

Master strukovne studije –

Multimedijalno inženjerstvo,

Računarsko inženjerstvo



Protokoli i tehnologije bežičnih sistema:

Lekcija 8: WLAN – Upravljanje i nadzor

leto 2018/2019

Branimir M. Trenkić



WLAN

802.11 WLAN - Usluge upravljanja i nadzora

Management and Control Services

Traženje mreže i pridruživanje

Pre korišćenja mreže – ona se mora prvo naći!

- Stanica mora **identifikovati kompatibilnu mrežu**
- Prvi korak:
 - Novo-aktivirana stanica mora **da istraži** koje mreže (pristupne tačke) su
 - 1) unutar njenog opsega i
 - 2) raspoložive za pridruživanje
- To se može postići:
 - **pasivnim** skeniranjem ili
 - **aktivnim** skeniranjem

Traženje mreže i pridruživanje

- **Parametri** koji se **koriste u** procesu traženja—
(mogu biti specificirani od strane korisnika)
- **BSSType** (independent, infrastruktura ili both)
 - Tip mreže koja se traži
- **BSSID** (individual ili broadcast)
 - Stanica može da traži određenu mrežu (individual) ili bilo koju koja je u dometu (broadcast)
- **SSID** (“network name”)
 - String bitova dodeljen ESS – interpretira se kao (human-readable) ime mreže

Traženje mreže i pridruživanje

- ***ScanType*** (active ili passive)
 - Način traženja (skeniranja)
- ***ChannelList***
 - ***Traženje*** prouzrokuje ili (I) slanje Probe Request okvira ili (II) osluškivanje kanala kako bi se detektovalo postojanje mreže. Ovim parametrom se ***određuje lista kanala*** u kojima to treba sprovesti. Listu kanala je moguće konfigurisati na različite načine. Kao listu kanala (direct-sequence) ili obrazac skakanja (frequency hopping)



Traženje mreže i pridruživanje

- ***MinChannelTime* i *MaxChannelTime***

- Ove vrednosti specificiraju ***određena vremena koja se koriste u procesu skeniranja*** jednog kanala



Pasivno skeniranje

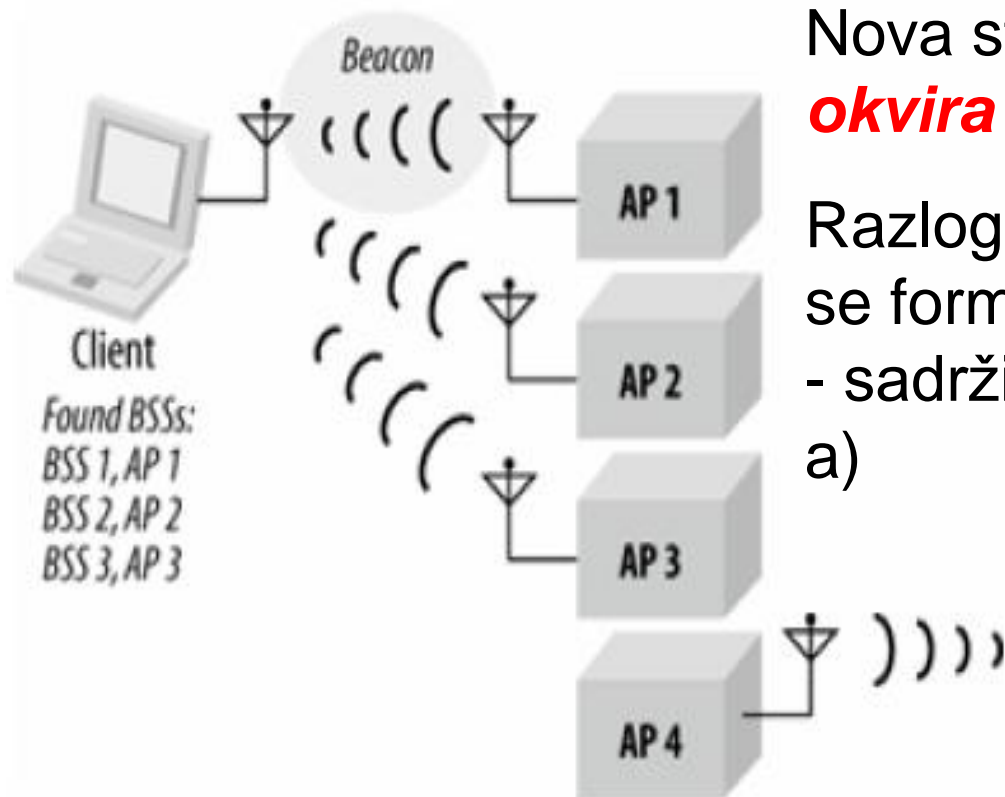
- *Štedi energiju* baterije – ne zahteva slanje
- Nova stanica ***osluškuje svaki kanal*** predhodno ***definisani period vremena*** u okviru koga ***detektuje Beacon- okvire*** koji su poslani sa drugih stanica



Pasivno skeniranje

- **Beacon okvir** **nosi** oznaku sinhronizacije kao i druge parameter fizičkog (PHY) sloja (npr. obrazac frekvencijskog skakanja) što će omogućiti:
 - Konfigurisanje novo-aktivne stanice, i
 - Komunikaciju dve stanice

Pasivno skeniranje



Nova stanica prihvata **tri Beacon okvira** sa tri različite AP

Razlog: **Izveštaj skeniranja** koji se formira kao rezultat skeniranja - sadrži samo **tri stavke** (tri BSS-a)

Aktivno skeniranje

- A.** Ako je nova stanica već konfigurisana
- *Postavljeno* je preferirano **SSID ime** za asocijaciju
 - *Stanica šalje Probe Request* okvir koji sadrži taj SSID i čeka odgovor od preferirane mreže u formi **Probe Response** okvira
- B.** Moguća je i **difuzija Probe Request** okvira
- Zahteva **odgovor svih mreža** unutar opsega stanice sa *Probe Response* okvirom
 - Na ovaj način će nova stanica biti **informisana o svim** raspoloživim **mrežama**



Aktivno skeniranje - procedura

- Stanice koriste sledeću proceduru prilikom aktivnog skeniranja:

1. korak

Pomeranje ***u određeni kanal*** sa liste i ***čekanje*** na

- a) ***indikaciju dolaznog okvira*** ili

Kanal se koristi i može se izvršiti njegovo ispitivanje

- b) ***isteka ProbeDelay*** vremenske kontrole

Vremenska kontrola spečava blokiranje cele procedure usled ne-aktivnog kanala – beskonačno čekanje na dolazni okvir

Aktivno skeniranje - procedura

2. korak

Preuzimanje kontrole nad kanalom putem DCF-a i **slanje *Probe Request*** okvira

3. korak

Čeka ***istek MinChannelTime*** vremenske kontrole

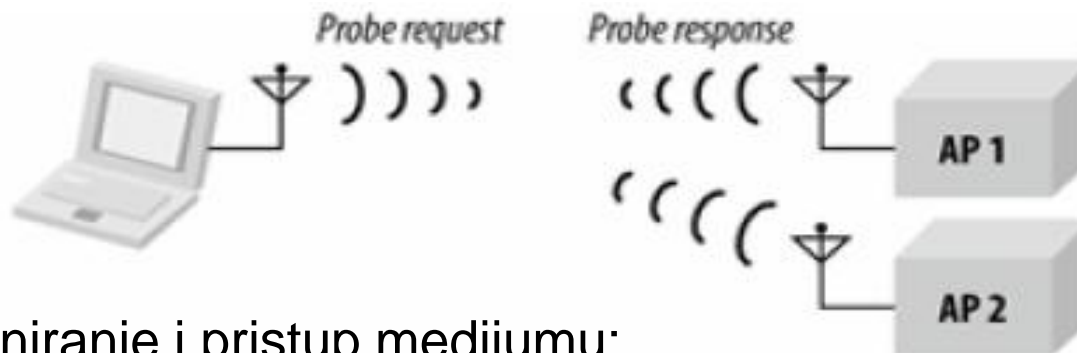
- Ako se tokom čekanja ni jednom ***ne detektuje zauzetost kanala*** – mreža ne postoji. ***Prelazak na sledeći kanal***
- U suprotnom – čeka se još ***MaxChannelTime*** vreme i nakon toga se ***obrađuju prispeli Probe Response*** okviri



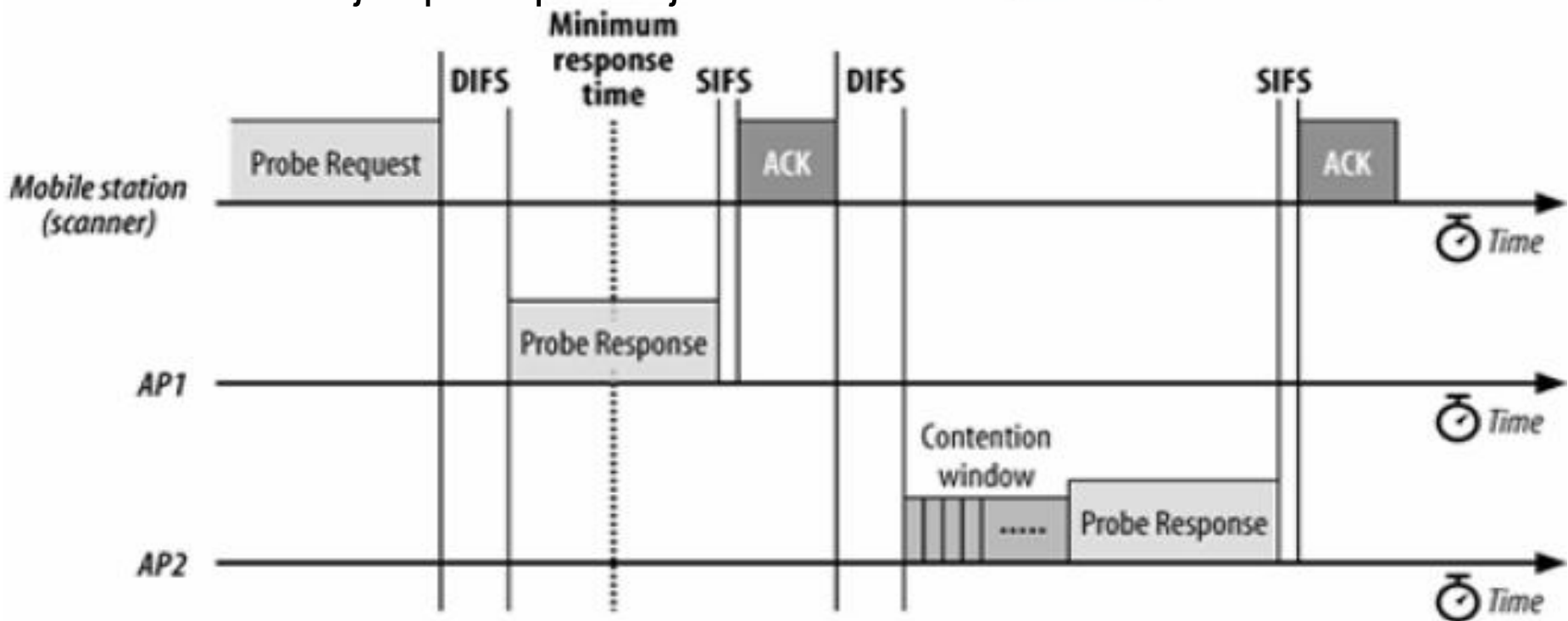
Aktivno skeniranje

- **Stanica** u BSS-u koja je **odgovorna za slanje Probe Response okvira** – to je **stanica koja je poslala poslednji Beacon okvir** u tom BSS-u
 - U infrastrukturnom režimu – **pristupna tačka**
- *Probe Response* okvir je *unicast* upravljački okvir koji **zahteva potvrđivanje (ACK)**

Aktivno skeniranje



Aktivno skeniranje i pristup medijumu:



Aktivno skeniranje - Izveštaj

- **Izveštaj skeniranja** je rezultat procesa traženja. Izveštaj sadrži sve nađene BSS-ove i njihove parametre
- **Na bazi Izveštaja** – **stanica određuje mrežu** na koju će pokušati da se pridruži
- Pored BSSID, SSID i BSSType, Izveštaj uključuje i sledeće parametre:
 - **Beacon interval** (ceo broj)
 - **DTIM period** (ceo broj), (*Delivery Traffic Indicator Map*)
 - **BSSBasicRateSet**

Traženje mreže i pridruživanje

- Nakon kompletiranja rezultata skeniranja, stanica može da **selektuje jednu mrežu sa kojom želi da ostvari povezivanje**
 - **Povezivanje** (joining) – **setovanje BSS parametara** saglasno vrednostima preferirane mreže ili mreže selektovane od strane stanice ili korisnika, iz Izveštaja skeniranja
- U ovoj fazi **nije omogućen pristup** selektovanoj mreži
- **Prijavljivanje** (Autentifikacija) i **Asocijacija** su procesi koji mu predhode

Prijavljivanje (Autentifikacija)

- Authentication
- Bežične mreže imaju **ograničeno fizičko osiguranje** da spreče neautorizovan pristup
- *Usluga prijavljivanja*
 - Mehanizam kojim stanica može da **uspostavi svoj identitet** (da se identifikuje)
 - 802.11 standard definiše ovu **uslugu u cilju kontrole pristupa** mreži
 - **Usluga stanice** - AP je privilegovana u tom smislu

Prijavljivanje (Autentifikacija)

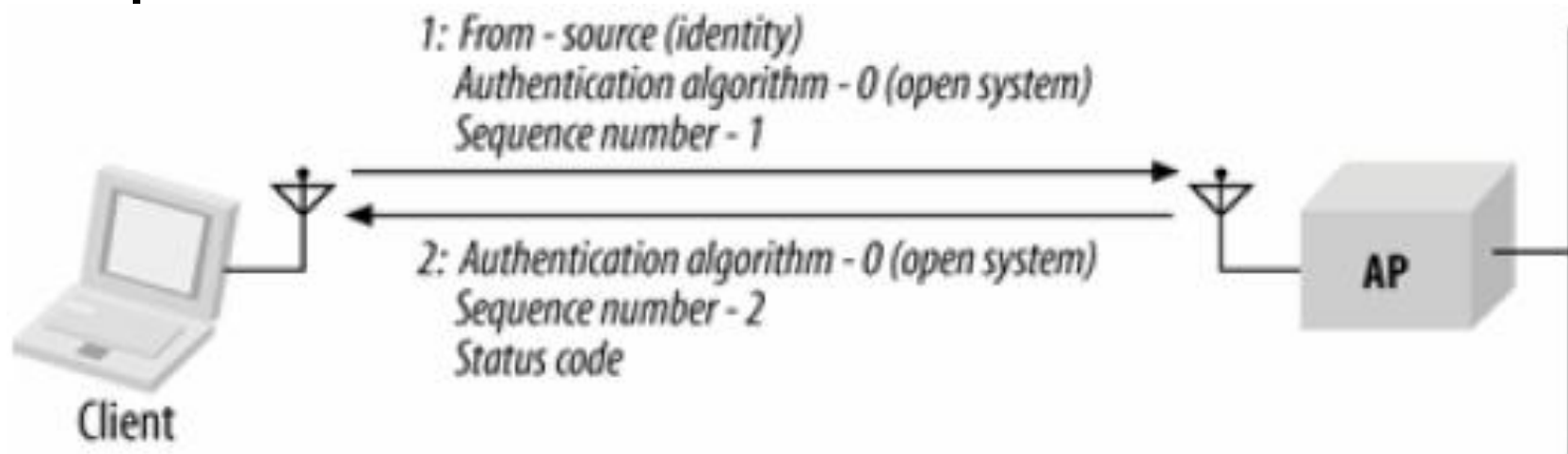
- *Authentication*
- **Bez** ovog **dokaza o identitetu**, stanici **nije dozvoljena upotreba bežične mreže** za prenos podataka
 - Sve 802.11 stanice moraju **provesti proceduru za prijavljivanje pre komunikacije** sa drugom stanicom bez obzira u kakvoj se konfiguraciji koristile



Prijavljivanje u otvorenom sistemu

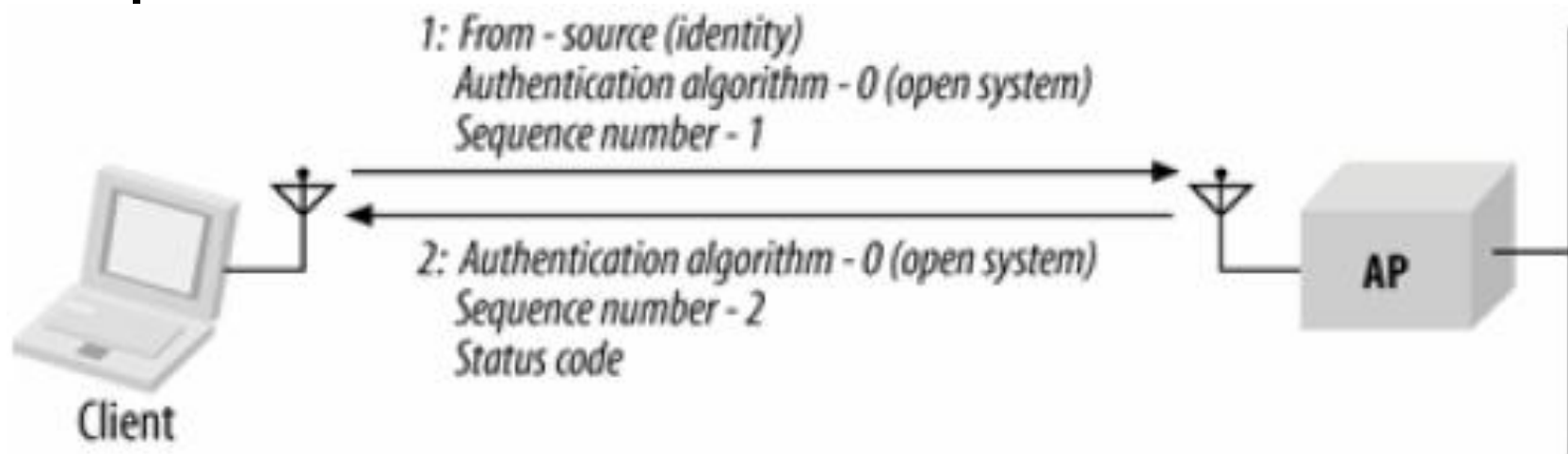
- **Open system authentication**
- Ovo je **osnovni metod** prijavljivanja
- Vrlo **jednostavan proces** iz **dva koraka**:
 1. **Stanica koja želi da se prijavi** drugoj stanici **šalje formu za prijavljivanje** koja sadrži njene podatke za identifikaciju
 2. **Prijemna stanica vraća nazad formu** kojom obaveštava da li prihvata identifikaciju stanice koja se prijavljuje

Prijavljivanje u otvorenom sistemu - Procedura



- **Prvi okvir** (sub-type = *Authentication*):- Faktički “*Authentication Request*”
- **Identitet** svake stanice – **MAC adresa** (izvorišna adresa u zaglavlju okvira)
- **Dva** informaciona **polja u telu okvira**
 - **Identifikator algoritma** prijavljivanja (0 = *open system*)
 - **Redni broj okvira** (1)

Prijavljivanje u otvorenom sistemu - Procedura

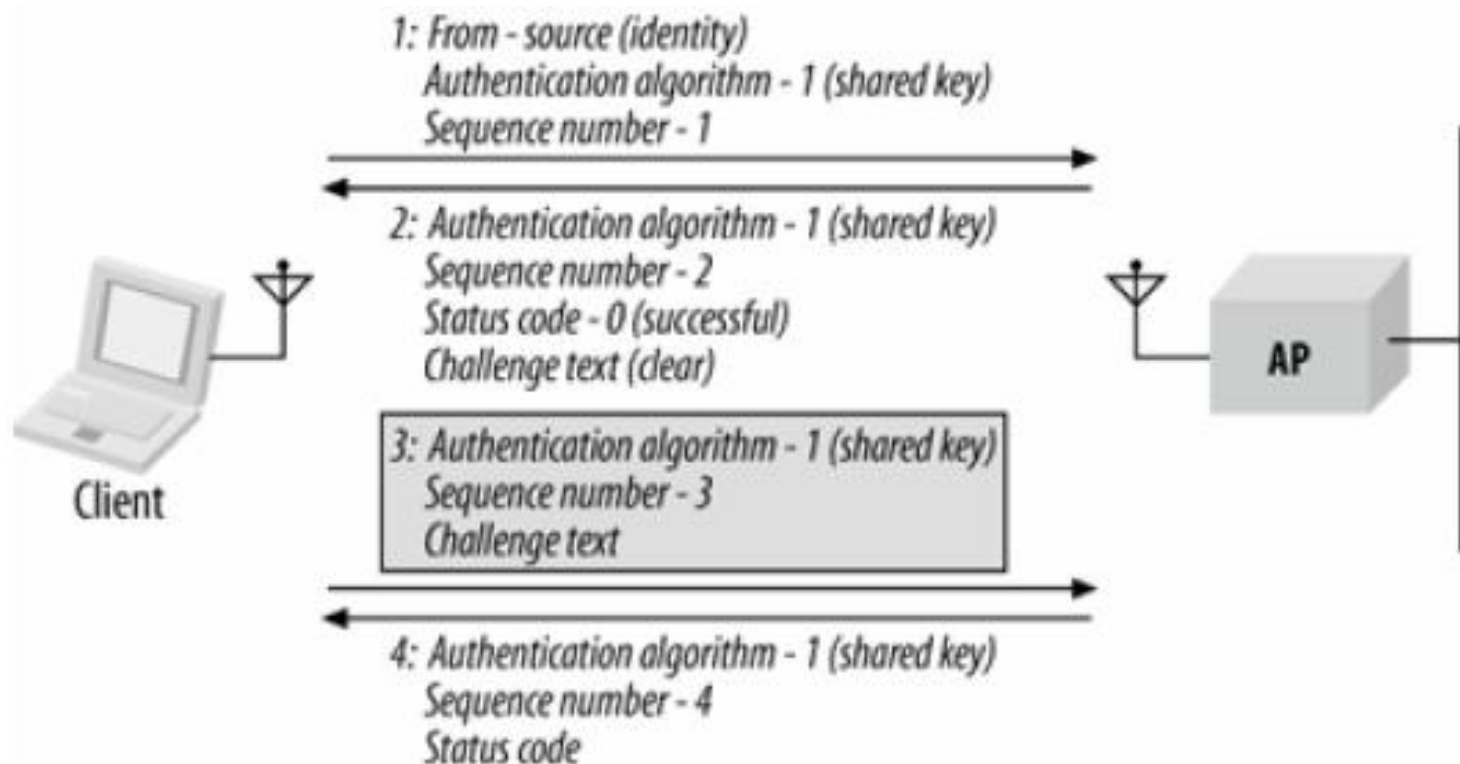


- **AP** obrađuje *Authentication Request* i **vraća odgovor**
- **Okvir odgovora** je upravljačkog tipa (sub-type = *Authentication*)
- Sadrži **tri** informaciona **polja**:
 - **Identifikator algoritma** prijavljivanja (0 = open system)
 - **Redni broj** okvira (2)
 - **Status Code** – ishod procesa prijavljivanja

Prijavljivanje pomoću zajedničke šifre

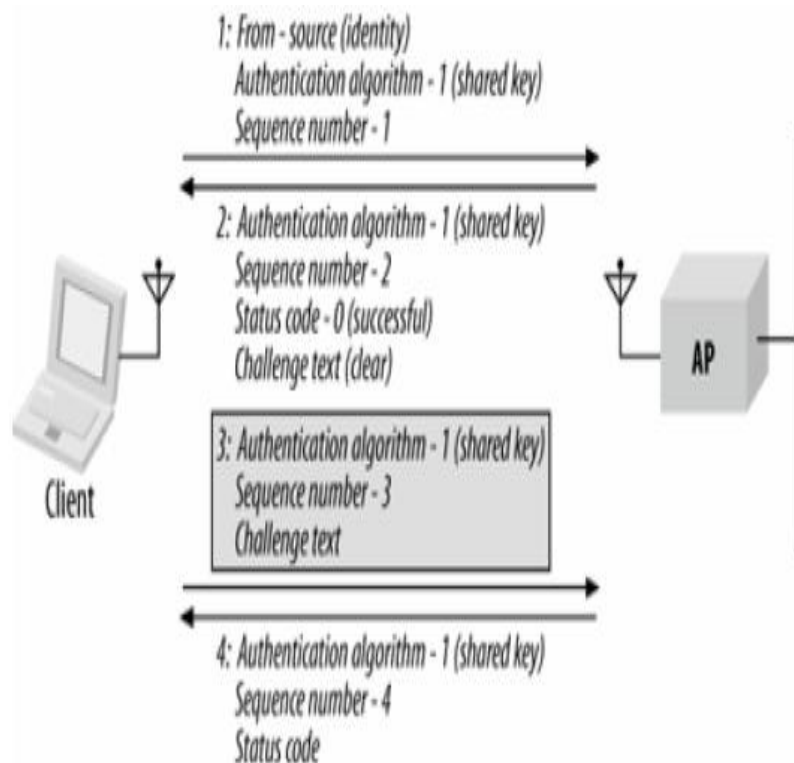
- **Shared Key Authentication**
- Podrazumeva se da je stanicama **predhodno distribuirana zajednička šifra** (kroz siguran kanal)
- **Teorijska osnova:-** Klijentu se šalje **tekst izazova**, a **odgovor dokazuje posedovanje** (poznavanje) **zajedničke šifre**
- Ova usluga **zahteva implementaciju WEP** (*Wired Equivalent Privacy*) **algoritma**
 - Stanice koje ga nemaju – ne mogu koristiti ovaj način prijavljivanja

Prijavljivanje pomoću zajedničke šifre - Procedura



- **Prvi okvir** je sličan *open-system* okviru (**identifikator algoritma + redni broj** okvira)

Prijavljivanje pomoću zajedničke šifre



Umesto slepog odobrenja pristupa

Drugi okvir služi kao – izazov (*challenge*)

Sadrži *četiri* informaciona *polja*:

1. **Identifikator algoritma**
(1 - zajednički ključ)
2. **Redni broj** (=2)
3. **Status Code**

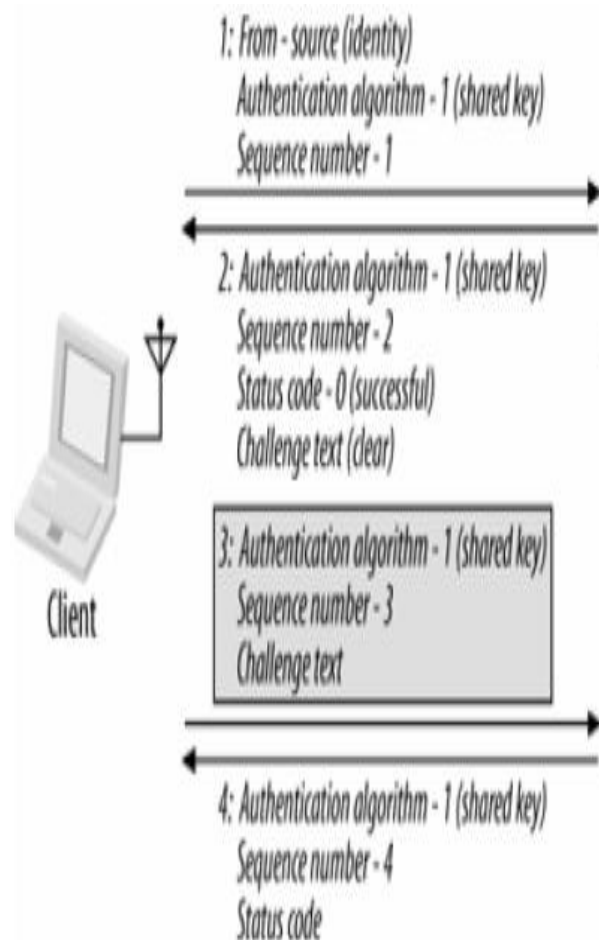
AP može da odbije zahtev

Ako AP odluči da nastavi postupak
(Status Code=0)

U tom slučaju:- četvrto polje

4. **Tekst izazova** (challenge text)

Prijavljivanje pomoću zajedničke šifre



Treći okvir – odgovor stanice na izazov

Stanica enkriptuje tekst izazova (WEP šifra)

1. **Identifikator algoritma**
(1-zajednički ključ)
2. **Redni broj (=3)**
3. **Enkriptovani tekst izazova**

AP vrši dekripciju trećeg polja u primljenom okviru

Dekriptovan tekst = izvornom?

Četvrti okvir –

1. **Identifikator algoritma (=1)**
2. **Redni broj (=4)**
3. **Status Code=0 (prijava uspešna!)**



Asocijacija

- ***Nakon*** uspešno realizovanog procesa ***prijavljivanja*** (autentifikacije) – ***uspostavljanje asocijacije***
- To je ***usluga distributivnog sistema***
- Predstavlja ***logičko povezivanje stanice sa*** određenom ***pristupnom tačkom***
- Omogućuje pristupnoj tački da distribuiraju podatke ka stanici i da ih prima od stanice



Asocijacija

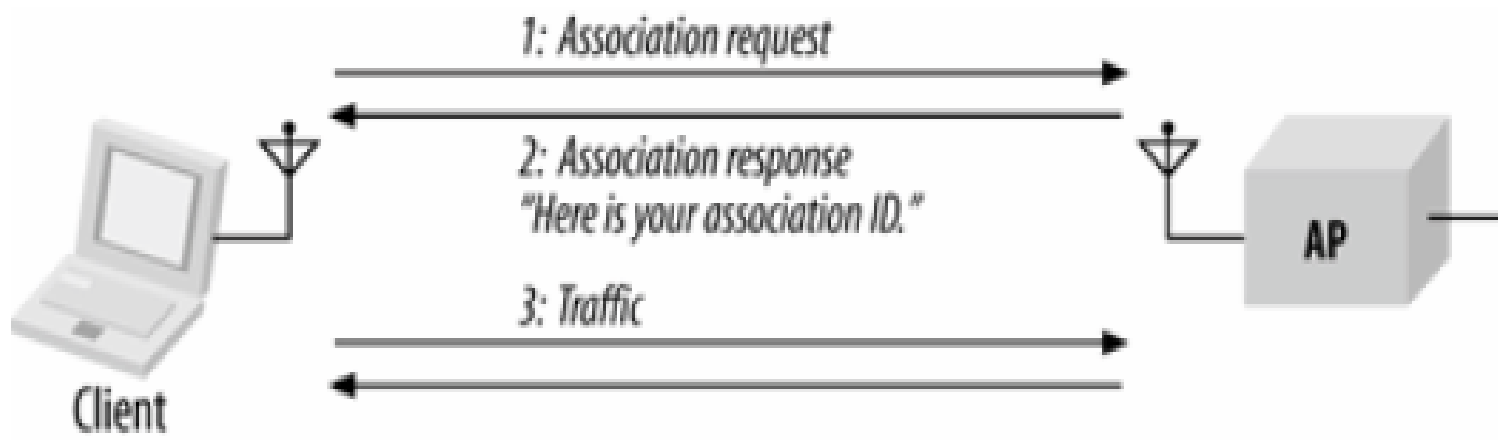
- **Logička veza** između stanice i pristupne tačke
- ***Svaka stanica mora biti povezana na neku pristupnu tačku*** pre nego što joj se dozvoli da razmenjuje podatke sa distributivnim sistemom kroz pristupnu tačku
- **Neophodna** da bi distributivni sistem znao ***gde i kako da komunicira sa tom stanicom***



Asocijacija

- **Stanica aktivira uslugu** asocijacije **samo jednom**, tipično **kad postaje član** određenog skupa stanica
- **Stanica** može izvršiti asocijaciju **sa samo jednom pristupnom tačkom**,
- **Pristupna tačka** može izvršiti asocijaciju **sa više stanica**

Asocijacija - procedura



- **Inicira se od strane stanice** (Client)
- **Nije potrebno sekvenciranje** okvira – koristi se **trostepena procedura usaglašavanja** (hand-shake)
- **Svaki** unicast **upravljački okvir** zahteva L2 **potvrđivanje**
- Asocijacija odobrena: *Association Response* (status kod (0) i **AID**)
- Asocijacija odbijena: *Association Response* (status kod)



Reasocijacija

- Vrší ***transfer asocijacje*** sa jedne pristupne tačke na drugu
- Usluga reasocijacije je ***slična usluzi asocijacije***
- ***Razlika:- Uključuje informaciju o pristupnoj tački*** s kojom je stanica ***prethodno*** bila u asocijaciji



Reasocijacija

- ***Uzastopnim ponavljanjem reasocijacije*** - **stanica se kreće** kroz određenu široku mrežu
 - Gubi kontakt sa poslednjom pridruženom pristupnom tačkom
 - Želi da bude u asocijaciji sa novom pristupnom tačkom



Reasocijacija

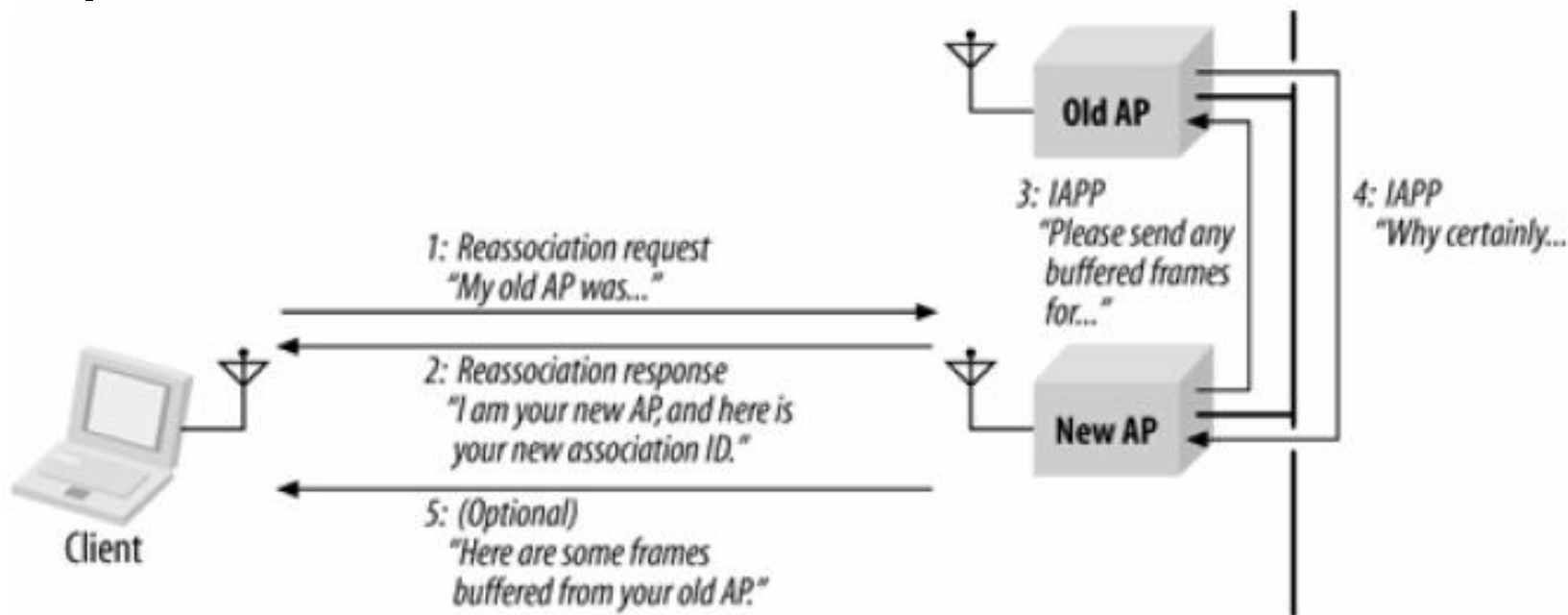
- Uslugu pruža ***distributivni sistem***
- Mobilna ***stanica uvek inicira*** reasocijaciju
- Koristeći uslugu reasocijacije, mobilna stanica
 - ***Obezbeđuje informacije novoj pristupnoj tački*** s kojom će stupiti u asocijaciju
 - ***Održava vezu sa starom*** pristupnom tačkom sa kojom će izvršiti deasocijaciju



Reasocijacija

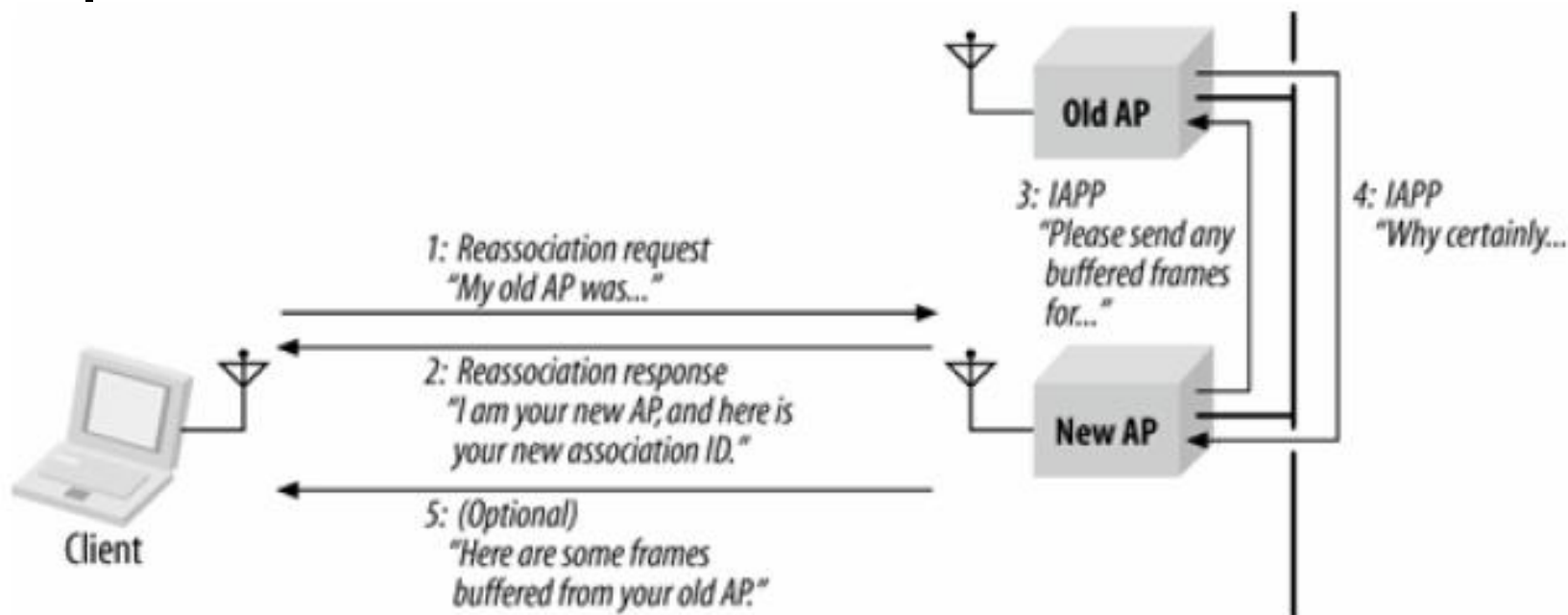
- Nova pristupna tačka ***stupa u kontakt*** sa starom kako bi:
 - Pribavila ***pakete podataka koji čekaju na isporuku*** mobilnoj stanici,
 - Pribavila ***ostale informacije*** koje mogu biti relevantne za novu asocijaciju

Reasocijacija - Procedura



- **Nova AP mora komunicirati sa starom AP** kako bi utrdila **da li je** predhodna **asocijacija postojala**
- **Inter-access point protokol (IAPP)**
- Ako nova AP ne može da utvrdi da li je stara AP autentifikovala stanicu – **nova AP prekida proceduru**

Reasocijacija - Procedura



- **Nova AP obrađuje** Reassociation Request slično obradi Association Request
- **Nova AP kontaktira staru AP** kako bi okončala tekuću asocijaciju sa stanicom
- Svi **okviri baferovani** za stanicu se **šalju novoj AP** (putem ³⁵IAPP-a)



Deasocijacija

- Usluga **distributivnog sistema**
- Vrši **raskid postojeće asocijacije**
- Ova **usluga se koristi**:
 - Da **prinudi stanicu da prekine asocijaciju** sa pristupnom tačkom, ili
 - Da **stanica informiše pristupnu tačku** da joj više nisu potrebne usluge dotične pristupne tačke
- **Nakon** izvršene usluge **deasocijacije** - stanica **mora da izvrši asocijaciju** da bi ponovo komunicirala sa pristupnom tačkom



Deasocijacija

- ***Pristupna tačka može izvršiti deasocijaciju*** neke stanice zbog
 - ***Ograničenja resursa*** ili
 - ***Gašenja*** ili uklanjanja pristupne tačke iz određenog razloga
- Kada stanica dobije obaveštenje da više neće koristiti usluge pristupne tačke, ona može izvršiti deasocijaciju da obavesti pristupnu tačku kako joj uspostavljena logička veza više nije potrebna



Deasocijacija

- Stanica treba da izvrši deasocijaciju ***kada napušta mrežu***
 - Inače ništa drugo u arhitekturi ne osigurava da će se ovo dogoditi
- ***Deasocijacija*** predstavlja obaveštenje i ***može je izvršiti bilo koja strana*** koja se nalazi u asocijaciji
- Nijedna strana ne može odbiti prekid asocijacije



Distribucija

- Ova usluga omogućuje **transfer podataka** između entiteta **kroz distributivni sistem**
- Distribucija je primarna **usluga koji koriste 802.11 stanice**
- Omogućuje **transfer podataka pomoću** najneophodnijih **informacija** koje su **dovoljne za određivanje krajnje destinacije**



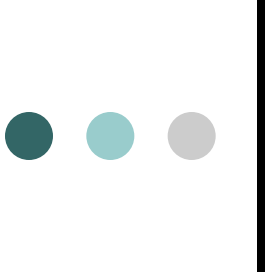
Distribucija

- *Tri asocijacione usluge* (asocijacija, reasocijacija i deasocijacija) **obezbeđuju neophodne podatke** za funkcionisanje distribucione usluge
- Distribucija u okviru distributivnog sistema **ne mora uključivati nikakve dodatne podatke** izvan tri asocijaciona servisa
- Podrazumeva se da **ciljna stanica mora biti u asocijaciji** sa nekom pristupnom tačkom da bi **distributivni sistem** mogao **pravilno proslediti podatke**



Integracija

- Integracija **obezbeđuje transfer podataka između distributivnog sistema** IEEE 802.11 bežične mreže i **neke mreže drugog tipa**
- Stanica koja obezbeđuje ovu funkciju zove se **portal**
- Portal je apstraktni arhitekturni **koncept** koji je tipično **smešten u okviru pristupne tačke**
- Integracioni servis **prevodi format** podataka 802.11 mreža u format koji može da se koristi u drugim tipovima mreža i obratno



Još neke usluge koje obezbeđuje stanica.....



Odjavljivanje

- *Deauthentication*
- ***Uklanja postojeću prijavu***
- Koristi se da ***eliminiše mogućnost korišćenja mreže*** od strane ***prethodno autorizovanog*** korisnika
- Kad se ***stanica odjavi***, ona više ***ne može pristupiti bežičnoj mreži*** bez ponovnog izvođenja procedure prijavljivanja



Odjavljivanje

- **Odjavljivanje** predstavlja obaveštenje i **ne može biti odbijeno**
- Na primer, ako stanica želi da se odjavi iz određenog skupa stanica, ona **šalje okvir za odjavljivanje (deauthentication frame) svojoj pridruženoj pristupnoj tački**, da je obavesti o svom odjavljivanju
- **Pristupna tačka takođe može odjaviti stanicu** šaljući joj format za odjavljivanje



Privatnost

- *Privacy*
- **Sprečava neovlašteno pregledanje podataka** kroz primenu **WEP** (*Wireless Equivalency Privacy*) **algoritma**
- Dizajnirana da obezbedi **ekvivalentan stepen zaštite podataka kao kod ožičenih mreža** sa ograničenim fizičkim pristupom
- Ova usluga **štiti podatke samo dok se prenose** kroz bežični medijum



Privatnost

- ***Nije dizajnirana da obezbedi kompletnu zaštitu podataka*** koji se šalju između aplikacija širom neke mešovite mreže



Privatnost

- U bežičnoj mreži, **sve stanice** i ostali uređaji **mogu čuti saobraćaj podataka** koji se odvija u okviru dometa mreže, što **ozbiljno ugrožava nivo sigurnosti** bežične veze
- IEEE 802.11 standard se bori protiv ovog problema pomoću sigurnosne usluge koja se **zasniva na algoritmu za šifrovanje**



MAC servis za isporuku jedinica podataka

- *Jedinica podataka MAC usluge (MSDU) je jedinica podataka isporučena MAC pod-sloju od strane LLC pod-sloja (kontrolera)*
- Tačka u kojoj LLC pristupa servisu MAC pod-sloja (na vrhu MAC pod-sloja) se naziva MAC SAP, *tačka pristupa MAC usluzi*
- Ovaj servis obezbeđuje *isporuku MSDU-ova između ovih SAP-ova*