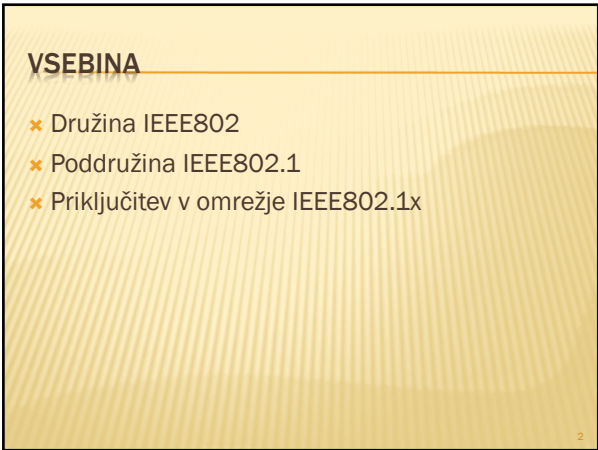
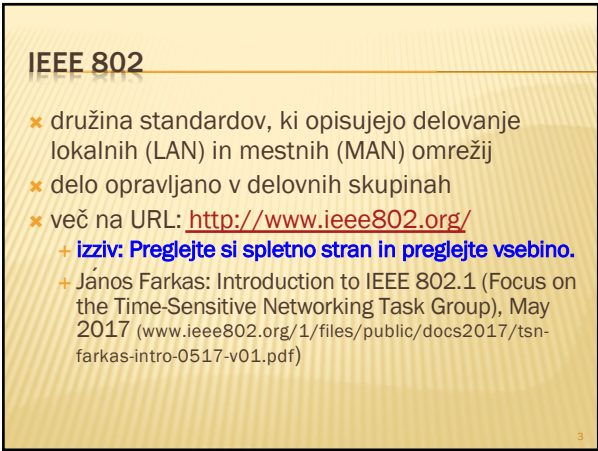


1



2



3

ARHITEKTURA IEEE 802

- ✘ osnovna arhitektura:
 - + spodaj: nadzor dostopa do medija (*media access Control, MAC*)
 - + zgoraj: logična povezavna plast (*logical link layer, LLC*)
- ✘ ločen dostop do medija in naslavljanje → prenašanje okvirjev

4

PROMET IN TOPOLOGIJA IEEE 802

- ✘ enoten naslovni prostor okvirjev
- ✘ (lokalna) mreža mora znati pravilno pošiljati okvirje

5

IEEE 802 DRUŽINA

- ✘ 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 DRUŽINA

- × 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
- × IEEE 802.24 Vertical Applications TAG

7

IEEE 802.1 – PREMOŠČANJE IN UPRAVLJANJE OMREŽIJ

- × Bridging (networking) and Network Management
- × povezovanje med pod-mrežami
- × upravljanje omrežij (npr. najmanjše vpeto drevo)
- × varnost v mrežah
- × deluje na vrhu LLC
- × več na URL: <http://www.ieee802.org/1/>
- + **izziv: Preglejte si spletno stran in preglejte vsebino.**

LLC
MAC
fizicna

8

IEEE 802.1 POD-DRUŽINA

- × 802.1b: upravljanje LAN/MAN
- × 802.1d: mostički na MAC plasti
- × 802.1e – 802.1g – umaknjeno
- × 802.1h: Ethernet MAC mostički
- × 802.1q: navidezni LAN (VLAN)
- × **802.1x: nadzor priključitve v mrežo** (Port Based Network Access Control)
- × ...

9

IEEE 802.1 POD-DRUŽINA

- ✘ Varnost:
 - + 802.1ab: postaje in nadzor dostopa do medija ter iskanje povezljivosti
 - + 802.1ae: varnost na MAC plasti
 - + 802.1ar: varno identificiranje enot
- ✘ Časovno občutljivo omrežje:
 - + 802.1as: časovno usklajevanje in časovno občutljive aplikacije v mrežah z mostički
- ✘ Upravljanje:
 - + 802.1ax: združevanje povezav (*link aggregation*)
 - + 802.1ba: avdio/video sistemi z mostički

10

10

NADZOR PRIKLJUČITVE V MREŽO (IEEE 802.1X)

- ✘ dostop v mrežo je storitev, ki omogoča rabo drugih storitev
 - + dostop do medmrežja, ...
- ✘ podrobnosti na URL
 - <http://www.ieee802.org/1/pages/802.1x-2010.html>

izziv: Preglejte si spletno stran. Kako je z vsebino?

11

11

NADZOR PRIKLJUČITVE V MREŽO (IEEE 802.1X)

- ✘ dostop v mrežo je storitev, ki omogoča rabo drugih storitev
 - + dostop do medmrežja, ...
- ✘ raba storitve je lahko prosta ali nadzorovana
- ✘ za nadzorovano rabo storitve potrebujemo
 - + ugotoviti, kdo je morebitni uporabnik; in
 - + ali ima pravico rabe storitve.
- ✘ overovljenje in avtorizacija (nekje tudi beleženje)
- ✘ naloga: v priključitev v mrežo nekako vplesti AAA

12

12

IEEE 802.1X ARHITEKTURA

- ✖ nastopajo trije gradniki:
 - + odjemalec (*supplicant*)
 - + overovitelj (*authenticator*)
 - + overovitveni strežnik (*authentication server*)
- ✖ odjemalec se prijavi overovitelju, ki pri overovitvenem strežniku preveri njegovo identiteto in ali je avtoriziran za dostop do mreže
- ✖ naloga: **vgraditi EAP na povezavno plast**
 - + **Izziv: Kako(!) overovitelj dejansko omogoči odjemalcu dostop do mreže?**

13

IEEE 802.1X EAPOL

- ✖ standard IEEE 802.1x definira EAP na povezavni plasti – EAP over LAN -> EAPOL
 - + kasneje je bil EAPOL uporabljen še v drugih pod-družinah IEEE 802.1x:
 - 802.1ae: varnost na MAC plasti
 - 802.1ar: varno identifikiranje enot
- ✖ EAPOL je definiran tako, da se njegova vsebina prenaša neposredno v Ethernet okvirjih z vsebinsko značko 0x888E (type):
 - + 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)

14

EAP – ZA OSVEŽITEV

- ✖ definiran v RFC 3748
- ✖ podpora za različne overovitvene protokole
- ✖ koračni protokol

15

IEEE 802.1X – DELOVANJE

- ✘ *inicializacija*: ko overovitelj (običajno tudi stikalo, WLAN dostopovna točka ipd.) zazna novega odjemalca, mu omogoči **samo** IEEE 802.1x komunikacijo
 - + od tu naprej se prične EAP protokol

16

IEEE 802.1X – DELOVANJE (NADALJEVANJE)

- ✘ *povabilo*: overovitelj (periodično) pošlje odjemalcu povabilo, da se naj predstavi
 - + odjemalec se predstavi overovitelju, ki predstavitev pošlje overovitvenemu strežniku (RADIUS)
 - + sedaj je overovitelj samo vmesni strežnik za overovitveni strežnik – dejansko overovitev izvede overovitveni strežnik
 - + zaupanje!! med overoviteljem in overovitvenim strežnikom
 - ✘ *izziv: Kako sprogramirati to zaupanje?*

17

IEEE 802.1X – DELOVANJE (NADALJEVANJE)

- ✘ *pogajanje*: se izvaja med odjemalcem in overoviteljem v skladu z EAP protokolom
 - + kateri overovitveni protokol,
 - + izziv in odgovor, ...


18

IEEE 802.1X - DELOVANJE (NADALJEVANJE)

- ✘ overovitev: sama overovitev odjemalca
- ✘ overovitelj, ko strežnik overovi odjemalca, dovoli odjemalcu dostop do lokalne mreže

19

19

EDUROAM 

- ✘ federacija overovitvenih strežnikov, ki si zaupajo
- ✘ uporabnik kateregakoli strežnika se lahko overovi pri kateremkoli overovitelju v federaciji
- + izziv: Kje je sedaj asimetrična kriptografija, ki jo uporablja EDUROAM v protokolu za overovljenje? Za overovitev koga jo uporabljamo? Odgovorite na forum za dodatne točke.

20

20

Hvala za pozornost
in
veliko uspeha v naprej!

21

21