PRAKTIKUM IZ RAČUNARA

- OSNOVI MREŽNE KOMUNIKACIJE -

Elektronska pošta

- Sistem elektronske pošte postoji od samih početaka Interneta i do danas predstavlja jedan od najvažnijih i najkorišćenijih mrežnih servisa.

- Elektronska pošta omogućava asinhronu razmenu poruka između korisnika bez potrebe da oni istovremeno budu povezani na Internet.

- Elektronska pošta se sastoji iz niza protokola koji u okviru TCP/IP slojevitog modela pripadaju aplikativnom sloju i oslanjaju se na TCP protokol na transportnom sloju kako bi se obezbedio siguran prenos poruka.

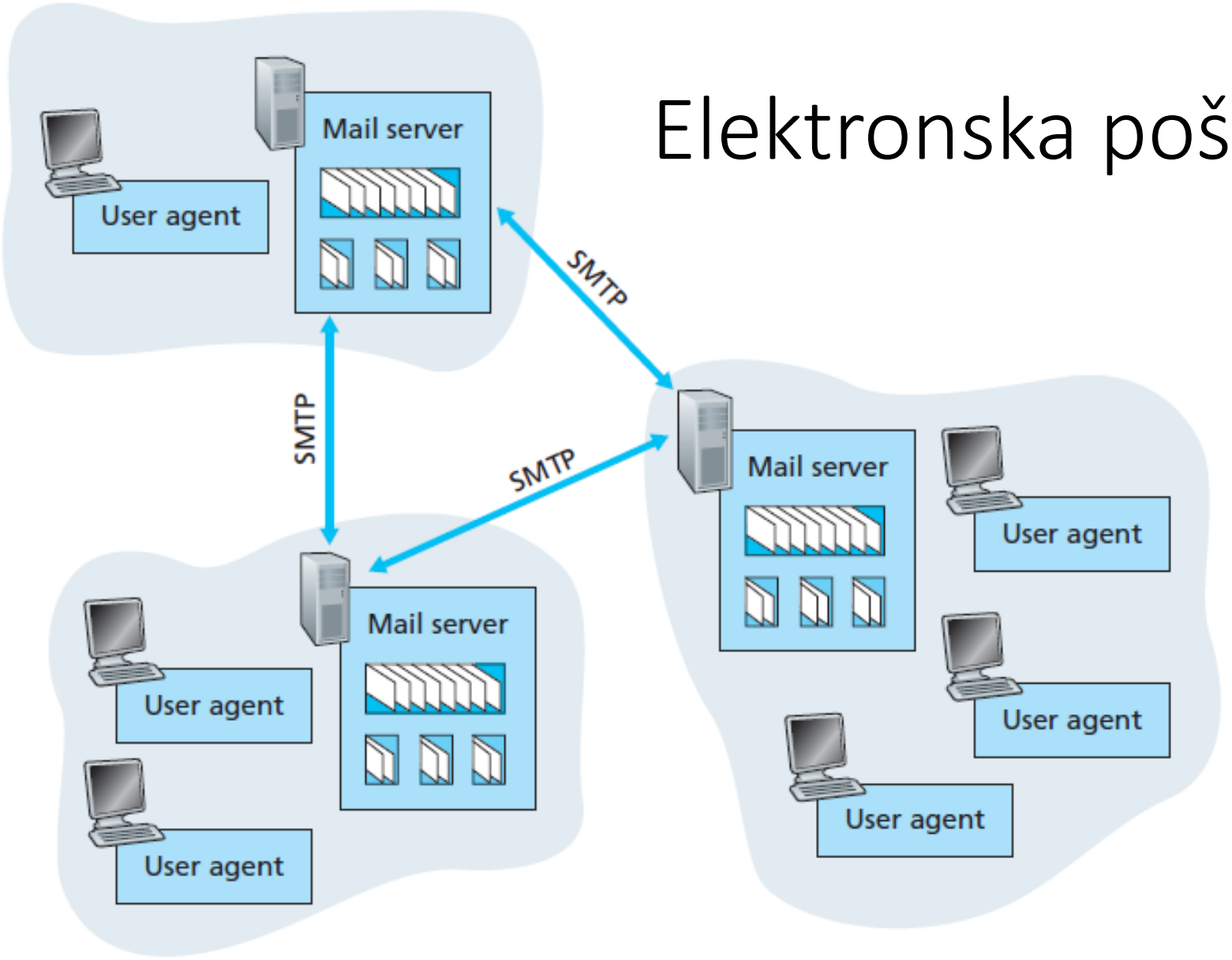
Elektronska pošta

- Elektronska pošta se sastoji iz 3 ključne komponente: **korisničkih agenata**, **servera elektronske pošte** i **protokola za prenos poruka**.

- **Korisnički agent** predstavlja aplikaciju koja omogućava korisniku da sastavlja, čita, čuva i šalje poruke. Primer korisničkih agenata su standardne aplikacije elektronske pošte poput Microsoft Outlook-a ili Mozilla Thunderbird-a.

- **Server elektronske pošte** prihvata poruke od korisničkih agenata. Za svakog korsnika u okviru servera se nalazi poštansko sanduče (*mailbox*) u koje se skladište odgovarajuće poruke. Korisnik može preko svog agenta pristupiti svom poštankom sandučetu na serveru i preuzeti odgovarajuće poruke.

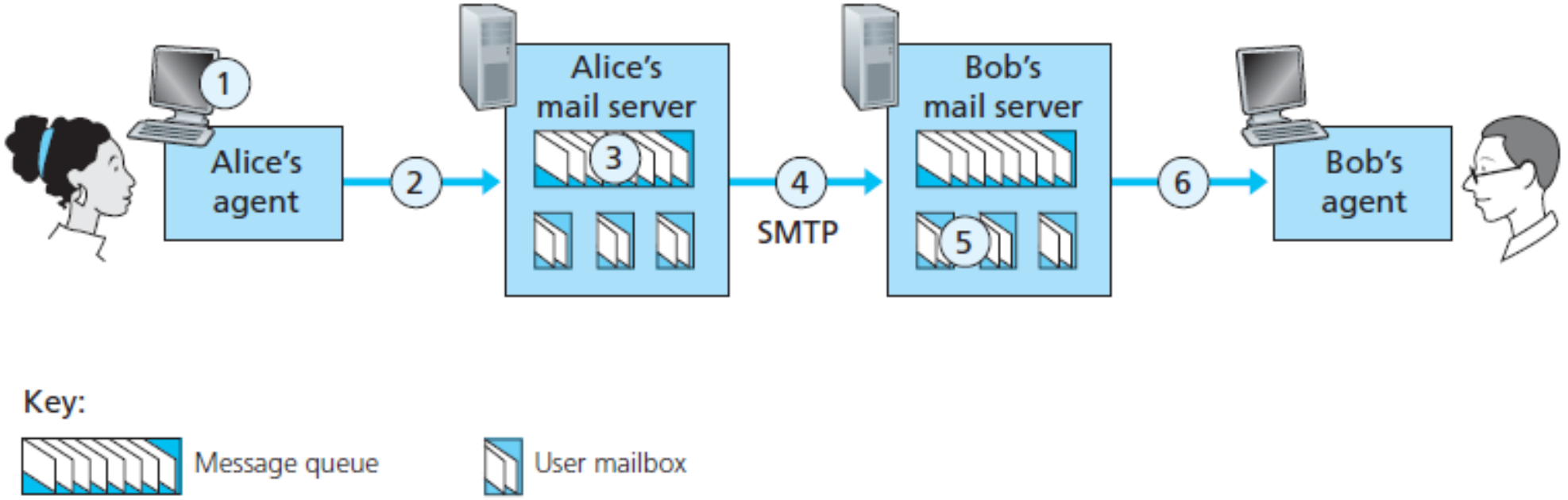
Elektronska pošta



- Komunikacija se obavlja korišćenjem jednostavnog protokola za prenos elektronske pošte (SMTP – Simple Mail Transfer Protocol)
- Svaki server elektronske pošte implementira i serverski i klijentski deo SMTP-a

SMTP (Simple Mail Transfer Protocol)

- SMTP predstavlja ključni protkol elektronske pošte i služi za prosleđivanje poruka između servera pošiljaoca i servera primaoca poruke.



SMTP

- U primeru sa prethodne slike Alis šalje poruku Bobu. Koraci koji se odvijaju u tom procesu su sledeći:

1. Alis sastavlja poruku u svom korisničkom agentu, navodi Bobovu adresu (bob@hamburger.edu) i šalje poruku.
2. Poruka se prosleđuje na Alisin odlazni server elektronske pošte.
3. Alisin server registruje odlaznu poruku u redu za čekanje i pokreće SMTP klijenta. SMTP klijent sa Alisinog servera uspostavlja TCP konekciju sa SMTP serverom koji se nalazi na Bobovom serveru elektronske pošte. Alisin server pre uspostavljanja TCP konekcije nalazi adresu Bobovog servera elektronske pošte hamburger.edu korišćenjem DNS servisa.
4. Poruka se prosleđuje na Bobov server elektronske pošte.
5. Poruka se skladišti u Bobovo poštansko sanduče koje se nalazi na serveru.
6. Bob pomoću svog korisničkog agenta pristupa svom poštanskom sandučetu na serveru i preuzima Alisinu poruku.

SMTP – primer razmene poruka

```
S: 220 hamburger.edu
C: HELO crepes.fr
S: 250 Hello crepes.fr, pleased to meet you
C: MAIL FROM: <alice@crepes.fr>
S: 250 alice@crepes.fr ... Sender ok
C: RCPT TO: <bob@hamburger.edu>
S: 250 bob@hamburger.edu ... Recipient ok
C: DATA
S: 354 Enter mail, end with "." on a line by itself
C: Do you like ketchup?
C: How about pickles?
C: .
S: 250 Message accepted for delivery
C: QUIT
S: 221 hamburger.edu closing connection
```

S – serverski SMTP
C – klijentski SMTP

SMTP – primer razmene poruke

- Prilikom uspostavljanja konekcije SMTP klijent koristi **port 25** da pristupi SMTP serveru na drugom računaru.
- Nakon iniciranja konekcije od strane SMTP klijenta, SMTP server se javlja sa porukom 220 da je konekcija uspostavljena.
- Klijent se zatim predstavlja komandom **HELO** i navodi ime svog domena.
- Nakon toga klijent navodi od koga je poruka (**MAIL FROM**) i za koga je namenjena (**RCPT TO**).
- Ukoliko server može da prihvati ovu poruku na svaku od ovih komandi odgovara porukom 250 koja označava potvrdu.
- Klijent nakon toga šalje komandu **DATA** iza koje sledi cela tekstualna poruka pri čemu se slanje poruke završava slanjem karaktera „.“
- Nakon toga klijent inicira zatvaranje konekcije slanjem komande **QUIT**.

Protokoli za pristupanje elektronskoj pošti

- SMTP je protokol koji se koristi za **slanje** elektronske pošte.
- Nakon što je poruka uspešno prosleđena do poštanskog sandučeta primaoca poruke, korisnik se može ulogovati na server elektronske pošte i pročitati poruku koja se nalazi u okviru njegovog poštanskog sandučeta.
- Za preuzimanje poruka na lokalni računar korisnika koriste se posebni protokoli od kojih su najpopularniji **POP3** (Post Office Protocol – Version 3) i **IMAP** (Internet Mail Access Protocol).

POP3

- POP3 korsiti TCP **port 110** za komunikaciju.
- Osnovni koraci u POP3 protokolu su **autorizacija**, **transakcija** i **ažuriranje**.
- U postupku autorizacije navodi se korisničko ime i šifra za pristup serveru.
- Nakon uspešne autorizacije korisničkom agentu su na raspolaganju 4 komande: **list**, **retr**, **dele** i **quit**.
- Ove komande se koriste za prikaz spiska trenutno dostupnih poruka, za dohvatanje određene poruke na osnovu rednog broja, brisanje poruke sa servera i raskidanje konekcije.
- Nakon raskidanja konekcije ulazi se u korak ažuriranja u kom se brišu sve poruke koje su označene za brisanje.
- U POP3 protokolu se obično nakon dohvatanja poruke poziva komanda brisanja čima se preuzeta poruka u koraku ažuriranja briše sa servera i ostaje samo na računaru korisnika.

POP3 – primer

1. autorizacija

```
telnet mailServer 110
+OK POP3 server ready
user bob
+OK
pass hungry
+OK user successfully logged on
```

2. transakcija

```
C: list
S: 1 498
S: 2 912
S: .
C: retr 1
S: (blah blah ...
S: ..................
S: ..........blah)
S: .
C: dele 1
C: retr 2
S: (blah blah ...
S: ..................
S: ..........blah)
S: .
C: dele 2
C: quit
S: +OK POP3 server signing off
```

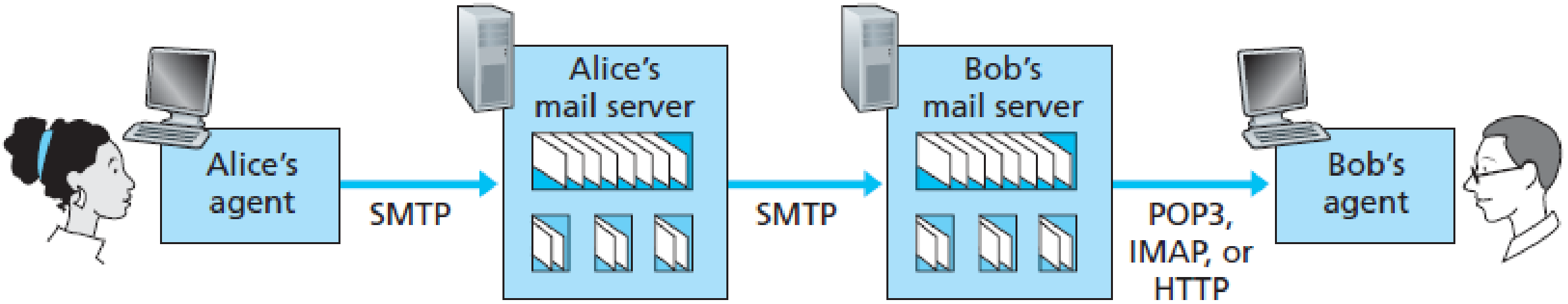
IMAP (Internet Mail Access Protocol)

- Osnovni problem kod POP3 protokola je nemogućnost složenije manipulacije porukama na serveru poput organizovanja u direktorijume, pretraga po sadržaju i sl.
- POP3 je namenjen za preuzimanje poruka na lokalni računar gde se obavlja dodatna organizacija poruka. Problem nastaje u slučaju da korisnik koristi više različitih uređaja za preuzimanje elektronske pošte što je danas potpuno uobičajena stvar.
- IMAP protokol sadrži niz komandi kojima se omogućava organizovanje poruka na samom serveru. Time se otvara mogućnost za skladištenje poruka na serveru umesto preuzimanja na lokalni računar korisnika. Na taj način korisnik može sa različitih uređaja na jedinstven način pristupiti svojim porukama elektronske pošte.

WEB pošta (Webmail)

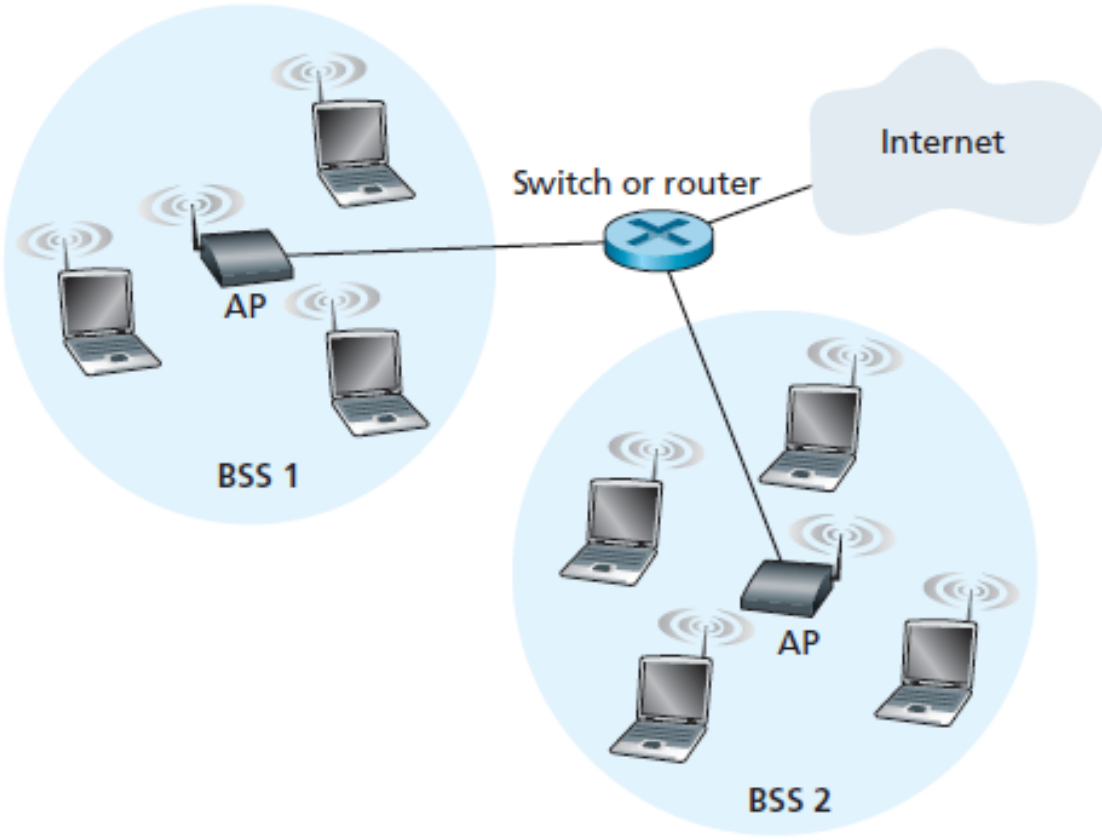
- Veliki broj korisnika danas zapravo koristi neki od dostupnih Web servisa za elektornsku poštu poput Google Mail, Yahoo Mail, Hotmail i sl.
- Razlika u odnosu na prethodne protokole je ta što se sada usluzi elektronske pošte pristupa preko web stranica korišćenjem HTTP protokola.
- Poruke se sastavljaju i pregledaju na serveru a ceo postupak se obavlja u Internet pretraživaču.
- Prenos elektronske pošte između ovih Web servera i drugih servera elektronske pošte se i dalje obavlja korišćenjem SMTP protokola.

Elektronska pošta - sumiranje



Bežične lokalne mreže

- Ključni elementi bežične mreže:
  - **Bežični uređaji** – uređaji koji se povezuju na mrežu , obično prenosni računari, pametni telefoni i sl.
  - **Bežični link** – način povezivanja sa baznom stanicom. Definiše se brzina prenosa, domet veze, opseg koji se koristi za prenos podataka i sl..
  - **Bazna stanica** – zadužena je za prenos podataka ka/od bežičnih uređaja i koordinisanje prenosa. Bazna stanica je obično povezana na Internet ili neku drugu mrežu. Pristupne tačke (AP – access points) predstavljaju primer baznih stanica u lokalnim mrežama.



Bežične lokalne mreže

- Za lokalne bežične mreže definisan je IEEE standard 802.11 koji je poznat i pod nazivom WiFi.
- Svaki uređaj povezan na 802.11 mrežu poseduje bežični mrežni interfejs sa jedinstvenom 48-bitnom MAC adresom.
- U 802.11 standardu u slučaju struktuiranih mreža uređaji se najpre povezuju na pristupnu tačku i preko nje primaju i šalju podatke.

Podešavanje pristupne tačke

- Prilikom podešavanja pristupne tačke najpre je potrebno postaviti naziv bežične mreže **SSID** (Service Set Identifier) na osnovu koga ostali uređaji mogu identifikovati pristupnu tačku.

- Svaki 802.11 standard definiše frekvencijski opseg u kom radi i ovaj opseg je podeljen na određeni broj komunikacionih kanala.
- Na primer 802.11b/g radi u opsegu 2.4-2.485GHz. Dostupan opseg od 85 MHz je podeljen na 11 kanala.
- Prilikom konfigurisanja pristupne tačke administrator podešava redni broj kanala na kojem će pristupna tačka raditi.

Podešavanje pristupne tačke

- Kako svi uređaji koji su u dometu mogu prihvatati i slati podatke bežičnim putem veoma je važno uspostaviti neki sigurnosni sistem.

- Kako bi se obezbedilo da samo učesnici u komunikaciji mogu da čitaju poruke, paketi koji se šalju bežičnim putem su enkriptovani.

- Standard 802.11 propisuje bezbednosni protokol WEP (Wired Equivalent Privacy). Međutim kako se ovaj vid zaštite pokazao kao slab vrlo brzo je napušten, i uveden je standard 802.11i. U okviru ovog standarda je najpre uveden WPA (Wi-Fi Protected Access) kao prelazno rešenje dok nije razvijen sigurniji WPA2 protokol koji se i danas koristi.

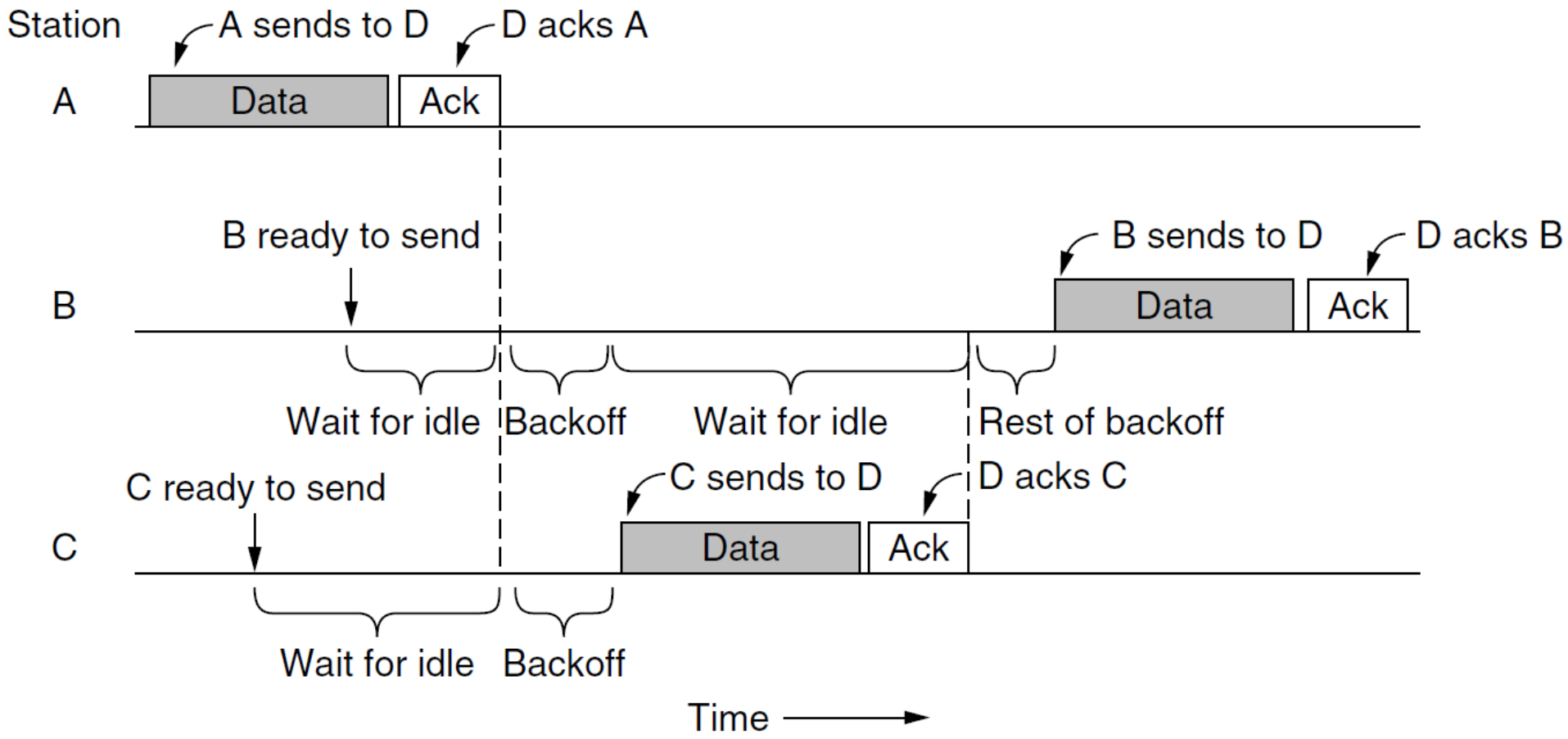
Pristupanje deljenom medijumu (MAC) u bežičnim mrežama

- Kod klasičnih eternet mreža pristup deljenom medijumu se obavlja korišćenjem protokola CSMA/CD (*Carrier Sense Multiple Access with Collision Detection*).
- Dakle svaki učesnik u komunikaciji prilikom slanja osluškuje kanal i ukoliko detektuje signal koji je različit od onog koji šalje zna da je došlo do kolizije. U tom slučaju se prekida slanje, čeka slučajan vremenski interval i nakon isteka ponovo pokušava slanje. U slučaju nove kolizije vremenski interval se eksponencijalno povećava.
- Kod bežičnih mreža detekcija kolizije je praktično nemoguća pošto je prilikom transmisije podataka signal koji dolazi od ostalih uređaja značajno slabiji u odnosu na signal koji se šalje i ne može se detektovati.

Pristupanje deljenom medijumu (MAC) u bežičnim mrežama

- Zbog toga se u bežičnim mrežama koristi CSMA/CA (*Carrier Sense Multiple Access with Collision Avoidance*).
- Kako bi se izbegla potreba ze detekcijom kolizije osluškivanjem kanala, uveden je paket potvrde prijema. Ako se ovaj paket ne primi u određenom vremenskom intervalu nakon slanja znači da je došlo do kolizije.
- Za razliku od standardnog eterneta gde se princip čekanja slučajnog vremenskog intervala primenjuje tek nakon detektovane kolizije, u bežičnim mrežama se ovaj princip primenjuje i nakon prvog slanja, kako bi se u startu izbegle potencijalne kolizije. Zato se ovaj protokol naziva *Collision Avoidance*.

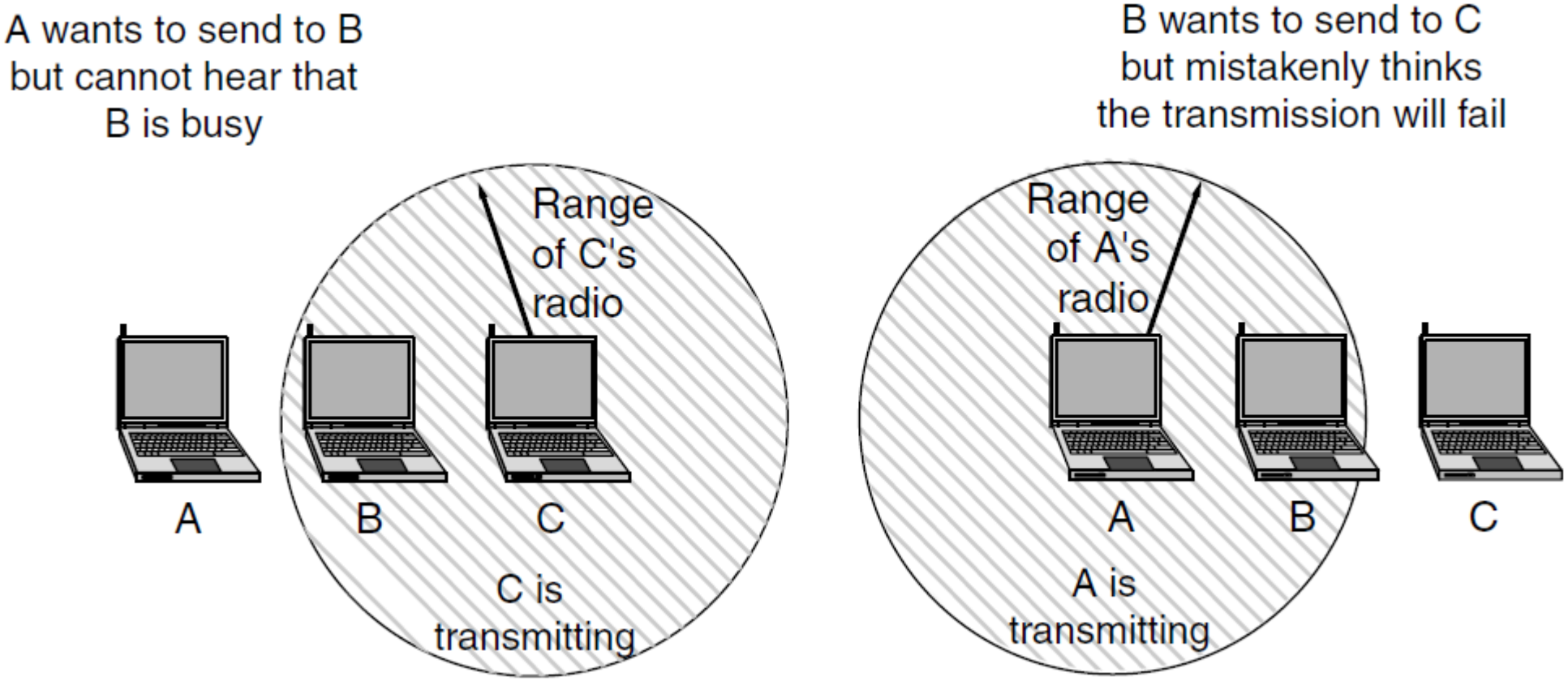
CSMA/CA - primer



CSMA/CA - primer

- U prethodnom primeru uređaj A šalje podatke. Uređaji B i C imaju spremne podatke za slanje ali detektuju da je kanal zauzet i čekaju da se trenutni prenos završi.
- Nakon oslobađanja kanala B i C biraju slučajan interval vremena koji čekaju pre nego što započnu slanje.
- Kako je vreme čekanja bilo kraće kod uređaja C on prvi kreće sa slanjem.
- B detektuje da je kanal zauzet i čeka da se oslobodi. Nakon oslobađanja kanala, uređaj B opet čeka slučajan interval vremena pre nego što započne slanje.
- Na ovaj način se značajno smanjuje broj kolizija u sistemu koje bi inače dosta usporavale prenos.

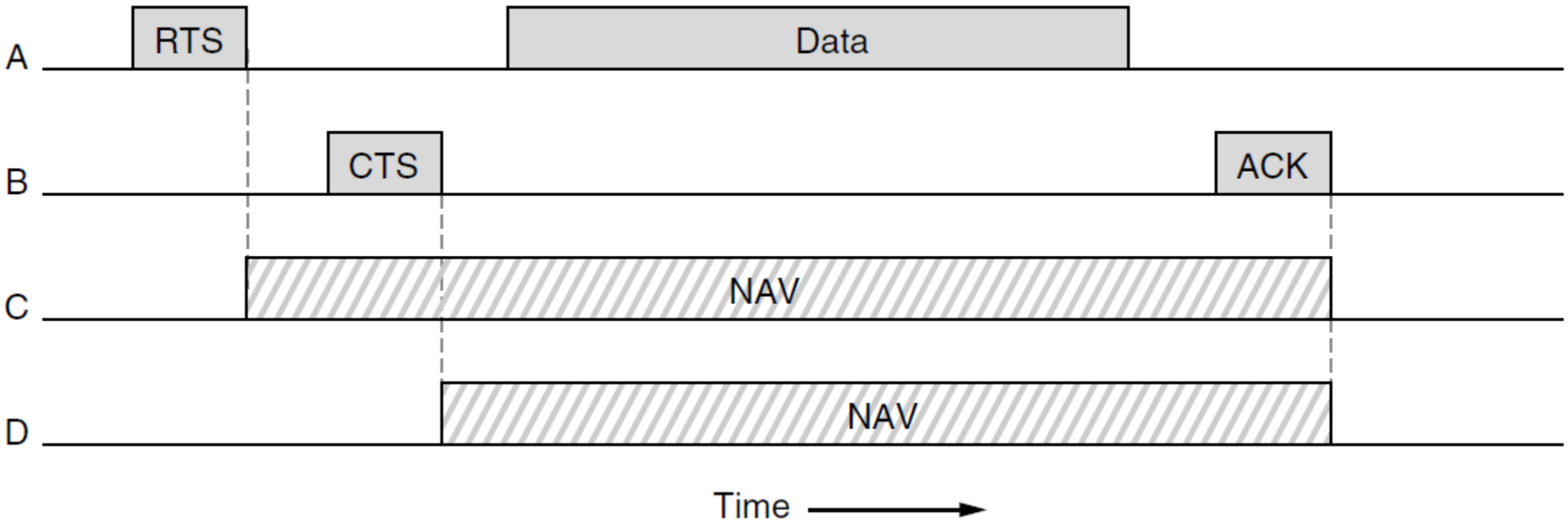
Problem sakrivenih i izloženih uređaja



Osluškivanje virtuelnog kanala

- Na prethodnoj slici je prikazan problem detekcije zauzetosti kanala osluškivanjem kanala uzimajući u obzir domete uređaja koji učestvuju u komunikaciji.
- Zbog toga je uveden protokol koji se zasniva na paketima RTS (Request to Send) i CTS (Clear to Send).
- U prethodnom primeru uređaj A želi da pošalje podatke uređaju B. On inicira ovu komunikaciju slanjem paketa RTS. Uređaj B može da primi ili odbije ovaj zahtev. U slučaju prihvatanja komunikacije B šalje paket CTS. Po prijemu CTS paketa uređaj A zna da može da pošalje podatke.
- Prilikom ove komunikacije svi uređaji koji su u dometu uređaja A će primiti RTS paket, dok će svi uređaji u dometu uređaja B primiti CTS paket. Na ovaj način će svi oni biti upoznati da je u toku prenos podataka i da treba neko vreme da se uzdrže od novih prenosa podataka. Ovo vreme se definiše vektorom za alokaciju kanala NAV (*Network Allocation Vector*).
- Uređaji koji su u dometu B a nisu u dometu A na osnovu CTS paketa znaju da je u toku prenos iako ne mogu da detekuju signal koji dolazi od A. Zbog toga se ovo naziva osluškivanje virtuelnog kanala.

Osluškivanje virtuelnog kanala



Priključivanje na pristupnu tačku

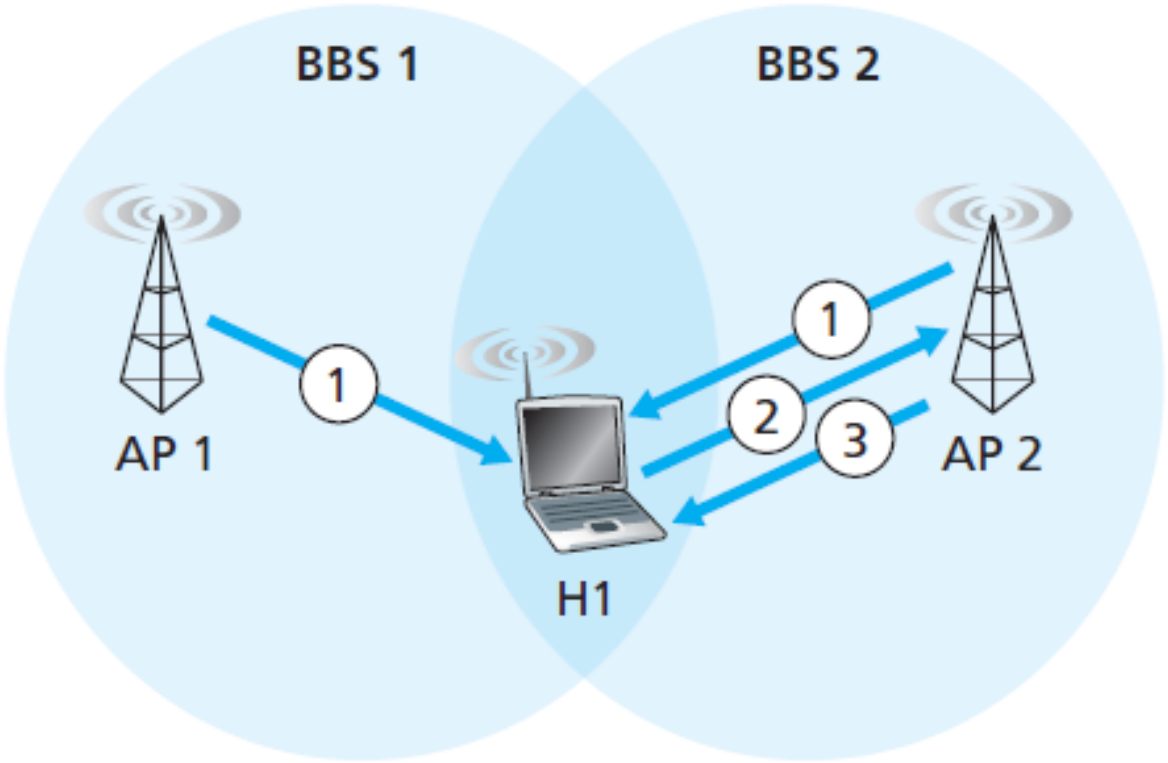
- Svaka pristupna tačka se nalazi u odgovarajućoj lokalnoj mreži.
- Da bi pristupio lokalnoj mreži, bežični uređaj se mora povezati na odgovarajuću pristupnu tačku.
- Standard 802.11 zahteva da pristupne tačke periodično odašilju signalne (*beacon*) pakete u kojima se nalaze **SSID** i **MAC** adresa pristupne tačke.
- Bežični uređaji skeniraju sve dostupne komunikacione kanale i detektuju ove signalne pakete. Na osnovu toga znaju koje su pristupne tačke na raspolaganju.

Priključivanje na pristupnu tačku

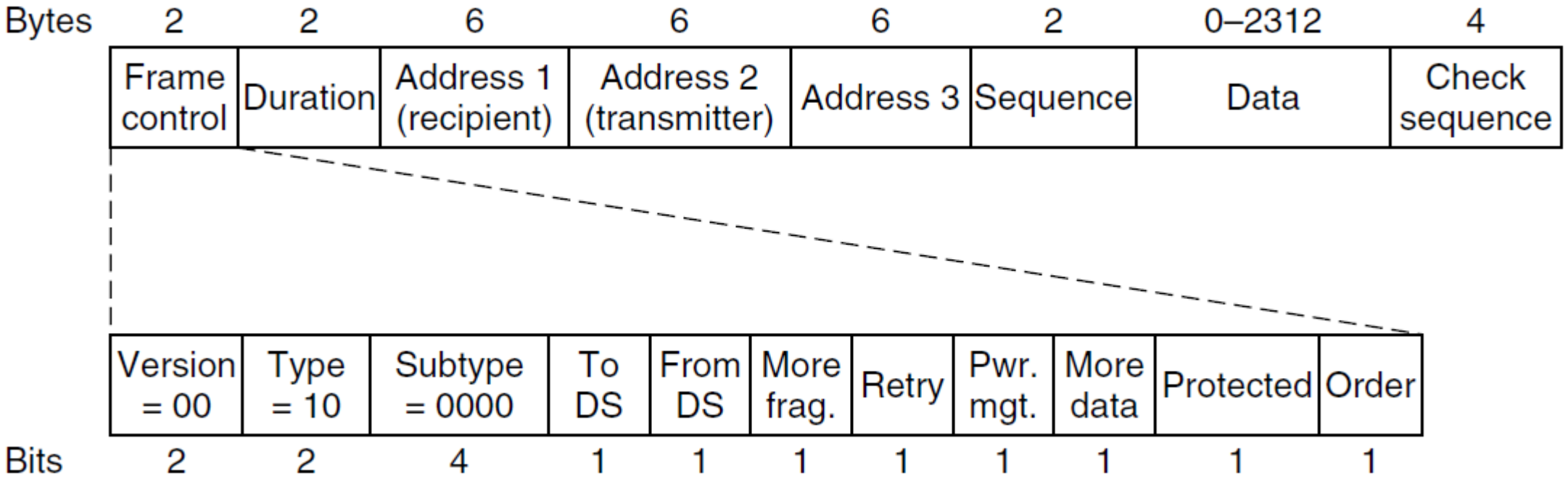
- Nakon selekcije odgovarajuće pristupne tačke, bežični uređaj šalje zahtev za priključenje na pristupnu tačku.
- Pristupna tačka kao odgovor na ovaj zahtev šalje odgovarajući paket potvrde.
- Nakon priključenja na pristupnu tačku bežični uređaj postaje deo lokalne mreže kojoj pristupna tačka pripada. U ovom koraku bežični uređaj obično šalje DHCP zahtev lokalnom DHCP serveru kako bi dobio odgovarajuću IP adresu i ostala podešavanja.
- Po dobijanju lokalne IP adrese ostatak sveta vidi bežični uređaj kao bilo koji drugi uređaj u okviru date lokalne mreže.

Priključivanje na pristupnu tačku

1. Pristupne tačke AP1 i AP2 šalju signalne pakete koje detektuje bežični uređaj H1.
2. H1 odlučuje da se poveže na pristupnu tačku AP2 i šalje zahtev za priključenje.
3. AP2 šalje pakete potvrde čime je H1 uspešno priključen na pristupnu tačku AP2.



Struktura 802.11 paketa



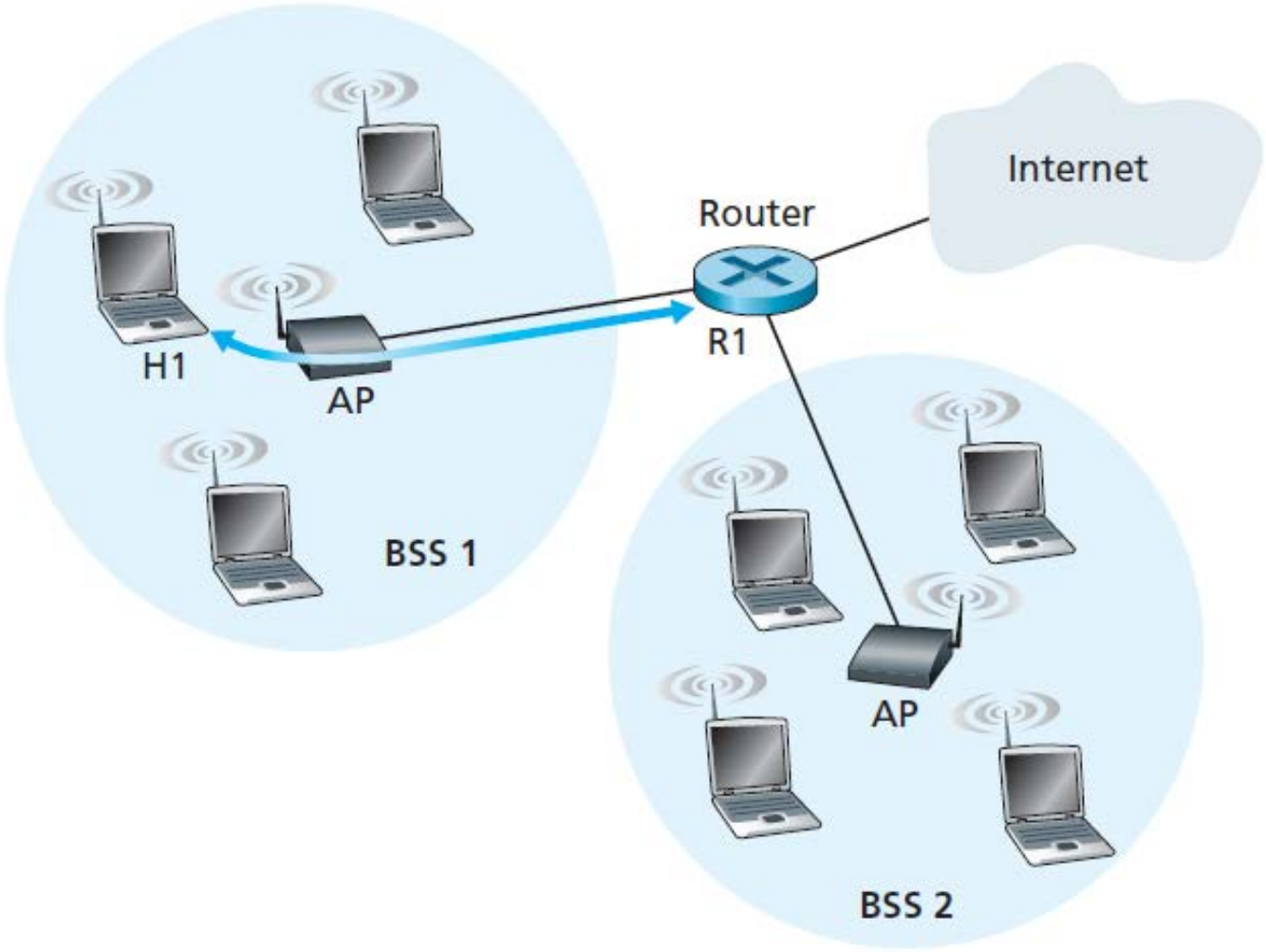
Struktura 802.11 frejmova

- Najveća razlika u odnosu na standardne 802.3 eternet pakete je postojanje 3 adrese.

- Adresa 1 predstavlja MAC adresu bežičnog uređaja koji prima poruku.
- Adresa 2 predstavlja MAC adresu bežičnog uređaja koji šalje poruku.
  - Dakle prve dve MAC adrese predstavljaju adrese bežičnog uređaja ili pristupne tačke na koji se bežični uređaj povezuje.
- Adresa 3 sadrži MAC adresu rutera lokalne mreže na koji je povezana pristupna tačka.

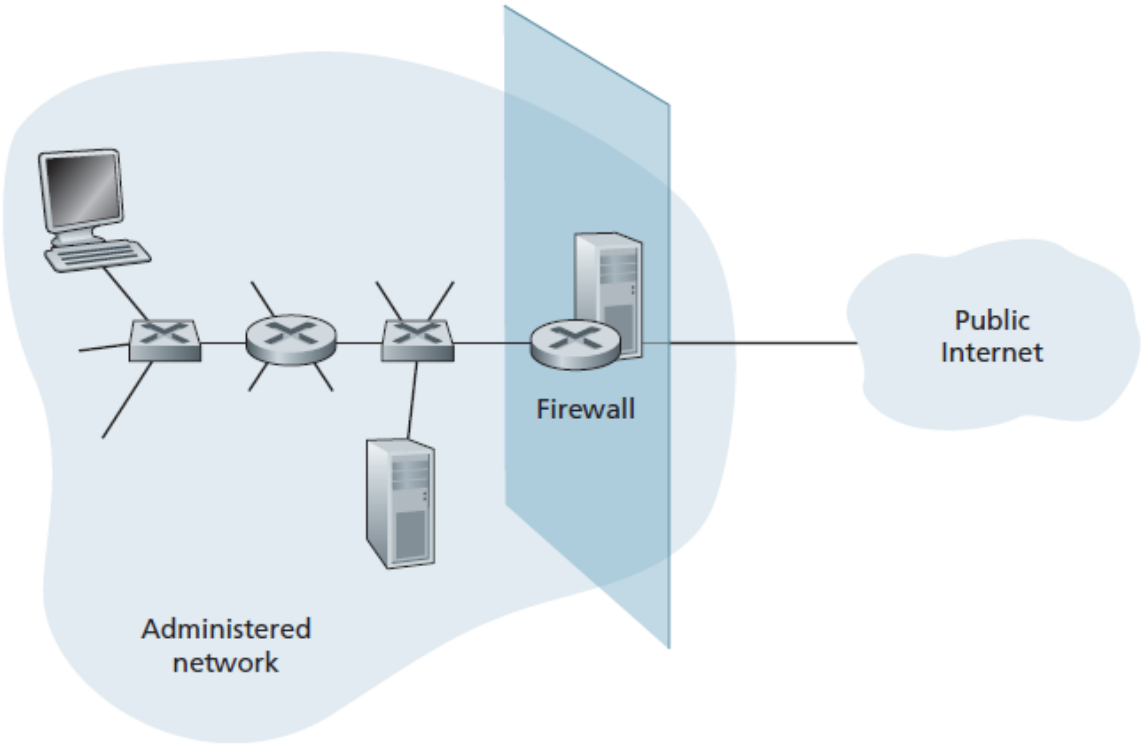
Komunikacija bežičnog uređaja sa lokalnom mrežom

- Prilikom slanja poruke sa R1 na H1 ruter šalje standardni eternet paket u kojem za odredišnu MAC adresu postavlja adresu uređaja H1 a za izvorišnu stavlja svoju MAC adresu.
- U pristupnoj tački AP se pre slanja bežičnim putem obavlja konverzija standardnih eternet 802.3 frejmova u 802.11. U ovom koraku se u prve dve adrese upisuju MAC adrese H1 i AP dok se u polje adrese 3 upisuje MAC adresa rutera R1.



Zaštitne barijere (firewalls)

- Zaštitna barijera predstavlja kombinaciju hardverskih i softverskih komponenti kojima se izoluje interna mreža organizacije od javne mreže, odnosno Interneta.
- Sav saobraćaj koji se razmenjuje između lokalne i javne mreže prolazi kroz zaštitnu barijeru. Na ovaj način se omogućava administratoru mreže da definiše pravila koji saobraćaj će biti propušten a koji saobraćaj će biti blokiran.



Zaštitne barijere

- Postoje tri kategorije zaštitnih barijera:
  1) **Paketski filtri** – omogućavaju proveru sadržaja svakog paketa koji prolazi kroz zaštitnu barijeru. Poruke se filtriraju na osnovu izvorišne/odredišne IP adrese, protokola koji se koristi (TCP, UDP, ICMP...), izvorišnog/odredišnog broja TCP/UDP porta i sl
  2) **Filtri bazirani na stanjima** – paketski filtri filtriraju poruke samo na osnovu sadržaja trenutne poruke. Filtri bazirani na stanjima uzimaju u obzir i pojavu prethodnih poruka, odnosno posmatraju poruku u kontekstu trenutno aktivnih konekcija. Na primer ovi filtri mogu da odbace sve TCP poruke ukoliko sama konekcija nije inicijalno pokrenuta sa lokalne mreže.
  3) **Mrežni prolaz za aplikacije** – predstavlja posrednika između korisničkih aplikacija i spoljnjeg sveta. Mrežni prolaz za aplikacije može blokirati saobraćaj na osnovu sadržaja (nedozvoljeni sajtovi, virusi, sumnjivi podaci i sl...)

Definisanje liste pravila

- Postoje dva pristupa prilikom kreiranja liste pravila u zaštitnoj barijeri:

1. **Blokiraj sav saobraćaj a zatim definiši kojim porukama je dozvoljeno da prođu.**

   Ovaj pristup pruža najveću sigurnost pošto je sav neželjeni saobraćaj blokiran. Administrator mreže mora da obezbedi listu pravila kojom se omogućava funkcionisanje dozvoljenih aplikacija iz lokalne mreže. Sa strane korisnika ovakav pristup je prilično restriktivan i za svaku novu aplikaciju potrebno je novo podešavanja liste pravila od strane administratora.

2. **Dozvoli sav saobraćaj a zatim definiši kojim porukama je zabranjen prolaz.**

   Ovaj pristup omogućava da sve aplikacije osim onih nedozvoljenih ispravno rade. Administrator mreže mora da obezbedi listu pravila kojom se blokira protok sumnjivog saobraćaja. Problem sa ovim pristupom je što administrator mora eksplicitno da identifikuje sve potencijalne pretenje čime se ostavlja prostor da neke od pretnji neće biti blokirane.

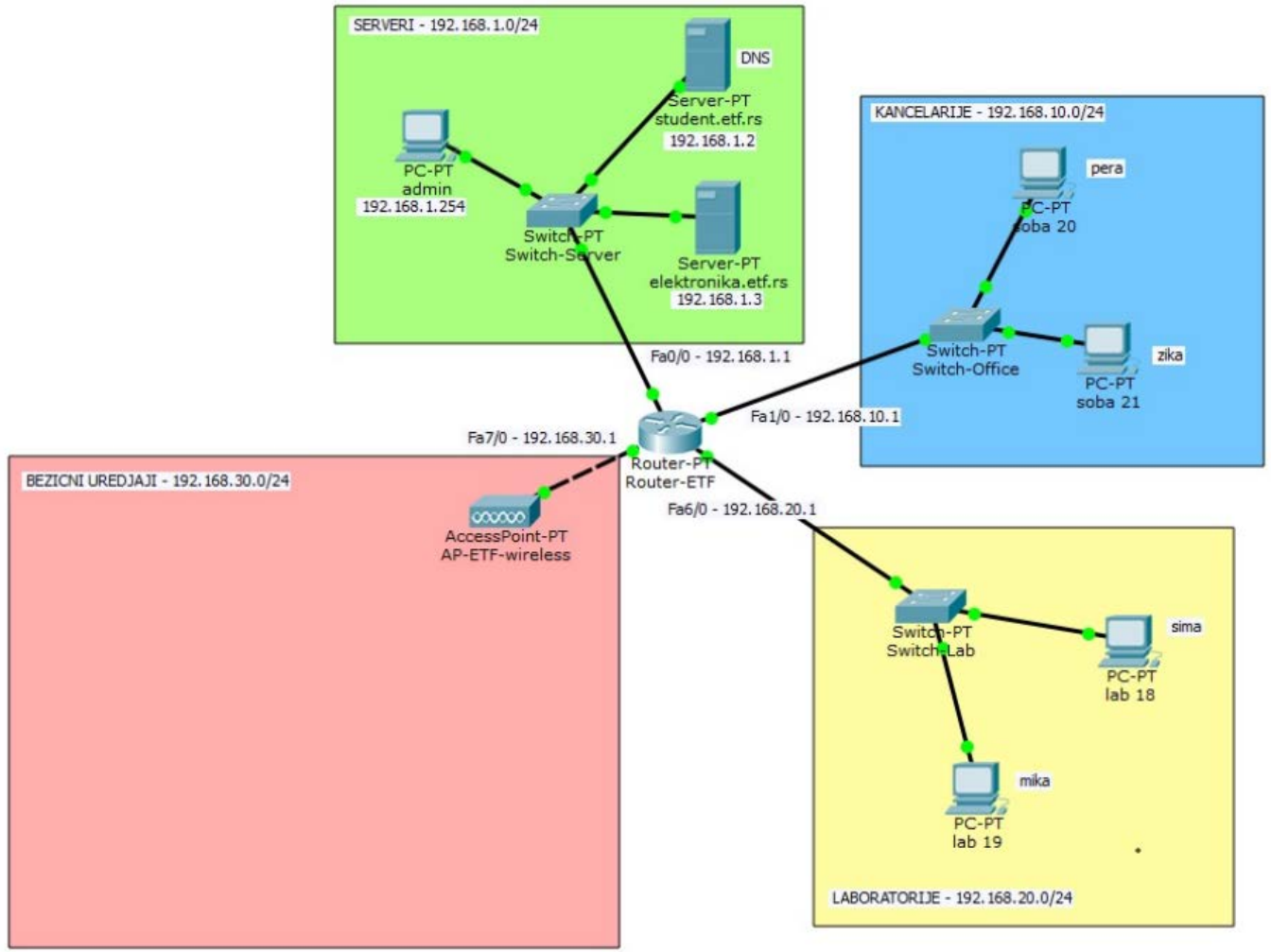
Definisanje liste pristupa – access-list

- Prilikom definisanja liste pristupa koristi se komanda **access-list** koja ime sledeće argumente:
  1) Broj koji predstavlja oznaku liste.
  2) Komanda **deny/permit** u zavisnosti da li se određeni saobraćaj blokira ili propušta.
  3) Protokol na koji se pravilo odnosi (**tcp**, **ip**, **icmp**, **udp**).
  4) Izvorišna adresa koja se može zadati u 3 različite forme:
     a. Korišćenjem adrese grupe računara i maske.
     b. Korišćenjem adrese jednog računara. U ovom slučaju pre te adrese se navodi ključna reč **host**.
     c. Korišćenjem ključne reči **any** kojom se označava bilo koje izvorište.
  5) Odredišna adresa za koju važe ista pravila kao za izvorišnu adresu.
  6) Ako se navede ključna reč **eq** mogu se filtrirati samo poruke koje pristupaju određenom TCP/UDP portu.

Podešavanje zaštitne barijere - primer

- Zaštitnu barijeru je potrebno konfigurisati tako da je korisnicima iz bežične mreže zabranjeno:

1) FTP pristup svim računarima.
2) Slanje elektronske pošte preko servera elektronika.etf.rs.
3) Ping računara zaposlenih na fakultetu.



Podešavanje zaštitne barijere - primer

access-list 101 deny tcp any any eq ftp

Zabranjuje se sav ftp saobraćaj.

access-list 101 deny tcp any host 192.168.1.3 eq smtp

Zabranjuje se slanje **smtp** poruka serveru sa IP adresom 192.168.1.3. Na ovaj način se onemogućava slanje elektronske pošte korišćenjem navedenog servera.

access-list 101 deny icmp any 192.168.10.0 0.0.0.255

Zabranjuje se pingovanje računara koji se nalaze u okviru lokalne mreže 192.168.10.0/24. Na taj način se onemogućava da neko van lokalne mreže ispita da li postoje računari sa određenim IP adresama.

access-list 101 permit ip any any

Pravila iz liste pristupa se evaluiraju redom i postupak se prekida prvi put kada dođe do poklapanja sa nekim od pravila. Ukoliko nijedna od zabrana nije primenjena dolazi se do komande kojom se dozvoljava sav IP saobraćaj tako da će poruka koja je prošla sve zabrane biti propuštena. Ovako definisana lista pristupa predstavlja primer pristupa **dozvoli sav saobraćaj i blokiraj samo neželjene poruke**.

Podešavanje zaštitne barijere - primer

```
Router(config)#access-list 101 deny tcp any any eq ftp
Router(config)#access-list 101 deny tcp any host 192.168.1.3 eq smtp
Router(config)#access-list 101 deny icmp any 192.168.10.0 0.0.0.255
Router(config)#access-list 101 permit ip any any
Router(config)#interface Fa7/0
Router(config-if)#ip access-group 101 in
Router(config-if)#exit
Router(config)#exit
Router#
%SYS-5-CONFIG_I: Configured from console by console

Router#
```

Pristupna tačka bežične mreže je povezana na port Fa7/0 rutera. Zbog toga je lista pristupa 101 konfigurisana tako da filtrira sav saobraćaj koji ulazi na ovaj port rutera.