PREPORUKE ZA MONITORING 802.11 b/g/n WIRELESS INFRASTRUKTURE

RECOMMENDATION FOR MONITORING OF 802.11 b/g/n WIRELESS INFRASTRUCTURE

Ivan Ivanović[1], **Esad Saitović**[1]
Računarski Centar Univerziteta u Beogradu

Sadržaj – *U ovom radu je opisana implementacija monitoring sistema u wireless okruženje. Rad je nastao usled potrebe za monitoringom eduroam*[2] *wireless servisa u AMRES*[3]*-u. Eduroam predstavlja servis koji ima za cilj da pruži nesmetan bežični pristup Internetu svim akademskim građanima bilo gde u svetu.*

Abstract – *This document presents implementation of the monitoring system in wireless enviroment. The work was created by the need for monitoring of the eduroam wireless service in AMRES.Eduroam presents service whose goal is to provide uninterrupted wireless Internet access to academic people anywhere in the world.*

1. Uvod

Eduroam servis predstavlja servis razvijen u međunarodnom akademskom okruženju u okviru TERENA-TF-Mobility projekta. Cilj eduroam-a je da profesorima i studentima obezbedi nesmetan bežični pristup internetu bilo gde u svetu. AMRES je takođe postao član eduroam zajednice i trenutni cilj AMRES-a je da za kratko vreme obezbedi veliki broj wireless pristupnih tačaka. Postoji više načina na koji se može rešiti implementacija eduroam servisa, međutim najvažniji deo implementacije ovog servisa predstavlja autentifikacija korisnika prilikom pristupa eduroam servisu i monitoring wireless infrastrukture. Nadgledanje eduroam servisa se može podeliti na dva dela. Prvi deo monitoringa obuhvata prikupljanje informacija o pristupima korisnika. (vreme pristupa korisnika eduroam servisu, količina prenetih informacija, koju IP adresu je dobio korisnik....) Drugi deo monitoringa predstavlja nadgledanje same fizičke infrastrukture. Da bi se ispravno sprovelo nadgledanje pristupa korisnika eduroam servisu prvo je potrebno obezbediti nadgledanje fizičke infrastrukture.

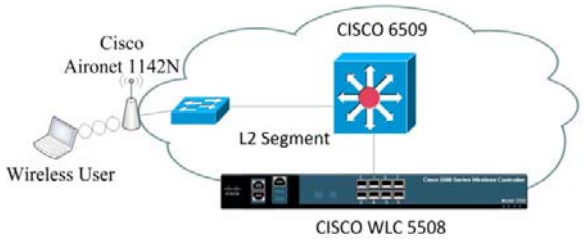
Politika eduroam servisa je takva sa zabranjuje uvid u osetljive informacije korisnika ovog servisa, stoga i monitoring mora biti prilagođen takvim uslovima. Parametri kao što je korisničko ime se ne smeju pojavljivati javno čak ni u sistemu za monitoring. Potrebno je implementirati wireless monitoring dovoljno detaljno da pruži uvid u trenutno stanje wireless mreže ali sa druge strane ne sme se zadirati u privatnost korisnika eduroam wireless infrastrukture.

Prva glava ovog rada opisuje wireless okruženje koje je korišćeno prilikom implementacije monitoringa. Druga glava opisuje arhitekturu wireless okruženja gde je implementiran monitoring. Treća glava rada se odnosi na najčešće korišćene protokole za nadgledanje mreže – SNMP protokol i SysLog protokol, kao i na prednosti korišćenja ovakvog monitoringa. Četvrta glava daje pregled najčešće korišćenih varijabli i parametara za nadgledanje mreže. Peta glava predstavlja zaključak. Uređaji koji su se koritili prilikom postavljanja wireless monitoringa su Cisco WLC5508 wireless kontroler i Lightweight Cisco 1142N Aironet access point.

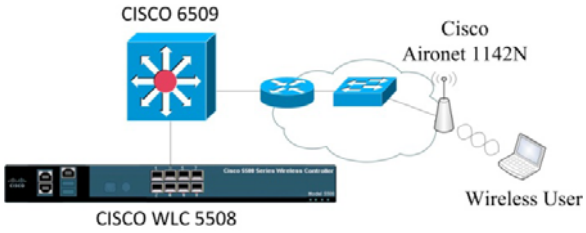
2. Arhitektura wireless okruženja

Logička arhitektura mreže gde se koristi WLC[4] predstavlja zvezdu. U centru se nalazi WLC kontroler a AP[5] se može direktno povezati na njega, kao što je prikazano na slici 1, ili se može nalaziti u posebnoj mreži, kao što je prikazano na slici 2.U AMRES-u su trenutno implementirana tri WLC-a i planira se da se na svaki od njih priključiti oko 100 AP-ova. U situacijama gde je moguće pomoću 802.1q protokola pušten je vlan segment ka svim krajnjim institucijama i AP-ovima je dodeljena IP adresa iz posbnog subneta koji je izdvojen za eduroam servis. U situacijama gde ovakva segmentacija nije bila moguća AP-u je dodeljena fiksna IP adresu iz opsega udaljene mreže. Kako se koriste Lightweight AP cela njihova podešavanja i konfiguracija se nalaze na WLC kontroleru. Kada AP završi sa "boot" procesom i konfigurisanjem parametara koje mu je WLC poslao wireless okruženje postaje funkcionalno za rad. Pored WLC i AP uređaja u ovakvoj arhitekturi postoji još L2 i L3 uređaja koji povezuju celu mrežu. Monitoring ovih ostalih uređaja je takođe bitan za ispravno funkcionisanje eduroam wireless servisa.

[2] eduroam – Education Roaming
[3] AMRES – Akademska mreža Srbije
[4] WLC – Wireless Controller
[5] AP – Access Point



Slika 1 – Arhitektura wireless mreže kada je AP povezan direktno WLC na L2 segmentu



Slika 2 – Arhitektura wireless mreže kada se AP i WLC ne nalaze na istom L2 segmentu

3. Protokoli za nadgledanje

Monitoring mreže u situaciji kada postoji samo jedan WLC kontroler može biti jednostavan. Dosta funkcionalnosti postoji i na samom kontroleru tako se sa njega, direktno preko web pristupa, mogu dobiti pojedine informacije o stanju mreže. Problem se javlja u situaciji kada postoji više WLC kontrolera. U ovoj situaciji menadžment mreže nije centralizovan što doprinosi lošem upravljanju i nadgledanju mreže. Da bi se stekao uvid u trenutno stanje mreže bilo bi potrebno da se priđe svakom kontroleru posebno i da se proveri stanje svih AP-a. To zahteva dosta vremena i otklanjanje problema se na ovaj način povećava. Proizvođači wireless mrežne opreme su uvideli ovaj problem i ponudili softverska rešenja (Cisco wireless control system - WCS) koja pružaju centralizovani nadzor cele infrastrukture. Ovakva rešenje su skupa i jedan od ciljeva ovoga rada je da čitaoce informiše o tome koji su parametri bitni za nadgledanje sa WLC i AP uređaja kako bi se oni kasnije integrisali u već postojeći sistem za monitoring. Protokol koji nam nudi ovakvo rešenje za monitoring je SNMP protokol. WLC i AP takođe podržavaju SNMP protokol, a kako se većina monitoring sistema bazira na SNMP protokolu integracija sa postojećim monitoring rešenjima je jednostavna. Pojedine informacije o AP se mogu očitati samo sa WLC kontorlera što zahteva dodatnu analizu SNMP varijabli koje su podržane od strane proizvođača uređaja.

Kako je monitoring pomoću SNMP protokola već implementiran u AMRES-u, monitoring eduroam wireless servisa predstavlja samo proširenje postojećeg monitoring sistema.

Drugi protokol pomoću koga se može prikupiti dosta informacija o stanju sistema je SysLog protokol. Za razliku od SNMP protokola koji se koristi za periodično očitavanje parametara sa udaljenih uređaja, SysLog reaguje na trenutne promene na uređajima i odmah šalje informacije ka SysLog serveru, sa kratkim opisom problema koji se javio. Integracija sa postojećim monitoring sistemom pruža uvid u celokupno stanje mreže i na taj način smanjuje vreme otklanjanja problema.

4. Šta nadgledati?

Parametri koji su bitni za nadgledanje i koji nam mogu dati informacije o trenutnom stanju u wireless infrastrukturi su sledeći:

- Stanje fizičkih interfejsa.

Informacija o trenutnom stanju interfejsa nam govori kakvo je trenutno stanje linkova. Da li je došlo do prekida nekog linka, da li se aktivirao backup link... Ovde je obuhvaćen monitoring ne samo interfejsa WLC-a i AP-ova već i ostalih mrežnih uređaja koji ih međusobno povezuju.

- Saobraćaj na pojedinim interfejsima.

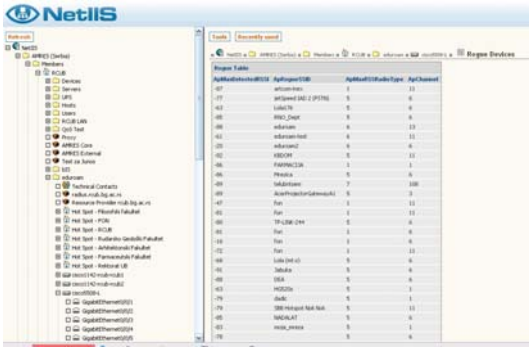
To može biti saobraćaj na fizičkim interfejsima AP-a ili WLC-a. Na taj način se može videti koliko je koji AP opterećen, kao i tendencija povećanja/smanjenja količine saobraćaja tokom vremena. Pored količine prenetih bajtova po sekundi poželjno je pratiti i preneti saobraćaj izražen u paketima po sekundi. Takođe se preporučuje da se nadgleda odbačeni saobraćaj koji se javio usled greške. Na taj način se može detektovati smetnja koja se javlja u blizini AP-a.

- Saobraćaj po svakom VLAN segmentu na AP-u (Multiple SSID).

Doprinos svakog od vlan (SSID) razdvojenih segmenata u ukupnom saobraćaju koji je ostvaren na pojedinim AP-ovima.

- Uticaj signala drugih AP-ova na posmatrani AP.

Prilikom pokretanja AP-a, WLC ima obavezu da odabere kanal na kojem će AP raditi. WLC to čini na osnovu informacije o trenutno zauzetim kanalima u okruženju AP-a i nivou signala na pojedinim kanalima. U slučaju da dođe do ometanja na kanalu na kome radi AP, WLC će sam promeniti kanal, a korisnik može pomoću SNMP-a dobiti informaciju o smetnji (SSID, snaga, kanal) i informaciju o novom kanalu koji je WLC dodelio AP-u. Na slici 3 je dat primer tabele iz NetIIS monitoring sistema gde se nalaze informacije o svim wireless mrežama koje se nalaze u okruženju eduroam AP-a kao i dodatne informacije o jačini signala tih mreža, SSID nazivu, wireless standardu i kanalu na kome rade.



Slika 3 – Primer uticaja drugih wireless mreža na eduroam AP

- Monitoring MAC adresa koje pripadaju uređajima koji koriste eduroam infrastrukturu.

Za svaki uređaj koji pristupi AP-u se putem SNMP-a može proveriti koja je njegova MAC adresa.

- Trenutni broj korisnika koji koriste pojedine AP.

Na osnovu ove informacije se mogu isključiti AP-i koji se ne koriste i prebaciti ne lokacije gde su potrebniji.

- Nadgledanje DHCP pool-a.

U ovakvoj infrastrukruri dodeljivanje IP adresa krajnjim uređajima se može vršiti na više načina. WLC pruža mogućnost i pokretanja DHCP servisa na njemu tako da on može biti odgovoran za raspodelu IP adresa. Uparivanje MAC adresa krajnjih uređaja i IP adresa koje su krajnji uređaji dobili putem DHCP-a predstavlja veoma bitnu informaciju u slučaju pojave problema i potrebe za detaljnijom analizom. Monitoring DHCP pool-a nam takođe pruža uvid u iskorišćenost opsega adresa koje su dodeljene tom pool-u.

- Statičke informacije o AP-ima

Da bi eduroam servis mogao da se koristi potrebno je obezbediti informaciju korisnicima o tome gde se nalaze AP-i, koliko AP-a postoji na određenoj lokaciji, koji tip enkripcije se korist, geografska širina i dužina, itd. Informacija o AP-ima se mora napraviti u predefinisanoj XML formi. AMRES je iskoristio postojeći sistem za monitoring (NetIIS) i u njega se sve ove informacije ručno unose za svaki novi AP koji se postavi. Kako NetIIS predstavlja i informacioni sistem sve informacije o pojedinim eduroam lokacijama se veoma lako dobijaju iz njega. Primer se može naći na sledećem linku http://monitor.eduroam.org/eduroam_map.php?kml=europe_capital gde se nalazi mapa cele evrope sa svim pristupnim tačkama i propratnim informacijama o dostupnim AP-ima. Sve informacije za Srbiju se na mapi dobijaju direktno iz NetIIS-a i svakodnevno se automatski ažuriraju.

5. Zaključak

Eduroam predstavlja servis čija se ekspanzija i popularnost očekuje u skoroj budućnosti. Dobra priprema okruženja za monitoring ovakvog servisa omogućuje nam da svaka institucija ili fakultet koji žele da uvedu ovaj servis mogu nesmetano da vrše nadzor cele infrastrukture i pravovremeno rešavaju probleme ako se jave.

LITERATURA

[1] Douglas Mauro, Kevin Schmidt - Essential SNMP, O'Reilly Media, July 2001

[2] www.net-snmp.org

[3] Cisco white papers - (www.cisco.com)