Univerza v Ljubljani
Fakulteta za računalništvo in informatiko

Marko Dolničar

DINAMIČNO RAZVRŠČANJE UPORABNIKOV BREZŽIČNEGA OMREŽJA EDUROAM V LOČENA OMREŽJA VLAN

diplomsko delo

visokošolski strokovni študijski program prve stopnje računalništvo in informatika

Mentor: doc. dr. Mojca Ciglarič

Ljubljana 2013

Univerza v Ljubljani
Fakulteta za računalništvo in informatiko

Tržaška 25
1001 Ljubljana, Slovenija
telefon: 01 476 84 11
01 476 83 87
faks: 01 426 46 47
01 476 87 11
www.fri.uni-lj.si
e-mail: dekanat@fri.uni-lj.si

Št. naloge: 00413 / 2013
Datum: 8.4.2013

Univerza v Ljubljani, Fakulteta za računalništvo in informatiko izdaja naslednjo nalogo:

Kandidat: **MARKO DOLNIČAR**

Naslov: **DINAMIČNO RAZVRŠČANJE UPORABNIKOV BREZŽIČNEGA OMREŽJA EDUROAM V LOČENA OMREZJA VLAN**
DYNAMIC ASSIGNMENT OF EDUROAM USERS TO SEPARATE VIRTUAL LANS

Vrsta naloge: Diplomsko delo visokošolskega strokovnega študija prve stopnje

Tematika naloge:

Opišite zgradbo in delovanje brezžičnega omrežja Eduroam. Opišite omrežne tehnologije in protokole, ki jih uporabljamo v tem omrežju. Na kratko navedite tudi tehnična določila, ki jo mora izpolnjevati omrežna oprema, ki jo uporablja Eduroam. Nato raziščite, kateri od znanih napadov na brezžična omrežja predstavljajo grožnjo tudi uporabnikom Eduroama. Opišite anatomijo teh napadov in pojasnite ranljivosti protokolov, ki omogočajo, da so napadi dejansko izvedljivi. Navedite vaše predloge, kako bi lahko posamezne napade preprečili ali pa zmanjšali njihovo tveganje. Nato postavite testno okolje, ki bo zgrajeno po vzoru Eduroama. Reproducirajte izbrane napade, da se prepričate, če so resnično izvedljivi. Nato v testnem okolju uveljavite varnostne ukrepe, ki ste jih predlagali v prejšnjem koraku, in ponovno poskusite izvajati izbrane napade. Rezultate svojih testov dokumentirajte in kritično komentirajte. Navedite, kaj bi pomenilo za Eduroam, če bi hoteli tovrstne varnostne ukrepe implementirati v celotnem omrežju.

Mentor: M. Ciglarič
doc. dr. Mojca Ciglarič

Fakulteta za računalništvo in informatiko • UNIVERZA V LJUBLJANI • 2

Dekan:
prof. dr. Nikolaj Zimic

Izjava o avtorstvu diplomskega dela

Spodaj podpisani Marko Dolničar, z vpisno številko **63090433**, sem avtor diplomskega dela z naslovom:

DINAMIČNO RAZVRŠČANJE UPORABNIKOV BREZŽIČNEGA OMREŽJA EDUROAM V LOČENA OMREŽJA VLAN

S svojim podpisom zagotavljam, da:

- sem diplomsko delo izdelal samostojno pod mentorstvom doc. dr. Mojce Ciglarič,
- so elektronska oblika diplomskega dela, naslov (slov., angl.), povzetek (slov., angl.) ter ključne besede (slov., angl.) identični s tiskano obliko diplomskega dela
- soglašam z javno objavo elektronske oblike diplomskega dela v zbirki "Dela FRI".

V Ljubljani, dne 11. novembra 2013 Podpis avtorja:

Zahvaljujem se materi, ki mi je omogočila študij, podjetju Telesistemi d.o.o. in zavodu Arnes, za posojeno opremo ter ženi in ostalim, ki so mi pri študiju kakorkoli pomagali. Zahvaljujem se tudi mentorici doc. dr. Mojci Ciglarič, za mentorstvo pri pisanju te diplomske naloge.

Posebno zahvalo namenjam Andreju Krevlu, ki me je navdušil nad omrežno varnostjo in si vzel čas za dodatne projekte.

Dvastu

Kazalo

Povzetek

V sklopu diplomske naloge smo preučili brezžično omrežje eduroam, ki zaradi mehanizmov za avtentikacijo in avtorizacijo uporabnikov pred priključitvijo v omrežje, velja za varno brezžično omrežje. Kljub temu pa nima mehanizmov za varovanje priključenih uporabnikov pred zlonamernimi uporabniki priključenimi v isto omrežje. Zaradi varnostnih pomanjkljivosti protokolov uporabljenih v omrežju eduroam lahko zlonamerni uporabnik omrežja s prestrezanjem podatkov pride do zaupnih podatkov drugih uporabnikov. Po vzpostavitvi testnega omrežja z enakimi lastnostmi kot jih ima omrežje eduroam, smo uspešno preizkusili nekaj napadov na povezavni plasti. Na koncu predstavimo rešitev, ki uporabnike loči med seboj v ločena podomrežja z uporabo VLAN-ov, s tem pa prepreči napade na povezavni plasti. Rešitev tudi kritično ovrednotimo.

Ključne besede: eduroam, varnost, FreeRADIUS, VLAN, stikalo, dostopna točka, MITM, zastrupljanje ARP.

Abstract

The aim of the diploma thesis was to thoroughly study the eduroam network, which is, with its authentication and authorisation mechanisms, considered a secure service. However, the network lacks mechanisms to protect the logged-in users from malicious users on the same network. Security vulnerability as a result of insecure protocols of eduroam may result in any malicious user being able to access other users' confidential information. After having set up a test network identical to eduroam, we successfully tested it with some attacks on the Data Link layer. Finally, we provide a solution to enhance security, by separating the users into individual sub networks using VLANs and consequently preventing the attacks on Data Link layer.

Keywords: eduroam, security, FreeRADIUS, VLAN, switch, access point, MITM, ARP poisoning.

Poglavje 1

Uvod

Brezžično omrežje eduroam velja za varno omrežje, saj lahko do omrežja dostopajo le avtenticirani in avtorizirani uporabniki. V omrežju je poskrbljeno tudi za varen prenos uporabniškega imena in gesla od uporabnika do strežnika, ki uporabniško ime in geslo preveri. Kljub varnemu in nadzorovanemu dostopu do omrežja, pa omrežje ne nudi mehanizmov, ki bi zaščitili uporabnika po priključitvi v omrežje. V omrežju se lahko nahaja kakšen zlonameren uporabnik, ki bi rad prestrezal promet in tako prišel do zaupnih podatkov drugih uporabnikov. Omrežje eduroam je sicer nastavljeno tako, da se nekateri incidenti beležijo, vendar pa ni avtomatiziranega obveščanja administratorjev ali uporabnikov o incidentih.

V okviru diplomske naloge smo vzpostavili testno omrežje po vzorčnih navodilih zavoda Arnes in nato izvedli nekaj napadov, ki izkoriščajo protokole povezavne in omrežne plasti. Nekateri izmed predstavljenih napadov imajo za posledico onemogočanje storitve, nekateri pa prestrezanje uporabnikovega prometa (MITM).

Razvili smo rešitev, ki uporabnike brezžičnega omrežja eduroam loči med seboj. Vsak uporabnik je tako sam v svojem navideznem omrežju, kar prepreči napade na povezavni plasti - tudi prestrezanje prometa drugih uporabnikov.

V drugem poglavju bomo predstavili protokole, ki se uporabljajo v om-

režju eduroam in so pomembni za razumevanje delovanja napadov oziroma predstavljene rešitve. Tretje poglavje opisuje varnostne pomanjkljivosti v omrežjih eduroam v Sloveniji in nekatere napade, ki so zaradi njih možni. Strojna in programska oprema, uporabljena v testnem omrežju, je predstavljena v četrtem poglavju, peto poglavje pa podrobneje predstavi našo rešitev z uporabo ločenih VLAN-ov.

Poglavje 2

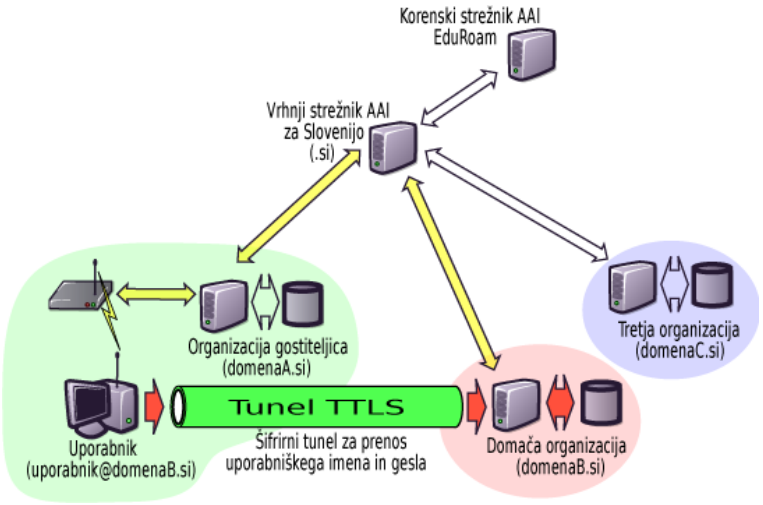
Eduroam

Eduroam (EDUcational ROAMing) je mednarodna federacija brezžičnih omrežij za uporabnike iz izobraževalne in raziskovalne sfere. Študenti, učenci, pedagogi, raziskovalci in drugi lahko uporabljajo vsako brezžično omrežje eduroam, v Sloveniji ali tujini. Za uporabo je potrebno le vključiti napravo z brezžičnim vmesnikom in to ne glede na to kje: na domači ustanovi ali na primer na Univerzi v Edinburgu [1].

Začetek omrežja eduroam sega v leto 2002, ko je Klaas Wierenga predlagal standard 802.1X za mednarodno rešitev brezžičnih omrežij na izobraževalnih ustanovah [13].

Ta rešitev uporablja standard 802.1x in hierarhijo posredniških strežnikov RADIUS proxy. Vloga posredniških strežnikov je, da posredujejo uporabnikove poverilnice do domače organizacije, kjer se opravi avtentikacija in avtorizacija. Domačo organizacijo določa "kraljestvo"(ang. realm), ki je pripona uporabniškem imenu, ločena z znakom @.

Pri uporabniku *izmisljeni.uporabnik@uni-lj.si* je domača organizacija uni-lj.si. Od koderkoli se ta uporabnik poveže v omrežje eduroam, se njegovo uporabniško ime in geslo po varni povezavi (šifrirano, TLS) prenese do domače organizacije, ki opravi avtentikacijo in avtorizacijo, rezultat pa vrne strežniku Radius pri organizaciji gostiteljici. Organizacija gostiteljica tako izve le ali naj uporabniku dovoli dostop do omrežja ali ne, ne pa tudi njegovih poveril-



Slika 2.1: Hierarhija strežnikov Radius

nic.

Vsaka organizacija ki se želi priključiti v eduroam, mora vzpostaviti strežnik Radius in ga povezati z nacionalnim vrhnjim strežnikom (NTLR - National Top Level Radius), ta pa je nato povezan z regionalnim vrhnjim strežnikom Radius (slika 2.1). Delovanje lahko primerjamo s sistemom DNS (Domain Name System).

Nacionalne strežnike Radius praviloma upravljajo nacionalna raziskovalna in izobraževalna omrežja – v Sloveniji je to Akademska in raziskovalna mreža Slovenije (Arnes). Arnes testira posamezne tipe brezžične opreme, nudi pomoč, vzdržuje vzorčne nastavitve in sistem eduroam na odprtokodni tehnološki osnovi Linux CentOS, OpenLDAP ter FreeRADIUS [2].

2.1 802.1X

802.1X je standard, ki zagotavlja avtentikacijski mehanizem napravam, ki se želijo priključiti v omrežje. Definira enkapsulacijo protokola EAP over LAN (EAPOL). 802.1X avtentikacijo sestavljajo tri strani: odjemalec, avtentikator in avtentikacijski strežnik. Odjemalec je naprava, ki zahteva avtentika-

cijo (računalnik, prenosnik, pametni telefon, ...). Avtentikator je omrežno stikalo ali dostopna točka pri brezžični komunikaciji, avtentikacijski strežnik pa je navadno strežnik RADIUS [3]. Avtentikator ne posreduje nikakršnega prometa med odjemalcem in omrežjem, dokler je odjemalec neavtenticiran. Izjema je promet 802.1X, ki omogoča avtentikacijo odjemalca.

Delovanje protokola:

1. Ko avtentikator zazna novega odjemalca, mu periodično pošilja pakete z zahtevo po identiteti.

2. Odjemalec odgovori na zahtevo avtentikatorju, ki jo posreduje do avtentikacijskega strežnika.

3. Avtentikacijski strežnik nato pošlje izziv odjemalcu, preko avtentikatorja. V tej fazi avtentikacijski strežnik predlaga način avtentikacije, ki naj jo uporabi odjemalec. Če se odjemalec strinja s predlagano metodo EAP (način avtentikacije), jo začne uporabljati in avtentikacijskemu strežniku pošlje zahtevo EAP. Odjemalec lahko tudi zavrne metodo EAP, če je ne podpira. V takem primeru odjemalec sporoči strežniku metode, ki jih podpira.

4. Strežnik bodisi dovoli bodisi zavrne dostop do omrežja.

2.2 RADIUS

Remote Authentication Dial In User Service je protokol, ki skrbi za avtentikacijo, avtorizacijo in beleženje.

Protokol deluje na modelu odjemalec/strežnik. Ponudnik storitve (NAS – Network Access Server), na primer brezžična dostopna točka, ima vlogo odjemalca RADIUS. Odjemalec posreduje informacije o uporabniku do strežnika RADIUS in na podlagi odgovorov strežnika ustrezno ukrepa. Strežnik sprejema zahteve, avtenticira uporabnike in posreduje konfiguracijske nastavitve odjemalcu, ki zagotavlja storitev uporabniku. Strežnik RADIUS je lahko

tudi v vlogi odjemalca drugemu strežniku RADIUS (posredniški strežnik RADIUS).

Odjemalec in strežnik si delita skupno skrivnost (shared secret), ki se nikoli ne pošilja v omrežje. Ta skupna skrivnost se, v primeru PAP, uporabi kot šifrirni ključ med avtentikatorjem in strežnikom RADIUS, pri pošiljanju gesel [14].

Transakcije so sestavljene iz trojk različnih dolžin, po modelu (atribut, dolžina, vrednost). Tako lahko dodamo nove vrednosti atributov, brez motenja obstoječe implementacije. Zaradi razširljivosti je uporabljen tudi v omrežju eduroam.

Strežnik RADIUS podpira različne avtentikacijske metode, kot so PPP PAP, CHAP, Unix login in druge [3].

Arnes svetuje uporabo EAP-TTLS + PAP zaradi najboljšega razmerja med varnostjo in uporabnostjo ter zaradi podpore odjemalcu eduroamclient, ki nastavi brezžično povezavo eduroam v operacijskih sistemih Windows ter namesti digitalna potrdila [2].

Protokol določa sporočila, ki si jih pošiljata odjemalec in strežnik. Vrste sporočil:

- Access-Request

  V sporočilu Acceess-Request se nahajajo podatki o uporabniku - uporabniško ime in geslo. Poleg informacij o uporabniku mora biti v takem sporočilu tudi neka informacija o ponudniku storitve - napravi preko katere se želi uporabnik povezati. Lahko se uporabi naslov IP.

- Access-Accept

  S sporočilom Access-Accept strežnik RADIUS pošlje podatke, ki omogočijo storitev uporabniku.

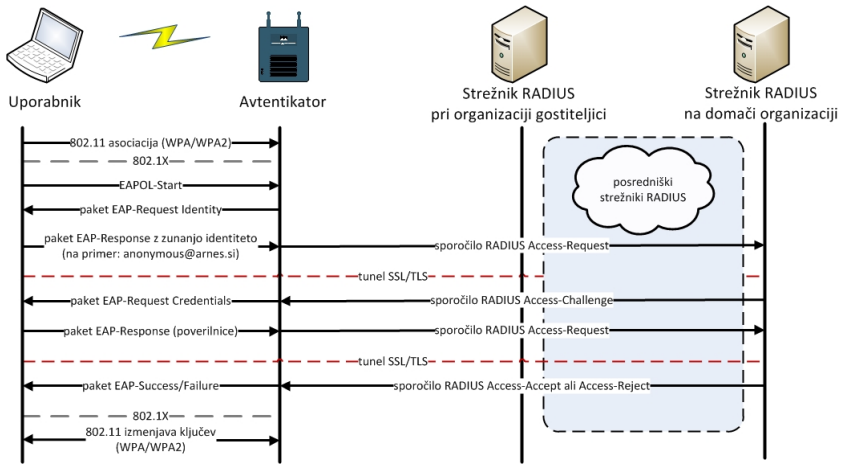
- Access-Reject

  Če kateri od podatkov, ki jih je strežnik dobil v sporočilu Access-Request, ni sprejemljiv (na primer napačno geslo), strežnik odgovori

s sporočilom Access-Reject. V takem sporočilu so lahko tudi dodatni podatki, ki jih ponudnik storitve lahko prikaže uporabniku.

- Access-Challenge

  V primeru, da strežnik RADIUS od uporabnika zahteva, da odgovori na izziv, mu pošlje sporočilo Access-Challenge [10].



Slika 2.2: Prijava v eduroam preko posredniškega strežnika RADIUS

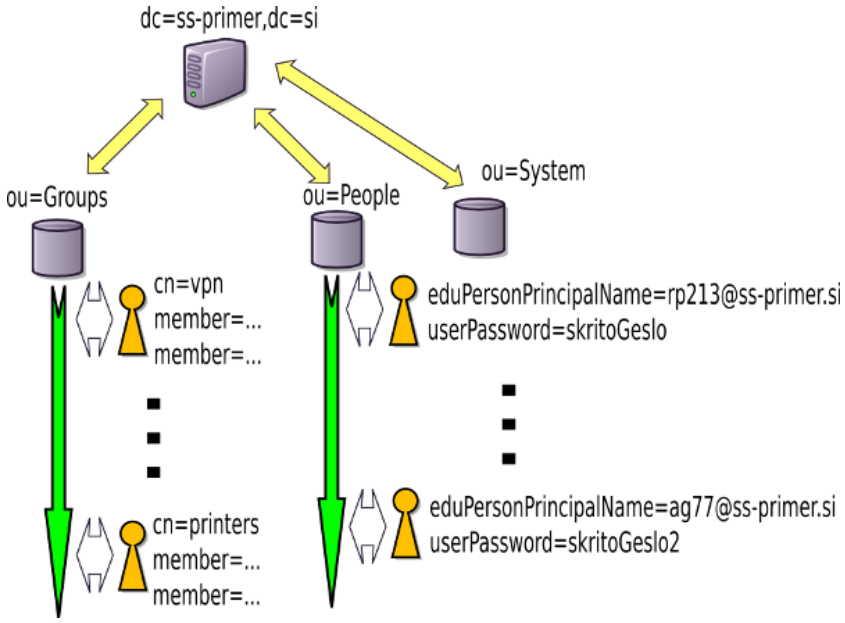
Na sliki 2.2 je prikazan postopek prijave uporabnika pri organizaciji gostiteljici. Najprej se uporabnik asociira na dostopno točko in dostopni točki javi, da se želi prijaviti, s paketom EAPOL-Start. Dostopna točka na ta paket odgovori z zahtevo po identitet (EAP-Request Identity), na katero uporabnik odgovori z anonimno identiteto - paket EAP Response. Dostopna točka to v sporočilu Access-Request posreduje strežniku RADIUS. Na podlagi pripone v anonimni identiteti strežnik RADIUS ve kam posredovati zahtevo Access-Request. Ko zahtevo prejme strežnik RADIUS na domači organizaciji, se vzpostavi tunel SSL/TLS preko katerega domač strežnik RADIUS zahteva uporabniško ime in geslo uporabnika s sporočilom Access-Challenge. Dostopna točka, ki prejme sporočilo Access-Challenge, ga zapakira v paket EAP-Request Credentials in pošlje uporabniku. Uporabnik sporoči podatke v paketu EAP-Response Identity, dostopna točka pa jih posreduje

strežniku RADIUS v novem sporočilu Access-Request. Če strežnik dovoli dostop do omrežja, pošlje dostopni točki sporočilo Access-Accept, le-ta pa uporabniku posreduje EAP-Success. V primeru da strežnik dostop zavrne, pošlje sporočilo Access-Reject.

2.3 Imenik LDAP

Imenik LDAP (Lightweight Directory Access Protocol) je baza podatkov, ki pa za razliko od baz SQL ni relacijska, ampak je organizirana v drevesno strukturo, kot kaže slika 2.3. Optimizirana je za branje in ne za pogosto vpisovanje podatkov, definicije podatkov pa niso poljubne ampak so vpisane v shemah.

Imenik LDAP hrani podatke o različnih objektih v resničnem ali računalniškem svetu. Primarno se uporablja za shranjevanje podatkov o uporabnikih, skupinah uporabnikov ter podatkih o uporabnikih, ki jih potrebujejo računalniški sistemi [4].



Slika 2.3: DIT - Directory Information Tree

Na sliki 2.3 je prikazana struktura drevesa (DIT - Directory Information Tree). Na vrhu je koren drevesa, ki vsebuje skupine. Skupinam pravimo tudi organizacijske enote (angl. Organizational unit / OU) in vsebujejo objekte oziroma vnose [4].

Sheme določajo, kako so poimenovani posamezni atributi objekta, v grobem, kakšne vrednosti lahko zajemajo in na kakšen način se išče po njih (število ali niz, ali je občutljiv na velike ali male črke in podobno). Če želimo torej v imenik dodati nove objekte ali zaradi dodatne aplikacije posodobiti atribute, naložimo novo shemo. Katero shemo uporabimo, je tipično zapisano v dokumentaciji aplikacije, pogostokrat pa se uporabljajo kar privzete, standardizirane sheme, ki so prisotne že v osnovni postavitvi imenika LDAP [4]. Del sheme, natančneje opis atributov eduPersonAffiliation in eduPersonNickname, je prikazan na izpisu 2.1.

```
# eduPersonAffiliation
# Specifies a person's relationship(s) to the institution in
# broad categories such as student, faculty, staff, alum, etc
   .
attributetype ( 1.3.6.1.4.1.5923.1.1.1.1
        NAME 'eduPersonAffiliation'
        DESC 'eduPerson per Internet2 and EDUCAUSE'
        EQUALITY caseIgnoreMatch
        SUBSTR caseIgnoreSubstringsMatch
        SYNTAX '1.3.6.1.4.1.1466.115.121.1.15' )

# eduPersonNickname
# Specifies a person's nickname, or the informal name
# by which they are accustomed to be hailed.
attributetype ( 1.3.6.1.4.1.5923.1.1.1.2
        NAME 'eduPersonNickname'
        DESC 'eduPerson per Internet2 and EDUCAUSE'
        EQUALITY caseIgnoreMatch
        SUBSTR caseIgnoreSubstringsMatch
        SYNTAX '1.3.6.1.4.1.1466.115.121.1.15' )
```

Izpis 2.1: Opis dveh atributov iz sheme EduPerson

2.4 Protokol ARP

Omrežne naprave (računalniki, stikala, dostopne točke, ...) vzdržujejo tabelo ARP (Address Resolution Protocol), v kateri hranijo povezave naslovov povezavne plasti in naslovov IP. Tako vedo, na kateri naslov povezavne plasti poslati podatke, ki so namenjeni ustreznemu naslovu IP v istem podomrežju. Protokol ima dve vrsti sporočil: zahtevo in odgovor. Naprava, ki želi izvedeti naslov povezavne plasti druge naprave, pozna pa njen naslov IP, pošlje zahtevo na naslov broadcast. V zahtevi pove, kateri naslov IP, oziroma katera naprava s tem naslovom, naj ji sporoči naslov povezavne plasti. Ker je bila zahteva poslana na naslov broadcast, so to zahtevo sprejele vse naprave v omrežju. Naprava, katere naslov IP je bil v zahtevi, nato pošlje odgovor s svojim naslovom povezavne plasti direktno napravi, ki ga je zahtevala [6].

Ko je uporabnik povezan v omrežje eduroam, uporablja protokol ARP za razreševanje strojnih naslovov drugih uporabnikov in omrežnih naprav.

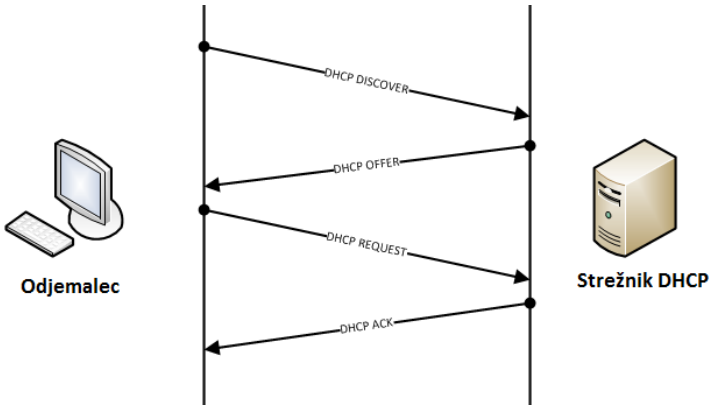
2.5 Protokol DHCP

Protokol DHCP (Dynamic Host Control Protocol) skrbi za dodeljevanje naslovov IP uporabnikom. Naprava, ki še nima naslova IP, prosi strežnik DHCP, naj ji ga dodeli. Protokol določa sporočila, ki so opisana spodaj, zaporedje sporočil pa je prikazano na sliki 2.4.

DHCPDISCOVER: Ker naprava (odjemalec) ob priklopu v omrežje ne ve na katerem naslovu se nahaja strežnik DHCP, najprej pošlje poizvedbo. Pošlje jo na naslov broadcast, da jo sprejmejo vse naprave v omrežju, med njimi tudi strežnik DHCP.

DHCPOFFER: Strežnik DHCP na poizvedbo odgovori s ponudbo naslova IP, masko podomrežja, privzetim prehodom in morebitnimi drugimi podatki (naslov strežnika DNS), če jih je odjemalec zahteval v poizvedbi. Prav tako strežnik odjemalcu sporoči, koliko časa bodo ti podatki veljavni (lease time).

DHCPREQUEST: Odjemalec po prejeti ponudbi pošlje strežniku zahtevo. V njej navede naslov, ki mu ga je strežnik ponudil.



Slika 2.4: Pridobivanje naslova IP s protokolom DHCP

DHCPACK: Strežnik potrdi zahtevo odjemalca. S tem je transakcija zaključena in odjemalec lahko uporablja dodeljeni naslov.

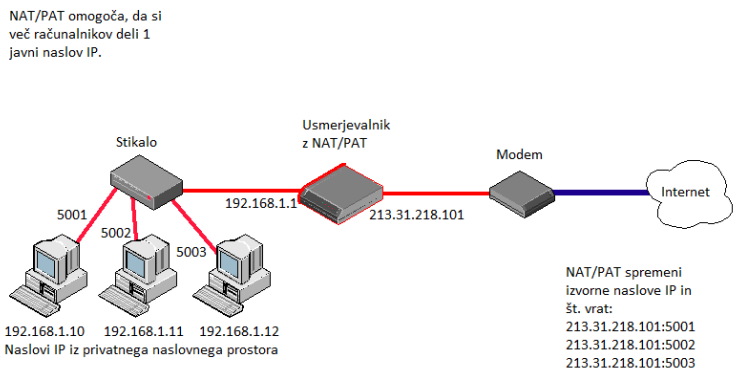
Pred potekom veljavnosti mora odjemalec poskrbeti za obnovitev naslova. To stori tako, da pošlje DHCPREQUEST, v katerem navede naslov IP, ki ga je uporabljal. Strežnik obnovitev potrdi s paketom DHCPACK.

Ker je eduroam zasnovan za preprosto uporabo, s čim manj potrebe po ročni konfiguraciji naprav končnih uporabnikov, se za dodeljevanje naslovov IP uporablja protokol DHCP.

2.6 NAT

NAT (Network address translation) se večinoma uporablja zaradi pomanjkanja naslovov IPv4. Ker je omrežnih naprav vse več in več, je naslovov IPv4 že zmanjkalo [8]. Z uporabo NAT smo podaljšali čas pred izčrpanjem naslovov IP, saj bi jih brez uporabe NAT-a, zmanjkalo že veliko prej.

NAT deluje tako, da si več naprav deli 1 javni naslov IP, za komunikacijo med seboj pa uporabljajo zasebne naslove IP, ki se ne usmerjajo v internet. Ti zasebni naslovi IP so lahko isti v vseh zasebnih omrežjih. V prometu, ki gre od teh uporabnikov v internet, se izvorni naslov IP preslika iz zasebnega naslova v javnega [9].



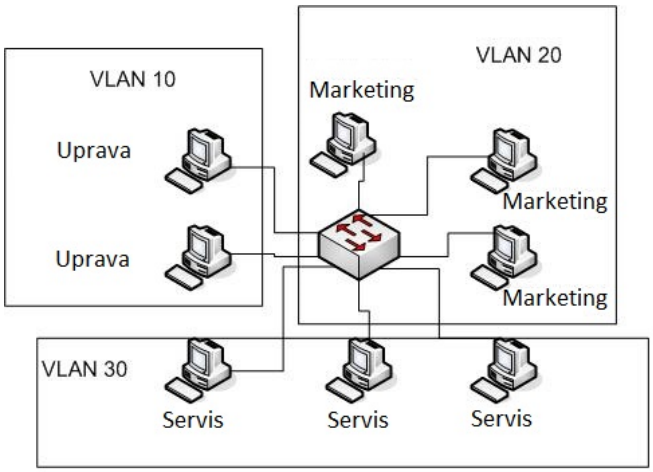
Slika 2.5: Delovanje NAT/PAT

Primer:

Računalnik A z zasebnim naslovom IP 192.168.1.1 želi odpreti spletno stran na naslovu 173.194.35.184. Ker se naslov spletne strani nahaja izven njegovega omrežja, bo zahtevo za spletno stran poslal svojemu privzetemu prehodu. Privzeti prehod, ki zna izvajati NAT, zahtevo preoblikuje tako, da pošiljateljev naslov IP 192.168.1.1 zamenja s svojim javnim naslovom IP [9]. Ker NAT prehod ve, iz katerih vrat je prišla izvorna zahteva po spletni strani, bo znal odgovor poslati pravilnemu računalniku. Problem pa se pojavi, ko je situacija obrnjena in bi nekdo z interneta rad dostopal do računalnika A. Računalnik A sedaj ni več dostopen z interneta – javni naslov ima namreč usmerjevalnik. To slabost delno odpravimo z uporabo posredovanja vrat (port forwarding). Napravi, ki izvaja NAT, nastavimo tabelo preslikav. V njej se nahajajo pari zasebnih naslovov IP in številk vrat. Ko naprava sprejme zahtevo, s ponorno številko vrat, ki se nahaja v tabeli, tako zahtevo posreduje na zasebni naslov IP, ki pripada tej številki vrat. S tem dosežemo, da je tudi naprava z zasebnim naslovom IP dosegljiva z interneta, vendar pa lahko neka vrata posredujemo samo eni napravi.

Slika 2.5 prikazuje kako se trije različni zasebni naslovi IP z uporabo NAT/PAT preslikajo v isti javni naslov IP z različno številko vrat.

V splošnem je uporaba NAT v omrežjih eduroam po svetu dovoljena,



Slika 2.6: Ločevanje uporabnikov v različne VLAN-e

a odsvetovana [25, 26]. Uporaba NAT v omrežjih eduroam v Sloveniji je dovoljena le za upravljanje dostopnih točk, ne pa tudi za uporabnike [2].

2.7 VLAN

VLAN (ang. Virtual Local Area Network) je logična domena broadcast (ang. broadcast domain), ki se konfigurira na stikalih. Z VLAN posežemo v logično topologijo omrežja. Omogoča združevanje odjemalcev glede na njihovo vlogo, udeležbo v projektni skupini ali uporabo določene aplikacije ipd., ne glede na njihovo fizično lokacijo v omrežju.

Z VLAN-i v omrežjih Ethernet tvorimo navidezna krajevna omrežja. Z navideznim krajevnim omrežjem ustvarimo logično skupino odjemalcev. VLAN-e lahko uporabljamo tudi v brezžičnih omrežjih saj tudi ta uporabljajo protokol Ethernet.

Dodatna prednost VLAN-ov je izolacija prometa broadcast v t.i. logične domene broadcast, kar ima za posledico razbremenitev vmesnikov in odjemalcev na stikalu (zmanjša promet ARP, poslan na naslov broadcast) [12].

Na sliki 2.6 je prikazano ločevanje uporabnikov istih oddelkov (Uprava, Marketing, Servis) na VLAN-e z isto številko.

V omrežju eduroam se na dostopnih točkah uporablja vsaj dva VLAN-a. Enega za upravljanje dostopne točke in drugega za uporabnike brezžičnega omrežja eduroam [27]. Če se poleg omrežja eduroam na istih dostopnih točkah uporablja tudi dodatno omrežje (na primer WPA2-PSK), mora biti v svojem, ločenem VLAN-u [28].

2.8 Protokol Neighbor Discovery

Protokol Neighbor Discovery se uporablja za razreševanje naslova povezavne plasti, za ugotavljanje sprememb tega naslova in za ugotavljanje dosegljivosti naprav v istem omrežju [22]. V primerjavi z omrežji IPv4, je protokol Neighbor Discovery ekvivalenten protokolu ARP, ki je opisan v poglavju 2.4.

Protokol definira naslednja sporočila:

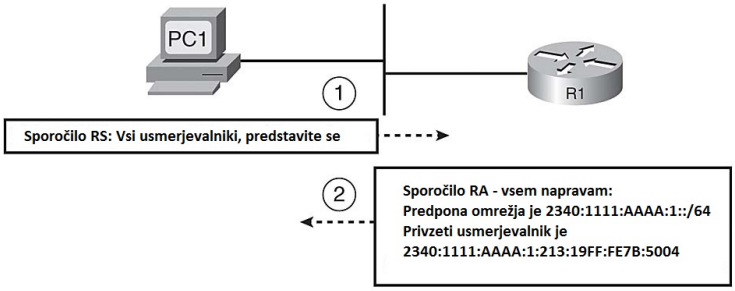
- Router Solicitation

  Sporočilo Router Solicitation pošlje naprava, ki želi izvedeti naslov usmerjevalnika (slika 2.7). Če taka naprava že pozna svoj naslov IPv6, ga vključi v zahtevo, drugače pa mora vključiti svoj naslov povezavne plasti.

- Router Advertisement

  Sporočila Router Advertisement pošiljajo usmerjevalniki napravam v omrežju periodično ali pa kot odgovor sporočilom Router Solicitation (slika 2.7). V teh sporočilih usmerjevalniki navedejo, ali je v omrežju strežnik DHCPv6, podatke o morebitnem strežniku DNS, časovno veljavnost privzetega usmerjevalnika in podobno. Navedejo lahko tudi podatke o predponi za uporabo pri samodejni nastavitvi naslova IPv6.

- Neighbor Solicitation



Slika 2.7: Sporočili Router Solicitation in Router Advertisement

Za ugotavljanje naslova povezavne plasti drugih naprav, naprava pošlje sporočilo Neighbor Solicitation. V takem sporočilu naprava pošiljateljica sporoči tudi svoj naslov povezavne plasti drugim napravam.

- Neighbor Advertisement

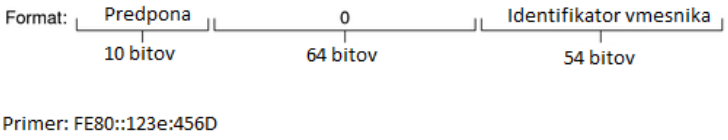
  Kot odgovor na sporočilo Neighbor Solicitation, naprava pošlje sporočilo Neighbor Advertisement in s tem sporoči svoj naslov povezavne plasti. Sporočilo lahko pošlje tudi samostojno (ne kot odgovor), če želi sporočiti spremenjene podatke o sebi. Ti spremenjeni podatki so na primer nov naslov povezavne plasti ali pa podatek o tem, da je naprava pošiljateljica usmerjevalnik [22].

2.8.1 IPv6 Stateless Address Autoconfiguration

Dokument [23] opisuje postopek in korake, ki jih mora upoštevati naprava, ki želi samodejno nastaviti omrežne vmesnike za uporabo IPv6. Proces samodejne nastavitve zajema generiranje naslova tipa *link-local* in *global*, ter preverjanje veljavnosti naslovov, s procesom odkrivanja podvojenih naslovov (Duplicate Address Detection) [23]. V tem poglavju bomo povzeli postopek samodejne nastavitve.

Naslov tipa link-local je sestavljen iz znane, vnaprej določene predpone (FE80::/64) in enolične končnice, ki predstavlja identifikator vmesnika (slika

2.8). Za končnico se v praksi večinoma uporablja naslov povezavne plasti.



Slika 2.8: Naslov IPv6 link-local

Preden naprava začne uporabljati naslov, se mora prepričati, da istega naslova ne uporablja katera druga naprava v omrežju. Na naslov, ki si ga želi nastaviti pošlje sporočilo Neighbor Solicitation. V primeru, da je naslov zaseden, bo naprava, ki ga zaseda, poslala odgovor Neighbor Advertisement.

Ko se naprava prepriča, da je naslov v omrežju enoličen, ga dodeli omrežnemu vmesniku. Šele sedaj lahko komunicira z drugimi napravami, s protokolom IPv6.

V naslednjem koraku avtomatske konfiguracije, naprava čaka na sporočilo Router Advertisement, v katerem so podatki za tvorbo naslova tipa global. Za pohitritev postopka lahko pošlje sporočilo Router Solicitation že med tvorbo naslova tipa link-local. Tudi enoličnost naslova tipa global je pred uporabo potrebno preveriti s sporočilom Neighbor Solicitation.

V novih sporočilih Router Advertisement so lahko dopolnjeni ali spremenjeni podatki, kot v prejšnjih (na primer dodatna predpona omrežja, spremenjen naslov povezavne plasti usmerjevalnika), zato morajo vsa taka sporočila naprave preveriti in si podatke po potrebi dopolniti ali spremeniti.

2.9 Tehnična določila opreme

Oprema, uporabljena v omrežju eduroam.si mora ustrezati tehničnim določilom, ki jih določi Arnes [7]. Izpostavili bomo samo določila, relevantna za to diplomsko nalogo. Dostopne točke morajo podpirati naslednje standarde oziroma funkcionalnosti, ki se uporabljajo v navideznih krajevnih omrežjih:

- protokol IEEE 802.1Q,
- dinamično umeščanje uporabnika v VLAN, glede na nastavitve RADIUS (Parameter Tunnel-Type=VLAN kot je definiran v RFC3580),
- dodeljevanje uporabnika v VLAN glede na SSID, na katerega se uporabnik priključuje (statična nastavitev v dostopni točki),
- ločen VLAN za upravljanje dostopne točke (angl. management access), lahko tudi zgolj neoznačen (angl. untagged, native).

Pri stikalih je zahtev več:

- protokol IEEE 802.1Q,
- vsaj 100 VLAN-ov/stikalo,
- vsaj 8 logičnih vmesnikov na fizičen vmesnik,
- se en ali več VLAN-ov oziroma logičnih vmesnikov uporabi za usmerjanje prometa IP (VLAN-e se zaključi na stikalu, dodeli se jim naslove IP),
- se hkrati en ali več VLAN-ov oziroma logičnih vmesnikov uporabi zgolj v L2 funkcionalnosti (torej za premoščanje ethernet prometa, ne da bi pri tem stikalo poskušalo usmerjati IP promet preko teh VLAN-ov),
- je promet med posameznimi VLAN-i možno usmerjati (v kolikor se VLAN-e zaključi na stikalu in se jim priredi naslove IP).

Poglavje 3

Varnostne pomanjkljivosti v eduroam.si

V omrežju eduroam.si je za varen prenos uporabniškega imena in gesla do domače organizacije poskrbljeno z uporabo šifrirnega tunela, s protokolom EAP-TTLS. Morebitni napadi na ta protokol oziroma prestrezanje uporabniškega imena in gesla niso del te diplomske naloge, saj smo se osredotočili na zagotavljanje varnosti že povezanih uporabnikov pred drugimi, zlonamernimi uporabniki.

V tem poglavju bomo predstavili napade na povezavni plasti, ki smo jih preizkusili v testnem omrežju eduroam. Nekateri napadi imajo za posledico onemogočanje storitve (DoS - Denial of Service), kar je za napadenega uporabnika sicer nevšečno, ne pusti pa hujših posledic. Z nekaterimi napadi pa napadalec preusmeri promet med napadenim uporabnikom in drugimi napravami (uporabniki, privzetim prehodom) preko svoje infrastrukture (MITM - Man In The Middle), s čimer lahko pridobi tudi zaupne in občutljive podatke, kot so na primer gesla, številka kreditne kartice, bančnega računa, ...

3.1 Zastrupljanje tabele ARP

Ker se vsi povezani uporabniki nahajajo v istem navideznem krajevnem omrežju (VLAN), lahko med seboj komunicirajo na povezavni plasti. Protokol ARP, ki skrbi za pretvarjanje naslovov povezavne plasti v naslove IP ima varnostno pomanjkljivost. Sam protokol nima vgrajenih mehanizmov za preverjanje oziroma zagotavljanje identitete pošiljatelja.

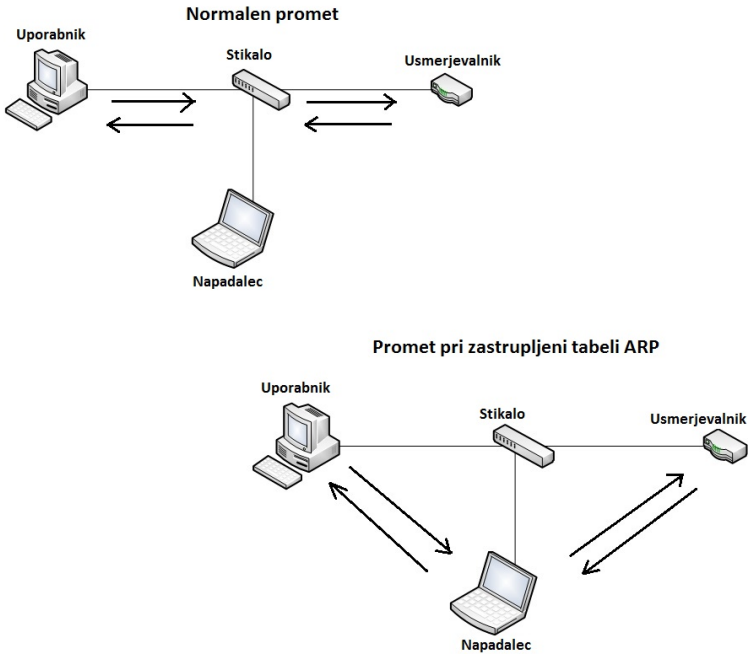
Ker ni mehanizma za preverjanje identitete, se lahko neka naprava, denimo da ima naslov povezavne plasti a0-0b-ba-34-f1-4b in naslov IP 192.168.1.125, predstavi drugim napravam z lažnim naslovom IP - na primer z naslovom privzetega prehoda (192.168.1.1). Vse naprave, ki prejmejo te podatke, si popravijo vnose v svojih tabelah ARP. Primer tabele ARP pred in po zastrupitvi je prikazan na izpisih 3.1 in 3.2.

```
arp -a

Interface: 192.168.1.100 --- 0xb
  Internet Address      Physical Address      Type
  192.168.1.1           00-22-6b-60-f4-95     dynamic
  192.168.1.119         00-22-3f-e0-9a-9e     dynamic
  192.168.1.200         00-11-43-77-11-5f     dynamic
  192.168.1.255         ff-ff-ff-ff-ff-ff     static
```

Izpis 3.1: Tabela ARP pred zastrupitvijo

```
arp -a

Interface: 192.168.1.100 --- 0xb
  Internet Address      Physical Address      Type
  192.168.1.1           a0-0b-ba-34-f1-4b     dynamic
  192.168.1.119         00-22-3f-e0-9a-9e     dynamic
  192.168.1.125         a0-0b-ba-34-f1-4b     dynamic
  192.168.1.200         00-11-43-77-11-5f     dynamic
  192.168.1.255         ff-ff-ff-ff-ff-ff     static
```

Izpis 3.2: Tabela ARP po zastrupitvi



Slika 3.1: Prestrezanje prometa z zastrupljanjem tabele ARP

Če ima neka naprava zastrupljeno tabelo ARP in želi poslati promet privzetemu prehodu na naslovu IP 192.168.1.1, bo v resnici poslala promet napadalcu, ki je poskrbel, da se je fizični naslov njegove naprave dodal v tabelo ARP napadene naprave, z naslovom IP privzetega prehoda - 192.168.1.1 (izpis 3.2). Napadalec lahko nato prejete podatke zavrže ali pa jih posreduje do pravega naslovnika – privzetega prehoda. Tak napad imenujemo zastrupljanje tabele ARP (ARP poisoning) in je prikazan na sliki 3.1. V primeru, da napadalec podatke zavrže, bo za napadenega uporabnika videti, kot da je privzeti prehod neodziven (onemogočanje storitve). Če pa napadalec podatke posreduje privzetemu prehodu, uporabnik ničesar ne posumi in še naprej pošilja podatke preko napadalca.

Ta napad smo uspešno izvedli v testnem in produkcijskem omrežju eduroam [18]. Napada v omrežjih, ki uporabljajo starejša stikala ni možno zaznati brez dodatnih programov za spremljanje tabele ARP na stikalu [17], če pa napadalec zastrupi samo tabelo ARP drugega uporabnika, ne pa tudi

stikala (1 way ARP poison), pa lahko tak napad zazna samo napadeni uporabnik.

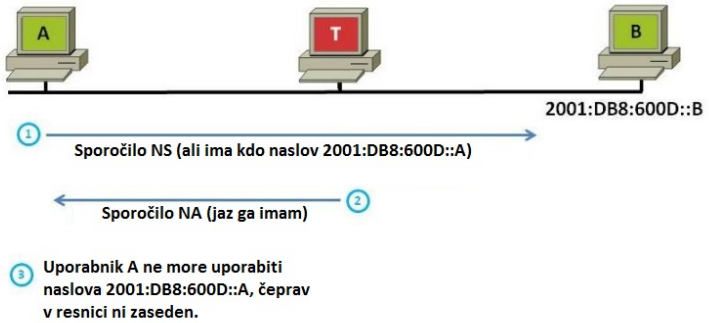
3.2 Onemogočanje pridobivanja naslova IPv6

Program `dos-new-ip6` je del zbirke programov `THC-IPv6 Attack Toolkit` za napade na ranljivosti protokola IPv6 [21]. Zbirko programov je objavila skupina THC (The Hacker's Choice). Pri izvajanju IPv6 napadov na testno omrežje eduroam, smo uporabili programe iz omenjene zbirke.

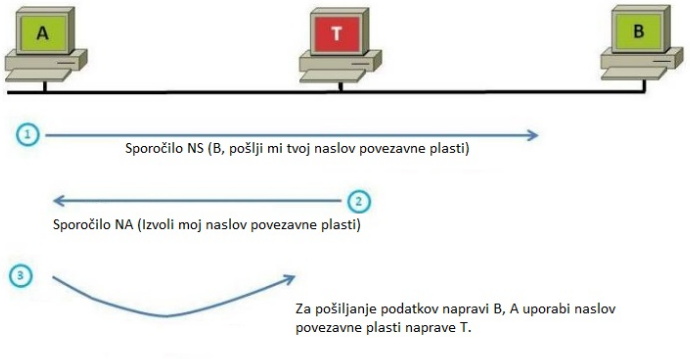
Preden uporabnik začne uporabljati IPv6 omrežje, si mora nastaviti naslov IPv6, sestavljen iz predpone omrežja in tipično naslova povezavne plasti (glej poglavje 2.8.1). Preden si nastavi naslov IPv6, vpraša ostale naprave v omrežju, če katera že uporablja ta naslov, tako da pošlje sporočilo Neighbor Solicitation.

Ta zelo preprost program posluša za morebitnimi sporočili Neighbor Solicitation in na vsako tako sporočilo lažno odgovori, da je ta naslov že zaseden s sporočilom Neighbor Advertisement (slika 3.2). S tem prepreči napravam konfiguracijo naslova IPv6, kar povzroči onemogočanje storitve IPv6 [17].

Napad smo uspešno izvedli v testnem omrežju eduroam.



Slika 3.2: Onemogočanje storitve - lažni odgovori na sporočila Neighbor Solicitation



Slika 3.3: Napad z lažnimi podatki v sporočilu Neighbor Advertisement

3.3 Zastrupljanje tabele sosedov

Tudi `parasite6` je del zbirke programov omenjene v poglavju 3.2. Ko naprava A želi poslati IPv6 pakete napravi B, pa ne ve njenega naslova povezavne plasti, najprej pošlje zahtevo Neighbor Solicitation in počaka na odgovor Neighbor Advertisement (glej poglavje 2.8).

Program `parasite6` odgovori na tako zahtevo z lažnim sporočilom Neighbor Advertisement, v katerega vstavi svoj naslov povezavne plasti (slika 3.3). Naprava A si shrani povezavo naslova IPv6 naprave B in naslova povezavne plasti napadalca, kar povzroči, da IPv6 promet namenjen napravi B pošlje napadalcu [17]. Ta napad lahko primerjamo z zastrupljanjem tabele ARP pri protokolu IPv4 (poglavje 3.1).

V testnem omrežju eduroam napad ni bil v celoti uspešen. Namesto prestrezanja prometa IPv6 smo dosegli onemogočanje storitve IPv6 [17].

3.4 Napad z lažnimi sporočili RA in tunelom 6to4

V omrežjih eduroam, ki ne uporabljajo protokola IPv6, lahko napadalec z ustrezno odprtokodno programsko opremo oglašuje svoje omrežje IPv6. Ostale naprave takega omrežja si torej samodejno nastavijo tudi naslove IPv6, kot privzeti prehod za promet IPv6 pa uporabljajo napadalca. Napadalec, mora imeti tudi svoj strežnik DNS, da lahko odgovarja na zahteve DNS drugih uporabnikov. S tunelom *6to4* napadalec poskrbi, da se paketi IPv6 enkapsulirajo v pakete IPv4 in tako lahko potujejo po IPv4 omrežjih do končnih strežnikov. Ob povratku tunel *6to4* poskrbi za dekapsulacijo [24].

Naprava uporabnika, ki pošlje poizvedbo DNS za neko spletno stran, dobi dva odgovora - naslov IPv4, ki ga pošlje legitimen strežnik DNS in naslov IPv6, ki ga pošlje napadalčev strežnik. Ker operacijski sistemi večinoma preferirajo naslove IPv6, pošljejo promet preko napadalca [17].

Napad smo preizkusili v testnem omrežju eduroam in z njim uspešno dosegli prestrezanje prometa (MITM) [17].

Poglavje 4

Testno okolje

V tem poglavju bomo opisali testno omrežje, ki smo ga uporabili za izvajanje napadov opisanih v poglavju 3 in za razvoj rešitve, ki preprečuje te napade (poglavje 5).

Strojna in programska oprema, ki smo jo uporabili v testnem okolju, ustreza tehničnim določilom zavoda Arnes za omrežje eduroam.

Ker nam testno okolje ni dopuščalo uporabe več kot enega naslova IP iz javnega naslovnega prostora, smo uporabili več omrežij iz zasebnega naslovnega prostora. Vsi naslovi IP v tej diplomski nalogi, ki so v omrežju 192.168.1.0/24, v testne namene služijo kot nadomestki javnih naslovov.

4.1 Strojna oprema

V testnem okolju smo uporabili stikalo Cisco Catalyst 3750 z naloženo programsko opremo (firmware) c3750-ipservicesk9-mz.122-55.SE1.bin. Dostopna točka, ki smo jo uporabili, je Cisco Aironet AIR 1242AG s programsko opremo c1240-k9w7-mx.124-21a.JA1.

Potrebno programsko opremo smo namestili na prenosna računalnika DELL Inspiron 6000 in HP Compaq 8510p.

Uporabniki testnega omrežja eduroam so uporabljali naprave:

- prenosni računalnik HP EliteBook 8470p, operacijski sistem Linux Fedora 19 Desktop Edition
- prenosni računalnik HP Pavilion dv6700, operacijski sistem Windows 7 in BackTrack Linux 5
- pametni telefon ZTE Blade, operacijski sistem Android 2.2

4.2 Programska oprema

Na prenosni računalnik DELL Inspiron smo namestili operacijski sistem CentOS 5, v virtualnem okolju (VmWare), nanj pa naslednje programe:

- strežnik FreeRADIUS, verzija 2.1.11
- strežnik DHCP, verzija isc-dhcpd-V3.0.5-RedHat
- imenik OpenLDAP, verzija 2.3.43
- baza mysql, verzija 9.5 Distrib 5.0.77, for redhat-linux-gnu (i686)

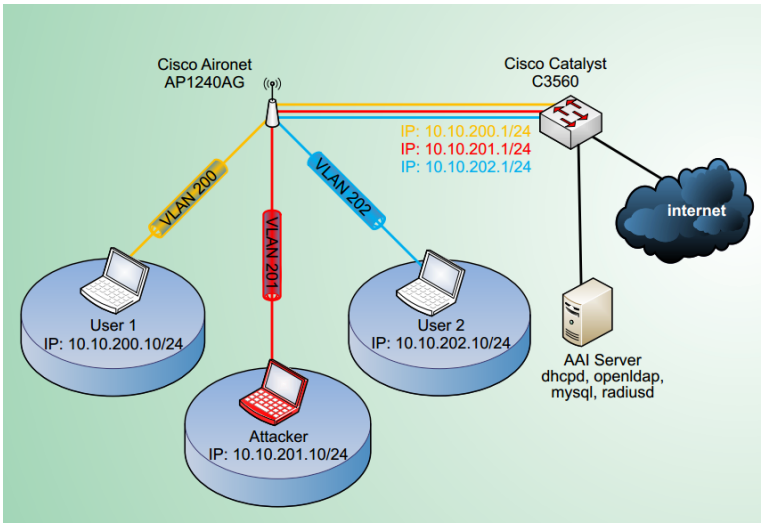
Prenosni računalnik HP Compaq je bil uporabljen zgolj kot privzeti prehod za uporabnike (odjemalce testnega omrežja eduroam). Nanj smo namestili operacijski sistem Linux Ubuntu Server 12.04.2 LTS, ki je opravljal NAT.

Poglavje 5

Rešitev

Kot smo prikazali v prejšnjem poglavju, so v omrežju eduroam možni razni napadi zlonamernih uporabnikov omrežja. Nekatere napade je možno preprečiti s filtri na stikalu oziroma na dostopni točki, nekatere je možno le zaznati z dodatnimi programi (ARPWatch, NDPMon), nekaterih pa se ne da niti preprečiti, niti zaznati (1 way ARP poison - poglavje 3.1).

Lotili smo se celovite rešitve, ki bi uporabnike med seboj ločila na različne VLAN-e in s tem odpravila napade na povezavni plasti (slika 5.1).



Slika 5.1: Ločevanje uporabnikov na različne VLAN-e

5.1 Dostopna točka in stikalo

Osnovne nastavitve opreme po vzorčnih nastavitvah Arnes-a, smo dopolnili z dinamičnim ločevanjem uporabnikov na omrežja VLAN. Nekaj konfiguracije je bilo opravljeno statično, avtomatizirali pa smo nastavljanje VLAN-ov na dostopni točki. Na stikalu smo dodali VLAN-e in jim dodelili naslove IP iz zasebnega naslovnega prostora (izpis 5.1).

```
interface Vlan200
 ip address 10.200.200.200 255.255.255.0
 ip helper-address 10.10.10.1
!
interface Vlan201
 ip address 10.201.200.200 255.255.255.0
 ip helper-address 10.10.10.1
```

Izpis 5.1: Del konfiguracije VLAN-ov na stikalu

S tem, ko ima VLAN na stikalu svoj naslov IP, lahko stikalo deluje kot usmerjevalnik med različnimi VLAN-i. Temu pravimo zaključevanje VLAN-ov na stikalu. Promet iz enega VLAN-a v drugega se torej usmerja (3. plast), medtem ko se promet v istem VLAN-u premošča (2. plast). Nastavili smo tudi `ip helper-address` (izpis 5.1), ki poskrbi, da lahko promet DHCP potuje med odjemalcem in strežnikom, ki nista v istem omrežju. Brez tega ukaza ne bi bilo možno pridobiti naslova IP, saj stikalo blokira promet broadcast med napravami, ki niso v istem omrežju.

Tudi na dostopni točki smo dodali ustrezne VLAN-e. Uporabljena dostopna točka ima 2 radijska vmesnika – 5 GHz in 2,4 GHz, ter fizični vmesnik. VLAN-e je potrebno dodati na vse vmesnike, saj ne vemo na kateri radijski vmesnik se bo povezal uporabnik. Dodajanje VLAN-ov na vmesnike smo avtomatizirali. Potek konfiguracije beležimo v dnevniško datoteko, da lahko morebitne napake preverimo. Za povezovanje do dostopne točke smo uporabili protokol SSH. Pri avtomatizaciji smo uporabili programski jezik Python in knjižnico "PXSSH". Knjižnica je namenjena prav povezovanju s protokolom SSH in upravljanju oddaljene naprave. Vgrajene ima metode za prijavo,

odjavo in prepoznavo ukazne lupine [11].

V programu smo najprej nastavili spremenljivke za število VLAN-ov, ki jih želimo nastaviti in začetno številko VLAN-a, ter naslove IP vseh dostopnih točk, ki jih želimo nastaviti. Tudi uporabniško ime in geslo za upravljanje dostopnih točk sta zapisana v programu, ker smo želeli čim bolj avtomatizirati proces nastavitve dostopnih točk, brez interakcije (vpisovanje gesla). Po prijavi na prvo določeno dostopno točko, program nastavi toliko VLAN-ov, kolikor smo jih določili v spremenljivki, nato pa se odjavi in prijavi na naslednjo dostopno točko, kjer ponovno nastavi isto število VLAN-ov, z začetno številko VLAN-a za 1 višjo od zadnje številke pri prejšnji dostopni točki. To stori za vse določene dostopne točke.

V izpisu 5.2 je prikazan postopek prijave in pošiljanje ukazov dostopni točki z uporabo knjižnice PXSSH. Vsak ukaz, ki ga želimo poslati dostopni točki, moramo podati kot argument klicu `pxssh.sendline([ukaz])`.

```
ssh = pxssh.pxssh(timeout=10, logfile=f)
ssh.login(AP, apUsername, apPassword, login_timeout=30,
   original_prompt="#", auto_prompt_reset=False)

ConfigureCisco()
...
def ConfigureCisco():

    global startVlan, noVLANS, bridgeGRP
    ssh.sendline("terminal length 0")
    ssh.sendline("en")
    ssh.sendline(enPassword)
    ssh.sendline("conf t")
    ...
```

Izpis 5.2: Uporaba knjižnice PXSSH za prijavo in konfiguracijo dostopne točke

Izpis 5.3 prikazuje ukaze za konfiguracijo enega VLAN-a na 5 GHz radijskem vmesniku in na fizičnem vmesniku. Za vsak VLAN na dostopni točki

je potrebno nastaviti tudi 2,4 GHz radijski vmesnik.

Število ukazov, potrebnih za konfiguracijo dostopnih točk, administratorjem vzame veliko časa in dopušča precej možnosti za napake. Avtomatizacija postopka pohitri zamudno in k napakam nagnjeno nastavljanje vmesnikov VLAN.

```
for i in range(noVLANS):
    vlan = str((i + startVlan))
    bgrp = str((i + bridgeGRP))

### 5 GHz ###
    interface Dot11Radio1
    encryption vlan " + vlan + " mode ciphers aes-ccm"
    interface dot1 1." + vlan
    encapsulation dot1Q " + vlan)
    ip access-group block_client_tx in
    ip access-group block_client_rx out
    no ip route-cache
    no cdp enable
    bridge-group " + bgrp
    bridge-group " + bgrp +" subscriber-loop-control
    bridge-group " + bgrp +" block-unknown-source
    no bridge-group " + bgrp + " source-learning
    no bridge-group " + bgrp + " unicast-flooding
    bridge-group " + bgrp + " spanning-disabled
    exit
...
### Wired interface ###
    interface FastEthernet0." + vlan
    encapsulation dot1Q " + vlan
    no ip route-cache
    bridge-group " + bgrp
    no bridge-group " + bgrp + " source-learning
    bridge-group " + bgrp + " spanning-disabled
    exit
```

Izpis 5.3: Ukazi za konfiguracijo dostopnih točk

5.2 Strežnik FreeRADIUS

Konfiguracijo strežnika FreeRADIUS smo prilagodili tako, da dodeljevanje uporabnikov v VLAN-e ni več statično, temveč RADIUS vsakič znova zažene program, ki mu sporoči v kateri VLAN naj dodeli uporabnika. Konfiguracijska datoteka »raddb/sites-available/default« je razdeljena na sklope, ki ustrezajo različnim fazam procesiranja zahtev RADIUS. Strežnik mora preveriti, da je uporabnik res ta, za kogar se izdaja - preveri torej ali se geslo ki ga je navedel ujema z geslom shranjenim v imeniku LDAP. Če je geslo pravilno, se izvede naslednja faza - avtorizacija. V tej fazi strežnik preveri, če ima uporabnik pravico do uporabe omrežja -na primer, da še ni pretekel datum veljavnosti uporabniškega imena/gesla. V naslednji fazi *post-auth* strežnik lahko sporoči dodatne nastavitve ponudniku storitve (npr. omejitev pasovne širine ali številko VLAN-a).

V konfiguracijski datoteki smo dopolnili sklop *post-auth*. Najprej strežnik FreeRADIUS požene program, ki mu vrne številko VLAN-a, ki naj ga dodeli uporabniku. Številko VLAN-a si shrani v spremenljivko `Tmp-Integer-0` in v naslednjem koraku sporoči vrednost te spremenljivke dostopni točki (izpis 5.4).

```
post-auth {
 # Procesiraj postauth_users le za zahteve iz domacih NAS-ov
    if (!"%{Proxy-State}") {
        files
    }

    Post-Auth-Type REJECT {
        attr_filter.access_reject
    }
    ###  VLAN ASSIGNMENT ###
    update control{
            Tmp-Integer-0=`/home/radius/setvlan.sh`
    }
```

```
    update reply {
        Tunnel-Medium-Type = "IEEE-802"
        Tunnel-Type = "VLAN"
        Tunnel-Private-Group-ID = "%{control:Tmp-Integer-0}"
    }
}
```

Izpis 5.4: Dopolnjena konfiguracijska datoteka strežnika RADIUS

Program, ki sporoči ustrezen VLAN strežniku FreeRADIUS, ga najprej prebere iz datoteke prostih VLAN-ov, nato pa ga iz nje izbriše, da ne bi naslednjič sporočil istega VLAN-a.

```
#!/bin/bash

lockfile /home/radius/lock

# Read the first free vlan
first=$(head -n 1 /home/radius/freevlans.txt)
vlan=4010
if [ -z $first ]; then
        echo $vlan
        rm -f /home/radius/lock
        exit 0
fi

if [ $first -lt 200 -o $first -gt 2009 ]; then
        echo $vlan
        rm -f /home/radius/lock
        exit 0

else
        vlan=$first
        sed -i '1d' /home/radius/freevlans.txt
fi

rm -f /home/radius/lock

echo $vlan
```

```
exit 0
```

Izpis 5.5: Program za dodeljevanje VLAN-ov

V primeru, da bi bilo uporabnikov več, kot je na voljo VLAN-ov, ima program za dodeljevanje statično vnesen privzet VLAN, v katerega dodeli vse nadaljnje uporabnike. Ti uporabniki se torej nahajajo v istem podomrežju - tako, kot je v trenutnih implementacijah eduroam.si

5.3 Strežnik DHCP

Konfiguracijo strežnika DHCP je bilo potrebno razširiti z ustreznimi navideznimi omrežji (VLAN-i), da je vsaka naprava v svojem VLAN-u dobila ustrezen naslov IP. Strežnik v teh VLAN-ih dodeljuje samo 1 naslov IP, saj se v posameznem podomrežju nahaja le 1 uporabnik. Stikalo ima statično določen naslov IP. V privzetem VLAN-u je naslovov več.

V izpisu 5.6 sekcija *shared-network vlan200* prikazuje konfiguracijo strežnika DHCP za enega uporabnika. Strežnik bo uporabniku dodelil naslov IP 10.200.200.10 in privzeti prehod 10.200.200.200. Podobno je tudi v sekciji *shared-network vlan201*, le z drugačnim naslovom IP za uporabnika in za privzeti prehod. V sekciji *shared-network vlan4010* je na voljo 31 naslovov IP.

```
shared-network "vlan4010" {

# omrezje /24 z 255 IPji
subnet 10.10.10.0 netmask 255.255.255.0 {
    pool {
        option routers 10.10.10.2;
        range 10.10.10.10 10.10.10.40;
    }
}
}

shared-network "vlan200" {
```

```
subnet 10.200.200.0 netmask 255.255.255.0 {
    pool {
        option routers 10.200.200.200;
        range 10.200.200.10 10.200.200.10;
   }
}
}

shared-network "vlan201" {

subnet 10.201.200.0 netmask 255.255.255.0 {
    pool {
        option routers 10.201.200.200;
        range 10.201.200.10 10.201.200.10;
    }
}
}
```

Izpis 5.6: Dopolnjena konfiguracijska datoteka strežnika DHCP

V omrežju z veliko uporabniki, bi konfiguracijska datoteka vsebovala veliko vnosov, zato bi z avtomatizacijo vnosov prihranili kar veliko časa in zmanjšali možnosti za napake.

5.4 1:1 NAT

Za ločevanje uporabnikov v VLAN-e smo porabili 4 naslove IP za vsakega uporabnika. Vsak uporabnik je namreč v svojem omrežju, ki poleg naslova IP za uporabnika potrebuje še naslov broadcast in naslov omrežja. Svoj naslov IP potrebuje tudi stikalo, za zaključevanje VLAN-a.

Ker potrebujemo 4 naslove IP na uporabnika, smo uporabili naslove z zasebnega naslovnega prostora. Da bi uporabnikom zagotovili javno povezljivost, smo uporabili 1:1 NAT, ki vsak uporabniku dodeljen zasebni naslov IP preslika v svoj javni naslov IP. To smo dosegli s pravili *iptables* na operacij-

skem sistemu Ubuntu Linux. Najprej smo v operacijskem sistemu omogočili uporabo VLAN-ov z ukazom v izpisu 5.7.

```
modprobe 8021q
```

Izpis 5.7: Omogočanje uporabe VLAN-ov v operacijskem sistemu Ubuntu Linux

Za pravilno delovanje VLAN-ov je potrebno dodati navidezne omrežne vmesnike, kot prikazuje izpis 5.8.

```
/sbin/vconfig add eth0 [stevilka VLAN-a]
```

Izpis 5.8: Dodajanje navideznih omrežnih vmesnikov

Da operacijski sistem deluje kot usmerjevalnik paketov, dosežemo z ukazom v izpisu 5.9.

```
echo 1 > /proc/sys/net/ipv4/ip_forward
```

Izpis 5.9: Vklop posredovanja paketov

Z uporabo iptables smo določili pravila, po katerih deluje usmerjanje in manipulacija paketov. Za vsak naslov IP, ki je v strežniku DHCP na voljo uporabnikom, smo določili v kateri izvorni naslov IP naj se pretvori ob odhodu z usmerjevalnika. Določili smo tudi obratne preslikave, torej, v kateri ponorni naslov IP je potrebno popraviti pakete, da bodo dosegli uporabnika.

```
iptables -t nat -A POSTROUTING -o eth0.4009 -s 10.10.2.10 -j
   SNAT --to-source 192.168.1.22
iptables -t nat -A POSTROUTING -o eth0.4009 -s 10.10.3.10 -j
   SNAT --to-source 192.168.1.23
iptables -t nat -A POSTROUTING -o eth0.4009 -s 10.10.4.10 -j
   SNAT --to-source 192.168.1.24
iptables -t nat -A PREROUTING -i eth0.2002 -d 192.168.1.22 -j
    DNAT --to-destination 10.10.2.10
iptables -t nat -A PREROUTING -i eth0.2003 -d 192.168.1.23 -j
    DNAT --to-destination 10.10.3.10
iptables -t nat -A PREROUTING -i eth0.2004 -d 192.168.1.24 -j
    DNAT --to-destination 10.10.4.10
```

```
iptables -A FORWARD -s 192.168.1.22 -j ACCEPT
iptables -A FORWARD -s 192.168.1.23 -j ACCEPT
iptables -A FORWARD -s 192.168.1.24 -j ACCEPT
iptables -A FORWARD -d 10.10.2.10 -j ACCEPT
iptables -A FORWARD -d 10.10.3.10 -j ACCEPT
iptables -A FORWARD -d 10.10.4.10 -j ACCEPT
```

Izpis 5.10: Pravila iptables

Prva tri pravila iptables v izpisu 5.10 spreminjajo pakete pri izhodu iz naprave, ki izvaja NAT tako, da izvorni naslov IP spremenijo iz zasebnega naslova v javni naslov. Naslednja tri pravila naredijo ravno obratno - pri prihodu paketov v napravo popravijo ponorni naslov IP iz javnega v zasebnega, da lahko paketi dosežejo uporabnike. Z zadnjimi pravili sporočimo napravi, ki izvaja NAT, da sprejme pakete (z izvornimi ali ponornimi naslovi IP določenimi v izpisu) v obdelavo.

5.5 Evalvacija rešitve

Z ločevanjem uporabnikov v ločena navidezna omrežja smo morebitnim napadalcem preprečili napade na povezavni plasti. Vsak uporabnik v svojem omrežju po povezavni plasti lahko komunicira le s stikalom. Komunikacija z drugimi uporabniki tako poteka na omrežni plasti, saj povezavna plast ne omogoča komunikacije z drugimi omrežji.

Na povezavni plasti z drugimi uporabniki komunicira stikalo in ne več uporabnik. Stikalo v tem primeru deluje kot usmerjevalnik (slika 5.1).

V tako razdeljeno omrežje smo povezali dve napravi in preverili, da sta dobili ustrezna naslova IP. Preverili smo tudi povezljivost med napravama s paketi ICMP ping, ki so potrdili povezljivost med napravama.

Na napravi z operacijskim sistemom BackTrack Linux smo zagnali odprtokoden program EtterCap, ki opravi napad z zastrupljanjem tabele ARP [15]. Napada pričakovano ni bilo možno izvesti, ker naprava ni mogla komunicirati z nobeno drugo napravo kot s stikalom.

Poglavje 6

Zaključek

V tem diplomskem delu smo uspešno ločili uporabnike testnega omrežja eduroam na različne VLAN-e. Rešitev, ki smo jo razvili, ne prepreči samo določenih napadov, ampak zaradi ločevanja uporabnikov v različna podomrežja prepreči komunikacijo med njimi na povezavni plasti, s tem pa prepreči vse napade na povezavni plasti.

To rešitev smo predstavili na konferenci Terena Networking Conference 2013 [16], kjer smo dobili nagrado za najboljši študentski projekt [19, 20].

Uporabljena dostopna točka Cisco podpira le 16 VLAN-ov na fizičnem vmesniku, kar je za tipična brezžična omrežja premalo, saj se na eno dostopno točko poveže več kot 16 uporabnikov. Take dostopne točke bi lahko uporabili le za postavitve, kjer je dostopnih točk veliko, uporabnikov pa malo. V našem primeru smo testno omrežje prilagodili tako, da vse nadaljnje uporabnike umesti v isti VLAN, kar pa z vidika varnosti seveda ni primerno, saj ti uporabniki niso zaščiteni pred ostalimi uporabniki v istem VLAN-u. Strežnik RADIUS bi lahko nastavili tako, da bi zavračal prijave uporabnikov, ki ne bi mogli biti v ločenem VLAN-u. S tem bi zagotovili varnost vseh uporabnikov.

Želeli smo tudi olajšati začetno konfiguracijo tako, da bi se VLAN-i na dostopni točki nastavljali sproti, med postopkom prijave uporabnika v omrežje. Ugotovili smo, da to ni možno, ker dostopna točka po nastavitvi VLAN-a na radijskem vmesniku, vmesnik resetira. Po resetiranju vmesnika se nedo-

končan postopek prijave prične od začetka, s čimer nastane zanka in postopek se ne more uspešno končati.

Program za avtomatizacijo nastavitve VLAN-ov na dostopnih točkah smo zasnovali tako, da vsaki dostopni točki nastavi različne VLAN-e. Za pravilno delovanje omrežja z več dostopnimi točkami bi morali prilagoditi tudi program za določanje VLAN-a, saj trenutno predvideva, da je v omrežju samo ena dostopna točka in ne preverja katere VLAN-e ima dostopna točka na voljo.

Varnost omrežja eduroam v Sloveniji se izboljšuje, saj Arnes redno dopolnjuje vzorčno konfiguracijo in testira nove verzije programske opreme. Nekateri napadi, ki smo jih predstavili v [18, 17] tako niso več možni na pravilno nastavljeni in posodobljeni opremi. Ker pa omrežja eduroam po ustanovah niso povsod redno in dosledno vzdrževana, nismo prepričani, če so programska oprema in nastavitve povsod v skladu z vzorčnimi nastavitvami.

Rešitev celovito odpravlja napade na povezavni plasti, ne glede na protokole uporabljene na višji plasti (IPv4 / IPv6). Dodatna prednost rešitve je tudi v tem, da v splošnem odpravi napade na povezavni plasti in tako ni potrebnih dodatnih programov ali naprav, ki bi odpravljale vsak napad posebej.

Čeprav z implementacijo koncepta porabimo štirikrat več naslovov IPv4 kot običajno, pa prikažemo tudi možno rešitev z uporabo 1:1 NAT, ki to slabost odpravi. Pomanjkljivost, ki ostaja, je omejitev števila VLAN-ov (16), ki jih lahko hkrati uporabimo na fizičnem vmesniku dostopne točke. To sicer ni slabost koncepta, ampak pomanjkljivost opreme, uporabljene v implementacijah eduroam. Morda bo novejša programska oprema (firmware) podpirala večje število VLAN-ov, lahko pa namesto obstoječih dostopnih točk uporabimo cenovno ugodne dostopne točke, ki delujejo na operacijskem sistemu Linux, vendar pa le-te trenutno še niso uradno podprte s strani zavoda Arnes.

Literatura

[1] (2013) Federacija izobraževalnih omrežij Eduroam. Dostopno na: http://www.eduroam.si

[2] (2013) Slovenska izobraževalno raziskovalna federacija. Dostopno na: http://aai.arnes.si/eduroam/index.html

[3] (2013) IEEE 802.1X - Wikipedia, the free encyclopedia. Dostopno na: http://en.wikipedia.org/wiki/IEEE_802.1X

[4] (2013) Slovenska izobraževalno raziskovalna federacija. Dostopno na: http://aai.arnes.si/ldap/struktura.html

[5] W. Goralski, *The illustrated network: how TCP/IP works in a modern network*, Morgan Kaufmann Publishers, 2009, pogl. 5.

[6] (2013) David C. Plummer, "An Ethernet Address Resolution Protocol". Dostopno na: http://tools.ietf.org/html/rfc826

[7] (2013) ArnesAAI - Tehnična določila opreme. Dostopno na: http://aai.arnes.si/eduroam/priklop.html#tehnicna_dolocila

[8] (2013) RIPE Network Coordination Centere. Dostopno na: http://www.ripe.net/internet-coordination/news/announcements/ripe-ncc-begins-to-allocate-ipv4-address-space-from-the-last-8

[9] A. S. Tanenbaum, *Computer Networks*, Pearson Education, Inc., 2003, str. 444-448.

[10] (2013) C. Rigney, S. Willens in drugi, "Remote Authentication Dial In User Service (RADIUS)". Dostopno na:
http://www.ietf.org/rfc/rfc2865.txt

[11] (2013) Pxssh. Dostopno na:
http://pexpect.sourceforge.net/pxssh.html

[12] (2013) dr. Janez Stergar, "Virtualna krajevna omrežja - VLAN". Dostopno na:
http://www.egradiva.net/moduli/upravljanje_ik/69_vlan/01_datoteka.html

[13] (2013) Klaas Wierenga, "proposal for inter NREN roaming". Dostopno na:
http://www.terena.org/activities/tf-mobility/start-of-eduroam.pdf

[14] (2013) Shared secrets. Dostopno na:
http://technet.microsoft.com/en-us/library/cc740124%28v=ws.10%29.aspx

[15] (2013) Ettercap (computing) - Wikipedia, the free encyclopedia. Dostopno na:
http://en.wikipedia.org/wiki/Ettercap_(computing)

[16] (2013) Marko Dolničar, "Layer 2 user isolation in Eduroam.si". Dostopno na:
https://tnc2013.terena.org/core/poster/23

[17] (2013) Marko Dolničar, "eduroam and IPv6". Dostopno na:
https://tnc2012.terena.org/core/poster/20

[18] (2013) Marko Dolničar in Jan Bočko Kuhar, "Eduroam insecurities". Dostopno na:
https://tnc2011.terena.org/core/poster/24

[19] (2013) Marko Dolničar wins the sponsored student poster contest at TNC2013. Dostopno na:
http://www.terena.org/news/fullstory.php?news_id=3422

[20] (2013) Študent FRI na prestižni konferenci. Dostopno na: http://www.fri.uni-lj.si/si/novice_in_dogodki/arhiv/15914/novica.html

[21] (2013) The Hacker's Choice. Dostopno na: https://www.thc.org/releases.php

[22] (2013) T. Narten, E. Nordmark in drugi, "Neighbor Discovery for IP version 6 (IPv6)". Dostopno na: http://tools.ietf.org/html/rfc4861

[23] (2013) S. Thomson, T. Narten in drugi, "IPv6 Stateless Address Autoconfiguration". Dostopno na: http://www.ietf.org/rfc/rfc4862.txt

[24] (2013) 6to4 - Wikipedia, the free encyclopedia. Dostopno na: http://en.wikipedia.org/wiki/6to4

[25] (2013) eduroam(UK) Technical Specification. Dostopno na: https://community.ja.net/library/janet-services-documentation/eduroamuk-technical-specification

[26] (2013) Miroslav Milinović, Stefan Winter in drugi "eduroam Policy Service Definition". Dostopno na: https://www.eduroam.org/downloads/docs/GN3-12-192_eduroam-policy-service-definition_ver28_26072012.pdf

[27] (2013) ArnesAAI - Nastavitve Cisco AP-1130, AP-1230, AP-1240. Dostopno na: http://aai.arnes.si/eduroam/ap-cisco.html

[28] (2013) ArnesAAI - Dodatno omrežje za obiskovalce. Dostopno na: http://aai.arnes.si/eduroam/psk.html

Slike

Izpisi