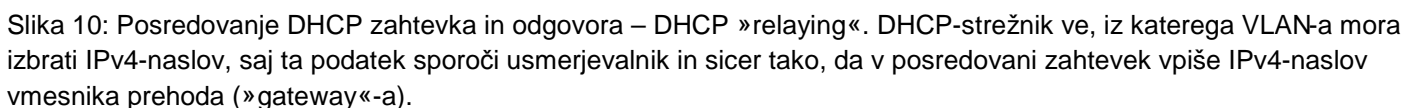
[switch1]
interface FastEthernet1/0/24
description --- router, Gig1/0/21 ---
switchport trunk allowed vlan 1,11,12,21,22,99

```

```
vlan 99
 name management
!
interface FastEthernet1/0/24
 switchport trunk allowed vlan add 99
 switchport trunk allowed vlan remove 1
!
interface Vlan1
 shutdown
no interface Vlan1
!
interface Vlan99
 no shutdown
 description --- management ---
 ip address 153.5.188.1 255.255.255.192
!
exit
vlan dot1q tag native
end
```

3. Na usmerjevalniku ukinemo VLAN 1 in nastavimo VLAN 99. Do stikal in skupnega strežnika lahko sedaj dostopamo preko usmerjevalnika.

V delavnici se strežnik ne nahaja v istem omrežju kot računalniki, zato bomo usmerjevalnik nastavili tako, da bo posredoval DHCP-zahteve in odgovore med računalniki in strežnikom – »DHCP relaying«. Tovrstno posredovanje prikazuje spodnja slika:



Vaja 9: Konfiguracija DHCP-strežnika. Na usmerjevalniku nastavi posredovanje DHCP zahtevkov. S »tcpdump« preveri, kako to poteka.

Primer:

PC (MAC-naslov 0011:955C:ECAA):

```
09:05:34.004114 IP (tos 0x10, ttl 16, id 0, offset 0, flags [none], proto 17, length: 328) 0.0.0.0.68 >
255.255.255.255.67: BOOTP/DHCP, Request from 00:11:95:5c:ec:aa, length: 300, xid:0xbb9e9021, flags: [none]
Client Ethernet Address: 00:11:95:5c:ec:aa [|bootp]
```

server (komunikacija z relay-em na 153.5.188.5, UDP port 67):

```
09:05:34.003476 IP (tos 0x0, ttl 255, id 10, offset 0, flags [none], proto: UDP (17), length: 328)
153.5.188.225.67 > 153.5.188.5.67: BOOTP/DHCP, Request from 00:11:95:5c:ec:aa, length: 300, hops:1,
xid:0xbb9e9021, flags: [none]
Gateway IP: 153.5.188.225
Client Ethernet Address: 00:11:95:5c:ec:aa [|bootp]
09:05:34.005801 IP (tos 0x0, ttl 64, id 0, offset 0, flags [DF], proto: UDP (17), length: 356)
153.5.188.5.67 > 153.5.188.225.67: BOOTP/DHCP, Reply, length: 328, hops:1, xid:0xbb9e9021, flags: [none]
Your IP: 153.5.188.238
Gateway IP: 153.5.188.225
Client Ethernet Address: 00:11:95:5c:ec:aa
sname "dhcp" [|bootp]
```

PC (dobi IP-naslov 153.5.188.238):

```
09:05:34.012226 IP (tos 0x0, ttl 255, id 11, offset 0, flags [none], proto 17, length: 356) 153.5.188.225.67
> 153.5.188.238.68: BOOTP/DHCP, Reply, length: 328, hops:1, xid:0xbb9e9021, flags: [none]
Your IP: 153.5.188.238
Gateway IP: 153.5.188.225
Client Ethernet Address: 00:11:95:5c:ec:aa
sname "dhcp" [|bootp]
```

Primer konfiguracije strežnika DHCP /etc/dhcpd.conf:

```
server-name dhcp;
ddns-update-style none;
ignore client-updates;
allow unknown-clients;
get-lease-hostnames true;
ping-check true;
option nis-domain          "delavnica.arnes.si";
option domain-name        "delavnica.arnes.si";
option domain-name-servers 153.5.188.5, 193.2.1.66;
option ntp-servers         153.5.188.4, 193.2.1.72;
option netbios-node-type   2;
max-lease-time             14400;
default-lease-time         3600;
one-lease-per-client       true;
authoritative;

subnet 153.5.188.0 netmask 255.255.255.192 {
}

subnet 153.5.188.224 netmask 255.255.255.240 {
    option routers          153.5.188.225;
    option subnet-mask      255.255.255.240;
    pool {
        range 153.5.188.227 153.5.188.238;
    }
}
```

Dodatne teme za zahtevnejše udeležence

Zmogljivost

iperf, <http://ndt.arnes.si/>

S programom »iperf« izmerimo prepustnost omrežja za prenos podatkov po protokolu TCP. iperf je nameščen na strežniku v delavnici. Namestili ga bomo tudi na računalnike udeležencev. V omrežju ARNES se nahaja tudi testni iperf -strežnik – *iperf-test.arnes.si*. Tega bomo uporabili za test prepustnosti iz omrežja delavnice proti omrežju ARNES/internetu.

Vaja 10: Na strežniku poženi iperf – udeleženec z uporabniškim imenom »u x« naj uporabi TCP vrata 5000+x, npr.:

```
[root@server ~]# iperf -s -p 5011
-----
Server listening on TCP port 5011
TCP window size: 85.3 KByte (default)
-----
```

Izmeri prepustnost za TCP promet s svojega računalnika proti strežniku v delavnici.

Dodatno: Izmeri še prepustno v obratni smeri, tako da strežnik iperf poženeš na svojem računalniku, na strežniku v delavnici pa uporabiš odjemalca »iperf -c«.

Primer:

Meritev prepustnosti proti strežniku v delavnici:

```
$ /opt/misc/bin/iperf -c 153.5.188.5 -p 5011
-----
Client connecting to 153.5.188.5, TCP port 5011
TCP window size: 640 KByte (default)
-----
[ 3] local 193.2.1.240 port 32954 connected with 153.5.188.5 port 5011
[ 3] 0.0-10.0 sec 111 MBytes 93.1 Mbits/sec
```

Uporaba Arnesovega strežnika iperf z IPv6:

```
[root@server ~]# iperf -V -c iperf-test.arnes.si -p 5555 -i 5 -t 15
-----
Client connecting to iperf-test.arnes.si, TCP port 5555
TCP window size: 16.0 KByte (default)
-----
[ 3] local 2001:1470:fac0::5 port 48580 connected with 2001:1470:8000:60a:0:600d:4:a11 port 5555
[ ID] Interval      Transfer      Bandwidth
[ 3] 0.0- 5.0 sec  50.1 MBytes  84.1 Mbits/sec
[ ID] Interval      Transfer      Bandwidth
[ 3] 5.0-10.0 sec  50.9 MBytes  85.3 Mbits/sec
[ ID] Interval      Transfer      Bandwidth
[ 3] 10.0-15.0 sec  50.1 MBytes  84.1 Mbits/sec
[ ID] Interval      Transfer      Bandwidth
[ 3] 0.0-15.0 sec   151 MBytes  84.4 Mbits/sec
```


DNS

A, AAAA in PTR zapisi. Domena delavnica.arnes.si. Strežnik BIND.

DNS skrbi za preslikavo med imeni IP-sistemov in njihovimi IP-naslovi. Zapisi, s katerimi imenom določimo IPv4-naslove, se imenujejo A-zapisi. Preslikave iz imen v IPv6-naslove pa so v AAAA-zapisih. Zapisi, ki IP-naslovom (za IPv4 in IPv6) priredijo imena, se imenujejo PTR-zapisi.

Na strežniku 153.5.188.5 je nameščen DNS strežnik BIND. Konfiguracijske datoteke se nahajajo v `/opt/named-chroot/var/named/data/`.

Vaja 11: V ustrezno konfiguracijsko datoteko vpiši ime in IP-naslov svoje računalnika, restartaj DNS strežnik in preveri, ali preslikava med imeni in IP-naslovi pravilno deluje.

Primer:

IPv4 PTR zapisi v `188.5.153.in-addr.arpa-prim`:

```
#####
; /opt/named/188.5.153.in-addr.arpa-prim
#####
;### Default TTL #####
$TTL 86400
#####
@ IN SOA server.delavnica.arnes.si. hostmaster.arnes.si. (
    2009032409 ; SERIAL_NUMBER
    28800 ; refresh
    7200 ; retry
    1814400 ; expire 21d
    3600 ; TTL (1h)
)
; #####
; name servers for this domain
; #####
188.5.153.in-addr.arpa. IN NS server.delavnica.arnes.si.
; #####
1 IN PTR switch1.delavnica.arnes.si.
2 IN PTR switch2.delavnica.arnes.si.
3 IN PTR switch3.delavnica.arnes.si.
4 IN PTR router.delavnica.arnes.si.
5 IN PTR server.delavnica.arnes.si.
;
; #####
97 IN PTR a.org1.delavnica.arnes.si.
113 IN PTR p.org1.delavnica.arnes.si.
129 IN PTR a.org2.delavnica.arnes.si.
145 IN PTR p.org2.delavnica.arnes.si.
161 IN PTR a.org3.delavnica.arnes.si.
177 IN PTR p.org3.delavnica.arnes.si.
193 IN PTR a.org4.delavnica.arnes.si.
209 IN PTR p.org4.delavnica.arnes.si.
225 IN PTR a.org5.delavnica.arnes.si.
241 IN PTR p.org5.delavnica.arnes.si.
```

IPv6 PTR zapisi v `0.c.a.f.0.7.4.1.1.0.0.2.ip6.arpa-prim`:

```
#####
; 0.c.a.f.0.7.4.1.1.0.0.2.ip6.arpa.
#####
;
@ 21600 IN SOA server.delavnica.arnes.si. hostmaster.arnes.si. (
    2006080906 ; SERIAL_NUMBER
    28800 ; refresh
    7200 ; retry
    3600000 ; expire 1000h
    21600 ; TTL
)
; #####
$TTL 86400
; #####
0.c.a.f.0.7.4.1.1.0.0.2.ip6.arpa. IN NS server.delavnica.arnes.si.
```

A in AAAA zapisi v delavnica.arnes.si-prim:

A in AAAA zapisi v delavnica.arnes.si-prim:

Protokol STP («spanning tree«)

Kaj se zgodi v primeru zank v omrežju?

Kako stikala poskrbijo, da je pot ethernet-okvirjev točno določena in brez zank? Opisali bomo mehanizem, s katerim stikala gradijo drevo poti med stikali.

Stanja vmesnikov: LIStening, LeRNIing, FoRWarding – delujoče stanje, BLoCKing – povezava preko tega vmesnika je prekinjena. Kasneje bomo spoznali tudi stanje BroKeN.

Vaja 12: V omrežju naredimo zanko med stikali (glej sliko 3). Preglej stanje vmesnikov. Poišči vmesnik v stanju BLK - »blocking«.

Uporabi ukaz »show spanning-tree vlan 1«.

Zanimiv (animiran) prikaz delovanja STP:

http://www.cisco.com/image/gif/paws/10556/spanning_tree1.swf.

L2-backup

Uporabimo STP.

Stikala petih organizacij so poleg povezave z usmerjevalnikom povezana tudi med seboj (glej sliko 1). Te medsebojne povezave izkoristimo za rezervne povezave («backup») z omrežjem ARNES. STP poskrbi, da v omrežju ni zank. V primeru, da se neka povezava prekine, se promet samodejno preusmeri preko rezervnih povezav.

Vaja 13: Vzpostavi »backup« povezave in sicer preko naslednjih povezav:

Organizacija 1	switch1 – switch2 - router
Organizacija 2	switch1 – switch2 – router
Organizacija 3	switch2 – switch3 – router
Organizacija 4	switch1 – switch3 – router
Organizacija 5	switch1 – switch3 – router
Skupni strežniki	switch1 – switch2 – router switch1 – switch3 – router

Preveri delovanje tako, da prekineš glavno povezavo med stikalom in usmerjevalnikom.

Varnost

Filtri (Cisco ACL), nmap.

Na usmerjevalniku lahko filtriramo IP-promet s filtri ACL – Cisco »access lists«. ACL je urejen spisek pravil, s katerimi je nek promet dovoljen ali prepovedan. IP-pakete klasificiramo glede na:

- IP-naslov izvora prometa,
- IP-naslov cilja,
- protokol (poljuben IP-protokol, ICMP, TCP, UDP ipd.),
- dodatni podatki za nekatere protokole, npr. vrata za protokol TCP.

Filter deluje na vmesniku. Definiramo ga lahko za promet v obeh smereh, v smeri proti lokalnemu omrežju ali iz lokalnega omrežja proti internetu.

Primer filtra, ki dovoljuje ves promet lokalnega strežnika, ves ICMP-promet in promet običajnih TCP-storitev do odjemalcev v lokalnem omrežju:

```
ip access-list extended Primer
permit icmp any any
permit ip host 153.5.188.5 any
permit tcp any 153.5.188.0 0.0.0.255 established
deny ip any any log
!
ipv6 access-list Primer6
permit icmp any any
permit ipv6 host 2001:1470:FAC0::5 any
permit tcp any 2001:1470:FAC0::/64 established
remark --- local ---
permit ipv6 any FE80::/10
permit ipv6 any FF02::/16
deny ipv6 any any log
!
```

Z »nmap« ugotovimo, katera vrata so odprta na nekem IP-sistemu. Primer – odprta vrata na strežniku v delavnici:

```
# nmap 153.5.188.5

Starting Nmap 4.20 ( http://insecure.org ) at 2009-04-06 11:24 CEST
Interesting ports on 153.5.188.5:
Not shown: 1689 closed ports
PORT      STATE      SERVICE
22/tcp    open       ssh
25/tcp    filtered  smtp
53/tcp    open       domain
80/tcp    open       http
111/tcp   open       rpcbind
953/tcp   open       rndc
1720/tcp  open       H.323/Q.931
5011/tcp  open       telepathattack

Nmap finished: 1 IP address (1 host up) scanned in 1.566 seconds
```

Vaja 14: S filtri na usmerjevalniku zaščiti lokalno omrežje organizacije.

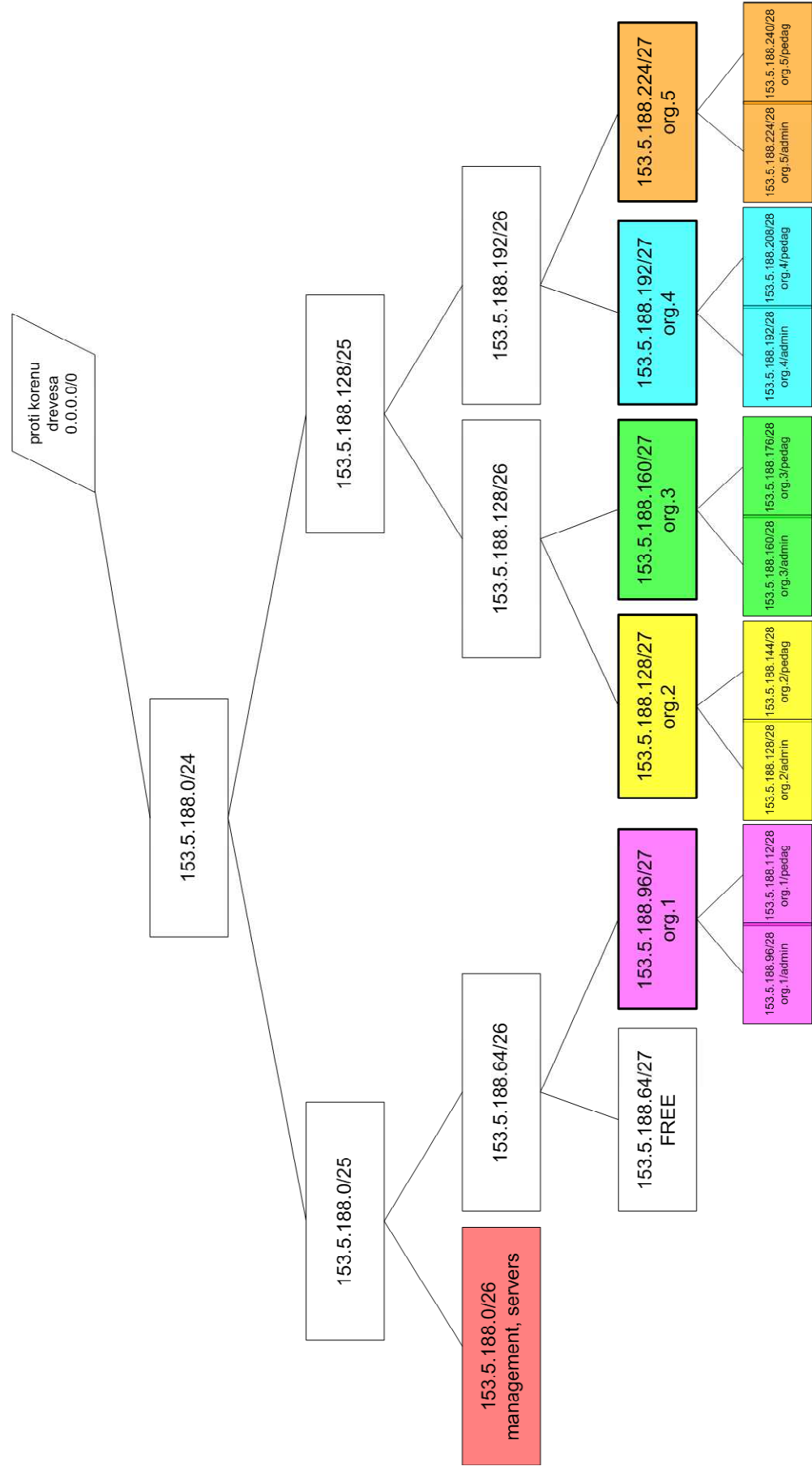
Priloge

Shema IP-omrežij

org.	omrežje	del.mesto	up.ime	VLAN	VLAN-ID	IP-podomrežje	IPv6-podomrežje	IP-naslov (vaja 1)
1	adm	1	u11	org1adm	11	153.5.188.96/28	2001:1470:fac1:1::/64	153.5.188.11
1	adm	2	u12	org1adm	11	153.5.188.96/28	2001:1470:fac1:1::/64	153.5.188.12
1	ped	3	u13	org1ped	12	153.5.188.112/28	2001:1470:fac1:2::/64	153.5.188.13
1	ped	4	u14	org1ped	12	153.5.188.112/28	2001:1470:fac1:2::/64	153.5.188.14
1	ped	5	u15	org1ped	12	153.5.188.112/28	2001:1470:fac1:2::/64	153.5.188.15
2	adm	6	u21	org2adm	21	153.5.188.128/28	2001:1470:fac2:1::/64	153.5.188.21
2	adm	7	u22	org2adm	21	153.5.188.128/28	2001:1470:fac2:1::/64	153.5.188.22
2	ped	8	u23	org2ped	22	153.5.188.144/28	2001:1470:fac2:2::/64	153.5.188.23
2	ped	9	u24	org2ped	22	153.5.188.144/28	2001:1470:fac2:2::/64	153.5.188.24
2	ped	10	u25	org2ped	22	153.5.188.144/28	2001:1470:fac2:2::/64	153.5.188.25
3	adm	11	u31	org3adm	31	153.5.188.160/28	2001:1470:fac3:1::/64	153.5.188.31
3	adm	12	u32	org3adm	31	153.5.188.160/28	2001:1470:fac3:1::/64	153.5.188.32
3	ped	13	u33	org3ped	32	153.5.188.176/28	2001:1470:fac3:2::/64	153.5.188.33
3	ped	14	u34	org3ped	32	153.5.188.176/28	2001:1470:fac3:2::/64	153.5.188.34
4	adm	15	u41	org4adm	41	153.5.188.192/28	2001:1470:fac4:1::/64	153.5.188.41
4	adm	16	u42	org4adm	41	153.5.188.192/28	2001:1470:fac4:1::/64	153.5.188.42
4	ped	17	u43	org4ped	42	153.5.188.208/28	2001:1470:fac4:2::/64	153.5.188.43
4	ped	18	u44	org4ped	42	153.5.188.208/28	2001:1470:fac4:2::/64	153.5.188.44
5	adm	19	u51	org5adm	51	153.5.188.224/28	2001:1470:fac5:1::/64	153.5.188.51
5	adm	20	u52	org5adm	51	153.5.188.224/28	2001:1470:fac5:1::/64	153.5.188.52
5	adm	21	u53	org5adm	51	153.5.188.224/28	2001:1470:fac5:1::/64	153.5.188.53
5	ped	22	u54	org5ped	52	153.5.188.240/28	2001:1470:fac5:2::/64	153.5.188.54
5	ped	23	u55	org5ped	52	153.5.188.240/28	2001:1470:fac5:2::/64	153.5.188.55
5	ped	24	u56	org5ped	52	153.5.188.240/28	2001:1470:fac5:2::/64	153.5.188.56
1	management LAN			management	99	153.5.188.0/26	2001:1470:fac0::/64	
1	switch1			management	99		-	153.5.188.1
1	switch2			management	99		-	153.5.188.2
1	switch3			management	99		-	153.5.188.3
1	router			management	99		2001:1470:fac0::4	153.5.188.4
1	server			management	99		2001:1470:fac0::5	153.5.188.5

Tabela 1: VLAN-i in IP-omrežja v delavnici.

IPv4-subneting v omrežju delavnice



Povezave omrežnih naprav v delavnici

router	Gig1/0/24	SIRIKT router/ARNES/internet	-
router	Gig1/0/21	switch1	Fast1/0/24
router	Gig1/0/22	switch2	Fast0/12
router	Gig1/0/23	switch3	Fast0/24
switch1	Fast1/0/22	switch2	Fast0/10
switch1	Fast1/0/23	switch3	Fast0/23
switch2	Fast0/11	switch3	Fast0/22
switch1	Fast1/0/1 – 12	PC-ji org.1 in org.2	
switch2	Fast0/1 – 8	PC-ji org.3	
switch3	Fast0/1 – 12	PC-ji org.4 in org.5	
strežnik	Eth0	switch1	Fast1/0/13

Tabela 2: Povezave opreme v delavnici.