Iskra

Iskra Sistemi, d.d.

Priporočilo članicam Univerze omrežje METULJ

Pripravili:
Roman Novak, sistemski inženir, Iskra Sistemi, d.d.
Gašper Cotman, projektni vodja trženja, Iskra Sistemi, d.d.
Andrej Krevl, asistent, UL FRI
Matjaž Pančur, asistent, UL FRI
Anton Jagodic, vodja službe za informatiko, UL

Ljubljana, julij 2007

1. Uvod

Dokument vsebuje priporočila za posodabljanje lokalnih omrežij članic Univerze v Ljubljani, načine priklopa na univerzitetno metro omrežje Metulj ter načine segmentiranja notranjih omrežij članic Univerze. Priporočila so narejena z namenom optimiziranja univerzitetnega omrežja v celoti, tako jedrnega dela kot tudi lokalnih omrežij članic. Dokument zajema optimizacijo omrežja tako z vidika zanesljivosti delovanja kot tudi večje zmogljivosti delovanja. Univerzitetno omrežje, zgrajeno po teh priporočilih, omogoča varno in zanesljivo delovanje z velikimi hitrostmi in je kot tako primerna podlaga za implementacije trenutno aktualnih aplikacij kot bodočih aplikacij npr. video na zahtevo, IP telefonija, server/client aplikacije na nivoju Univerze, IPv6 ipd.

2. Oris omrežja Metulj

Omrežje Univerze v Ljubljani je sestavljeno iz hrbteničnega omrežja, na katerega je priključenih 26 članic Univerze v Ljubljani. Hrbtenično omrežje tvorijo 10-gigabitna IP/MPLS usmerjevalna stikala v treh glavnih vozliščih. Nanje so priključena povezovalna vozlišča in vozlišča članic univerze. Članice dostopajo do hrbteničnega omrežja z različnimi tehnologijami, v odvisnosti od danih možnosti. Večina članic je v omrežje Metulj povezana z eno optično povezavo hitrosti 1 Gb/s.

Hrbtenico omrežja tvorijo tri vozlišča: Vozlišče EF, vozlišče FKKT in vozlišče FE/FRI. Med seboj so povezana s povezavami hitrosti 10 Gb/s (Shema 3). Na njih so priključena tako povezovalna vozlišča (vozlišča, preko katerih dostopa več članic/oddlekov), kot tudi uporabniška omrežja posameznih članic. V odvisnosti od potreb in v skladu z možnostmi so nekatere članice povezane na povezovalna ali hrbtenična vozlišča z večimi povezavami.

Hrbtenična vozlišča so preko treh ločenih 1 Gb/s povezav priključena na omrežje ARNES, ki skrbi za povezavo v Internet. Univerza uporablja širok javni IP naslovni prostor, dodeljen s strani ARNES-a.

Omrežje Metulj omogoča tudi izvedbo storitev MPLS VPN, kar pomeni, da se lahko katerikoli oddelek/enota posamezne fakultete poveže s katerimkoli drugim oddaljenim oddelkom/enoto druge ali iste fakultete preko MPLS VPN omrežja, ki zagotavlja varno in zanesljivo povezavo za potrebe komuniciranja oddelkov. Za vzpostavitev MPLS VPN povezave je potrebno kontaktirati Univerzo oz. upravljalca omrežja Metulj (helpdesk@uni-lj.si).

Neprestano se izvaja kontrola delovanja naprav omrežja Metulj, prav tako se izvajajo statistične obdelave posameznih parametrov omrežja, na podlagi katerih se vrši tudi optimizacija omrežja.

Metulj v osnovi povezuje zgradbe UL med seboj v smislu članica-Metulj-Arnes. Priporoča se, da je osnovna priklopna točka vsake članice stavba dekanata. Vse ostale zgradbe članice se ali preko lastnih linij ali pa vlan-ov povezujejo preko te

enotne vstopne točke v omrežje Metulj. Prav tako se priporoča, da je v primeru oddaljenih oddelkov usmerjanje za oddaljene oddelke rešeno na tej enotni točki povezave. Visoko razpoložljivost te povezave zagotavljamo z ustrezno vzdrževalno pogodbo. Trenutno ni potreb po redudančnih linijah članic (glede na statistiko izpadov).

3. Pravila uporabe omrežja Metulj

Omrežje Metulj je namenjeno zaposlenim in študentom Univerze v Ljubljani. Omrežje Metulj upravlja Informacijska služba Univerze v Ljubljani (IS UL).

Pravico pridobitve dostopa do omrežja Metulj imajo vse organizacije, ki so del Univerze v Ljubljani, njihovi zaposlenci, sodelavci in študentje, kot tudi morebitni zunanji partnerji za katere se predhodno odobri dostop do omrežja Metulj. Dostop do omrežja se sme omogočiti tudi morebitnem gostujočem kadru in tujim študentom, ki so vključeni v redno pedagoško dejavnost članice.

3.1. Nedopustna uporaba omrežja Metulj

1. Nepooblaščena pridobitev in uporaba dostopa do omrežja.
2. Oglaševanje po elektronski pošti in pošiljanje verižnih pisem.
3. Uporaba dostopa do omrežja za pridobitniške dejavnosti.
4. Namerno motenje in onemogočanje dela drugih uporabnikov omrežja.
5. Uničevanje in spreminjanje podatkov, ki so v lasti drugih uporabnikov.
6. Kršenje tajnosti ali objava podatkov, ki so v lasti drugih uporabnikov.
7. Objava in pošiljanje podatkov, ki kršijo avtorske pravice.
8. Ustvarjanje, pošiljanje ali objavljanje podatkov z žaljivo ali pornografsko vsebino.
9. Posredovanje lažnih ali zavajajočih osebnih podatkov servisom na omrežju, ki take podatke zahtevajo pri uporabi.
10. Uporaba servisov, ki niso namenjeni javni uporabi.
11. Uporaba programov ali postopkov, katerih namen ali posledica je krnenje integritete in stabilnega delovanja računalnika, računalniškega sistema ali omrežja.

IS UL si pridržuje pravico do ustreznih ukrepov na omrežju Metulj, če presodi, da so bila kršena pravila dopustne uporabe tega omrežja. Med ukrepe spada onemogočanje dostopa oz. odvzem pravice dostopa do omrežja Metulj.

4. Pravila zunanjega priklopa članic na robno napravo Metulja (Edgelron)

Članica se na zunanji strani stikala na omrežje Metulj priklopi preko 1 Gb/s optičnih vrat na robnem stikalu Metulja. Priklop, robno stikalo in konfiguracijo robnega stikala zagotovi Univerza, članica univerze pa je dolžna zagotoviti ustrezne pogoje za priklop.

Pogoji za priklop:

- komunikacijska omara širine 19"
- prostor v omari v višini 2U
- električno napajanje 220V
- ustrezne klimatske razmere v prostoru (največ 20 stopinj celzija)
- omejen dostop do komunikacijske omare samo za pooblaščene osebe

Zelo priporočljiv je tudi sistem neprekinjenega napajanja (UPS) ustrezne moči, na katerega se lahko priklopi tudi ostale naprave članice v omari.

5. Pravila notranjega priklopa članic na robno napravo Metulja (Edgelron)

Članica lahko na robno stikalo priklopi svojo mrežno opremo (stikala, usmerjevalniki, požarni zidovi, ipd.).

Po dogovoru z IS UL lahko članica svojo mrežno opremo priklopi na:

1. Gigabitna vrata 1000BaseT (baker).
2. Gigabitna vrata 1000Base –X (optika).

Hkratno delovanje bakrene in optične povezave ni možno. Za priklop na optiko je potrebno dokupiti še ustrezen vtičnik SFP.

Robna naprava ima poleg gigabitnih vrat tudi 24 10/100BaseT vrat. Vrata 1-12 so namenjena javnem dostopanju do Metulja. Vrata 13-24 pa se lahko uporabijo za zasebne MPLS povezave. Za vsak priklop dodatne naprave na katerakoli od vrat je potrebno pridobiti soglasje IS UL (za pridobitev soglasja se lahko članice obrnejo na helpdesk@uni-lj.si).

6. Priporočila za notranje omrežje članic

Priporočila za notranje omrežje članic zajemajo priporočila za pasivni in aktivni del omrežja z namenom doseganja zanesljivega, varnega delovanja LAN omrežja posamezne članice.

6.1. Posodobitev pasivnega dela omrežja

6.1.1. Preverjanje lokalnih instalacij pasivne opreme – skica z meritvami

Za posodobitev oz. preverjanje kakovosti LAN omrežja članice je najprej potrebno preveriti lokalne inštalacije vodov, tako optičnih kot bakrenih. V tem koraku je najpomembneje, da se izdela natančna shema poteka vodov, ustrezno označi zaključne točke (vtičnice, patch paneli itd.) in odstrani odvečne in nepotrebne vodnike.

Za omrežja velikosti do 5 uporabnikov lahko ta dela izvede kar osebje članice, za večja omrežja z več uporabniki pa priporočamo zunanjega izvajalca.

6.1.2. Meritve na optiki in na bakrenih povezavah

Po končanem prvem koraku se priporoča opravljanje meritev na omrežni infrastrukturi, v koliko te niso bile opravljene v zadnjih dveh letih. Meritve je potrebno narediti tako na bakrenih kot tudi na optičnih vodih. Za izvajanje meritev priporočamo usposobljenega zunanjega izvajalca.

6.1.3. Nadgradnja lokalnega omrežja (nadomeščanje bakrenih povezav z optičnimi, zamenjava neustreznih instalacij)

Na podlagi rezultatov meritev se naredi načrt zamenjave neustreznih povezav. Priporočamo tudi zamenjavo morebitnih bakrenih povezav med posameznimi vozlišči z optičnimi, saj le-te nudijo večjo zanesljivost delovanja. Vse bakrene povezave morajo zagotavljati 1 Gb/s prepustnost! Po obnovi oz. prenovi ožičenja je potrebno še enkrat opraviti meritve zamenjanih in novih vodov (tako bakrenih kot optičnih). Zunanji izvajalci pasivne opreme običajno to naredijo že hkrati s prenovo.

6.1.4. Ustrezna ureditev sistemskih prostorov (klimatizacija, ustrezne omare ipd.)

Na koncu je potrebno še oceniti stanje sistemskih prostorov. Za glavni sistemski prostor se priporočajo vsaj naslednje karakteristike:

- klimatska naprava zadostne moči, da je v prostoru tudi poleti največ 20 stopinj
- dvojni pod
- kovinske 19-palčne omare za opremo z možnostjo zaklepanja
- vsi kabli so speljani pod podom ali v nadometnih kanalih
- neprekinjeno napajanje zadostne moči za vso nameščeno opremo z avtonomijo vsaj 15 minut
- če so v prostoru okna, priporočamo žaluzije in rešetke na oknih
- alarmna naprava
- gasilni aparat CO_2
- urejen in ustrezno označen prostor
- omejen dostop do prostora (s posebno kartico ali vsaj posebno proceduro pri vratarju/varnostniku)

V kolikor glavni sistemski prostor ne odgovarja zgornjim priporočilom, priporočamo, da se članica za prenovo oz. ureditev dogovori z zunanjim izvajalcem pasivne opreme.

6.2. Posodobitev aktivnega dela omrežja

6.2.1. Hrbtenica lokalnega omrežja (prehod na optiko)

Priporoča se, da hrbtenica lokalnega omrežja temelji na optičnih povezavah zaradi večje zanesljivosti in morebitnih nadgradenj na višje hitrosti v prihodnosti.

Hrbtenica lokalnega omrežja naj temelji na 1 Gb/s povezavah, saj lahko v primeru počasnejših povezav med vozlišči prihaja do zasičenj in posledično motenj v delovanju, počasnega delovanja ipd. na samih aplikacijah. Motnje so opazne predvsem v časih večjih obremenitev.

Jedrno stikalo, na katerem se stikajo vsa vozlišča naj bo L2/L3 stikalo, katero zna opravljati tudi funkcijo usmerjanja. Ta stikala imajo dovolj veliko hitrost stikanja, da zdržijo tudi večje obremenitve omrežja, prav tako običajno omogočajo povezovanja v sklad, imajo možnost redundančnega napajanja itd. Poleg tega se s z L2/L3 stikalom izognemo še dodatnemu usmerjevalniku za usmerjanje prometa na L3.

Za priklop uporabnikov, ki nimajo velikih omrežnih potreb, v vozliščih zadostujejo 100 Mb/s priključki, za zahtevnejše uporabnike pa se priporoča 1 Gb/s priključek.

Za priklop lokalnih vozlišč na centralno stikalo se lahko uporabi tudi t.i. dvodomni priklop stikal, kar pomeni, da ima vozliščno stikalo eno povezavo direktno do centralnega vozlišča, drugo pa na sosednje vozlišče. S tem dosežemo delovanje lokalnega vozlišča tudi ob izpadu ene od povezav.

Priporoča se, da se nove delovne postaje in strežniki kupujejo z 1 Gb/s mrežnimi karticami, hkrati s posodabljanjem delovnih postaj in strežnikov naj se vrši tudi nadgrajevanje vozlišč na stikala z 1 Gb/s priključnimi mesti. Za priklop strežnikov se priporoča 1 Gb/s priključno mesto, prav tako se priporoča 1 Gb/s povezava proti robni napravi Metulja.

6.2.2. Zamenjava serijskih povezav z optičnimi povezavami

V kolikor ima članica še kakšen oddaljeni oddelek priklopljen preko serijske povezave, se priporoča, da se le-ta čim prej zamenja z optično povezavo od oddaljenega oddelka do matične fakultete.

6.2.3. Shema priporočenih fizičnih povezav LAN omrežja in priklopa na omrežje

Shema 1 v prilogi prikazuje priporočen splošni princip lokalnih LAN omrežij s fizičnimi povezavami in hitrostmi znotraj le-teh. Priklop vozlišč je dvo-domen.

6.2.4. Segmentiranje notranjega dela omrežja – ločitev skupin med seboj

Uporabnike notranjega dela omrežja lahko razdelimo v več skupin na podlagi varnostne občutljivosti podatkov, do katerih dostopajo. Omrežja, ki vsebujejo podatke z različno varnostno občutljivostjo morajo biti fizično ločena med seboj, prehod med njimi pa strogo omejen in nadzorovan.

V univerzitetnem okolju lahko identificiramo naslednje logične skupine (segmente) uporabnikov:

1. *Eduroam* – brezžično omrežje na katerega se povezujejo študentje, profesorji in gostje iz tujih univerz, ki so prav tako vključene v Eduroam. V tem segmentu se promet ne sme filtrirati (razen za preprečevanje DDoS napadov, širjenja

internetnih črvov ipd.) Brezžične dostopne točke delajo s hitrostjo 54 Mb/s, zato za omrežje Eduroam priporočamo uporabo L3 stikala z vrati hitrosti 100 Mb/s, z možnostjo priklopa na hrbtenično omrežje s hitrostjo 1 Gb/s.

2. *DMZ* – na to omrežje priključimo strežnike, ki so javno dostopni, vendar pa jih želimo s požarnim zidom zavarovati (promet do strežnika filtriramo, dovolimo dostop le do vrat na katerih poslušajo strežniki). Za omrežje DMZ priporočamo uporabo stikal z vrati hitrosti 1 Gb/s.
3. *Kioski* – ta segment omrežja vključuje javno dostopne računalnike, ki ponujajo dostop do osnovnega portala članice, prijavo na izpite, ogled elektronske pošte ipd. (promet na tem segmentu strogo filtriramo). Za to skupino uporabnikov zadostuje priklop na omrežje s hitrostjo 100 Mb/s.
4. *Učilnice* - ta segment omrežja združuje računalnike v računalniških učilnicah (v tem segmentu filtriramo dostop do Interneta, hkrati pa dovolimo dostop do nekaterih strežnikov v skupini DMZ). Za delovne postaje v tej skupini zadostuje priklop na omrežje s hitrostjo 100 Mb/s, za morebitne strežnike v tem segmentu pa priporočamo priklop s hitrostjo 1 Gb/s.
5. *Zaposleni* – ta del omrežja vsebuje računalnike osebja zaposlenega na fakulteti. V ta segment vključimo tudi strežnike za intranet (datotečni, tiskalniški strežniki ipd.) Za priklop uporabnikov, ki nimajo velikih omrežnih potreb, zadostujejo 100 Mb/s priključki, za zahtevnejše uporabnike pa priporočamo 1 Gb/s priključek.
6. *Uprava* – združuje upravo članice (dekan, tajnik, finančno računovodske službe, kadrovsko službo, ipd.), ki običajno upravlja z varnostno občutljivejšimi podatki kot pedagoški kader. Za delovne postaje v tej skupini zadostuje priklop na omrežje s hitrostjo 100 Mb/s, za morebitne strežnike v tem segmentu pa priporočamo priklop s hitrostjo 1 Gb/s.
7. *Management* – ta del omrežja je namenjen nadzoru in upravljanju mrežne infrastrukture v Metulju. V želji po centralizaciji helpdesk-a lahko članica nudi podatke o delovanju notranjega omrežja (in storitev) Informacijski službi UL (protokoli SNMP, Netflow, SFlow). Za nadzor naprav v upravljavskem omrežju zadostujejo priključki s hitrostjo 100 Mb/s.

Shemi 2a in 2b v prilogi prikazujeta priporočeno L2 segmentacijo notranjega omrežja članice. Segmentacijo notranjega omrežja lahko izvedemo s tehnologijo VLAN-ov. VLAN-i nam omogočajo gradnjo neodvisnih logičnih omrežij znotraj istega fizičnega omrežja.

VLAN-e zaključimo na L3 stikalu ali na požarnem zidu, kjer vzpostavimo tudi ustrezne omejitve za prehajanje prometa med VLAN-i. Segment Management se razteza čez celotno omrežje Metulj.

Članice lahko za označevanje VLAN-ov uporabijo poljubne številke izven intervala 0-500. VLAN-i iz tega intervala so predvideni za potrebe omrežja Metulj in IS UL.

6.2.5. IP številke

Članice morajo IP številke za katere zaprosijo tudi dejansko porabiti. Glede na to, da UL trenutno nimam pomanjkanja IP številk naj članice na vseh segmentih omrežja uporabijo javne IP številke.

Članice, ki jim primanjkuje IP številk, lahko pridobijo dodatne IP številke, tako da na naslov helpdesk@uni-lj.si pošljejo zahtevo za dodelitev dodatnih številk IP (Obrazec IP-01).

Priporočamo, da članice *v največji možni meri uporabljajo dinamično dodeljevanje IP številk (DHCP)* v kombinaciji z avtentikacijo IEEE 802.1x in ustreznimi AAA mehanizmi. Priporočamo uporabo podobnih AAA mehanizmov, kot se uporabljajo v omrežju Eduroam.

6.2.6. IPv6

UL načrtuje postopen prehod na uporabo IPv6 naslovnega prostora. Povezava v omrežje ARNES bo v »native« načinu vzpostavljena v poletju 2007. Po uspešni vzpostavitvi povezave z ARNES bo vsaki članici dodeljen en /48 kos IPv6 naslovnega prostora, ustrezno pa bo nastavljena tudi omrežna oprema v Metulju. Članice se bodo lahko začele v zadnji četrtini leta 2007 priklapljati v omrežje IPv6.

Priporočamo, da se pri nakupih nove omrežne opreme zahteva združljivost z IPv6 v »native« načinu delovanja (velja za vso omrežno opremo). Kompatibilnost z IPv6 morajo zagotavljati tudi operacijski sistemi, na kar je potrebno paziti predvsem pri specializiranih operacijskih sistemih (Windows 2003, Windows Vista, Windows XP, Linux, FreeBSD in OpenBSD imajo ustrezno podporo skladom IPv6).

7. Varnostna politika

7.1. Varnostna politika omrežja Metulj

Na infrastrukturi omrežja Metulj so vzpostavljeni ustrezni varnosti elementi. Na napravah so nastavljene določene omejitve za omejevanje DoS in DDoS napadov, nastavljene so omejitve za omejevanje »rizičnega« prometa podatkov (predvsem najbolj pogosta vrata TCP/UDP, katere uporabljajo dobro znani virusi, črvi ipd.). Te nastavitve so namenjene predvsem zaščiti *infrastrukture omrežja Metulj* in kot take niso namenjene zaščiti omrežij članic. Omrežja članic so posledično zaščitena le na najbolj grobem nivoju in sicer pred množičnimi DDoS napadi ter nekaj najbolj razžirjenimi črvi/virusi. *Varovanje omrežij pred nevarnostmi z interneta je prepuščeno članici.*

V primeru zlorabe omrežja Metulj lahko IS UL v skladu s točko 3 izključi članico iz omrežja Metulj.

7.2. Varnostna politika članic

Dobra in učinkovita ter dosledno upoštevana varnostna politika omrežja preprečuje krajo podatkov, izgubo podatkov ter ne nazadnje mnogo stabilnejše delovanje lokalnega informacijskega sistema, kjer ni potrebno kar naprej na novo nameščati delovnih postaj zaradi virusov, črvov in ipd. Za varnost lokalnega omrežja je dolžna skrbeti vsaka članica posebej v skladu z lastno politiko varovanja omrežja in v skladu s pravili uporabe omrežja Metulj. Podajamo nekaj priporočil za varnostno politiko omrežja članice:

- Potrebno je poskrbeti za fizično varnost opreme, predvsem sistemskega prostora. Sistemski prostor mora biti tehnično ustrezno varovan (alarmna naprava, dostop na kartico ipd.), v prostoru se nahaja vpisna knjiga, kamor se mora vpisati vsak vstop v prostor.
- Potrebno je ustrezno segmentirati uporabnike v uporabniške skupine v lokalnem omrežju in ustrezno omejiti pretok podatkov med njimi (6.2.4)
- Nastaviti je treba ustrezno politiko dostopanja proti omrežju Metulj
- Za politiko dostopanja do javnega omrežja priporočamo, da se nastavi tako, da se najprej prepove ves dostop proti zunanjemu omrežju, nato pa eksplicitno dovoljuje kam lahko dostopa katera uporabniška skupina ali uporabnik (npr. študentje lahko brskajo po internetu in prebirajo e-pošto, informatiki imajo popolni dostop ipd.)
- Javni strežniki morajo biti v t.i. DMZ coni na požarnem zidu – to pomeni da so na požarnem zidu obravnavani kot posebna skupina, ki nima pravice do dostopa v notranje omrežje. To je zelo pomembno v primeru vdora na javni strežnik.
- Za povečano varnost lahko namesto požarnega zidu namestimo napravo, ki združuje požarni zid in pregledovalnik vsebine. Pregledovalnik vsebine pregleduje vsebino vsega prometa proti internetu in glede na politiko ustrezno ukrepa. Primer: na pregledovalniku vsebine lahko nastavimo, da uporabniki ne morejo odpirati .exe datotek z interneta ali npr. da ne smejo obiskovati strani z ilegalno vsebino ipd.) Prav tako je možno na pregledovalniku vsebine pregledovati ves promet (http, smtp, ftp) za morebitne viruse, črve ipd. in jih seveda blokirati še preden pridejo v lokalno omrežje. Pregledovalniki vsebine so na voljo tudi kot ločene naprave in jih lahko dodamo obstoječemu požarnemu zidu.
- Priporočamo, da se v omrežju namestijo naprave za odkrivanje vdorov ali za preprečevanje vdorov (Intrusion Detection System – IDS ali Intrusion Prevention System - IPS), ki nam omogočajo zgodnje odkrivanje napadov in njihovo preventivno preprečevanje.

8. Priporočila za strojno opremo članic

Za strojno omrežno opremo se priporoča oprema priznanih omrežnih proizvajalcev, ki imajo dovolj velik delež na trgu, in oprema katerih je dovolj zmogljiva, zanesljiva in razširljiva za morebitne bodoče potrebe. Izbrani omrežni proizvajalec mora imeti zastopnika v Sloveniji, nuditi mora zamenjavo v roku enega delovnega dne, podporo tudi po koncu izdelave dodolčenega modela ipd. Priporoča se, da je vsa oprema lokalnega omrežja od istega proizvajalca, saj različna oprema lahko povzroči neskladnosti med delovanjem, prav tako je oteženo upravljanje. Priporočljivo se je izogibati nekakovostnih proizvajalcev omrežne opreme namenjene uporabi v domovih in manjših pisarnah (oprema SOHO), saj le-ta pod večjo obremenitvijo povzroča nepredvidljive težave, v skrajnih primerih lahko tudi odpove. Prav tako je podpora dostikrat zelo slaba.

V skladu s shemo priporočenih fizičnih povezav LAN omrežja in priklopa na omrežje se priporoča:

- za »L2 stikalo« na oddelčnih vozliščih model z vsaj 24 10/100 Mb/s vrati in vsaj dvema 1 Gb/s optičnima priključkoma SFP, podporo RSTP protokola, podpora Link Aggregation (Channel Bonding), GVRP, 802.1x, Flow Control, PoE (kot primer navajamo model proizvajalca Foundry - FastIron Edge 2402 PoE)

- za »L2 stikalo – GB« za agregacijo strežnikov model z vsaj 20 10/100/1000 Mb/s vrati in štirimi SFP vrati ter podporo RSTP protokola, podporo Link Aggregation (Channel Bonding), QOS, GVRP, 802.1x, Flow Control (kot primer navajamo model proizvajalca Foundry - EdgeIron 24G)

- za centralno »L2/L3 stikalo« pa se priporoča modularno stikalo z vsaj 8 optičnimi vrati SFP, 16 vrati 100/1000 BaseT, redundančnim napajanjem, IP usmerjanjem, podporo RIP, OSPF, RSTP, 802.1x, Radius avtentikacije, zaščito pred DoS napadi (kot primer navajamo model proizvajalca Foundry - FastIron Edge X)

- za požarni zid se priporoča naprava z vsaj tremi gigabitnimi vmesniki, dovolj veliko zmogljivostjo za gigabitni promet ter možnostjo nadgradnje s pregledovalnikom vsebine

9. Storitve v omrežju Metulj

9.1. ActiveDirectory

Univerza v Ljubljani je v letu 2007 začela s projektom uvedbe centralnega imenika identitet na UL. V okviru projekta bo vsaka članica dobila strežnike namenjene gostovanju skupne domene ali pa prostor za gostovanje domene na virtualnem strežniku UL.

Za uspešno replikacijo imenika AD med domenskimi strežniki tako znotraj domene kot med domenami je potrebno na požarnih pregradah omogočiti komunikacijo do strežnikov preko naslednjih vrat:

Storitev	**Vrata / Protokol**
RPC endpoint mapper	135/tcp, 135/udp
RPC port for AD replication	22222/tcp (določen s strani IS UL in že v uporabi v obstoječem gozdu)
SMB over IP (Microsoft-DS)	445/tcp, 445/udp
LDAP	389/tcp
LDAP over SSL	636/tcp
Global catalog LDAP	3268/tcp
Global catalog LDAP over SSL	3269/tcp
Kerberos	88/tcp, 88/udp
DNS	53/tcp, 53/udp
Network time protocol (NTP)	123/udp

Navedena vrata je potrebno omogočiti le za nabor številk IP, na katerih se nahajajo domenski strežniki za domeno UNI-LJ. Nabor IP številk za domenske strežnike vzdržuje IS UL (helpdesk@uni-lj.si).

9.2. Eduroam

Storitev Eduroam omogoča uporabniku varen in preprost dostop do (brezžičnega) omrežja lastne organizacije in gostovanje v omrežjih drugih institucij, vključenih v sistem Eduroam. Storitev Eduroam so vpeljale tudi nekatere članice UL in rektorat UL.

9.2.1. Članice, ki imajo za Eduroam lastno infrastrukturo

Članice, ki so samostojno vzpostavile imenik LDAP, strežnik FreeRadius in strežnik DHCP morajo za pravilno delovanje omrežja Eduroam na požarnih omogočiti komunikacijo do strežnikov preko naslednjih vrat:

Storitev	**Vrata / Protokol**
Radius autehntication	1812/tcp
Radius accounting	1813/tcp
Radius proxy	1814/tcp
LDAP	389/tcp
LDAP over SSL	636/tcp

Vrata morajo biti dostopna »top-level« LDAP in Radius strežnikom iz UL za avtentikacijo in avtorizacijo uporabnikov, ki gostujejo na drugih organizacijah in za replikacijo LDAP imenika.

9.2.2. Članice, ki uporabljajo infrastrukturo IS UL

Članice, ki nimajo lastnih strežnikov LDAP in FreeRadius morajo omogočiti dostop iz stikala, na katerem zaključujejo omrežje Eduroam na njihovi strani, do strežnikov na UL preko naslednjih vrat:

Storitev	**Vrata / Protokol**
Radius autehntication	1812/tcp
Radius accounting	1813/tcp
Radius proxy	1814/tcp

9.2.3. DHCP

Zaradi lažjega upravljanja številk IP namenjenih za brezžično omrežje Eduroam, priporočamo, da se za dodeljevanje številk IP v omrežju Eduroam uporabi strežnik DHCP, ki se nahaja na IS UL. Za uporabo skupnega DHCP strežnika je potrebno na stikalu, kjer se zaključuje omrežje Eduroam na članici, nastaviti *»ip helper address«*, ki omogoča spreminjanje DHCP multicast zahtev v unicast zahteve. Poleg tega je potrebno na požarnih omogočiti komunikacijo do DHCP strežnika na UL preko naslednjih vrat:

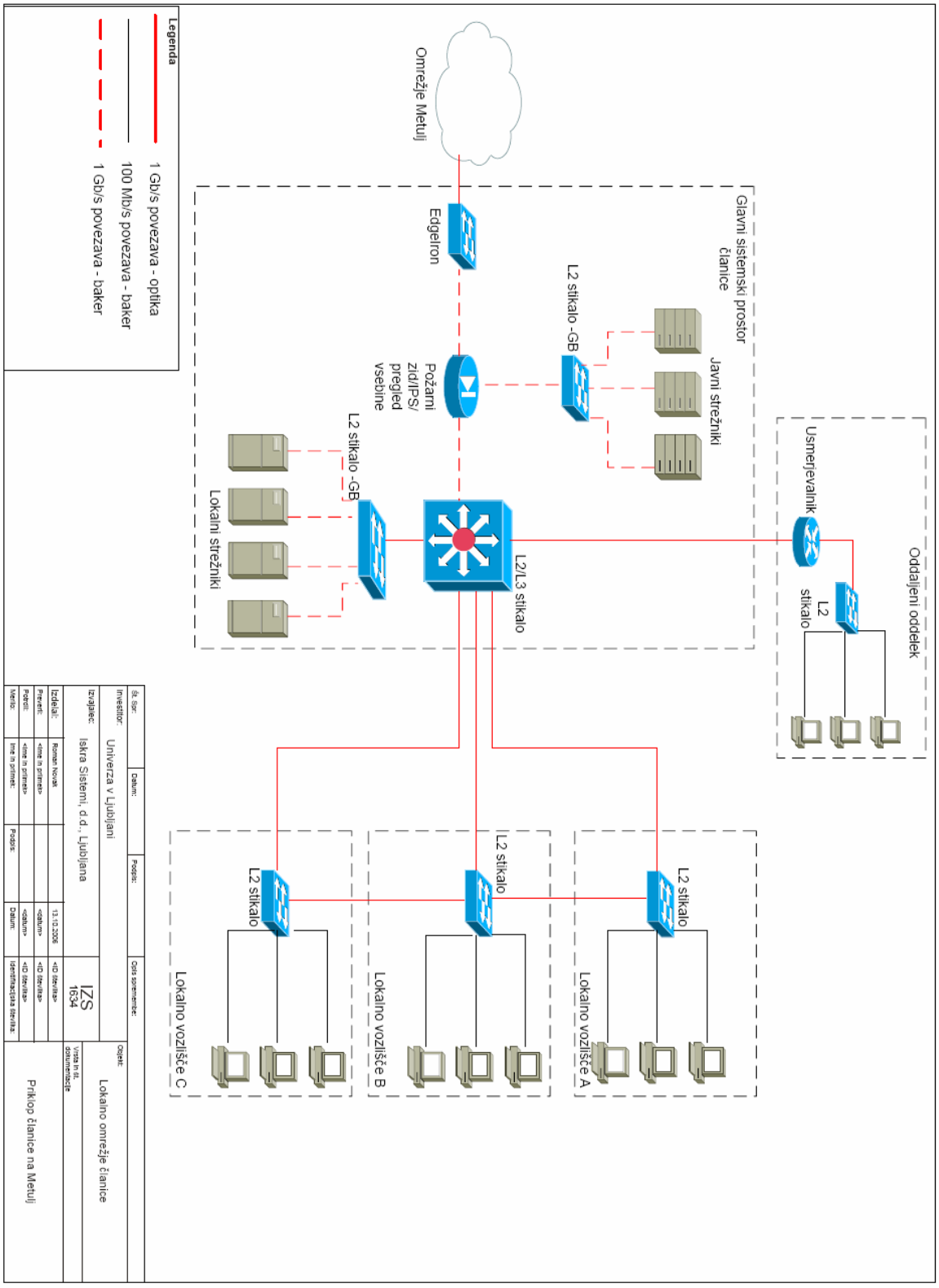
Storitev	Vrata / Protokol
DHCP unicast	67/udp

Za omogočanje dinamičnega dodeljevanja naslovov se je potrebno predhodno dogovoriti z IS UL (helpdesk@uni-lj.si). Ustrezno usmerjanje naslovov IP mora zagotoviti članica sama.

10. Priloge

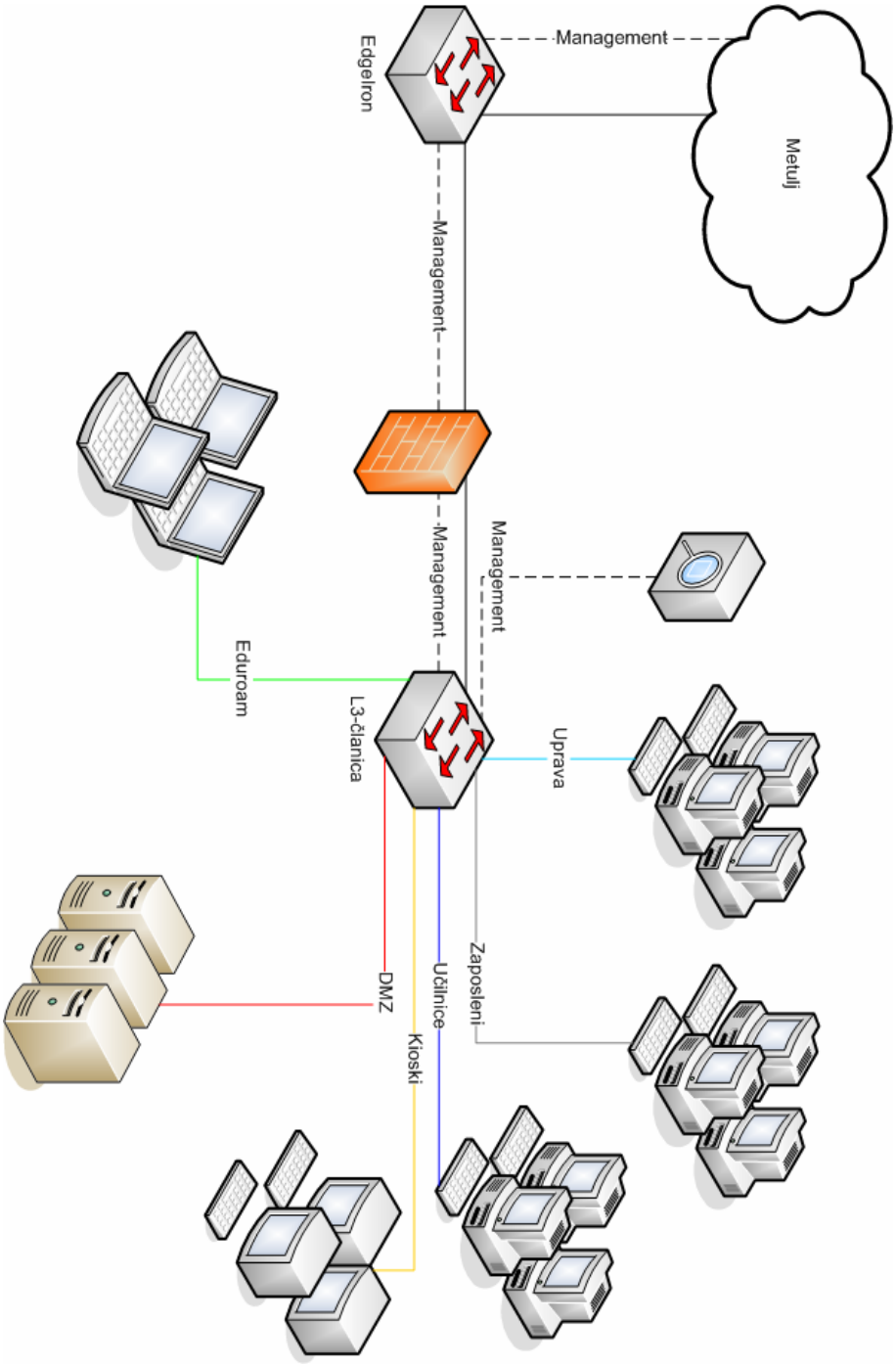
10.1. Shema 1 – Fizične povezave LAN

Shema prikazuje priporočene fizične povezave v notranjem (LAN) omrežju in priklop na omrežje Metulj.



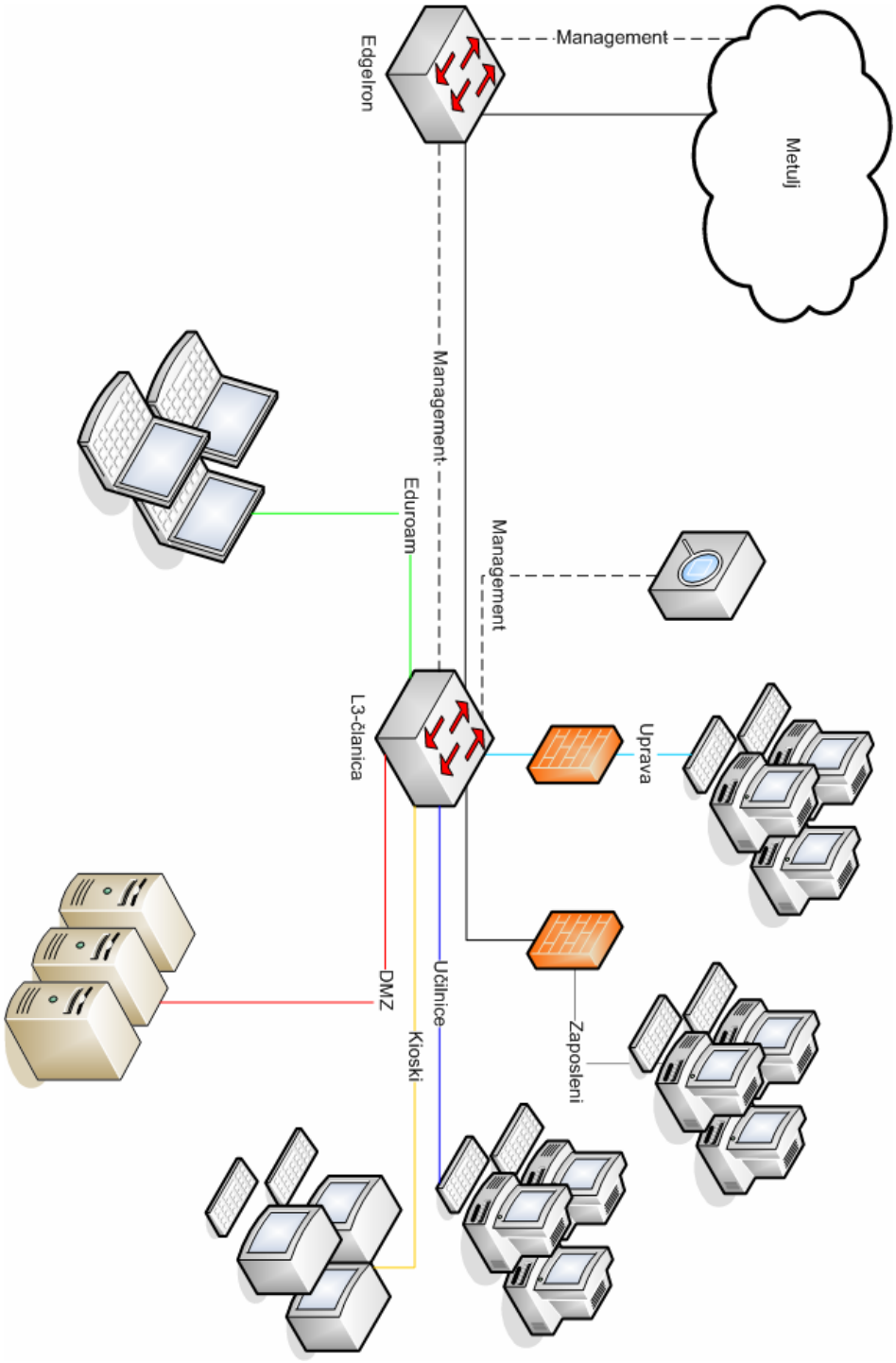
10.2. Shema 2a – L2 segmentacija

Shema predstavlja L2 segmentacijo notranjega omrežja članice (VLAN-i). Požarna pregrada je umeščena med L3 stikalo in robno stikalo omrežja Metulj, kar pomeni da mora biti dovolj zmogljiva za hitrosti 1 Gb/s in mora podpirati veliko število hkrati vzpostavljenih sej.



10.3. Shema 2b – L2 segmentacija

Shema predstavlja L2 segmentacijo notranjega omrežja članice (VLAN-i). Ker predstavljajo požarne pregrade, ki zmorejo hitrosti do 1 Gb/s, velik finančen zalogaj, lahko ščitimo le segmente, ki to najbolj potrebujejo. Tako lahko namestimo eno ali več manj zmogljivih požarnih pregrad za L3 stikalo članice, ki omejuje dostop do Interneta le posameznim segmentom uporabnikov.



10.4. Shema 3 – topografija omrežja

Shema prikazuje trenutno aktualno topografijo omrežja Metulj.