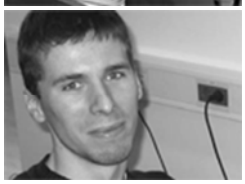
**Miha Dimec,
Aleš Zavodnik,
Matjaž Straus Istenič,
Miha Jemec,
Matej Vadnjal,
vsi Arnes**







Od optičnega vlakna do kakovostne komunikacije
From optical fibre to quality communication

Povzetek

Kakovostno komunikacijo omogoča zapleten splet različnih tehnologij. Omrežna storitev je nanizana v plasteh in sestavljena iz različnih elementov – od ustreznega prostora, električnega napajanja, bakrenih kablov ali optičnih vlaken, povezovalnih tehnologij do kompleksnejših omrežnih protokolov in programske opreme. Uporabniku je ta struktura skrita, kljub temu pa vsi njeni gradniki neposredno vplivajo na uporabnikovo izkušnjo pri uporabi omrežne storitve.

Prispevek in predavanja predstavljajo to sestavljenko s primeri iz prakse. Opisani so mehanizmi, s katerimi zagotavljamo in nadziramo kakovost komunikacije in omrežnih storitev: osnovna komunikacijska infrastruktura, tehnologija namenskih povezav ”točka–točka”, mehanizmi QoS in varna uporaba protokola IPv6 v lokalnih omrežjih. Prispevek zaključuje kratka predstavitev nekaterih orodij, s katerimi nadziramo in upravljamo Arnesovo omrežje.

Ključne besede: ustrezen prostor, infrastruktura, dokumentacija, optično vlakno, DWDM, CWDM, točka–točka, kakovost storitev, kakovost komunikacije, QoS, IPv6, samodejne nastavitve, SLAAC, DHCPv6, varnost omrežja, upravljanje omrežja, nadzor omrežja

Abstract

Systems engineers and network administrators acknowledge that quality assurance for network services is not straightforward. This group of talks will explore the daily challenges. A complex mesh of varied technologies enables quality communication. Network services are linked in layers and consist of various elements – suitable premises, electricity supply, copper cables or optical fibres, connection technologies for complex network protocols, and software. This structure is hidden from users, although all of its elements directly affect their experience of network services. The article and the conference talks describe this combination through practical examples. We will show the mechanisms we use to ensure quality communication and network services. We will describe the technology for dedicated point-to-point connections for services that require high quality, secure and private communications. We will emphasise the importance of the modern, easy-to-use IPv6 protocol. The talk concludes with an outline of a subset of tools used to monitor key connection parameters in the ARNES network.

Key words: proper conditions, infrastructure, documentation optical fibre, DWDM, CWDM, point-to-point, quality of service, quality of communication, QoS, IPv6, stateless autoconfiguration, SLAAC, DHCPv6, network security, network management

Kakovostna infrastruktura

Quality begins within the infrastructure

Miha Dimec

Kakovost komunikacije in storitve ni povezana zgolj s pretokom IP-paketkov, nastavitvami opreme in nadzorom. Kakovost storitve začnemo zagotavljati na področjih, ki na prvi pogled niso povezana z informacijsko tehnologijo:

- ustrezen prostor z vso potrebno infrastrukturo;
- zanesljiva povezljivost do ponudnika interneta;
- izdelan scenarij dogodkov, ki se lahko zgodijo in ki vplivajo na našo storitev;
- dokumentacija, ki poleg stanja vsebuje tudi vse pomembne kontaktne podatke.

The quality of communication depends not only on the configuration and monitoring of routers and switches. The work of providing quality communications begins in areas which many IT staff believe are not related to the quality of communications at all:

- Ensure that your IT equipment is located in a suitable room or place;
- Ensure that your connectivity to the ISP meets all the conditions for reliability and stability;
- Be prepared for many situations that may arise and affect the quality of your communications. Prepare procedures to solve the problem in advance;
- Documentation, documentation, documentation and documentation.

Pri zagotavljanju kakovostne komunikacije pogosto pozabljamo ali zanemarjamo pomembnost infrastrukture, na kateri gradimo in ponujamo svoje storitve. Na kakovost komunikacije posredno vplivajo vsi parametri prostora, v katerem se nahaja naša oprema, fizični potek povezljivosti do našega internetnega ponudnika, urejenost in vodenje naše dokumentacije ter usposobljenost in znanje naših ter zunanjih vzdrževalcev. V praksi ugotavljamo, da se ta problematika pogosto težko obrazloži projektantom, vodjem finančnega sektorja in (pri dokumentaciji) vzdrževalcem stavbe. Zato je namen tega prispevka izboljšanje stanja na omenjenem področju.

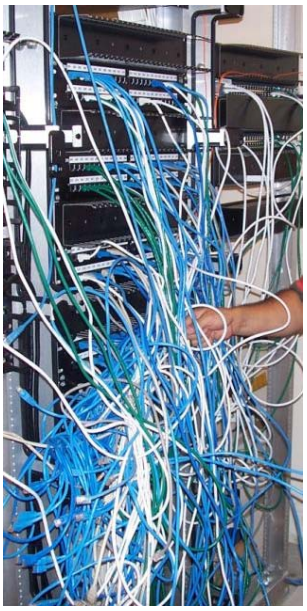
Komunikacijska in strežniška oprema, s katero izvajamo storitve, mora nekje imeti svoj prostor. Za tak prostor pa ne sme biti edini pogoj zgolj električni priključek. Prostor mora biti dovolj velik za vsa vzdrževalna dela, omogočati mora ustrezno klimo, imeti mora ustrezne električne priključke, zanesljive komunikacijske vode do ponudnika interneta, onemogočati dostop za nepooblaščene osebe in imeti vsaj osnovno protipožarno zaščito. Bo kakovostna komunikacija sploh še mogoča, če se bo oprema poleti pregrevala in zaradi tega nehala delovati? Bo oprema pravilno delovala, če bo njeno napajanje preobremenjeno z drugimi porabniki, kot so npr. sesalec, električni kuhalnik ipd.

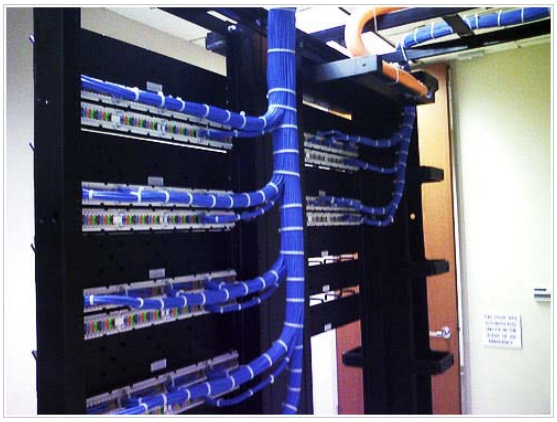
SLIKA 9: SODOBNA OMREŽNA INFRASTRUKTURA?

Prostor naj bo ustrezno velik, da so v njem mogoča vzdrževalna dela, da je prezračevanje ustrezno in ni »toplih con«, da lahko kasneje v njem montirate klimatsko napravo (mogoča montaža zunanje enote, odtok kondenza).

SLIKA 10: DOVOLJ PROSTORA ZA NEMOTENO DELO

Vzor za urejenost kablov naj ne bodo špageti v posodi kot tudi ne »state of the art«.





SLIKA 11: "ŠPAGETI" OMREŽJE ALI UMETNOST?

Povezava do ponudnika interneta bo omogočala kakovostnejšo storitev, če bo znano, kje poteka. Če nimate podatkov, kdaj se bodo izvajala določena vzdrževalna dela v vaši stavbi oz. njeni bližnji okolici, ali če nimate podatkov, ali se bodo dela izvajala na področju, kjer potekajo kabli od vas do vašega ponudnika interneta, vas lahko posledično preseneti nepričakovan daljši izpad vaših storitev. Povezava z dvema različnima ponudnikoma interneta še ne zagotavlja, da le-ta ne poteka po istem kablu, po istem kanalu ali isti ulici.

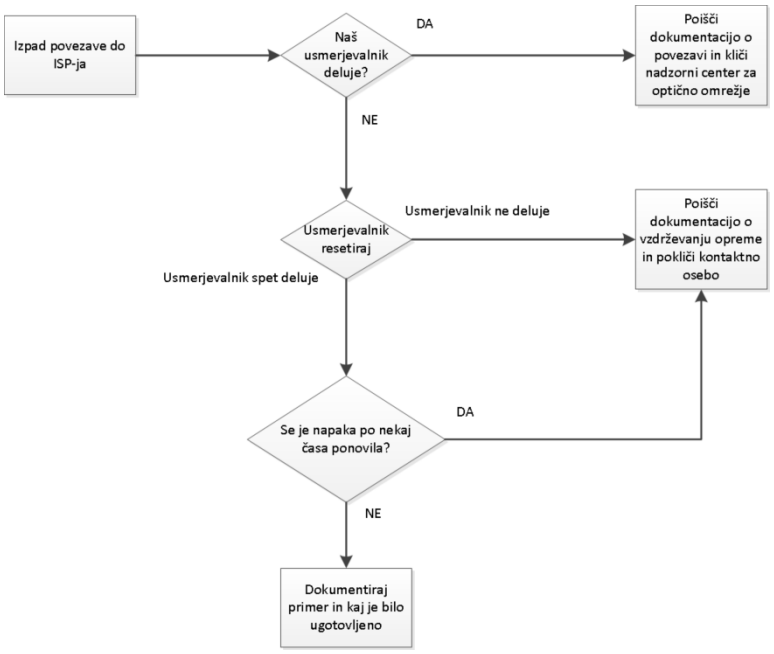
SLIKA 12: ZDAJ VEMO, KJE POTEKAJO NAŠE OPTIČNE POVEZAVE.

Dokumentacija je ključ do kakovostne storitve. Če nimate dokumentirane opreme, nastavitev, kontaktov ponudnika interneta, vzdrževalcev opreme, hišnikov, vzdrževalnih pogodb, garancij in odgovornih oseb, bo lahko izpad storitev dolgotrajen in bo negativno vplival na izkušnjo vaših uporabnikov.

Ob vzpostavitvi storitve predvidevajte mogoče dogodke, ki lahko vplivajo na njeno kakovost in pripravite scenarije, kako se jih lotiti; na primer v primeru okvare usmerjevalnika:

- Katere uporabnike moram o tem obvestiti in kako?
- Kje je rezervna oprema?
- Kje je shranjena konfiguracija?
- Kje je opisan postopek, kako shranjeno konfiguracijo postaviti na rezervno opremo?
- Ali za usmerjevalnik še velja garancija?
- Ali imamo za usmerjevalnik podpisano pogodbo o vzdrževanju?
- Kontaktni podatki servisne službe.
- Ali smo zabeležili vse podatke o izpadu storitve za kasnejša poročila?

Izdelajte graf poteka, ki naj bo čim bolj pregleden in enostaven. V krizi bo vaš zaveznik.



SLIKA 13: PRIMER GRAFA POTEKA, KAKO RAVNATI V PRIMERU TEŽAV V OMREŽJU

Na praktičnih primerih bo na predavanju razložena pomembnost dobrega načrtovanja, razgledanosti, dobrega dokumentiranja in postopkov ob težavah. Zagotavljanje kakovostnih storitev se začne pri infrastrukturi.

Viri

- Arnesova dokumentacija
- www.fotosearch.com
- spletni viri

Sodoben transport paketkov

Modern transport of packets

Aleš Zavodnik

Z naraščanjem prometa morajo ponudniki omrežij IP poiskati načine, kako zagotoviti zadostne kapacitete in prilagodljivost omrežij glede na zahteve uporabnikov. Skoraj vsi paketki v svetovnem spletu danes prepotujejo večji del svoje poti po optičnih vlaknih. Za zagotavljanje zanesljive poti najprej potrebujemo kakovostno optično vlakno. Ko nam optično vlakno ne nudi več zadostnih kapacitet, lahko uporabimo dodatna vlakna ali pa eno od WDM-tehnologij.[10] Trenutno nam na Arnesu
WDM-tehnologije omogočajo zagotavljanje več hkratnih 10-gigabitnih povezav, v načrtu pa imamo tudi že prve povezave prepustnosti 40 Gb/s, po potrebi pa bomo lahko podprli tudi 100 Gb/s.

Poseben poudarek je podan namenskim povezavam za posamezne zahtevnejše projekte, kar na Arnesu dosežemo z opremo, katere osnovni gradniki so obstoječa WDM-omrežja.

In dealing with increasing traffic, IP network providers need to find new ways to ensure sufficient network capacity and flexibility to meet user requirements. Today almost all packets travelling over the Internet are routed through optical fibres. To ensure reliable transport, you must first provide high quality optical fibre. When a fibre no longer offers sufficient capacity, we can use additional fibres or a WDM technology. ARNES WDM technology currently provides multiple concurrent 10-gigabit links, and we plan to upgrade some links to 40 Gbps. If required, we can also support 100 Gbps.

Particular emphasis is given to dedicated links for more complex and specific projects.

Equipment to support these new features was actually an upgrade of the existing ARNES WDM network.

Optično vlakno

Enorodovno optično vlakno je danes najbolj razširjeno. Ima zelo tanko sredico, narejeno iz čistega silicija, plašča in ovoja proti mehanskim poškodbam. Njihova prednost pred bakrenimi vodniki je predvsem v veliko večjih kapacitetah, nižji ceni, majhnih izgubah in lažjem vzdrževanju.

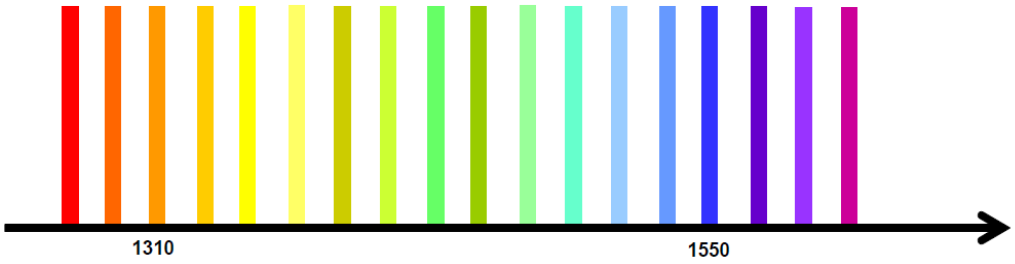
Za osvetlitev optičnega vlakna običajno uporabljamo dve valovni dolžini – 1310 nm in 1550 nm. Implementacija je preprosta, diode ali laserji svetijo v širokem pasu in niso temperaturno občutljivi.

[10] WDM ali Wavelength-division Multiplexing je tehnologija, ki omogoča prenos več signalov preko enega samega optičnega vlakna, tako da se za posamezne signale uporabi svetloba z različno valovno dolžino.

SLIKA 14: VALOVNE DOLŽINE SVETLOBE V OPTIČNEM VLAKNU.

CWDM – coarse wavelength division multiplexing

Ta tehnologija uporablja več valovnih dolžin s širino signala 20 nm. ITU-standard predvideva 18 kanalov v pasu od 1271 nm do 1611 nm. Uporablja se predvsem za krajše razdalje in je še vedno cenovno ugodna.



SLIKA 15: VALOVNE DOLŽINE KANALOV CWDM

DWDM – dense wavelength division multiplexing

Le-ta uporablja tako imenovani C-pas od 1530 nm do 1565 nm. ITU-standard predvideva različne širine signalov. Najpogosteje je uporabljena širina 0,8 nm, kar nam omogoča do 40 hkratnih kanalov. Ker so širine kanalov majhne, morajo biti komponente natančneje izdelane in temperaturno stabilne. Posledica je seveda višja cena gradnikov.

SLIKA 16: VALOVNE DOLŽINE KANALOV DWDM

Kakovostne storitve v omrežju ARNES

Za posebne projekte ali specifične želje lahko vzpostavimo posebne povezave znotraj Slovenije in tudi v tujino, kjer nam to omogoča infrastruktura evropskega

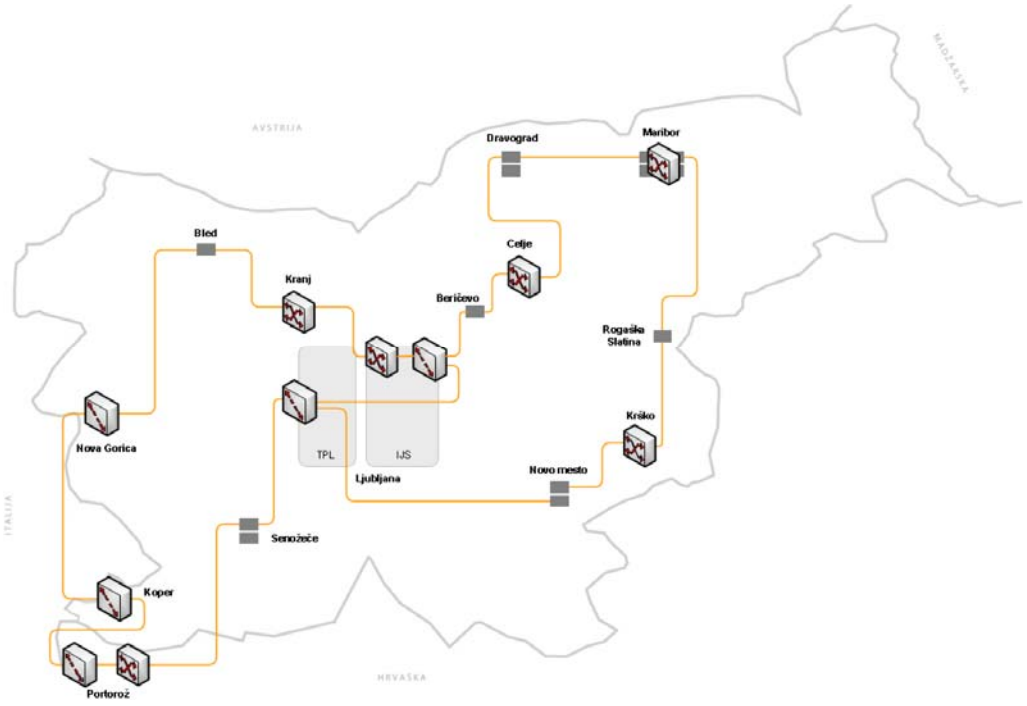
omrežja GÉANT. Takšne namenske povezave so ločene od produkcijskega IPv4- in IPv6-prometa. Uporabimo jih lahko za potrebe omrežij ”grid”, 3D-vizualizacij, omrežij v ”oblaku”, zahtevnih projektov v kemiji, genetiki, astronomiji, zdravstvu. Drugo področje uporabe je povezovanje redundantnih računalniških centrov in povezovanje fakultet v enotna omrežja.

Omrežje ARNES omogoča dva načina za vzpostavljanje tovrstnih povezav:

- Povezave prepustnosti 10 Gb/s vzpostavimo s pomočjo ločenih svetlobnih poti. Če potrebujemo večjo zanesljivosti, je treba vzpostaviti dve povezavi, vsako po svoji poti.
- Povezave prepustnosti 1 Gb/s lahko vzpostavimo s posebno opremo, ki omogoča zagotavljanje zasebnih ethernet povezav po dveh ločenih poteh skozi hrbtenico omrežja. V primeru prekinitve primarne poti se promet v manj kot 50 milisekundah samodejno preusmeri na rezervno pot.

Slika 17 prikazuje topologijo DWDM-omrežja in vozlišča, kjer je na voljo tovrstna oprema.

Seveda je treba tovrstne povezave speljati vse do ustrezne točke v omrežju priključene organizacije. Za ta namen priporočamo zakup dodatnih optičnih vlaken do hrbtenice omrežja ARNES ali pa uporabo tehnologije CWDM, ki poleg IP-povezave omogoča preko obstoječih optičnih vlaken vzpostavitev tudi namensko povezavo ”točka–točka”.



SLIKA 17: ZAGOTAVLJANJE NAMENSKIH POVEZAV V OMREŽJU DWDM

QoS – kakovost storitve

Just another word for dropping packets?

Miha Jemec

Ustrezno zagotavljanje kakovosti storitve posameznim tipom aplikacije (QoS) je v Arnesovem omrežju polno podprto. V prispevku si bomo podrobneje pogledali, kako so mehanizmi implementirani in kaj je bilo narejenega v zadnjem letu.

The ARNES network fully supports the provision of quality of service (QoS) to different kind of applications. This article examines how QoS is implemented and what has been done in the last year.

Kakovost storitve ima v omrežju ARNES že dolgo zgodovino. In veliko končnih uporabnikov, katerim omenjeni mehanizem (morda nevede) služi, bi lahko samo potrdilo, da so zadovoljni s storitvami, ki jih imajo, kar je ne nazadnje tudi najpomembnejše za zadovoljstvo uporabnikov omrežja. Mehanizmi zagotavljanja QoS namreč skrbijo, da imajo različni tipi aplikacij različne prioritete pri prenosu podatkov v omrežju in s tem dajejo uporabniku izkušnjo, da vse "pravilno" deluje. Bolj ali manj vsi poznamo motnje pri prenosu in gledanju IPTV, saj točno vemo, kako mora izgledati izkušnja pri gledanju televizije. Hkrati ne opazimo, če se prenos elektronske pošte ali odpiranje spletne strani zakasni za nekaj desetink sekunde. Zato lahko mirno odgovorimo, da je QoS na povezavah do Arnesovih članic nuja in daleč od naključnega odmetavanja paketov pri polnih povezavah.

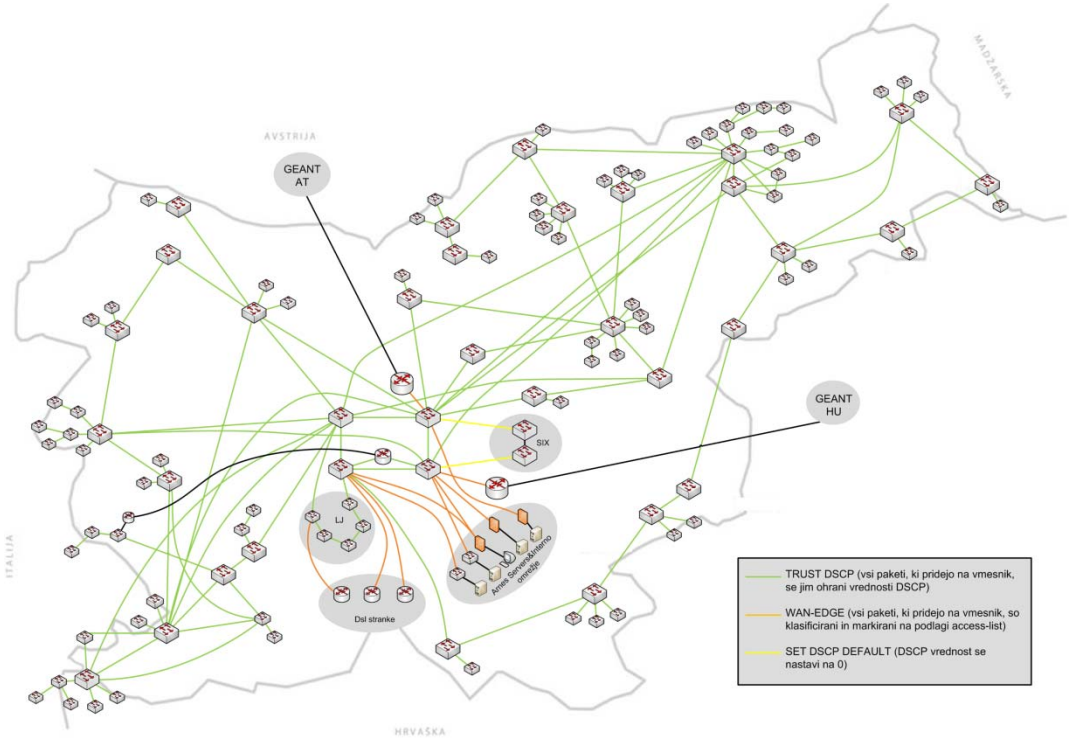
V primeru Arnesovih članic igra QoS najpomembnejšo vlogo pri končnih povezavah do članic, kadar je povezava narejena preko DSL-tehnologij. V vlogi IPTV v našem primeru večinoma nastopajo videokonference, v zadnjem času je vse več tudi telefonije (VoIP – *voice over IP*). Omenjeni dve storitvi imata pri prenosu paketov preko Arnesovega omrežja do članice (in obratno) vedno zagotovljeno najvišjo prioriteto. Sledijo jim storitve, ki jih razvrščamo med pomembnejše, med katere uvrščamo aplikacije tipa spletne pošte, oddaljenih dostopov (*telnet*, *ssh*), šifriranega spletnega prenosa (*https*) in raznih kontrolnih protokolov.

Do lanskega leta je v zadnji razred padel ves preostali promet, vendar smo lani zaradi povečanega prometa neposredne izmenjave datotek (”peer-to-peer”) ta razred razdelili. Tako imamo po novem razred ”best effort”, kamor spada običajen spletni promet in nekateri prenosi podatkov (npr. *ftp*), dodaten razred pa je namenjen prometu ”peer-to-peer” in raznim odjemalcem za neposredno izmenjavo datotek, ki uporabljajo protokol *BitTorrent*. Na tak način lahko poskrbimo, da imamo količinsko najagresivnejši promet pod kontrolo in predvsem da ne povzroča degradacije ostalega prometa. Promet delimo v naslednje razrede:

- PIP – razred ”Premium IP” z najvišjo prioriteto za potrebe videokonferenc ter VoIP-prometa;
- MC – razred ”Mission Critical”, namenjen protokolom: DNS, TELNET, RDP, SSH, MAIL, IMAP, IMAPS, POP3S, LDAP, LDAPS in RADIUS;
- MC-HTTPS – poseben razred za promet HTTPS;
- BE – ”Best Effort” – običajni internetni promet;

- LBE – ”Less than Best Effort” – promet ”peer-to-peer” prenosov.

Dodatno je bilo v lanskem letu z mehanizmi QoS nadgrajeno tudi omrežje v hrbtenici. Čeprav so hitrosti in kapacitete povezav v hrbtenici večinoma krepko nad povprečnim prometom, je vseeno življenje za sistemske inženirje mirnejše ob zavesti, da bi tudi v primeru izrednega in nenavadnega povečanja prometa, raznih anomalij ali morda celo prekomernega prometa kot posledice DoS-napadov omrežje še vedno bilo sposobno zagotavljati ustrezen nivo kakovosti storitve.



SLIKA 18: SHEMA OBMOČIJ KAKOVOSTI (DIFFSERV) V OMREŽJU ARNES

V omrežju ARNES uporabljamo za zagotavljanje kakovosti storitev model DiffServ. Slednji omogoča nivojsko obravnavo različnega tipa prometa in s tem zagotavljanje primerne obdelave prometa znotraj QoS-omrežja. Paketi določenega tipa storitve pripadajo ustrezni "klasi", posamezna "klasa" pa dobi določeno obravnavo na vsaki napravi (PHB – per hop behaviour). Ta model je enostaven, saj zagotavlja ustrezno obravnavo paketov brez potrebe poznavanja stanja prometnih tokov v omrežju na vsakem mrežnem elementu in brez dodatne signalizacije med napravami.

Prednosti tega modela so:

- razširljivost in neodvisnost (ni potrebe po informaciji o stanju prometnih tokov);
- zmogljivost (za potrebe klasifikacije je paket pregledan samo enkrat, in sicer na meji QoS-omrežja);
- združljivost (tehnologijo podpirajo vsi proizvajalci);
- prilagodljivost (vsaka naprava lahko uporablja različne načine določene funkcionalnosti glede na to, kaj naprava podpira).

Med slabosti lahko uvrstimo, da zaradi ne-End-to-End modela rezervacije pasovne širine lahko pride do napak, če katera izmed vmesnih naprav ni pravilno nastavljena. Prav tako ni mehanizma CAC (*Call Admission Control*), ki bi zagotavljal, da npr. visokoprioritetne aplikacije ne bi odžirale pasovne širine ena drugi. Le-to je treba zagotoviti z dodatnimi mehanizmi.

Celotno funkcionalnost zagotavljanja kakovosti storitev zagotovimo z:

- razvrščanjem in označevanjem paketov (classification and marking),
- mehanizmi omejevanja in glajenja prometa (policing and shaping),
- selektivnim odmetavanjem paketov (congestion avoidance),
- mehanizmi obravnavanja vrst (congestion management – queuing).

V omrežju ARNES se trudimo uporabnikom zagotoviti najboljše, kar tehnologija trenutno omogoča, zato sledimo razvojnim smernicam in omrežje nenehno prilagajamo potrebam in zahtevam uporabnikov.

Enostavno in varno na IPv6

The easy and safe way to IPv6

Matjaž Straus Istenič

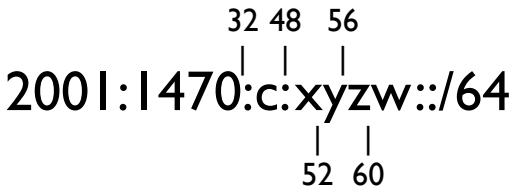
IPv6 je bil zasnovan z mislijo na skrbnika lokalnega omrežja. Delitev IPv6-omrežja je enostavnejša in preglednejša. Samodejna nastavitev omrežnih naprav je s primernimi orodji lahko dobro varovana in nadzorovana. Zavedati se moramo, da imajo nove in spremenjene lastnosti IP-protokola, ki sicer olajšajo delo skrbniku, velik vpliv na varnost v lokalnem omrežju. V praksi bomo morali znati združiti prednosti IPv6 z novimi varnostnimi izzivi in posodobiti svoja omrežja za sodobno in varno komunikacijo. IPv6 nam ponuja novo priložnost, da odpravimo pomanjkljivosti, ki so se prikradle v naša omrežja in storitve med dolgotrajnim krpanjem starega
IP-protokola.

IPv6 was designed with local systems administrators in mind. IPv6 subnetting is simple, transparent and straightforward. Autoconfiguration features that simplify the setup of IPv6 hosts can be properly secured and controlled with appropriate tools. As ever, new features and modified properties create new challenges, of which first hop security is one of the most important. Our goal is to use all the benefits of the new IP protocol, confront and solve the new security issues, and successfully upgrade our networks to provide modern, secure communications. IPv6 offers a new opportunity to correct deficiencies that have crept into our networks and services while mending the old IP protocol.

Enostavna delitev omrežja

Organizacija – članica omrežja ARNES pridobi del naslovnega prostora iz Arnesovega bloka `2001:1470::/32` v obsegu /48, npr. `2001:1470:c::/48`.[11] Tako velik segment naslovov zadošča za naslavljanje sistemov v več kot 65.000 lokalnih omrežjih, kar nam omogoča, da ga pregledno razdelimo po lokalnih omrežjih glede na njihovo namembnost. Sisteme v IPv4-omrežjih smo *številčili*, običajno v naraščajočem vrstnem redu, od IPv4-naslova prehoda, za katerega se zelo pogosto izbere prvi mogoči IPv4-naslov v omrežju, naprej. Z IPv6 je drugače – sisteme v IPv6-omrežjih pa *označujemo* s 64-bitnimi oznakami. Naslovni prostor organizacije delimo hierarhično na enako velike dele in se pri tem ne oziramo na varčevanje z naslovi. V taki delitvi se držimo pravila, po katerem naslovni prostor razmejimo tako, da je dolžina manjših delov vselej mnogokratnik štirih ali osmih bitov. Spodnja slika prikazuje, na katerih mestih se lahko odločimo za delitev naslovnega prostora /48 na lokalna omrežja /64.

[11] Večjim organizacijam, npr. univerzi, Arnes dodeli obseznejši blok IPv6-naslovov, tako da vsaka manjša enota, npr. fakulteta, dobi svoj /48.

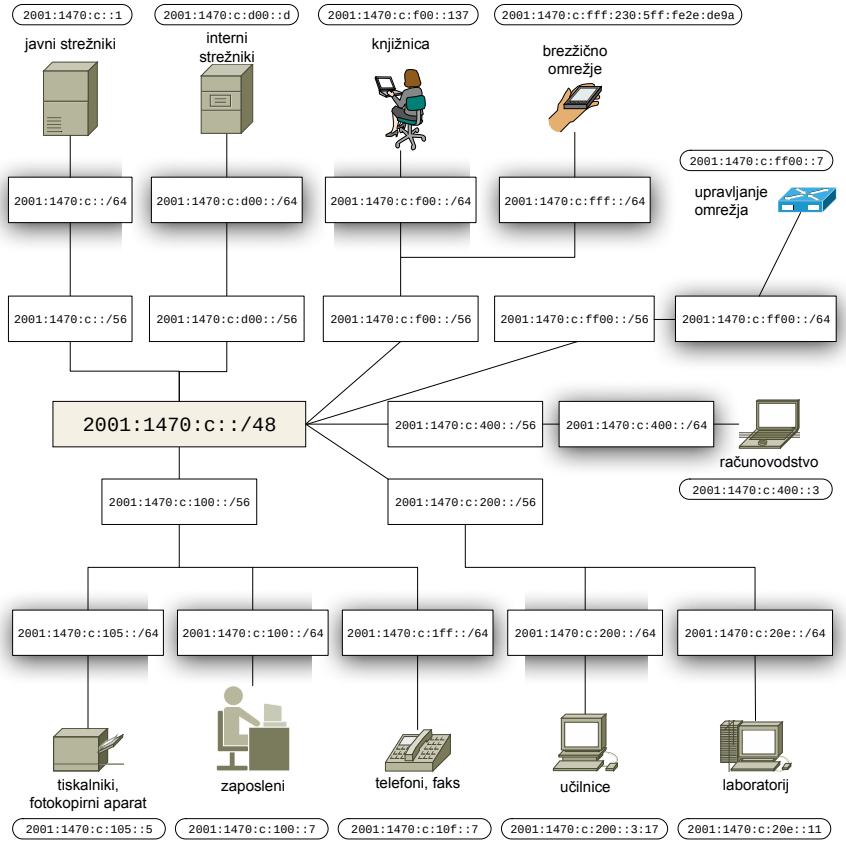


SLIKA 19: SHEMA IPV6-NASLOVA LOKALNEGA OMREŽJA. BLOK /48 RAZDELIMO HIERARHIČNO NA MANJŠE DELE, BODISI /52, /56 BODISI /60.

Zelo pregledna, praktična in razširljiva je delitev v treh nivojih. V prvem nivoju se odločimo za uporabo ene šestnajstine naslovnega prostora, drugo šestnajstino uporabimo za upravljanje omrežnih naprav, ostale pa prihranimo za morebitne oddaljene organizacijske enote, mobilne sisteme in druge razširitve v prihodnosti. Prostor nato razdelimo po skupinah uporabnikov, ki imajo skupno varnostno politiko. Štirje biti, ki jih uporabimo v tej delitvi, zadoščajo za delitev v 16 skupin. IPv6-naslov zapišemo takole:

`2001:1470:c:`*LSNN*`:`<64-bitna oznaka sistema>,

pri čemer za omrežja v organizaciji opustimo oznako *L* (*L* = 0), za omrežno infrastrukturo nastavimo *L* = f, ostalih oznak pa ne uporabimo. *S* je oznaka skupine in *NN* oznaka lokalnega omrežja. Primer take delitve prikazujeSlika 20.



SLIKA 20: PRIMER DELITVE IPV6-NASLOVNEGA PROSTORA: OMREŽJE ORGANIZACIJE `2001:1470:C::/48` JE RAZDELJENO NA 6 PODOMREŽIJ /56 ZA UPORABNIKE IN STREŽNIKE TER ENEGA ZA UPRAVLJANJE OMREŽNIH NAPRAV. IZ TEH DELOV JE IZBRAN NASLOVNI PROSTOR ZA POSAMEZNA LOKALNA OMREŽJA /64 (NA SLIKI SO NARISANA OSENČENO) IN KONČNE SISTEME.

Samodejna nastavitev omrežnih naprav

Z novo zasnovo delovanja v lokalnem omrežju prinaša IPv6 nekaj prednosti, ki poenostavljajo priklop in nastavitve omrežnih naprav:

- namesto posebnega protokola ARP (Address Resolution Protocol) so v IPv6 vgrajeni mehanizmi ND (Neighbour Discovery), ki slonijo na ICMP;
- IPv6 z mehanizmom SLAAC (Stateless Address Autoconfiguration) napravam omogoča samodejno določitev IP-naslova;
- iskanje usmerjevalnika in nastavitev privzetega prehoda poteka samodejno s poizvedbami po usmerjevalnikih RS (Router Solicitation) in oglaševanji usmerjevalnikov RA (Router Advertisements);
- z ND je predvidena tudi samodejna nastavitev DNS-strežnikov in domene;[12]
- protokol za samodejne nastavitve omrežnih naprav DHCP je temeljito predelan in posodobljen za IPv6.

Največjo poenostavitev za uporabnika prinaša mehanizem SLAAC z elementi ND, ki se pri tem uporabljajo (Hagen, 2006). Omrežna naprava si po priklopu v omrežje sama nastavi IPv6-naslove in privzeti prehod (nekoliko poenostavljen opis tega postopka je v okvirju 1), kar je očitna prednost pred IPv4, ob kateri pa se hitro sprožijo pomisleki glede varnosti. Kakšen IPv6-naslov ima določena naprava ob določenem času? Ali lahko sledimo spremembam tega naslova? SLAAC omogoča tudi delno anonimnost z izbiranjem naključnega IPv6-naslova (*Privacy Extension Address*). Le-to je dvorezen meč (Vyncke: IPv6 Security) – po eni strani ščiti anonimnost uporabnika, po drugi pa skrbniku otežuje sledljivost IPv6-naslovov in njihovih uporabnikov.

Z mehanizmi SLAAC ni mogoče nastaviti vseh parametrov omrežne naprave. Manjka celo nastavitev IP-naslovov rekurzivnih strežnikov DNS, ki je sicer že definirana kot standardna razširitev sporočil usmerjevalnikov (RA), vendar je v praksi zelo redko realizirana. To in pa želja po večjem nadzoru dodeljevanja IPv6-naslovov je pogost vzrok, da se v lokalnem omrežju omogoči DHCPv6. Poudarimo, da samodejna nastavitev z DHCPv6 ne deluje brez SLAAC, saj se omrežna naprava odloči za uporabo DHCP šele na podlagi sporočil usmerjevalnika (RA). Poleg tega DHCPv6 ne posreduje privzetega prehoda in velikosti omrežja.

[12] RFC 6106 (IPv6 Router Advertisement Options for DNS Configuration), nov. 2010.

1. Naprava določi svojo 64-bitno identifikacijsko oznako (ID) bodisi tako, da jo zgradi iz svojega omrežnega naslova (MAC), bodisi jo ustvari naključno. Za primer vzemimo ID `a:b:c:d`.
2. Naprava določi svoj lokalen (*link-local*) IPv6-naslov, tako da ID dopolni s predpono `fe80::/10`, npr. `fe80::a:b:c:d`. Zaradi enostavnosti bomo namenoma zamolčali preverjanje enoličnosti IPv6-naslovov (*Duplicate Address Detection*).
3. Naprava pošlje poizvedbo RS po usmerjevalnikih (*Router Solicitation*) na lokalen skupinski naslov "vsi usmerjevalniki" `ff02::2` (*all-routers link-local multicast address*). Če na poizvedbo ne dobi odgovora, se SLAAC zaključi in naprava ima zgolj lokalen naslov.
4. Naprava dobi odgovore RA-usmerjevalnikov v lokalnem omrežju (*Router Advertisements*). Za privzeti prehod nastavi lokalen naslov enega od njih.
5. Naprava zbere vse veljavne IPv6-predpone, ki so jih v svojih RA-sporočilih posredovali usmerjevalniki, in si za vsako od teh nastavi globalen IPv6-naslov, tako da predpono dopolni s svojim ID. Primer: s predpono `2001:1470:c:100::/64` se naprava naslovi z `2001:1470:c:100:a:b:c:d`.
6. Naprava preveri vsak RA, ali ima morda nastavljeni oznaki M (*managed address configuration flag*) ali O (*other configuration flag*).
    a. Če sta oznaki M in O obe enaki 0, se SLAAC zaključi brez uporabe DHCP.
    b. Če sta oznaki M in O obe enaki 1, je v lokalnem omrežju DHCPv6-strežnik ali posrednik za DHCPv6. Naprava pošlje DHCP-poizvedbo na skupinski naslov "vsi DHCP-posredniki" `ff02::1:2` (*all-DHCP-agents_and_servers link-local multicast address*). Če dobi odgovor, si nastavi dodatne IPv6-naslove in parametre, npr. naslov DNS-strežnika in zaključi s samodejnimi nastavitvami.
    c. Če je M = 1 in O = 0, je postopek podoben primeru M = O = 1, le da se DHCPv6 uporabi zgolj za nastavitev IP6-naslova in ne za druge nastavitve. Ta možnost je malo verjetna, saj je prednost DHCP prav v nastavitvah drugih omrežnih parametrov, kot npr. IPv6-naslova DNS-strežnika.
    d. Če je M = 0 in O = 1, potem je v lokalnem omrežju t. i. "stateless" DHCPv6-strežnik ali posrednik, ki skrbi le za dodatne omrežne parametre, npr. IPv6-naslov DNS-strežnika, in ne streže z IPv6-naslovi. Naprava pošlje DHCP-poizvedbo in če dobi odgovor, nastavi ustrezne parametre. Samodejne nastavitve so zaključene.

OKVIR 1: POTEK SAMODEJNE NASTAVITVE OMREŽNIH PARAMETROV IPV6-NAPRAVE

Zdi se, da smo ob vse prednosti samodejnih nastavitev, ki jih prinaša IPv6. Namesto DHCP, kot smo ga vajeni v IPv4-omrežjih, bomo morali skrbeti za dodaten
DHCP-strežnik za IPv6 ter za pravilno in kontrolirano delovanje samodejnih mehanizmov, kot je SLAAC. Brez skrbi – rešitev je v postopnosti uvajanja IPv6 skladno s tehničnim napredkom orodij za pomoč skrbnikom lokalnih IPv6-omrežij. V začetnih korakih se bomo odločili za:

- statične nastavitve omrežnih parametrov na strežnikih;
- statične nastavitve omrežnih parametrov na stacionarnih računalnikih;
- na vseh sistemih (Windows 7 in Vista, Mac OS X Lion) izklopimo naključno izbiranje IPv6-naslovov;
- na sistemih Windows izklopimo vmesnike tunelov (glej okvir 2).

```
netsh interface ipv6 set privacy state=disable
netsh interface ipv6 set global randomizeidentifiers=disabled
netsh interface ipv6 6to4 set state disabled default
netsh interface ipv6 isatap set state disabled
netsh interface ipv6 set teredo disabled
```

OKVIR 2: IZKLOP GENERIRANJA NAKLJUČNIH IPV6-NASLOVOV IN TUNELOV NA SISTEMU WINDOWS

S kontroliranimi ročnimi nastavitvami računalnikov v omrežje nismo vnesli dodatnega tveganja, vendar smo posodobitev na IPv6 morali omejiti zgolj na sisteme, ki so v našem upravljanju.

V naslednjem koraku bomo v omrežju omogočili samodejne nastavitve z mehanizmom SLAAC brez DHCPv6. Pred tem moramo poskrbeti za nadzor uporabe IPv6-naslovov na sistemih, ki jih upravljajo uporabniki sami, kot so prenosni računalniki, naprave v brezžičnem omrežju ipd. V času priprave tega prispevka je tak nadzor mogoč le na redki in dragi omrežni opremi, na voljo pa je tudi odprtokodni programski paket NDPMon (5), s katerim lahko učinkovito nadziramo samodejne nastavitve IPv6-naprav v lokalnem omrežju.[13]

Posodobitev na IPv6 zaključimo s postopno vpeljavo DHCPv6. V predhodnih korakih smo pridobili vse potrebne podatke za nastavitve DHCP-strežnika, predvsem ethernet naslove (MAC) vseh omrežnih naprav.

Varnost v lokalnem omrežju

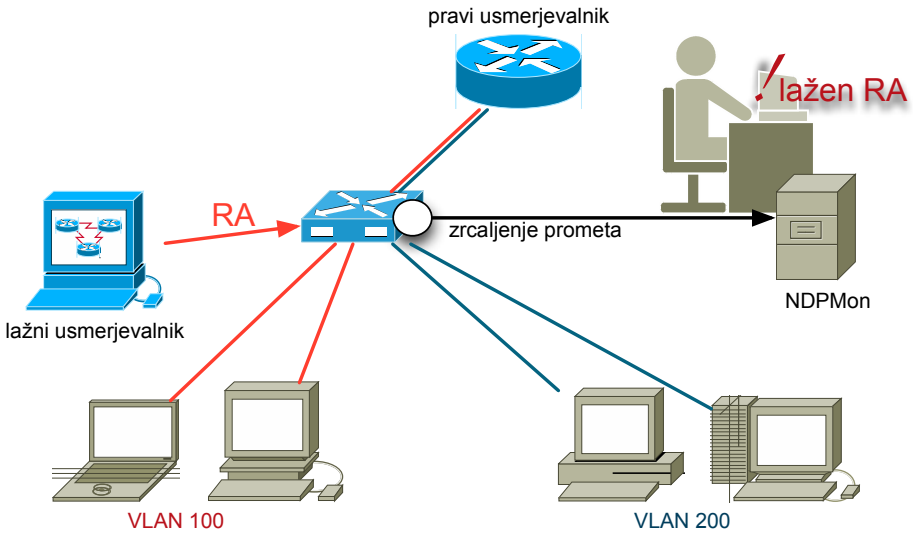
V IPv6 je vgrajenih veliko mehanizmov, ki omogočajo uporabo IPv6 v lokalnih omrežjih *ethernet*. Najpomembnejši so del protokola ND (*Neighbour Discovery Protocol*). Ti mehanizmi so preprosti in kot taki lahka tarča zlonamernih aktivnosti. SLAAC nima preverjanja identitete in overjanja ND-sporočil. Mogoče zlorabe se kar vrstijo (BRKSEC 3003):

[13] Delovanje NDPMon bomo prikazali na predavanju na Arnesovi konferenci v sklopu SIRikt 2012.

- lažni usmerjevalnik (do tega ”napada” pogosto pride nevede in ne zlonamerno, npr. sistem Windows z vključenim ”*Internet Connection Sharing*” se v omrežju lahko predstavi kot usmerjevalnik);
- lažna omrežna predpona med samodejno nastavitvijo naslova SLAAC;
- kraja IPv6-naslova med iskanjem sosedov (NS) in preverjanjem enoličnosti naslova (DAD) – sistem se ”zlaže”, da ima nek naslov;
- preusmerjanje prometa na napadalca (*Redirect*) – prisluškovanje;
- poplavljanje tabele sosedov (*Neighbour Cache Flooding*).

Proizvajalci omrežne opreme obljubljajo varovanje pred temi napadi, predvsem s posebno programsko opremo na (dragih!) stikalih, ki bo zagotavljala varnost IPv6-naprav na centraliziran način. Na seznamu lastnosti takega ”pametnega” stikala najdemo (v oklepaju navajam težko prevedljive angleške izraze):

- varovanje oglaševanja usmerjevalnika (RA-guard);
- nadzor NDP (NDP address glean/ inspection);
- skrb nad lastništvom naslovov (Address watch/ownership enforcement);
- spremljanje aktivnih naprav (Device Tracking);
- nadzor nad naslovi DHCP (Address Glean);
- varovanje DHCP (DHCP-guard);
- posrednik preverjanja enoličnosti naslova in iskanja sosedov (DAD/Resolution proxy);
- overjanje izvornega naslova (IP-Source-guard, SAVI);
- overjanje ciljnega naslova (IP-Destination-guard);
- posrednik DCHP (DHCP L2 relay).



SLIKA 21: NDPMON NADZIRA SPOROČILA V LOKALNEM OMREŽJU, ZAZNA IN SPOROČA NEPRAVILNOSTI.

Dokler te funkcije ne bodo podprte v cenovno dostopni komunikacijski opremi, se bomo morali zadovoljiti z nadzorom, kakršnega omogoča že prej omenjeni NDPMon (5). To orodje nadzira kontrolni promet v lokalnem omrežju (Slika 21) in zaznava ter sporoča naslednje nepravilnosti:

- napačen par naslovov ethernet MAC in IPv6;

- napačen ethernet MAC-naslov usmerjevalnika;
- napačen IPv6-naslov usmerjevalnika;
- napačno omrežno predpono;
- napačno preusmerjanje (*Redirect*);
- sporočilo lažnega usmerjevalnika;
- napad na mehanizem iskanja dvojnikov (*Duplicate Address Detection DoS*);
- menjave ethernet MAC-naslovov.

Poudariti moramo, da NDPMon zgolj nadzira omrežje in sporoča odkrite nepravilnosti, ne more pa jih preprečiti, kot to lahko storijo posebna stikala. Res je – varnostni izzivi v IPv6 so izjemno obsežni (Vyncke, BRKSEC 2003) (6), vendar ne smemo dovoliti, da postanejo ovira za uspešen prehod na novi IP-protokol. Začnimo postopoma, pridobivajmo znanje z uporabo dostopnih odprtokodnih rešitev in stopimo v korak z razvojem komercialne omrežne opreme. Na ta način bomo pravočasno pripravljeni za IPv6.

Viri

- Knjiga: Hagen, S. (2006): IPv6 Essentials, O'Reilly Media, Sebastopol, CA.
- Knjiga: Hogg S., Vyncke, E. (2009): IPv6 Security, Cisco Press, Indianapolis, USA.
- Predavanje: Vyncke, E., Cisco (2008): BRKSEC 2003, IPv6 Security Threats and Mitigations, Cisco Networkers, Barcelona, Španija (2009).
- Predavanje: Cisco (2010): BRKSEC 3003, Advanced IPv6 Security: Securing Link- Operations at First Hop, Cisco Live, London, UK (2011).
- Spletna stran: NDPMon http://ndpmon.sourceforge.net/ https://github.com/ayourtch/ndpmon-dot1q (31. 1. 2012).
- Spletna stran: The Hackers Choice http://freeworld.thc.org/thc-ipv6/ (31. 1. 2012).
- Spletna stran: Svetovna ”izstrelitev” IPv6 http://www.worldipv6launch.org/ (26. 1. 2012).

Sodobno upravljanje in nadzor omrežja

Network management and monitoring

Matej Vadnjal

Sodobno omrežje mora delovati zanesljivo. Zato moramo imeti dober pregled nad infrastrukturo in dogajanjem v omrežju, za kar potrebujemo kakovostna nadzorna orodja. V tem poglavju si bomo ogledali nekaj takih orodij, ki temeljijo na odprti kodi in s katerimi imamo izkušnje na Arnesu.

A modern network must also be reliable. We therefore need a good overview of what is happening in our network. To do so, we need quality monitoring tools. In this section we will examine some of those tools that are all *open source* and used by ARNES.Preverjanje delovanja omrežnih virov

Za vsako storitev in napravo v sodobnem omrežju moramo vedeti, ali deluje in ali deluje pravilno. Zato je treba delovanje teh virov redno preverjati. Icinga (1) je nadzorni sistem, ki ta preverjanja izvaja samodejno in operaterja obvešča o napakah.

Preverjanje je zasnovano modularno, tako da lahko nadzorujemo delovanje poljubne omrežne storitve ali naprave. Icinga že privzeto vsebuje precej modulov (v jeziku Icinge modulu rečemo *plugin*) za preverjanje najpogosteje uporabljanih omrežnih storitev, še veliko več pa jih lahko najdemo v spletni shrambi Monitoring Exchange (2). Če tam modula za svoje potrebe ne najdemo, ga lahko napišemo tudi sami.

Podobna modularna zasnova se uporablja tudi za obveščanje o napakah. Najpogosteje se uporabljajo moduli za pošiljanje elektronske pošte in SMS-sporočil , najdemo pa lahko tudi vrsto drugih bolj ali manj uporabnih vtičnikov.

Icinga administratorju omogoča nastavitev kupa parametrov, med pomembnejšimi pa so interval preverjanja, število neuspešnih rezultatov preverjanja za sprožitev alarma ter pogostost in časovna obdobja, v katerih se pošiljajo obvestila o alarmih.

Najpogostejša uporaba Icinge je preverjanje dosegljivosti omrežnih naprav. Na Arnesu za to uporabljamo modul *check_icmp*, ki na IP-naslov omrežne naprave pošlje ICMP-paket *echo-request* in čaka na ICMP-odgovor *echo-reply* – t. i. *ping*. Če naprava dve zaporedni minuti ni dosegljiva, se sproži alarm. Reakcija Icinge na alarm je odvisna od kategorije pomembnosti naprave. Ta kategorija vpliva na to, kako bo dežurni operater obveščen o alarmu. Za alarm na zelo pomembni napravi Icinga pošlje SMS na mobilni telefon dežurnega kadarkoli – podnevi ali ponoči. Pri srednje pomembnih napravah se pošlje SMS le podnevi, v nočnem času pa se pošlje elektronsko sporočilo, na katerega se dežurni odzove zjutraj. Za alarme na manj pomembnih napravah pa se vedno pošlje le elektronsko sporočilo.

Icinga v dnevniške zapise beleži vse spremembe stanj preverjanih storitev ali naprav. Iz teh zapisov lahko nato tudi pridobi podatke o razpoložljivosti storitve ali naprave in jih predstavi v poročilu (slika 14).

Host State Breakdowns:

State	Type / Reason	Time	% Total Time	% Known Time
UP	Unscheduled	6d 21h 16m 43s	92.612%	92.612%
	Scheduled	0d 0h 0m 0s	0.000%	0.000%
	Total	6d 21h 16m 43s	92.612%	92.612%
DOWN	Unscheduled	0d 13h 11m 6s	7.388%	7.388%
	Scheduled	0d 0h 0m 0s	0.000%	0.000%
	Total	0d 13h 11m 6s	7.388%	7.388%
UNREACHABLE	Unscheduled	0d 0h 0m 0s	0.000%	0.000%
	Scheduled	0d 0h 0m 0s	0.000%	0.000%
	Total	0d 0h 0m 0s	0.000%	0.000%
Undetermined	1.5.1 Not Running	0d 0h 0m 0s	0.000%	
	Insufficient Data	0d 0h 0m 0s	0.000%	
	Total	0d 0h 0m 0s	0.000%	
All	Total	7d 10h 27m 49s	100.000%	100.000%

SLIKA 22: POROČILO O RAZPOLOŽLJIVOSTI NAPRAVE

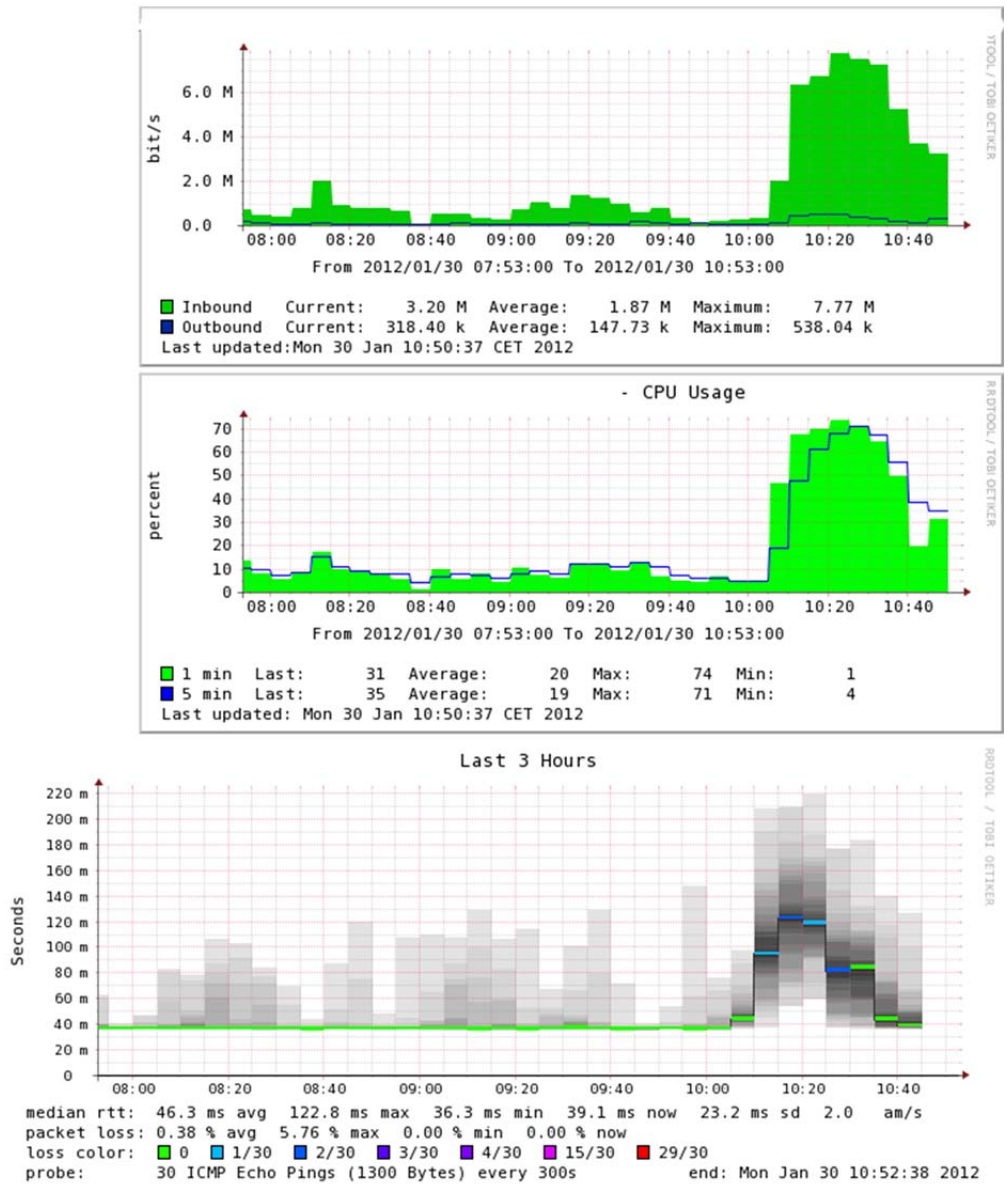
Obremenitev omrežnih virov

Za zagotavljanje kakovostnih storitev ni dovolj le, da vemo, ali storitev deluje ali ne, temveč moramo vedeti tudi, koliko je uporabljana. Lep primer je zasedenost povezave iz omrežja v internet. Če to količino narišemo na grafu, lahko hitro razberemo povprečno obremenitev povezave skozi čas in tako predvidimo, kdaj bo potrebna nadgradnja povezave.

Na Arnesu za zbiranje in prikaz takih podatkov uporabljamo Cacti (3). Cacti je primarno orodje za risanje grafov različnih omrežnih parametrov, kot bomo videli kasneje, pa zna še veliko več. S spletnim vmesnikom določimo, kateri omrežni parameter bi radi spremljali, in Cacti začne v ozadju pobirati podatke iz omrežne naprave ter jih shranjuje v datoteke RRD (4). Na grafu lahko nato spremljamo, kako se vrednost tega parametra spreminja skozi čas.

Najpogosteje uporabljamo Cacti, ko bi radi videli, koliko prometa se pretaka skozi omrežne vmesnike naših stikal in usmerjevalnikov. Seveda pa Cacti podpira risanje tudi vrste drugih parametrov, na primer obremenitev procesorja (CPU), zasedenost diska, avtonomijo brezprekinitvenega napajanja in še veliko drugih (slika 15). Cacti pridobiva te vrednosti iz omrežnih naprav prek protokola SNMP (5), lahko pa tudi napišemo lastno funkcijo, ki bo prišla do rezultata na poljuben način in ga vrnila Cactiju.

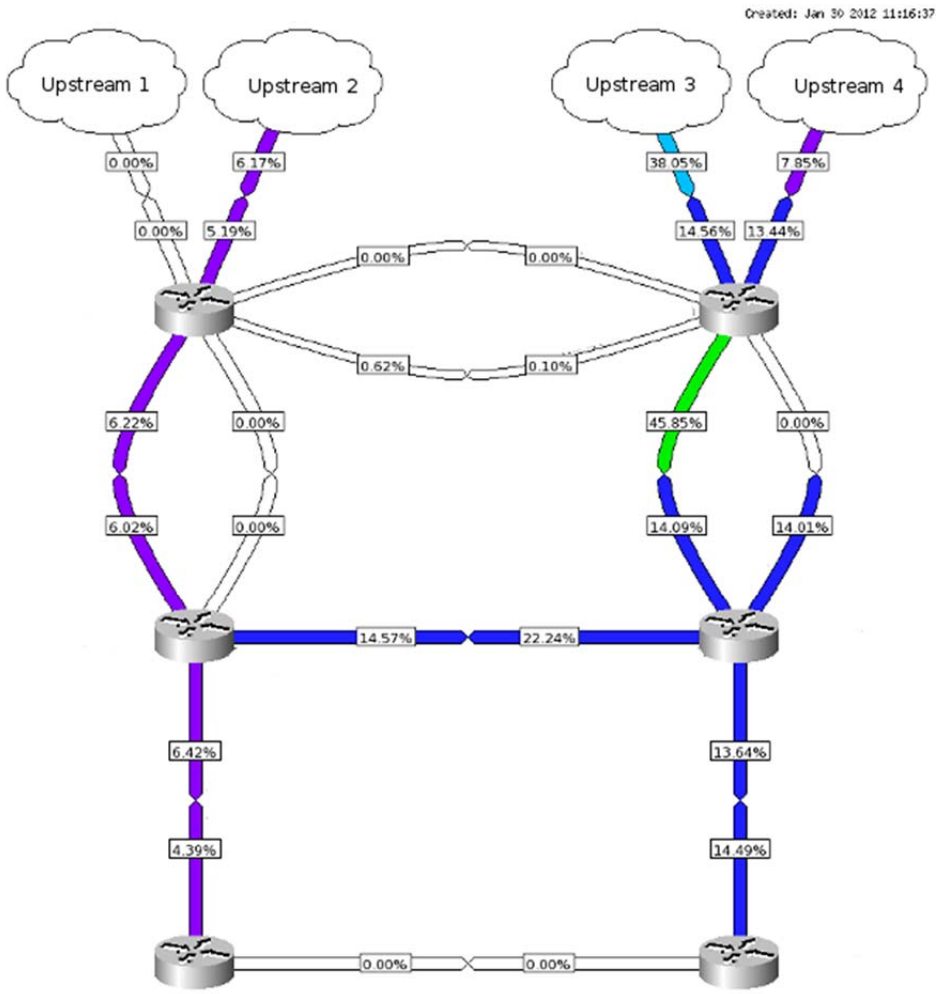
Z vgrajenim spletnim vmesnikom lahko pregledujemo grafe. Omogoča nam, da izbor prikazanih grafov omejimo z iskalnimi parametri in da izberemo časovno obdobje, ki naj bo prikazano. Tako lahko hitro primerjamo odčitke različnih grafov v časovnem intervalu, ki nas zanima, kar je zelo uporabno, kadar poskušamo odkriti vzrok slabšega delovanja v delu omrežja.



Slika 15: Primerjava različnih veličin v istem časovnem obdobju. Na prvem grafu je promet n vmesniku usmerjevalnika, na drugem obremenitev procesorja, na tretjem pa zakasnitev in izgube na povezavi do usmerjevalnika. Jasno je razvidno, da ima večja količina prometa negativen vpliv na obremenitev procesorja usmerjevalnika, zaradi česar se začnejo pojavljati tudi izgube paketov.

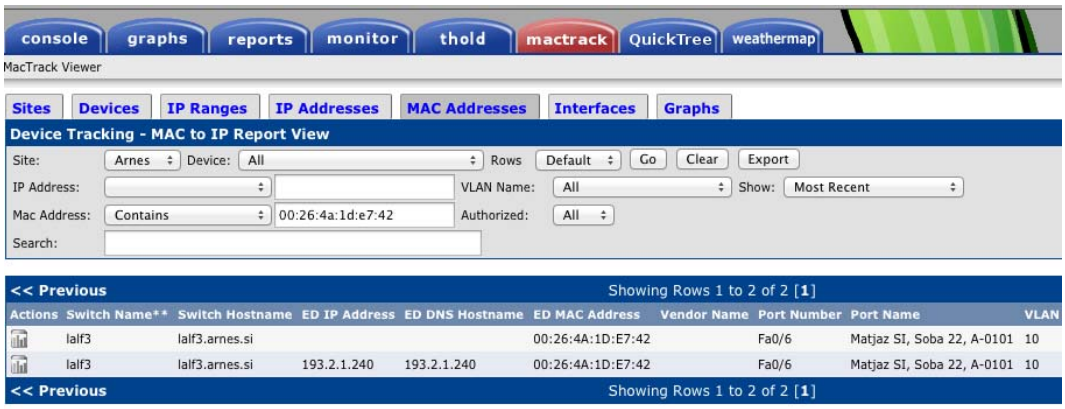
Cacti podpira tudi dodatne module, ki razširijo njegovo funkcionalnost. Nekaj popularnejših, ki jih uporabljamo tudi na Arnesu:

- Network Weathermap – vrednosti parametrov, ki jih Cacti zbira, prikaže na shemi omrežja. S tem orodjem na sliki določimo usmerjevalnike in povezave med njimi. Cacti nato vsako povezavo med usmerjevalniki obarva v barvi, ki ustreza zasedenosti povezave. Tako lahko hitro opazimo, če je katera povezava v omrežju preobremenjena (slika 16).



Slika 23: Trenutna zasedenost povezav v delu omrežja ARNES

- **ReportIt** – dodatek, ki generira tabele s poročili iz podatkov, zbranih v Cactiju. Tipičen primer uporabe je poročilo o prenesenem prometu v omrežje in iz njega v danem obdobju. ReportIt lahko nastavimo tudi tako, da nam sam periodično pripravi poročilo za pretekli mesec in ga pošlje po elektronski pošti.
- **Mactrack** – orodje, ki pobira podatke o vmesnikih, ethernet MAC in IP-naslovih ter DNS-zapisih iz omrežja in jih poveže v skupne zapise. Tako lahko z iskanjem po DNS-imenu naprave najdemo njen IP- in MAC-naslov ter vmesnik stikala, na katerega je priključena (slika 17).



SLIKA 17: CACTI MACTRACK

V tem delu smo na kratko predstavili dve orodji, ki upravljavcu omrežja lajšata zagotavljanje kakovostnih storitev. Seveda je na voljo tudi precej alternativnih rešitev, tako komercialnih kot tudi brezplačnih. Opisani orodji po Arnesovem mnenju ponujata najboljše razmerje med enostavnostjo uporabe in fleksibilnostjo.

Spletni viri

1. http://www.icinga.org/
2. https://www.monitoringexchange.org/
3. http://www.cacti.net/
4. http://www.rrdtool.org/
5. https://en.wikipedia.org/wiki/SNMP

Zaključek

Prispevek smo začeli s skrbjo za urejenost omrežne infrastrukture in dokumentacije, nadaljevali s kratkim opisom sodobne prenosne tehnologije s tehnologijo WDM in se nato posvetili zagotavljanju kakovosti komunikacije z mehanizmi QoS. Kakovostna komunikacija je tudi sodobna in varna, zato smo v nadaljevanju opisali nekaj osnovnih lastnosti novega protokola IPv6 s poudarkom na varovanju lokalnega omrežja. V vseh opisanih plasteh, od električnega napajanja preko optičnega vlakna do internetnega protokola, je potreben zanesljiv nadzor. Zato zaključujemo z opisom nekaj odprtokodnih upravljavskih in nadzornih orodij.

V omrežju ARNES uspešno združujemo opisano tehnologijo v enovito storitev z imenom ”kakovostna komunikacija”.