Seminar za IT specijaliste

Sustav nadzora davatelja pristupa bežičnoj mreži (WiFi)

Autor:
Dubravko Penezić, Dubravko.Penezic@srce.hr

Sadržaj

- Bežična mreža (WiFi) i davatelji usluga pristupa (SP)
- Parametri usluge bežičnog pristupa
- Načini provjere sustava
- Raspoloživi alati

Bežična mreža WiFi

- Mreža pristupnih točaka prema WiFi standardu

- WiFi Alliance https://www.wi-fi.org/
- Omogućuje korisnicima pristup Internetu
- Pristupni protokoli°

Pristupni protokoli

- Open – nekriptirani prolazak svih informacija
- WEP – jednostavna enkripcija statičkim ključevima (MAC autentikacija)
- WPA / TKIP – enkripcija dinamičkim ključevima, autentikacija ključem ili EAP (MAC podržan)
- WPA2 / AES – jača i brža enkripcija dinamičkim ključevima, autentikacija ključem ili EAP (MAC podržan)

Davatelj usluge pristupa (SP)

- Osoba ili organizacija/firma koja daje drugim korisnicima pod određenim uvjetima pristup Internetu
- eduroam, mobilni Internet (HT, VIP), ...
- AAA°

AAA

- **Autentikacija** - tko je korisnik°
- **Autorizacija** - smije li koristiti uslugu°
- **Accounting** - kako i kada je uslugu upotrebljavao°

Autentikacija

- Tko je korisnik, tko se spaja
- Korisnička oznaka (anonymous)
- MAC adresa (mogućnost promjene)
- Informativna potvrda Web captive portal

Autorizacija

- Smije li koristiti uslugu
- MAC autorizacija
- RADIUS autorizacija
- Poznavanje ključa (PSK)
- Ne koristi se

Accounting

- Što nam klijenti rade
- Početak sesije (osnovni podaci)
- Trajanje sesije (nadopuna osnovnih podataka, IP adresa)
- Kraj sesije (razlog prekida, trajanje, prenesena količina podataka)
- Podaci ovise o sustavu koji šalje podatke (AP, WLC)

Parametri usluge bežićnog pristupa

- Ispravan rad klijenta i pristupne infrastrukture (WiFi Alliance)°
- Spojenost na bežičnu mrežu (jačina i kvaliteta signala, mogućnost pristupa)°
- Spojenost na Internet (DHCP/IP adresa, ispravne konfiguracije)°
- Protočnost (brzina) prijenosa podataka do traženih resursa°

Ispravan rad klijenta i pristupne infrastrukture

- Zadovoljavaju jednake standarde vezane uz radio postavke (WiFi Alliance)
- Adekvatna radio pokrivenost pristupne infrastrukture
- Ispravna implementacija radio dijela na klijentu prema standardima uz adekvatnu antenu
- Ispravna programska podrška na klijentskoj strani, te na uređajima pristupne infrastrukture

Spojenost na bežičnu mrežu

- Ispravna povezanost na radio nivou između klijenta i pristupne infrastrukture
- Preklapanje radio kanala
- Fluktuacija jačine i kvalitete signala
- Fizičke prepreke, radio smetnje
- Ispravan rad autentikacijske i autorizacijske infrastrukture

Spojenost na Internet

- Ispravan rad DHCP servera
- Ispravne i dostupne IP adrese
- Ispravne konfiguracije mrežnih parametara
- Ispravan rad mrežne pristupne infrastrukture
- Obavijest o mrežnim ograničenjima (ako postoje)

Protočnost prijenosa podataka

- Količina spojenih korisnika
- Adekvatni dostupni mrežni resursi
- Obavijest o ograničenjima

Načini provjere sustava

- Provjera rada pristupnog sustava°
- Provjera rada klijenta°
- Provjera rada mrežne infrastrukture°
- Provjera rada autentikacijske infrastrukture°
- Provjera sustava s stajališta mrežne infrastrukture°
- Provjera sustava s stajališta korisnika°

Provjera rada pristupnog sustava

- Pregled logova pristupnih uređaja
- Pregled izvještaja o lokacijama i interferencijama
- Pregled lokacaija AP-ova i pristupnih antena

Provjera rada klijenta

- Adekvatna programska podrška u operativnom sustavu i/ili mrežnoj kartici
- Uključenost i mogućnost korištenja mrežne kartice
- Ispravnost konfiguracije i mogućnost pristupa očekivanoj bežičnoj mreži

Provjera rada mrežne infrastrukture

- Pregled logova mrežnih uređaja
- Pregled nadzornih sustava
- Fizički pregled mrežne opreme

Provjera rada autentikacijske infrastrukture

- Provjera logova autentikacijskih poslužitelja
- Provjera rada sustava autentikacije
- Provjera autentikacijskih servisa

Provjera sustava s stajališta mrežne infrastrukture

- Nadzorne sonde
- Sustavi za analizu logova

Provjera sustava s stajališta korisnika

- Simulacija realnog načina korištenja bežičnog pristupa internetu:
  - Generičke sonde
  - Klijetske aplikacije

Raspoloživi alati

- Veliki spektar raspoloživih alata
- Hardware-ska rješenja
- Programska rješenja
- Generička
- Specijalizirana

Puppet

- Nadzor konfiguracija
- Vračanje promijenjenih konfiguracija
- Moduli za generiranje standardnih konfiguracija
- Podesivo generičko riješenje
- https://github.com/puppetlabs/puppet

OSSEC

- Sustav za detekciju napada (anomalija)
- Nadzor logova
- Sustav obavještavanja
- Podesiv i generički , s modulima
- https://ossec.github.io/

PerfSONAR

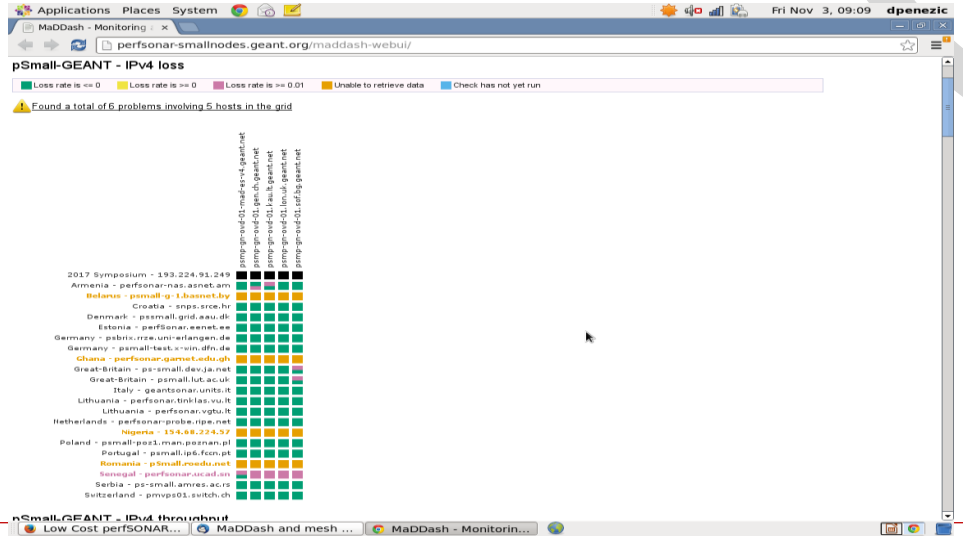
- Sustav za mjerenje i nadzor kompjuterske mreže (uglavnom žičane)
- Dedicirani poslužitelji
- Detekcija pogrešaka i utvrđivanje isporučenih kapaciteta
- https://www.perfsonar.net/
- https://learn.nsrc.org/perfsonar

SmallNode PerfSONAR

- GEANT
- Niža cijena
- Slabije performanse
- Veća usredotočenost na nadzor
- https://github.com/perfsonar/project/wiki/Low-Cost-perfSONAR-Nodes
- https://wiki.geant.org/display/timops/Small+Nodes+status

SmallNode WebUI

- http://perfsonar-smallnodes.geant.org/maddash-webui/



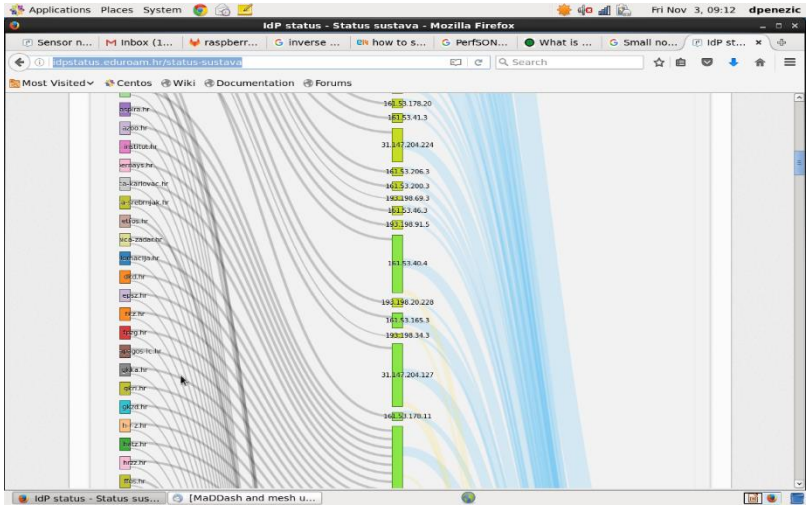
srce

Nadzor autentikacijskog sustava IdP

- http://idpstatus.eduroam.hr/
- Prihvat depersonaliziranih podataka o autentikacijama
- Pohranjivanje i analiza podataka
- Obavještavanje

Nadzor autentikacijskog sustava IdP (2)

- http://idpstatus.eduroam.hr/status-sustava



Nadzor autentikacijske infrastrukture

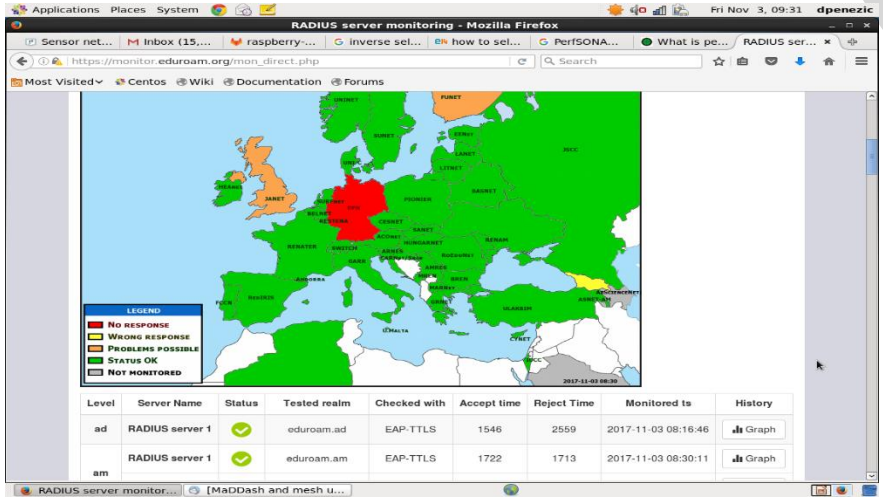
- Prikupljanje podataka iz infrastrukture
- Pohranjivanje i obrada (f-ticks - syslog msg)
- Nadzor skriptama, osnovnih funkcionalnosti
- Autentikacijske informacije

monitor.eduroam.org

- GEANT – nadzor evropske i svjetske RADIUS infrastrukture
- Specijalizirana programska podrška
- Provjera rada osnovnih funkcionalnosti
- Provjera specificnih nedostataka po potrebi

monitor.eduroam.org(2)

- https://monitor.eduroam.org/mon_direct.php

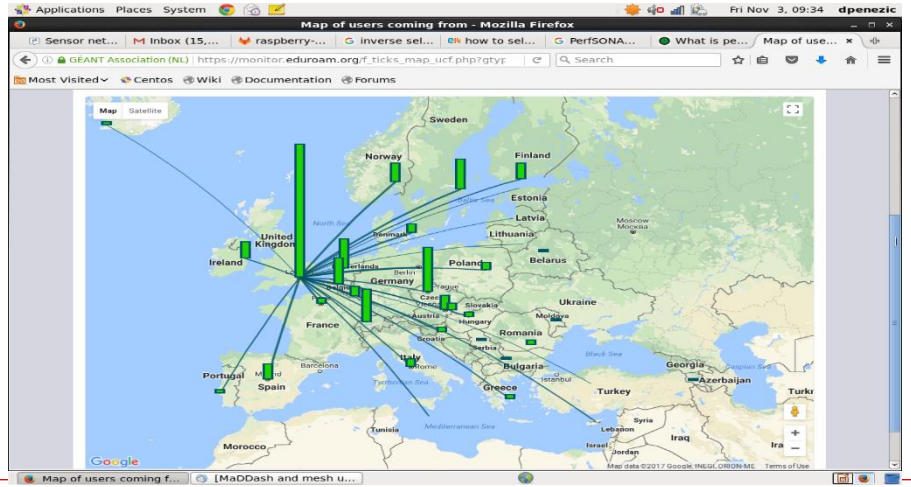


monitor.eduroam.org (3)

- Prihvat depersonaliziranih autentikacijski podataka s centralnih RADIUS poslužitelja
- Obrada i pohranjivanje
- Obavještavanje o anomalijama
- Specifična programska podrška
- F-ticks, syslog msg

monitor.eduroam.org (4)

- https://monitor.eduroam.org/f_ticks_about.php



Nadzorne sonde

- Širok spektar hardwarea
- http://7signal.com/ - dedicirana sonda $$$
- https://atlas.ripe.net/ - standardni žičani mrežni promet (radi se na bežičnom)
- Raspberry Pi – eduroam nadzorna sonda (http://monitor.eduroam.hr/)
- Maleni i micro kompjuteri - ESP8266

monitor.eduroam.hr

- http://monitor.eduroam.hr
- Riješenje bazirano na Raspberry Pi nadzornim sondama
- Vlastito programsko riješenje
- Sonde i centralni sustav za prikupljanje, obradu i prikaz podataka
- HR i svijet

monitor.eduroam.hr – prikupjeni podaci

- WiFi - okolina
- Jačina i kvaliteta signala za eduroam SSID
- Dohvat podataka o eduroamu putem klijentske programske podrške (dostupnost, jačina i kvaliteta signala)
- Pokušaj autentikacije
- Dohvat IP adresa
- Izvođenje testova na mrežnoj razini (speedtest.net)

monitor.eduroam.hr – prikaz podataka

- http://monitor.eduroam.hr/data
- Potrebna autentikacija i autorizacija za pristup

WiFiMon

- GEANT
- Web aplikacija
- Povezivanje podataka iz više izvora
- https://www.geant.org/wifimon
- Razvoj u zastoju

Pitanja ?

Dubravko Penezić, dpenezic@srce.hr

University of Zagreb
University Computing Centre

According to the Open Access Policy, Srce ensures that all research data made by Srce is accessible and free to use by the general public, especially educational and professional information and content derived from the actions and work of Srce.

www.srce.unizg.hr/en

creativecommons.org/licenses/by-nc/4.0/deed.en

www.srce.unizg.hr/oa-and-oer