UDK 004.72:621.395.34

# ANALIZA RAČUNALNE MREŽE NA TEHNIČKOM FAKULTETU U RIJECI
# ANALYSIS OF THE COMPUTER NETWORK AT THE FACULTY OF ENGINEERING IN RIJEKA

**Saša ŠKUNDRIĆ – Antun SOK**

***Sažetak :*** *Rad predstavlja analizu računalne mreže na Tehničkom fakultetu u Rijeci. Prikazano je sadašnje stanje mreže i predložena su moguća poboljšanja.*

**Ključne riječi:** - topologija
- strukturno ožičenje
- AAI@EduHr autentifikacija
- informatička sigurnost

***Summary:*** *The paper presents an analysis of the computer network at Faculty of Engineering in Rijeka. It shows the present condition of the network and proposes possible improvements.*

**Key words:** - topology
- structural cabling
- AAI@EduHr autentification
- informatical safety

## 1. UVOD

Godine 1998. započeo je projekt kojim je postojeću (veoma jednostavnu) lokalnu računalnu mrežu na Tehničkom fakultetu zbog njezine zastarjelosti trebalo zamijeniti novom. Projektom je predviđeno strukturno kabliranje lokalne računalne i telefonske mreže, čime su glavna zgrada i zgrada laboratorija Tehničkog fakulteta međusobno povezane u jedinstvenu računalnu i telefonsku mrežu.
Godine 2002. postojeće kabliranje unutar glavne zgrade Tehničkog fakulteta prošireno je novim (vertikalno kabliranje), dok je nadograđeni prostor iste zgrade u potpunosti prekabliran novim kabelima (horizontalno kabliranje). Unutar zgrade laboratorija Tehničkog fakulteta izvedeno je proširenje segmenata lokalne računalne i telefonske mreže.
Računalna mreža Tehničkog fakulteta u Rijeci zasnovana je na Ethernet tehnologiji. Središnji dio računalne mreže predstavlja Ethernet komutacijski prespojnik smješten u glavnom mrežnom ormaru na prvom katu glavne zgrade Fakulteta. Na priključke prespojnika predviđeno je spajanje poslužitelja, radnih stanica i osobnih računala.
Komunikacijski protokoli na OSI razini 2 su Ethernet IEE802.3 (10BaseT, 100BaseTX, 100BaseFX, 1000BaseSX) .

## 1. INTRODUCTION

The year 1998 marked the beginning of a project which required the substitution of the existing (and very simple) local computer network at the Faculty of Engineering in Rijeka, because the old network had expired. The Project included plans for the structural cabling of the local computer and telephone network. With this project, the main Faculty building and laboratory building have been mutually connected in a homogeneous computer and telephone network.
In 2002, the existing cabling inside the main building was expanded with new vertical cabling, while expansion part of the same building was to be entirely recabled (horizontal cabling). Within the main building, segments of the local computer telephone network were expanded.
The computer network at Faculty of Engineering in Rijeka is based on Ethernet technology. The main part of the network is an Ethernet communication switch located in the main network rack on the first floor of the main building. Switch connections were intended to connect to servers, workstations and personal computers.
Communication protocols on OSI layer 2 are Ethernet IEE802.3 (10BaseT, 100BaseTX, 100BaseFX, 1000BaseSX).

## 2. TOPOLOGIJA

Na Tehničkom fakultetu u Rijeci smješteno je devet mrežnih ormara:
1 – u Računalnom centru ( glavni dolazni ormar)
2 – u informatičkom kabinetu 2
3 – u informatičkom kabinetu 1
4 – u informatičkom kabinetu 4
5 – u telefonskoj centrali
6 – u Zavodu za brodogradnju i inženjerstvo morske tehnologije
7 – u Zavodu za tehničku mehaniku
8 – u Zavodu za konstruiranje u strojarstvu
9 – u Zavodu za mehaniku fluida i računalno inženjerstvo.

U mrežnim ormarima smještena je aktivna oprema računalne mreže i prespojni paneli strukturnog kabliranja. Sva aktivna oprema kompatibilna je s postojećom opremom proizvođača *Planet Technology Corp*. Aktivna oprema napaja se mrežnim naponom 220 V, 50 Hz. Potrebno je osigurati napajanje uređaja u ormaru putem zasebnoga strujnog kruga.
Glavni ormar zvjezdasto je povezan optičkim kablovima s ostalih osam ormara. Na glavni dolazni ormar dolazi uplink iz CARNet-a čije je glavno računalno-komunikacijsko čvorište za Rijeku smješteno u neposrednoj blizini glavnog ormara.
Tehnički fakultet od CARNet-a dobiva putem jednog linka dva VLAN-a, dva mrežna prostora (subnets): 161.53.40.0/24 i 193.198.102.0/24.

## 2. TOPOLOGY

At Faculty of Engineering in Rijeka there are nine network racks:
1 .at the Computer Center (main network rack )
2. at computer classroom 2
3. at computer classroom 1
4. at computer classroom 4
5. at the telephone exchange
6. at the Department of Naval Architecture and Ocean Engineering
7. at the Department of Engineering Mechanics
8. at the Department of Mechanical Engineering Design
9. at the Department of Fluid Mechanics and Computational Engineering

The active equipment of the computer network and the switch panels of the structural cabling are located in the network racks. All active equipment is compatible with existing equipment manufactured by *Planet Technology Corp*. Active equipment is charged by line voltage of 220V, 50Hz. It is necessary to assure the provision of power to the devices in the rack by way of their own electrical circuit.
The main rack is connected with the other eight racks by optical cables in so-called star network topology. An uplink from CARNet leads to the main rack, whose main computer-communication node for Rijeka is located in the immediate proximity of the main rack.
The Faculty of Engineering receives two network spaces (subnets) from CARNet through one link of two VLAN-s, with the two subnets being:
161.53.40.0/24 and 193.198.102.0/24


*Slika 1. CARNet mreža u Hrvatskoj*
*Figure 1. CARNet network in Croatia*

## 3. STRUKTURNO OŽIČENJE

Uporaba strukturno ožičenih sustava važna je prekretnica u mrežnoj tehnologiji posljednjih godina.
Strukturirano ožičeni sustavi sastoje se od većeg broja jednostavnih, pasivnih uređaja kao što su razvodne kutije, prolazne kutije, prespojne ploče, konektori za ožičenja i nosači kabela, raspoređenih na logički, strukturirani način.
Prijenosni mediji koji se koriste za izvedbu strukturnog ožičenja na Tehničkom fakultetu su:
- 4-parični neoklopljeni bakreni kabel minimalno poboljšane kategorije 5
- višeparični telefonski neoklopljeni bakreni kabel
- jednomodni i višemodni svjetlovodni kabeli.

Dužina pojedinih segmenata višeparičnih neoklopljenih kabela između mrežnih ormara i priključnih kutija ne prelazi 90 metara. Postoje i takozvani rezervni vodovi koji su postavljeni radi eventualnog proširenja veze.
Glavne komponente ožičenja su:
- zidna (podna) utičnica
- horizontalni razvod kabela
- katni mrežni ormari i prolazne kutije
- vertikalni razvod
- glavni mrežni ormar.

Zidna utičnica je mjesto gdje krajnji korisnik (profesor, student) uključuje svoje računalo u sustav ožičenja zgrade. Na tom mjestu fizički završava kabel s upredenim paricama, koaksijalni kabel ili optički kabel.
Horizontalni razvodni sistem je kabel koji povezuje zidnu utičnicu s najbližim mrežnim ormarom na istom katu, uključujući i opremu za držanje kabela (kabelski kanali, vodilice). Kabel s upredenim paricama najčešće je korišten medij za horizontalni razvod.
Prolazne kutije omogućavaju povezanost između horizontalnog razvoda i mrežne okosnice unutar zgrade ili vertikalnog razvoda. U mrežnim ormarima nalaze se aktivna oprema i prespojne ploče.
Vertikalni razvod ili mrežna okosnica povezuje pojedine mrežne ormare na katu ili prolazne kutije s glavnim mrežnim ormarom zgrade. Kao medij najčešće se koristi optički kabel.
Glavni mrežni ormar smješten je u glavnoj telekomunikacijskoj prostoriji zgrade. Svi razvodi završavaju u toj prostoriji.

## 4. AKTIVNA OPREMA

Optički kabel iz CARNet-a dolazi na ulazni prespojnik (*switch*) u glavnom ormaru iz kojeg su provedeni uplinkovi prema ostalim prespojnicima u ormarima.
Osnovna funkcija prespojnika je da prema MAC adresi usmjerava promet u lokalnoj mreži. MAC adresa je fizička adresa mrežne kartice računala (NIC).
Npr. ako PC 3 želi komunicirati s PC 2 (slika 2), pošalje mu podatak koji putuje preko prespojnika 1 koji vrši

## 3. STRUCTURAL CABLING

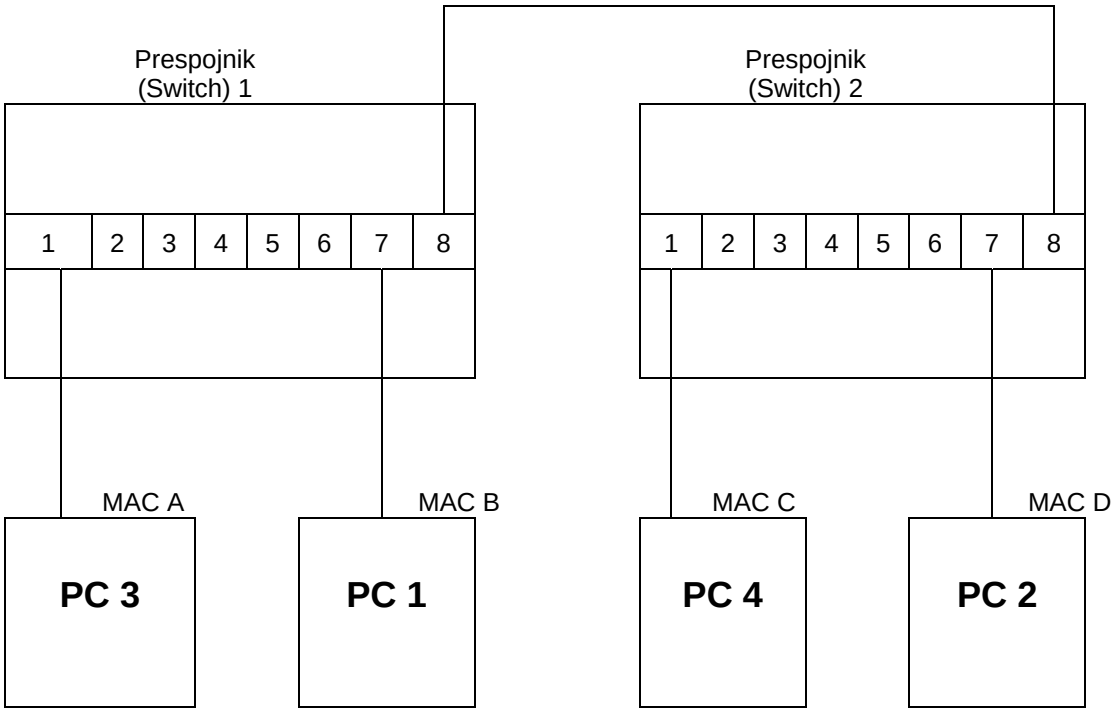
The application of structurally cabled systems is an important turning-point in computer network technology in the past few years. These are made of a major number of simple passive devices such as distribution boxes, pass-through boxes, switch boards, cable connectors etc., distributed in a logical, structured way.
Transport mediums used for structural cabling at the Faculty of Engineering are:
- 4-pair unshielded copper cable min. category 5
- multi-pair telephone unshielded copper cable
- one-mode and multi-mode fiber-optic cables

Each segment length of multi-pair unshielded cables between the computer network racks and the connection boxes is less then 90 meters. There are also so-called spare cables for potentially expanding connections.
The main components of cabling are:
- wall (floor) socket
- horizontal distribution of cables
- floor mount computer network racks and pass-through boxes
- vertical distribution
- main computer network rack.

The wall socket is where the end user (professor, student) plugs his computer into the wiring system of the building. At this location, the unshielded twisted pair cable, coaxial cable or optical cable physically comes to an end. The horizontal distribution system is a cable which connects the wall socket with the nearby computer network rack on the same floor, including cable holding equipment (cable channels, guides). The most frequently used medium for horizontal distribution is twisted pair cable.
Pass-through boxes enable connection between horizontal distribution and the network backbone inside the building, i.e., the vertical distribution. The active equipment and switch boards are placed in the network racks.
The vertical distribution or network backbone connects the floor mount network racks or pass-through boxes with the main computer network rack of the building. Optical cable is usually used as medium.
The main network rack is placed in the central telecommunication room of the building. All distribution ends in that room.

## 4. ACTIVE EQUIPMENT

Optical cable leads from CARNet to the main switch in the main rack. Links run from the main rack to other switches in the other racks. The main function of the switch is to direct traffic in the local network by the MAC address. The MAC address is the physical address of the computer network card (NIC).
For example, if PC 3 wants to communicate with PC 2 (Figure 2), it sends data frame through switch 1. Switch 1




(2)

| Prespojnik (Switch) 1 | |
|---|---|
| 1 | MAC A |
| 2 | |
| 3 | |
| 4 | |
| 5 | |
| 6 | |
| 7 | MAC B |
| 8 | MAC C i MAC D |

| Prespojnik (Switch) 2 | |
|---|---|
| 1 | MAC C |
| 2 | |
| 3 | |
| 4 | |
| 5 | |
| 6 | |
| 7 | MAC D |
| 8 | MAC A i MAC B |

*Slika 2. Komunikacija dvaju prespojnika*
*Figure 2. Communication of two switchers*

funkciju prespajanja odnosno odlučivanja. Prespojnik 1 pročita iz paketa odredišnu MAC adresu i na osnovi te adrese iz MAC tablice pronalazi na kojem portu se nalazi ta MAC adresa (port 8) te prosljeđuje paket na taj port. Na osnovi MAC tablice na prespojniku 2 podatak se šalje na njegov port 7. Prespajanje u prespojnicima je u drugom OSI sloju (podatkovni sloj).
Usmjerivač (*router*) smješten je u CARNet-u – Tehnički fakultet nema usmjerivača. Usmjerivač je uređaj OSI sloja 3 (mrežni sloj), vrši usmjeravanje prema IP adresama i usmjerava promet između različitih LAN-ova. Usmjerivač u CARNet-u povezuje sve fakultete u Rijeci, pa tako i Tehnički fakultet s ostatkom Hrvatske i svijeta.

reads the MAC Destination from data frame address and based on that address from the MAC table it finds the port on which that MAC address is located (port 8), and sends the data frame on to that port. Based on the MAC table on switch 2, the date frame is sent on to port 7. Switching is in the second OSI layer (data layer).
The router is located at CARNet, therefore the Faculty of Engineering does not have their own router. The router is an OSI layer 3 (network layer) device and its function is to reroute traffic towards different local networks according to IP address.
The router at CARNet connects all the faculties in Rijeka, including the Faculty of Engineering, with the

Zbog segmentiranja mreže potrebno je uključivanje usmjerivača, usmjerivači na fakultetu softverskog su tipa, ima ih 5, od kojih neki imaju više mrežnih kartica namijenjenih segmentiranju mreže. Jasnije rečeno, svi informatički kabineti spojeni su na jedan softverski usmjerivač i zauzimaju za promet jednu javnu IP adresu. Ostala četiri softverska usmjerivača namijenjena su:
- studentima
- fakultetskim službama
- akademiji Cisco
- knjižnici.

## 5. VATROZID

Vatrozid (*firewall*) je mrežni uređaj kojem je namjena filtriranje mrežnog prometa tako da se stvori sigurna zona. Kod usmjerivača korištenih na Fakultetu vatrozid omogućuje čitanje zaglavlja paketa te filtriranje nepoželjnih sadržaja prema tipu prometa.
Onemogućeno je da se studenti spajaju na druge mreže unutar Fakulteta, onemogućeno im je presretanje prometa iz dugih VLAN-ova (virtualnih mreža).
Vatrozid onemogućuje da se studenti spajaju na bilo koje računalo unutar Fakulteta.

## 6. AUTENTIFIKACIJA

Pri korištenju računala na Fakultetu ili čitanju elektroničke pošte preko web-sučelja, korisnik se mora prijaviti, identificirati. To čini tako da upiše korisničko ime i lozinku. Računalo ima spremljenu njegovu lozinku (ili njezin par), te ako ono što je upisao odgovara onome što je spremljeno, bit će mu omogućen pristup sustavu. Cilj je autentifikacije nedvosmisleno identificirati korisnika sustava i prema tome mu omogućiti raspolaganje njegovim podacima.
U svrhu toga na Fakultetu je prošlog ljeta uvedena međunarodna AAI@EduHr autorizacija i autentifikacija u okviru međunarodnog projekta.
AAI@EduHr je autentifikacijska i autorizacijska infrastruktura sustava znanosti i visokog obrazovanja u Republici Hrvatskoj. Sustav AAI@EduHr tehnički je realiziran uporabom distribuiranih LDAP imenika. Svaka ustanova iz sustava MZOŠ, koja je uključena u sustav AAI@EduHr kao matična ustanova ima vlastiti
LDAP imenik u kojemu su pohranjeni elektronički identiteti korisnika iz te ustanove. AAI@EduHr omogućava bilo kome bilo odakle u svijetu da se koristi računalima na Tehničkom fakultetu tako da se u informatičkom kabinetu logira sa svojim AAI@Edu korisničkim imenom i zaporkom.
Mana je AAI@EduHr-a što se autentifikacija vrši preko CARNet-a u Zagrebu.

rest of Croatia and the world.
Because of network segmentation, it is necessary to use routers, and there are 5 software routers at the Faculty, The router at CARNet connects all the faculties in Rijeka, including the Faculty of Engineering, with the rest of Croatia and the world.
and some of them have several network cards intended for network segmentation. More precisely, all computer classrooms are connected to one software router and have one IP address.
The other four routers are intended for:
- students,
- faculty services
- the Cisco Academy
- the library

## 5. FIREWALL

A firewall is a network device that is used to filter network traffic in order to create a safe zone. The firewall used by routers at the Faculty enable the reading of the data frame header and the filtering of unfavorable contents according to the type of traffic.
It is not possible for students to connect to other networks at the Faculty and to intercept traffic from other VLAN-s (virtual LAN-s).
The firewall does not enable students to connect to any computer they want from inside the Faculty.

## 6. AUTENTIFICATION

When using computers at the Faculty, or when reading electronic mail over the web server, the user must identify himself. He does this through registration of his username and password. The computer has stored passwords, so if the username and password correspond with the username and password stored in computer, he will be granted access into the system. The purpose of authentification is the unequivocal identification of the user, thereby making the data available to him.
With this intent, the international AAI@EduHr authorization and authentification as part of an international project has been held at the Faculty since last summer. AAI@EduHr is an authentification and authorization-based infrastructure of the sciences and higher education in the Republic of Croatia. The system AAI@EduHr is technically realized by use of a distributed LDAP directory. Every institution of MZOŠ that is included in the AAI@EduHr system has its own LDAP directory with the electronic identities of its users. With AAI@EduHr, anybody from all over the world can use the computers at the Faculty of Engineering if hi logs on through the information processing office with is AAI@EduHr username and password.
Autentification is realized through CARNet at Zagreb and that is fault of AAI@EduHr.

## 7. INFORMATIČKA SIGURNOST

Na svim usmjerivačima unutar pojedinih VLAN-ova vrši se logiranje ukupnog prometa, a logovi se čuvaju određen broj mjeseci. Svrha toga je da se u slučaju prijave sigurnosnog inicidenta može po mogućnosti otkriti tko je, kada i zašto učinio taj inicident.
Pomoću AAI@EduHr postignuto je da se zna tko je i kada radio za kojim računalom. Doneseni su pravilnici o korištenju računala na Fakultetu za zaposlenike, vanjske suradnike, studente, te pravilnici o uporabi računala u informatičkim kabinetima, čitaonici i laboratorijima.
Plan je u dogledno vrijeme osigurati informatičku opremu za korištenje bežične (*wireless*) mreže. U tu svrhu već se rade preliminarna ispitivanja i analize koje bi zračenje bilo manje: ako se postave vanjske antene ili unutarnja pristupna mjesta (*access points*). Cilj je postići da svaki student koji posjeduje prijenosno računalo može to računalo koristiti u odgovarajućim prostorijama na Fakultetu na nastavi ili vježbama.

## 8. SADAŠNJE STANJE MREŽE I MOGUĆA POBOLJŠANJA

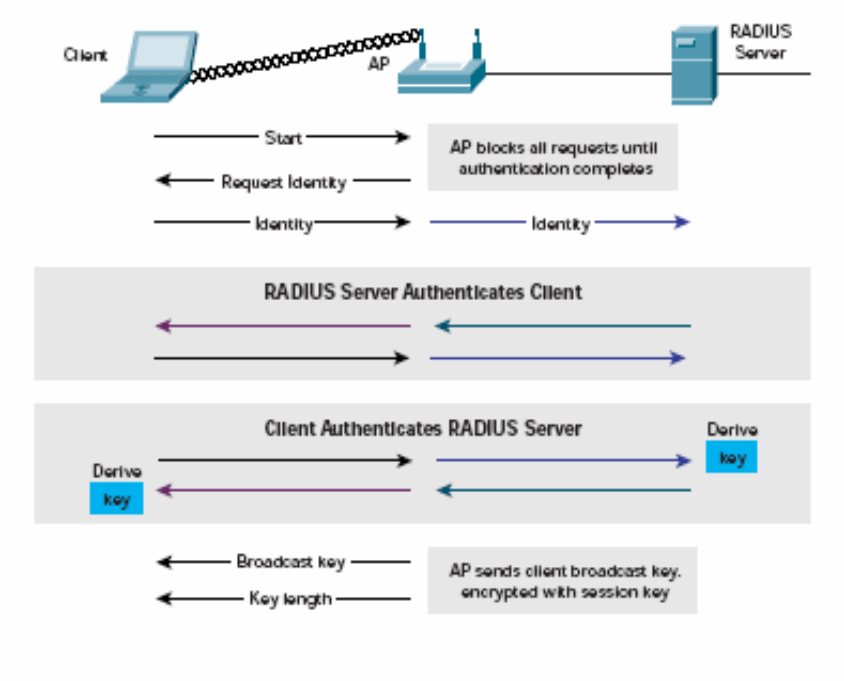
Koristi se zastarjela oprema malih mogućnosti, npr. glavni prespojnik za distribuciju ima ukupni promet od 9.6 Gb/s između bilo kojih portova, što je premalo i dolazi do zagušenja. U dogledno vrijeme trebalo bi zamijeniti prespojnike novima koji će imati brzinu 50 ili 100 Gb/s. Prespojnici nemaju 802.1X radijus autentifikaciju. Korištenjem 802.1X radijus autentifikacije omogućilo bi se svakome da se uz korištenje odgovarajućeg softvera pri spajanju na mrežu autentificira, te da ga prema njegovoj autentifikaciji prespojnik spoji u onaj VLAN u koji ima pravo pristupa. Korištenjem 802.1X protokola osobi koja želi pristupiti mreži onemogućen je pristup dok prespojnik ne izvrši autentifikaciju. Prespojnik blokira port na koji se osoba priključila svojim prijenosnim računalom i propušta samo 802.1X promet. Promet kao što je HTTP (prijenos www-stranica), FTP (prijenos datoteka između dvaju računala), SMTP i POP3 (razmjena elektroničke pošte) je blokiran. Komunikacija između prijenosnog računala i prespojnika (slika 3):
1.- osoba putem svojega prijenosnog računala šalje prespojniku zahtjev za propuštanje
2.- prespojnik odgovara računalu da je primio zahtjev i traži od računala autentifikaciju
3.- računalo šalje paket u kojem se nalaze ident. podaci
4.- prespojnik prosljeđuje identifikacijske podatke računala do servera za autentifikaciju
5.- server provjerava identifikaciju
6.- ako je autentifikacija u redu, prespojnik će prespojiti računalo u odgovarajuću VLAN mrežu, a ako nije, odbit će zahtjev računala.
Prespojnici koriste zastarjeli softver i operacijski sustav za koje nema mogućnosti nadogradnje i posljedica su toga učestaliji zastoji u radu.

## 7. INFORMATIC SECURITY

On all routers inside virtual networks, logs of all the traffic are stored for a certain period of time. The purpose of this is that in the case of a security incident, who caused and why they caused an incident can be discovered .
With AAI@EduHr, it is known who and when has been in a session and on which computer.
There are regulations at the Faculty for the use of computers for employees, external assistants, and students, as well as regulations for the use of computers in the informatics classrooms, library and laboratories.
There is now a plan to ensure informatics equipment for the use of wireless networking. To that extent, preliminary investigations have been carried out as to which radiation is relatively lower, especially with regard to the placement of either external antennas or internal access points. The goal is to make it possible for students to use their own laptops in the appropriate classrooms of the Faculty during class or interactive training.

## 8. PRESENT CONDITION OF NETWORK AND POSSIBLE IMPROVEMENTS

Equipment with limited possibilities is used, for example, the main switch for distribution has an overall traffic rate of 9.6 Gb/s between ports, which is too small and leads to congestion. In the near future, the switches should be substituted with new ones with speeds of 50 or 100 Gb/s. Switches do not have 802.1X radius authentification. With 802.1X, it would be possible for everyone to use the proper software to authenticate themselves and with that authentification the switch would connect them to the VLAN through which they would have access.
With the 802.1X protocol, it is possible for someone to block access to the network until the switch carries out authentification. The switch blocks the port on which someone is connected to his laptop and then allows only 802.1X traffic. Traffic as HTTP (www pages), FTP (file transfer), SMTP and POP3 (exchange of electronic mail) is blocked.
Communication between laptop and switch (Figure 3):
1.- someone with his laptop sends the switch a request for authentification
2.- the switch answers the laptop and that request is accepted and requests authentification
3.- the laptop sends the identification data
4.- the switch sends the identification data to the server for authentification
5.- the server checks the identification
6.- if the identification is valid, the switch will connect the laptop to a certain VLAN network, and if not, the switch will refuse the request from the laptop.
Switches use outdated software and an operating system which is not possible to upgrade. This consequently results in more frequent interruptions of work.




*Slika 3. 802.1X radijus autentifikacija*
*Figure3. 802.1X radius authentification*

## 9. ZAKLJUČAK

Na Fakultetu je umreženo više od 400 računala, a mreža je iz sigurnosnih razloga podijeljena u desetak virtualnih mreža.
Autentifikacija se obavlja preko AAI@EduHr sustava koji omogućava korištenje računala na Fakultetu uz logiranje AAI@EduHr korisničkim imenom i zaporkom.
Osnovni je nedostatak mreže nekvalitetan aktivni mrežni dio opreme koji je zastario. Oprema *Planet* koja se sada koristi trebala bi u što skorije vrijeme biti zamijenjena novom, npr. opremom *Cisco* koja je skuplja i traži veća ulaganja, ali bi jamčila sigurniji rad i ne bi se događali zastoji u radu. Trebalo bi postaviti cjeloviti Cisco-v Pix Firewall uređaj za cijeli Fakultet radi povećanja cjelokupne sigurnosti na Fakultetu, a time bi se mreža na Tehničkom fakultetu ponašala kao inteligentna mreža.

## 9. CONCLUSION

At the Faculty there are 400 computers and for safety reasons the network is divided into ten virtual networks.
AAI@EduHr provides authentification for the use of computers at the Faculty with usernames and passwords.
The main network fault is in outdated active equipment. Planet equipment should be replaced with new Cisco equipment as soon as possible. Cisco equipment is expensive but provides safety of work and less interruptions in work. There is the need for an integral Cisco Pix Firewall device for the Faculty with the purpose of enlarging overall security at the Faculty, and such network would function as an intelligent network.

## LITERATURA
## REFERENCES

[1] SCHATT, S., *Lokalne mreže*, ZNAK, Zagreb, 1995.
[2] BIGELOW, S. J., *Računarske mreže: Instaliranje, održavanje i popravljanje*, Mikroknjiga, Zagreb, 2004.
[3] GROTH, D., McGRE, D., *i - NET+ OSNOVE UMREŽAVANJA*, Kompjuter Biblioteka, Čačak, 2003.
[4] INTERNET

Strukovni prilog

Technical note

Adrese autora / Author's addresses:
Saša Škundrić, ing.
Prof. v. šk. mr. sc. Antun Sok, dipl. ing.
Sveučilište u Rijeci, Tehnički fakultet
Vukovarska 58
HR – 51000 Rijeka, Hrvatska