IEEE 802

CONTENT
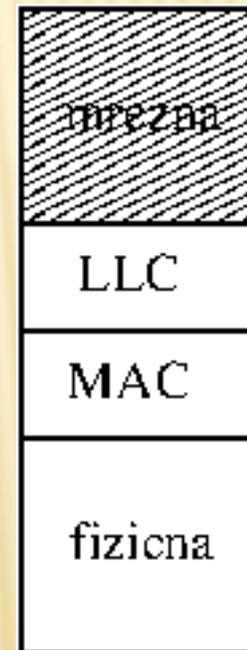
- IEEE802 family
- Working group IEEE802.1
- Connecting to IEEE802.1x network

IEEE 802

- Family of IEEE standards dealing with local area networks(LAN) and metropolitan area networks(MAN)
- Work is done in working groups
- More on URL: http://www.ieee802.org/
 - challange: Go to the website and review the contents.

3

IEEE 802 ARCHITECTURE

- Basic architecture:
  - bottom: *media access Control* (*MAC*)
  - top: *logical link layer* (*LLC*)
- Seperate access to the medium and addressing -> transfer of frames

mrezna
LLC
MAC
fizicna

TRANSPORT AND TOPOLOGY IEEE 802

✖ uniform frame addressing space

✖ (local) network has to know how to correctly send frames
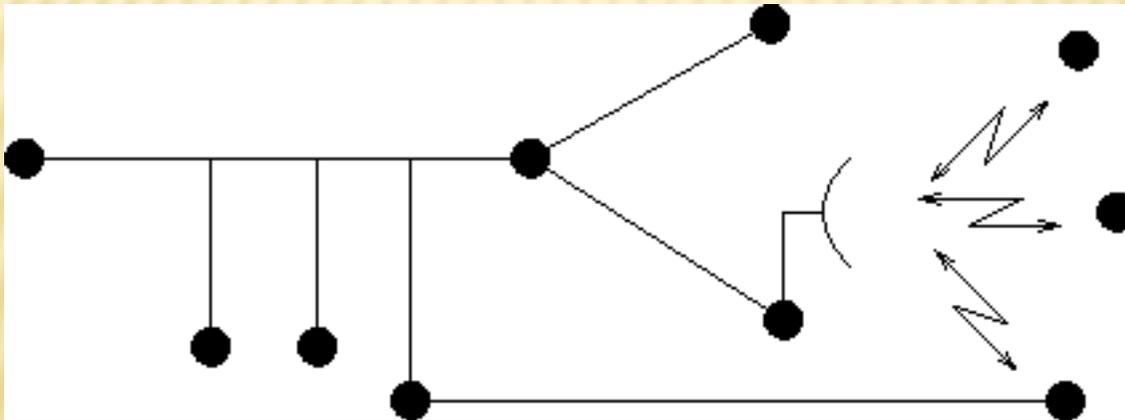
IEEE 802 FAMILY

- IEEE 802.1 Bridging (networking) and Network Management
- IEEE 802.2 Logical Link Control – LLC
- IEEE 802.3 Ethernet
- IEEE 802.4 Token bus
- IEEE 802.5 Defines the MAC layer for a Token Ring
- IEEE 802.6 MANs
- IEEE 802.7 Broadband LAN using Coaxial Cable
- IEEE 802.8 Fiber Optic TAG
- IEEE 802.9 Integrated Services LAN
- IEEE 802.10 Interoperable LAN Security

6

IEEE 802 FAMILY

- ✖ IEEE 802.11 Wireless LAN (WLAN) & Mesh (Wi-Fi certification)
- ✖ IEEE 802.12 demand priority
- ✖ IEEE 802.13 Used for 100BASE-X Ethernet
- ✖ IEEE 802.14 Cable modems
- ✖ IEEE 802.15 Wireless PAN (Bluetooth, …)
- ✖ IEEE 802.16 Broadband Wireless Access (WiMAX certification)
- ✖ IEEE 802.17 Resilient packet ring
- ✖ IEEE 802.18 Radio Regulatory TAG
- ✖ IEEE 802.19 Coexistence TAG
- ✖ IEEE 802.20 Mobile Broadband Wireless Access
- ✖ IEEE 802.21 Media Independent Handoff
- ✖ IEEE 802.22 Wireless Regional Area Network
- ✖ IEEE 802.23 *Emergency Services Working Group* (march 2010)

IEEE 802.1 – BRIDGING AND NETWORK MANAGEMENT

- *Bridging (networking) and Network Management*
- Connecting between sub-networks
- Network management (for example: smallest spanning tree)
- Network security
- Working on top of LLC
- More on URL:
http://www.ieee802.org/1/
  + challange: Go to the website and review the contents.

```
| LLC     |
| MAC     |
| fizicna |
```

IEEE 802.1 WORKING GROUP

- *802.1b: LAN/MAN management (removed)*
- 802.1d: bridges on MAC layer
- *802.1e – 802.1g: removed*
- 802.1h: Ethernet MAC bridges
- 802.1q: virtual LAN (VLAN)
- **802.1x: network access control** *(Port Based Network Access Control)*

IEEE 802.1 WORKING GROUP

- 802.1ab: stations, access control of the medium and conectivity searching
- 802.1ae: security on MAC layer
- 802.1ar: safe unit identification
- 802.1as: time synchronization and time-sensitive aplications in networks with bridges
- 802.1ax: *link aggregation*
- 802.1ba: avdio/video systems with bridges

NETWORK CONNECTION MANAGEMENT (IEEE 802.1X)

- Network access is a service, that enables usage of other services
  - Web access, …
- more on URL

    http://www.ieee802.org/1/pages/802.1x-2004.html

  - challange: Go to the website and review the contents.

NETWORK CONNECTION MANAGEMENT (IEEE 802.1X)

- Network access is a service, that enables usage of other services
  - Web access, ...
- Usage of a service can be free or controled
- For controled usage of service we need to:
  - Find out, who is a potential user; and
  - if he has premission for usage of service.
- authentication and authorisation (logging also somewhere)
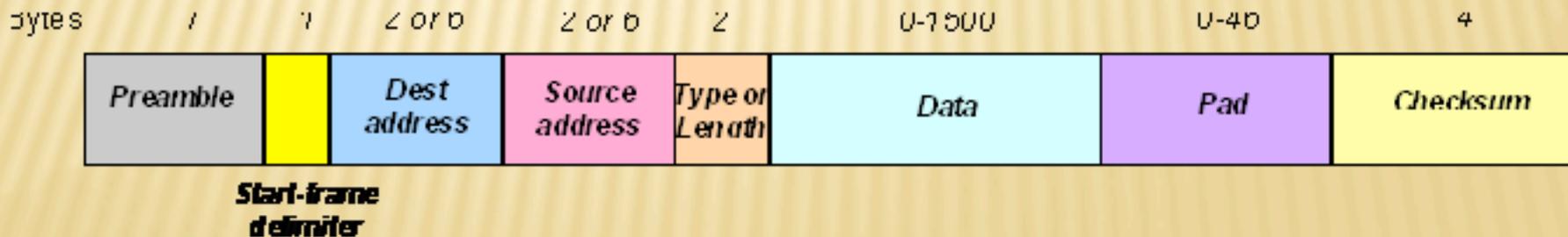- task: somehow insert AAA into establishment ofconecting to network

IEEE 802.1X ARHITEKTURA

- There are three building blocks:
  - *supplicant*
  - *authenticator*
  - *authentication server*
- supplicant signs in to authenticator, that checks his identity on *authentication server* and if he is authorised for access to the network
- task: *embend EAP on data link layer*
  - challange: How(!) authenticator really enables access to network for supplicant?

EAP   RADIUS

| *supplicant* | *authenticator* | *authentication server* |

IEEE 802.1X EAPOL

× standard IEEE 802.1x defines EAP on data link layer – EAP over LAN -> EAPOL

  + Later EAPOL was also used in other work groups IEEE 802.1x:

    × 802.1ae: security on MAC layer
    × 802.1ar: safe identification of units

× EAPOL is defined so that his content is sent directly in Ethernet frames with contents badge 0x888E:

  + Preamble (7-bytes) Start Frame Delimiter (1-byte)
  + Dest. MAC Address (6-bytes) Source MAC Address (6-bytes)
  + Length / Type (2-bytes)
  + MAC Client Data (0-n bytes)
  + Pad(0-p bytes) Frame Check Sequence (4-bytes)

| bytes	7	1	2 or 6	2 or 6	2	0-1500	0-46	4
	Preamble		Dest address	Source address	Type or Length	Data	Pad	Checksum

Start-frame delimiter

EAP – FOR REFRESHMENT

- Defined in RFC 3748
- Support for different authentication protocols
- stepping protocol

IEEE 802.1X – HOW DOES IT OPERATE

✖ *inicialization*: when avtenticator (usualy also switch, WLAN access point etc.) detects new supplicant, he enables him **only** IEEE 802.1x comunication

+ From here on EAP protocol starts
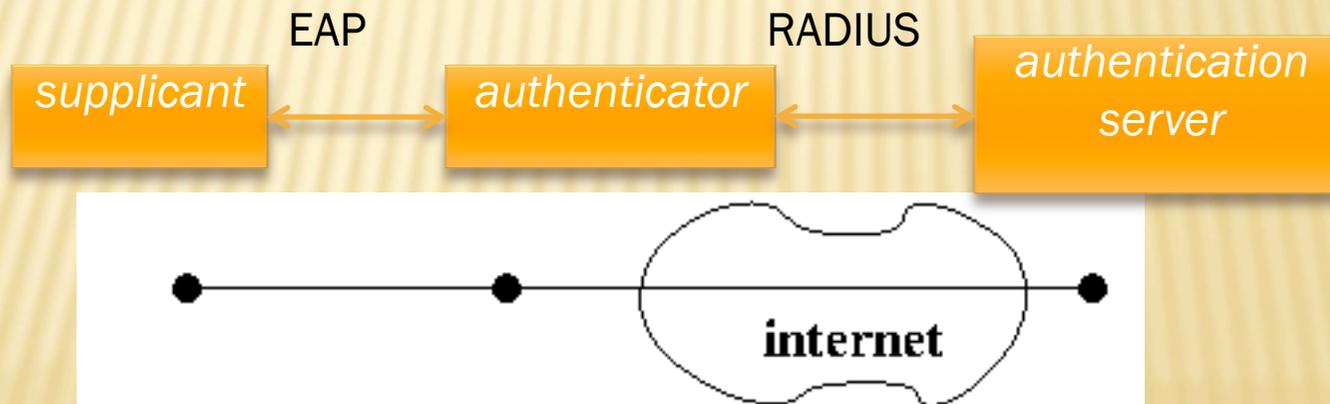
IEEE 802.1X – HOW DOES IT OPERATE (CONTINUED)

- *invitation*: authenticator (periodicaly) sends invitation to supplicant, to introduce himself
  - Supplicant introduces himself to authenticator, which sends introduction to avtentication server (RADIUS)
  - Avtenticator is now just an in between server for avtentication server – avtentication server is the one that actualy performs the authentication
  - trust!! between authenticator and autentication server
   - challange: How to program that trust?
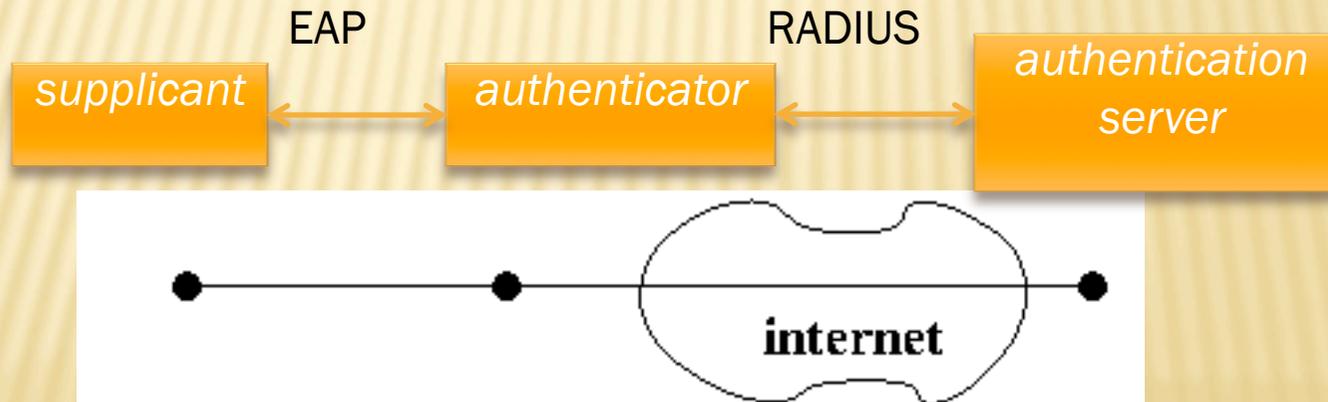
IEEE 802.1X – HOW DOES IT OPERATE (CONTINUED)

- ✖ negotiation: is performed between supplicant and authenticator in accordance with EAP protocol
  - ✛ which authenticacion protocol,
  - ✛ challange and response, ...

EAP		RADIUS	
supplicant	↔	*authenticator*	↔	*authentication server*

internet
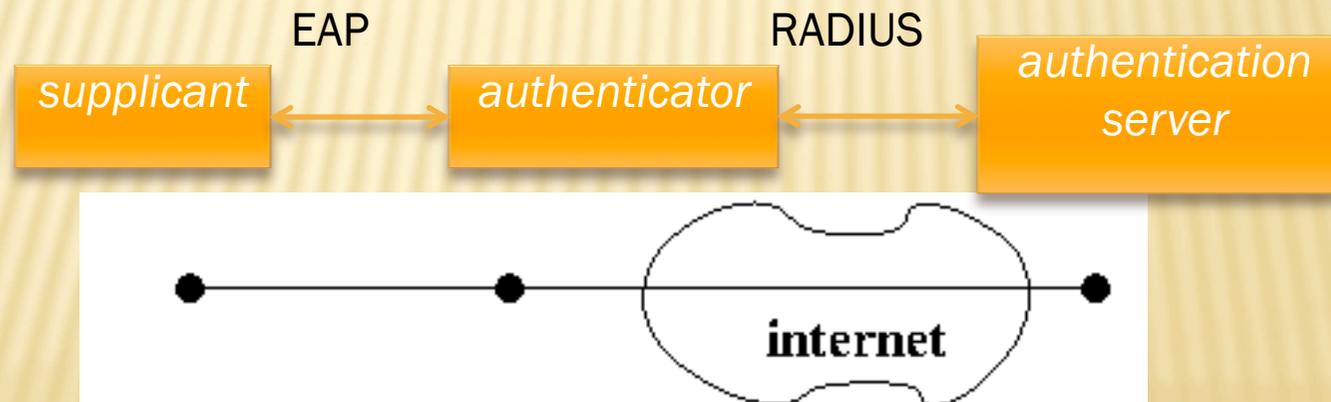
IEEE 802.1X – HOW DOES IT OPERATE (CONTINUED)

* *authentication*: supplicant authentication alone

* authenticator, when server authenticates supplicant, he grantes him access to the local network
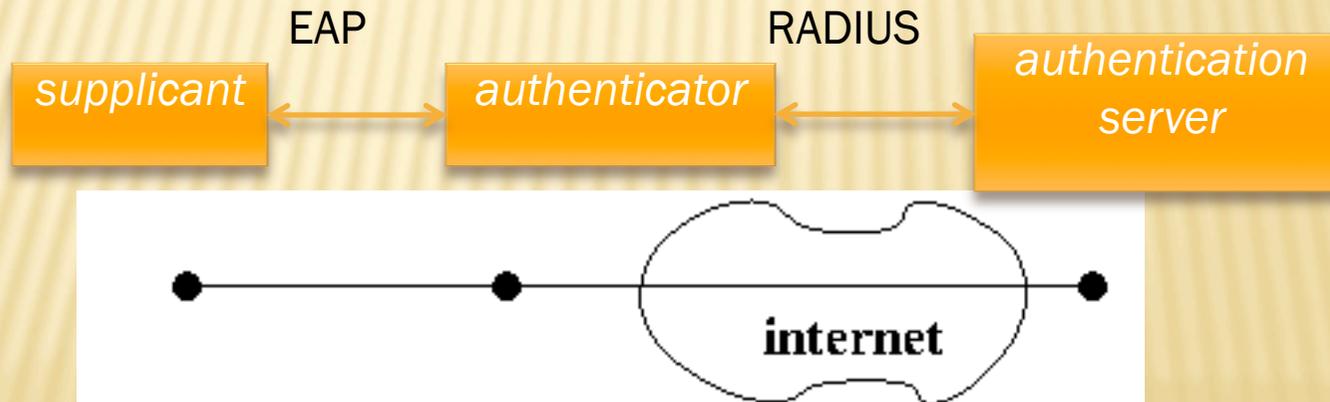
EDUROAM

- federations authentication servers, who trust each other
- user of wichever server can authenticate himself at wichever authenticator in federation
  - Challange: Where is now asimetric criptography, that EDUROAM uses in protocol for authentication? For authentication of who do we use it? Answer in the forum for extra points.

Thank you for your attention

and

good luck!