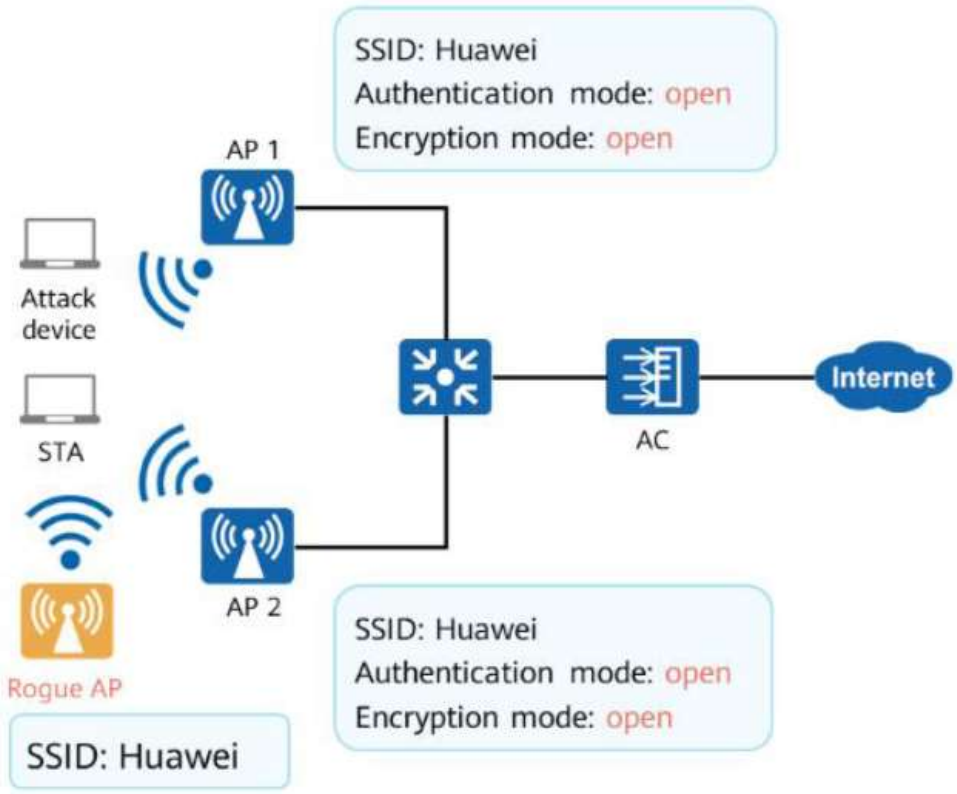
Projektovanje bežičnih mreža

Sadržaj

- Bezbednost bežičnih mreža
- WLAN arhitekture
  - WLAN komponente, arhitekture i mrežni modeli
  - WLAN roaming
  - Tipična rešenja
- Antene
- Prostorno planiranje

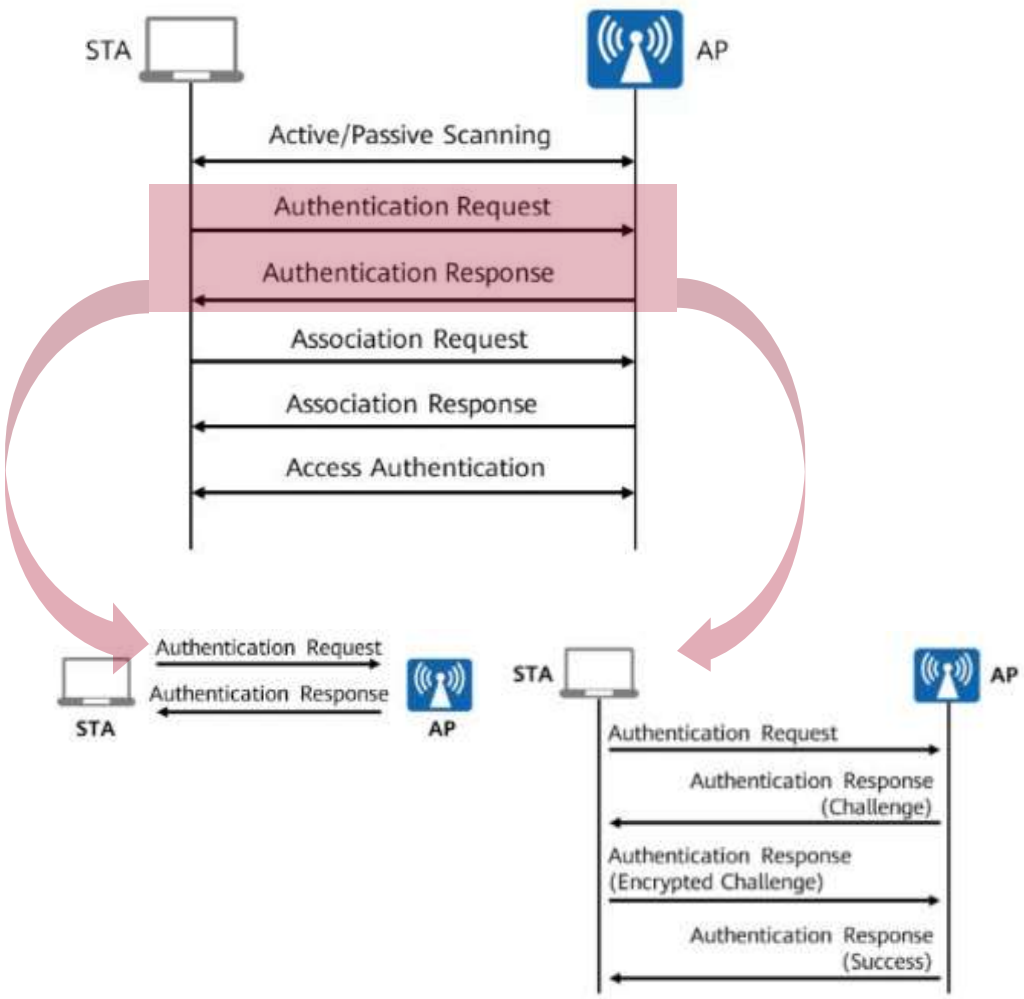
BEZBEDNOST

Tipične pretnje po bezbednost WLAN mreža



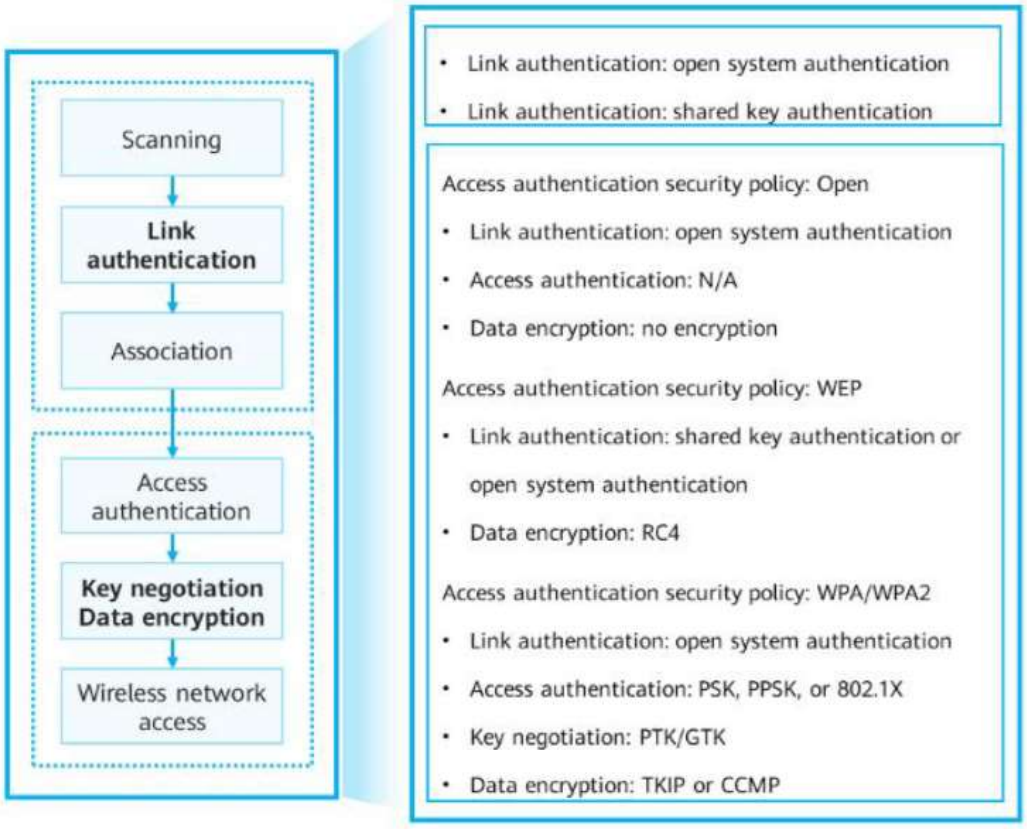
- **No authentication**: napadač se može povezati na bežičnu mrežu nesmetano i kompromitovati različite mrežne servise
- **Non-encrypted wireless data**: napadač može presretati ili modifikovati korisnički saobraćaj i na taj način sprovesti nedozvoljene radnje na mreži.
- **Perimiter threat**: AP koji ima podešen isti SSID kao SSID validne mreže. Na ovaj način se nepažljivi korisnici (većina) mogu povezati na AP napadača, preko koga on može prisluškivati saobraćaj.
- WLAN security:
  - Perimiter security
  - **Access Security**
  - **Service Security**

Proces povezivanja na WLAN mrežu (tradicionalan)



- U fazi link autentifikacije AP vrši proveru da li STA ima pravo pristupa.
- Faza link autentifikacije podrazumeva da AP ima podešenu šifru i da **svi korisnici** imaju tu istu šifru podešenu na klijentima.
- Ukoliko je **Shared Key** Auth.:
  - STA šalje zahtev za autentifikacijom
  - AP generiše „izazov" koji predstavlja slučajan „plaintext" podatak i šalje ga klijentu
  - Klijent šifrira dobijeni „izazov" šifrom koja je prethodno podešena
  - AP takođe šifrira istu tu poruku svojom šifrom, i ako je šifrirani tekst isti kao i šifrirani tekst koji je dobio od klijenta zaključuje da klijent ima ispravnu šifru.

802.11i model povezivanja na WLAN mrežu

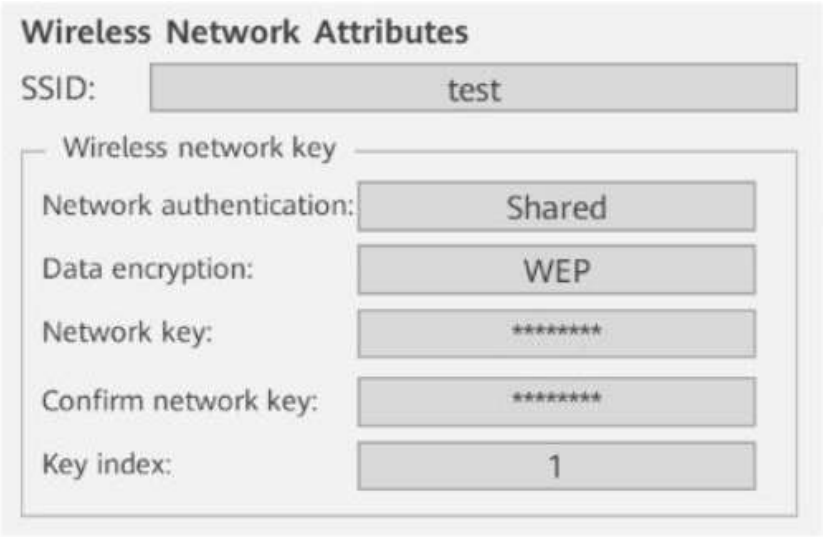


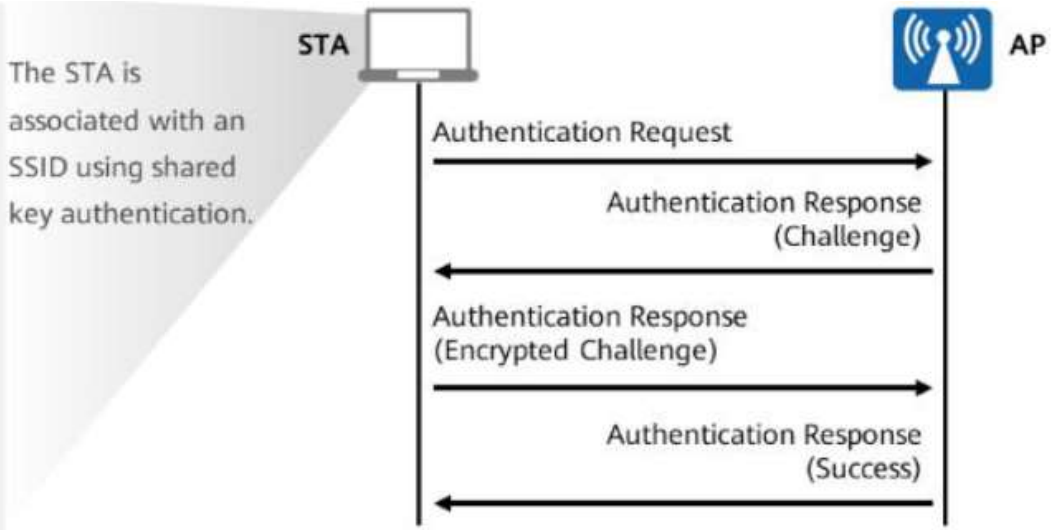
- Problemi kod link autentifikacije:
  - Svi korisnici dele istu šifru
  - Čak i da su podaci enkriptovani posle pristupa, regularno povezani korisnici imaju istu šifru za enripciju podataka (mogu se prisluškivati međisobno)
- 802.11i skup standarda koji se tiču bezbednosti uvodi:
  - Access authentication
  - Key negotiation i Data encryption
- Bez obzira da li se koristi **Access Authentication** ili ne, faza link auth. se ne preskače, već se u slučaju da se koristi AA, LA sprovodi kao open-auth.
- Access Authentication može biti:
  - Open
  - WEP
  - WPA/WPA2
    - PSK, PPSK ili 802.1X

WEP

- Wired Equivalent Privacy je originalni bezbednosni mehanizam IEEE 802.11 koji je prisutan u standardu praktično od samog nastanka.
- Vrši funkciju zaštite mreže od neautorizovanog pristupa.
- Koristi RC4 šifrator i statičke ključeve za enkripciju podataka.
- Sve STA koriste isti ključ za pristup

- WEP je **kripotgrafski nebezbedan** i postoje poznati napadi koji kriptoanalizom za desetak minuta dolaze do tačne šifre.

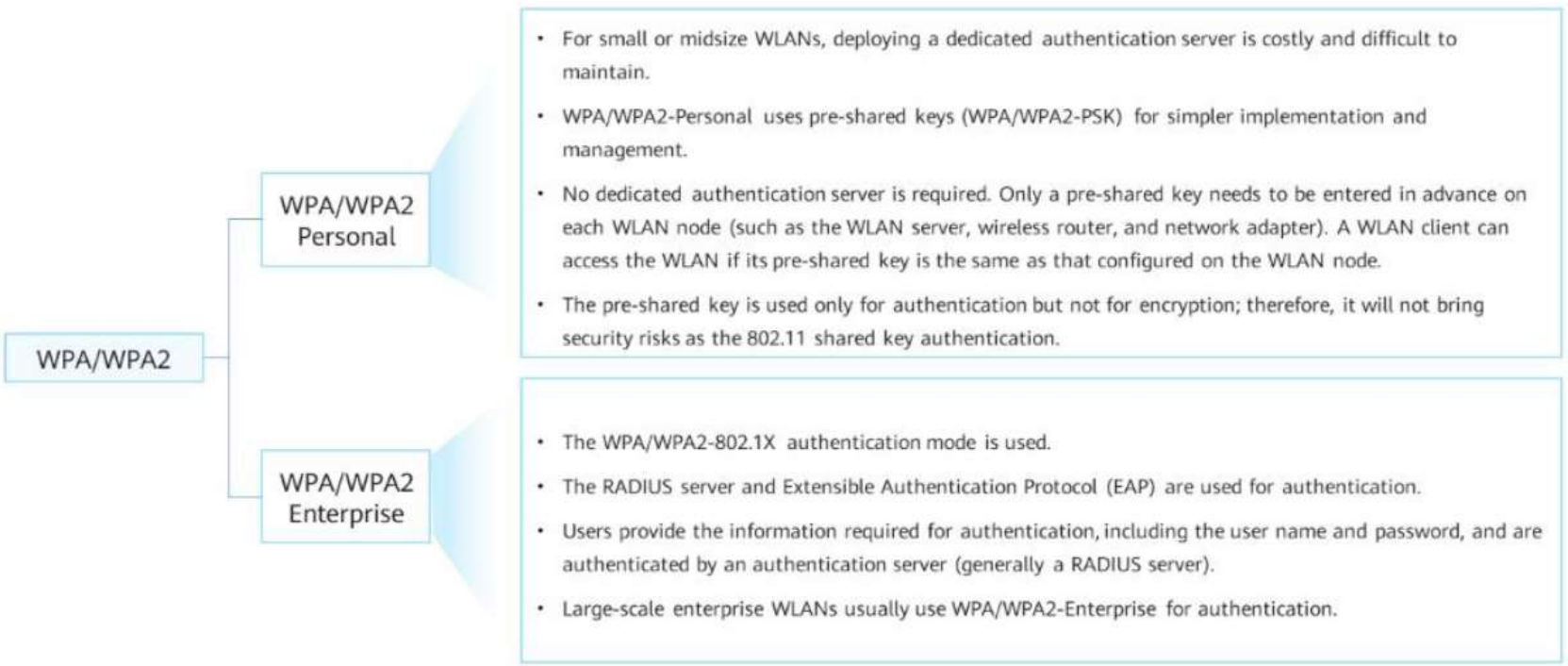




WPA/WPA2

- Da bi rešili problem nebezbednosti WEP-a, WiFi Alijansa je predložila **Wi-Fi Protected Access** (WPA).
- WPA uz RC4 koristi bezbedniji TKIP algoritam/protokol za upravljanje ključevima i eliminiše nebezbedne statičke ključeve iz algoritma (Temporal Key Integrity Protokol).
- Na ovaj način je obezbeđena hardverska kompatibilnost između WEP i WPA/TKIP uređaja.
- Pored TKIP, WPA može koristiti i noviji i bolji AES algoritam za enkripciju.

- WPA/WPA2 ima personal i enterprise varijantu.
  - Personal: koristi preshared-key tehniku. Pogodna za male mreže
  - Enterprise: koristi 802.1X autentifikacioni model za autentifikaciju korisnika korisničkim imenom i šifrom preko RADIJUS (AAA) servera.



Bezbednosne šeme bežičnih mreža

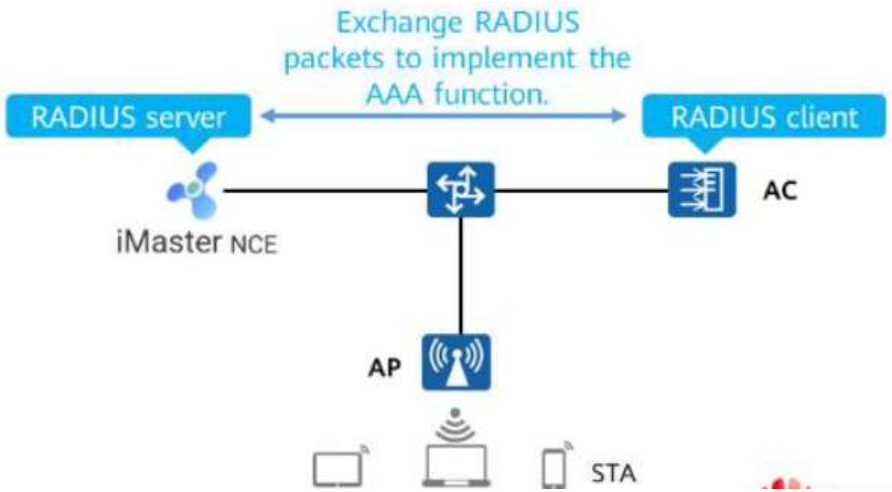
Security Policy	Link Authentication	Access Authentication	Encryption Algorithm	Recommended Application Scenario	Description
Open	Open system authentication	N/A	No encryption	Networks with low security requirements	Wireless devices can connect to a WLAN without authentication.
WEP-open	Open system authentication	No access authentication is provided. This security policy can be used together with Portal or MAC address authentication.	No encryption/RC4	Public places with high user mobility, such as airports, stations, business centers, and conference venues	It is insecure when used independently, because any wireless clients can access the WLAN without authentication. You are advised to configure this security policy together with Portal or MAC address authentication.
WEP-share-key	Shared key authentication	N/A	RC4	Networks with low security requirements	This security policy is not recommended due to its low security.
WPA/WPA2-PSK	Open system authentication	PSK authentication	TKIP/AES	Home users or small/midsize enterprise networks	This security policy has higher security than WEP shared key authentication. Additionally, no third-party server is required and the cost is low.
WPA/WPA2-802.1X	Open system authentication	802.1X authentication	TKIP/AES	Large-scale enterprise networks with high security requirements	This security policy provides high security and requires a third-party server, resulting in high costs.

AAA i RADIUS server

- Authentication, Authorization and Accounting (AAA) pruža mehanizam za upravljanje bezbednim pristupom mreži.
  - Authentication – provera da li korisnik ima pravo da pristupi mreži
  - Authorisation – autorizuje korisnika za korišćenje pojedinih servisa
  - Accounting – vođenje evidencije

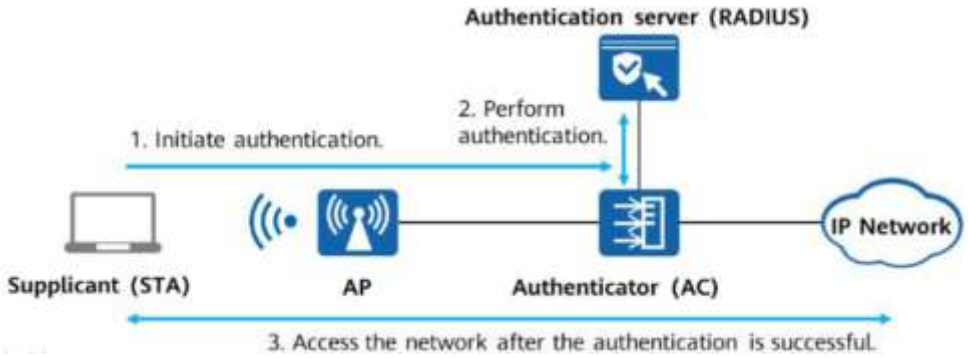
Authentication	Authorization	Accounting
A user enters the user name and password for identity authentication when accessing a network.	The user passes the identity authentication, and the network delivers the user authorization information (the user belongs to VLAN 10 and can access the Internet).	The user is connected to the network, and accounting is started.

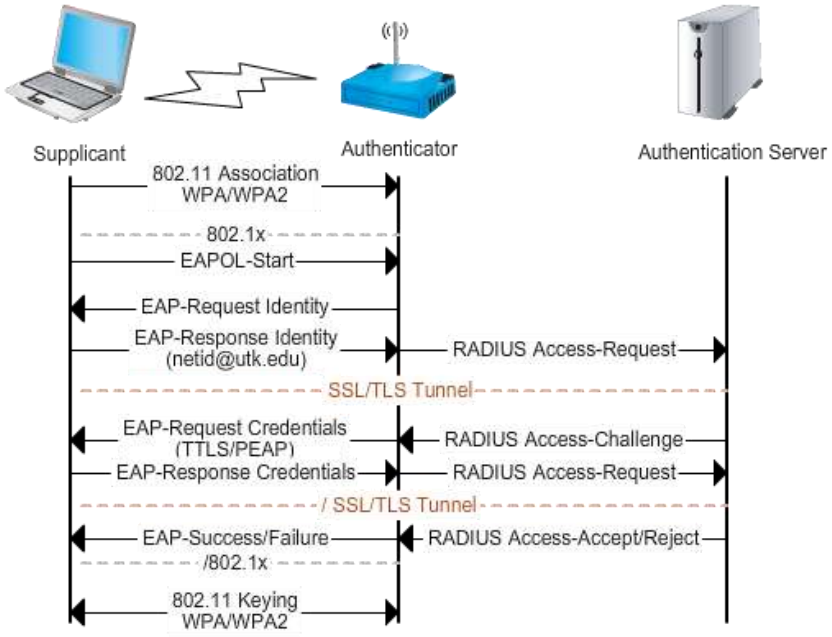
- AAA se može implementirati na različite načine.
- Najzastupljenija implementacija preko RADIUS-a
- RADIUS je protokol koji koristi klijent/server model
- Koristi UDP portove 1812 i 1813 za autentifikaciju i akaunting, respektivno.



8021X autentifikacija

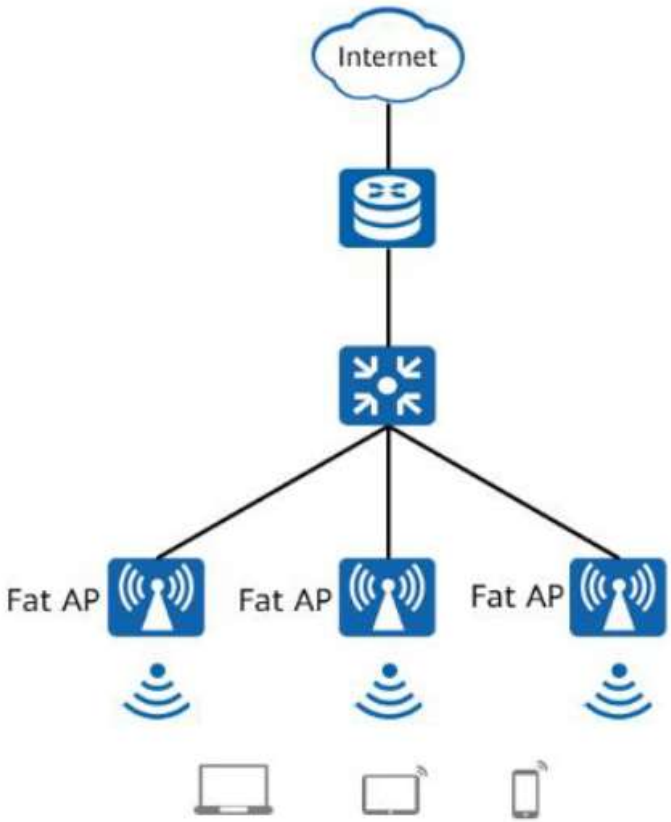
- 802.1X je model autentifikacije koji najčešće koristi RADIUS serve za autentifikaciju
- 802.1X definiše EAP (Extensible Authentication Protocol) za razmenu podataka između STA, autentifikatora i servera za autentifikaciju (slika)





WLAN ARHITEKTURE

Fat AP arhitektura

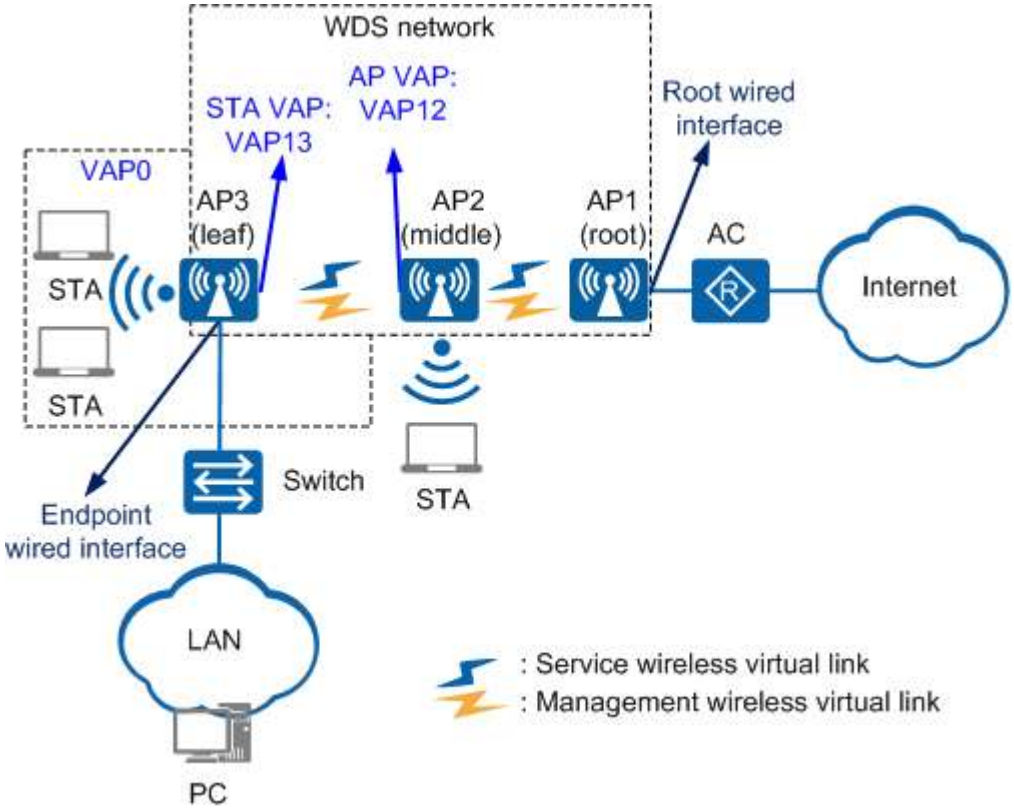


- Fat AP arhitektura se naziva i „autonomna" mrežna arhitektura *(autonomous network architecture*)
- Autonomna je u tom smislu da AP-u nije potrebna podrška drugih uređaja da bi funkcionisao.

- **Prednosti**
- Lako se postavlja.
- Cena koštanja je niska.

- **Mane**
- Ukoliko je potrebno pokriti veću površinu, za šta je potrebno više AP-ova, svaki od njih se nezavisno konfiguriše što predstavlja problem za upravljanje i oržavanje
- Ne preporučuje se zbog toga za veće mreže. Umesto ove arhitekture za veće mreže sa većim pokrivanjem preporučuje se Fit AP + AC

WDS arhitektura

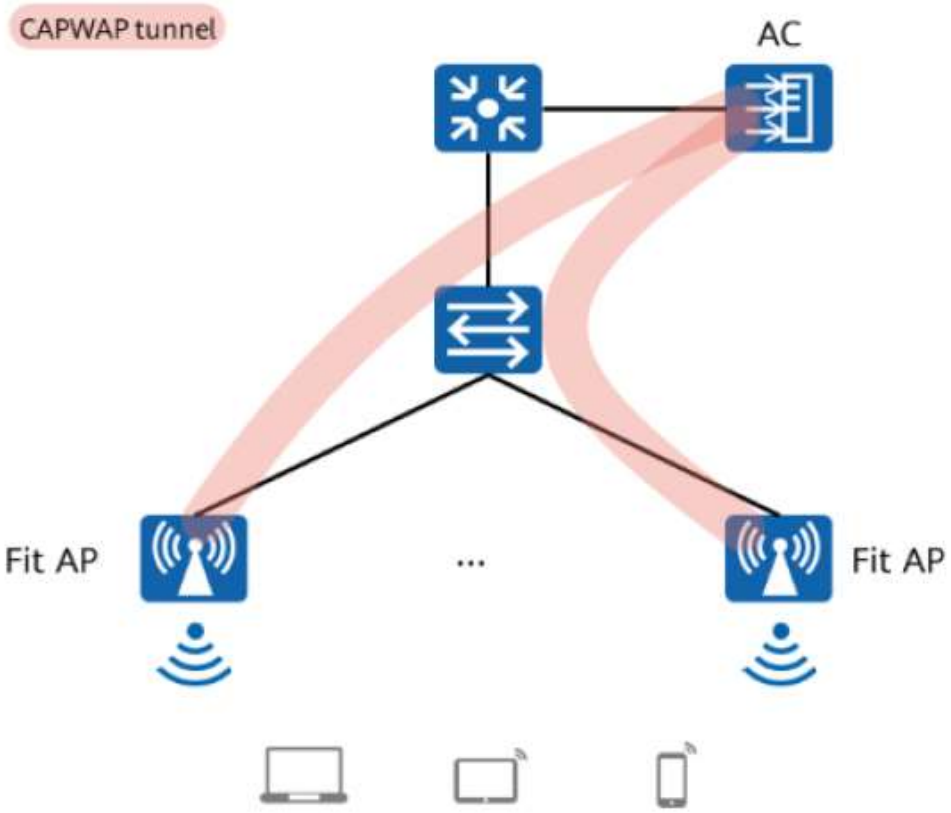


- Wireless Distribution System (**WDS**) je sistem koji omogućava bežičnu vezu između nekoliko AP-ova na IEEE 802.11 mreži.
- Omogućava da BSA bude proširen korišćenjem više AP-ova bez potrebe postavljanja žičane mreže između njih.
- Root AP je jedini koji treba da ima bar jedan port povezan na žičanu mrežu.

- Ovo je daleko lošije rešenje od Fit AP + AC mreže:
  - Performanse su prilično slabe (bandwidth se u najmanju ruku smanjujje duplo)
  - Nestabilniji rad

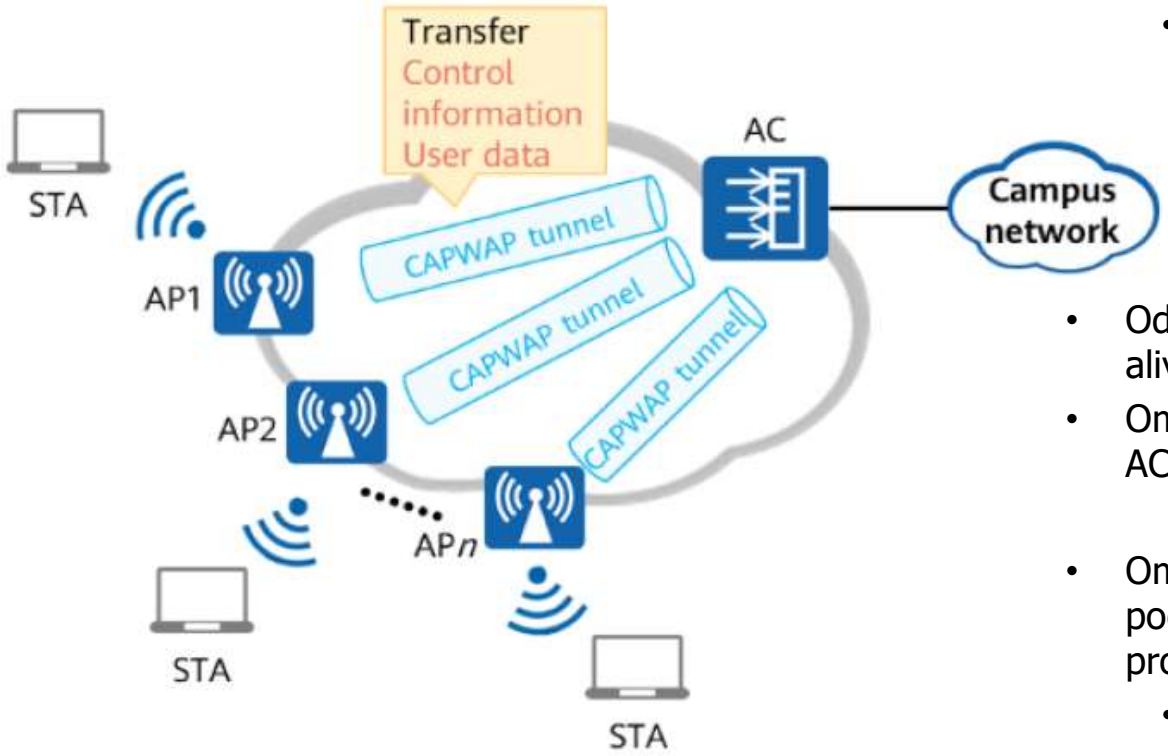
- Većina Fat AP-ova ima WDS mod
- Nije toliko u upotrebi danas zbog loših karakteristika

AC + Fit AP arhitektura



- **AC + Fit AP** je trenutno de facto standard za velike WLAN mreže (pokrivanje cele zgrade jedne kompanije, hotela, stadiona, i sl.)
- **Access Controler** (AC) je mrežni uređaj, vizuelno vrlo sličan običnom sviču, čija je uloga:
  - Centralizovana konfiguracija svih AP-ova kroz konfiguraciju grupa AP-ova
  - Kontrola pristupa WLAN-u
  - Prosleđivanje korisničkog saobraćaja (poput proxy servera, ako je podešen da radi u tunnel modu)
  - Prikupljanje statistike
  - Kongiguraciaj i upravljanje AP-ovima
  - Upravljanje roaming-om
  - Upravljanje bezbednošću
- **Fit AP** – nikakva podešavanja direkno se ne vrše na njemu.
  - Dobija IP adresu AC-a i uspostavlja **CAPWAP** (Control and Provisioning of Wireless Access Points) tunel do njega.
  - AC upravlja radom Fit AP-a
  - Fit AP ima funkciju L1 uređaja: enriptuje i dekriptuje 802.11 frejmove.

CAPWAP protokol



- Omogućava AP-ovima da **automatski** (plug-and-play) otkriju za postojanje AC-a
  - Ukoliko su **na istom** brotkast domenu, nakon što Fit AP dobije adresu od DHCP servera, brotkastuje *discovery* paket
  - Ukoliko **nisu na stoj IP** mreži, AP uz IP adresu treba da od DHCP-a dobije i IP adresu AC-a (preko DHCP opcije 43)

- Održava konekciju između AC-a i AP-a keep alive mehanizmom
- Omogućava da nakon uspostavljanja veze AC uploaduje konfiguraciju na AP

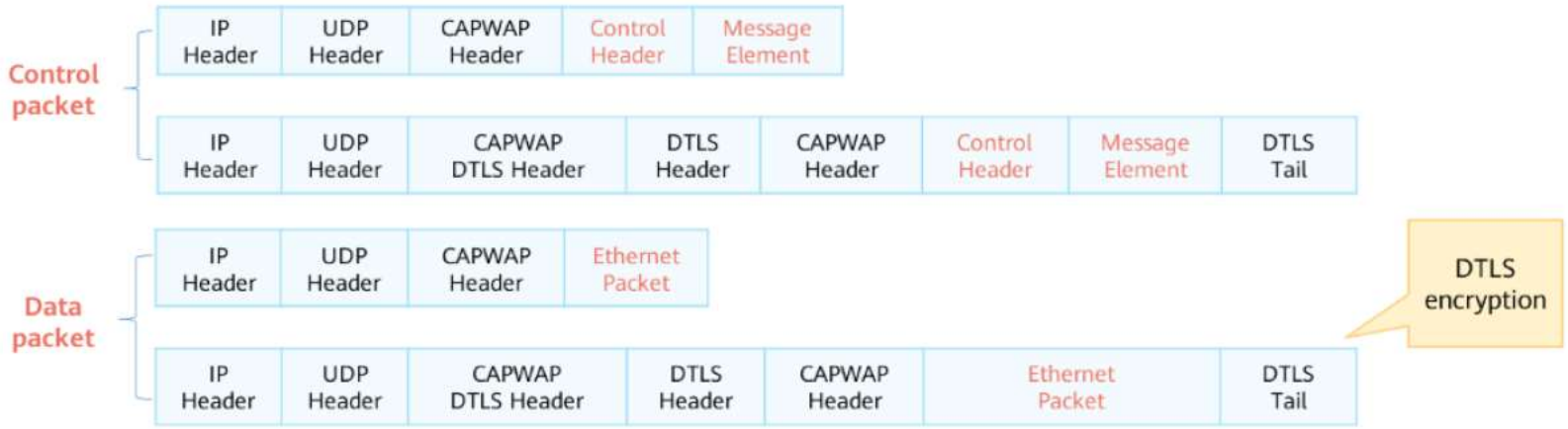
- Omogućava enkapsulaciju korisničkih podataka od STA u pakete CAPWAP protokola i njihovo tunelovanje do AC-a
  - Na ovaj način se lako rešava problem rominga kada STA prelazi sa jedan AP na drugi, a AP-ovi nemaju isti IP adresni opseg. STA može da zadrži svoju IP adresu i ne izgubi konekciju prilikom prelaska.

CAPWAP format paketa

- CAPWAP je standardni protokol i podržavaju ga svi proizvođači AP-ova
- CAPWAP ima dva tipa paketa:
  - Kontrolne pakete – koriste se za uspostavljanje veze, keep alive i slanje konfiguracije
  - Data pakete – koriste se za tunelovanje korisničkog saobraćaja
- Management: UDP port 5246
- Service data traffic: UDP port 5247

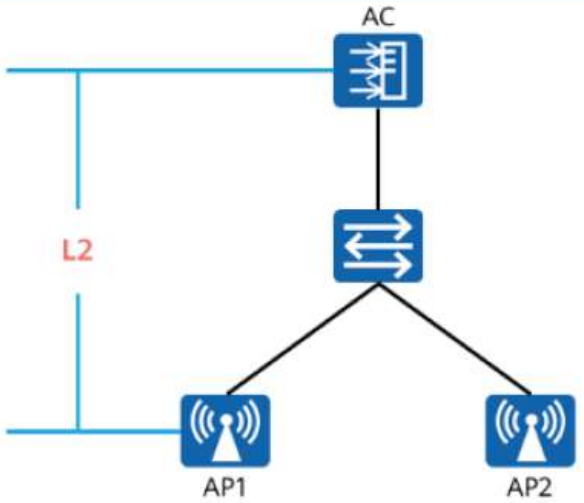
Packet Type	Function	UDP Port	Encryption
Control packet	Managing APs	5246	Mostly ciphertext
Data packet	Forwarding service data	5247	Mostly plaintext

The formats of the control packet and data packet are as follows:



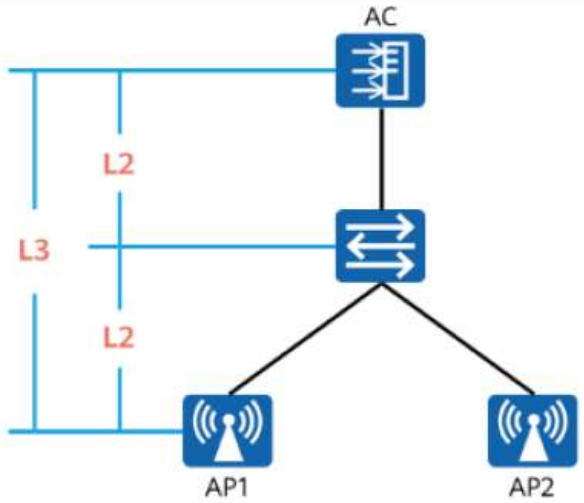
Layer 2 i Layer 3 networking

Layer 2 Networking



- **Description:** The AC and Fit APs are in the same broadcast domain. The Fit APs can directly discover the AC through local broadcast. The networking, configuration, and management are simple.
- **Application scope:** Layer 2 networking applies to small-scale networks, such as small-sized enterprise networks and is not recommended for large-sized enterprises that use complex WLAN networking, and require fine-grained management.

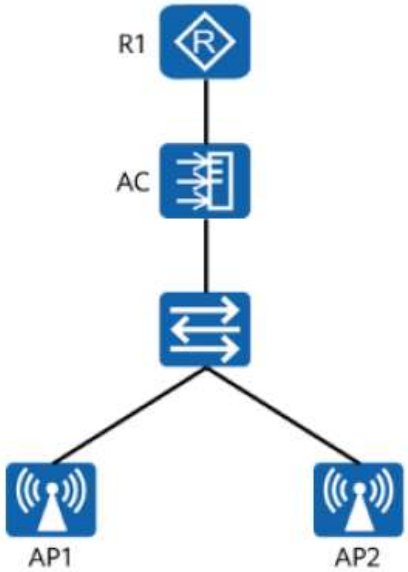
Layer 3 Networking



- **Description**: The AC and Fit APs are in different network segments. The intermediate network must ensure that the Fit APs and AC are reachable to each other. Additional configurations are required to enable the Fit APs to discover the AC. The networking is flexible and easy to expand.
- **Application scope**: Layer 3 networking is suitable for medium- and large-scale networks. For example, on a large-scale campus network, APs are deployed in each building for wireless coverage, and the AC is deployed in the core equipment room for unified management and control. In this case, a complex Layer 3 network must be deployed between the AC and Fit APs.

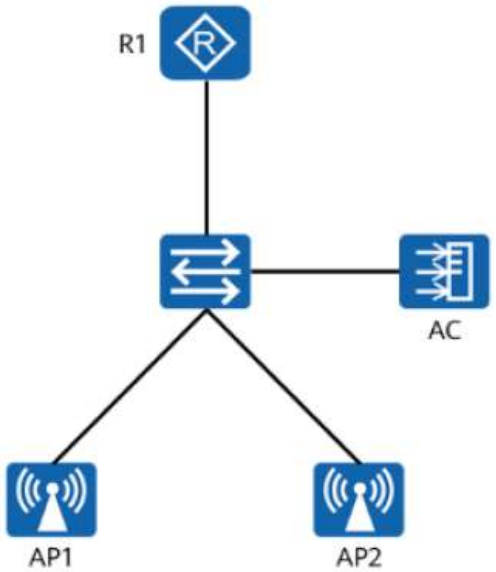
In-Path i Off-Path networking

In-Path Networking



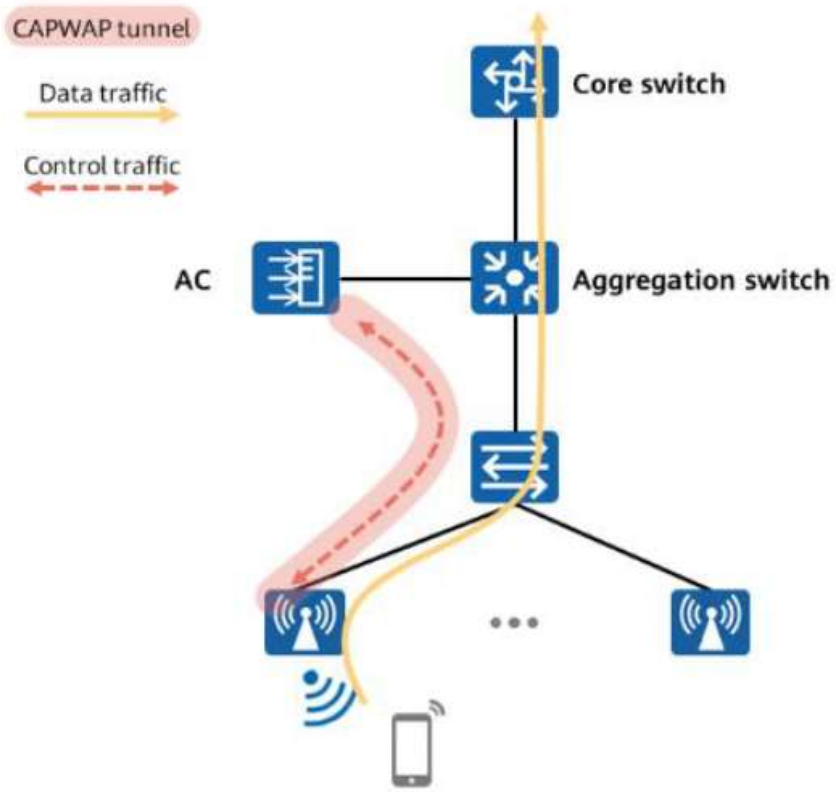
- **Description**: An AC functions as both a wireless access controller and an aggregation switch to centrally forward and process the data and management services of APs.
- **Application scope**: newly deployed small- and medium-scale centralized WLANs

Off-Path Networking

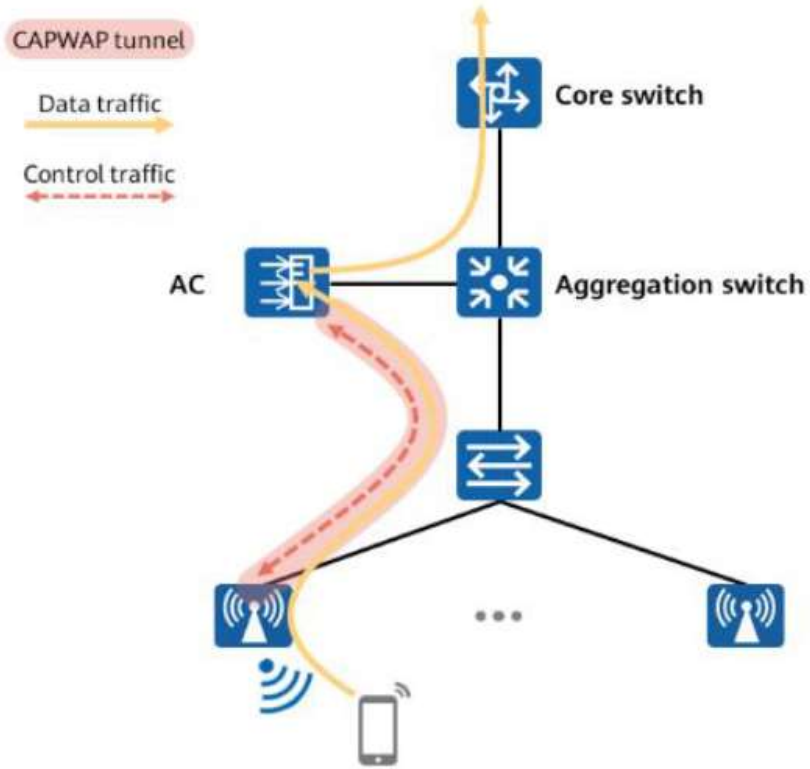


- **Description**: An AC is connected to the live network in off-path mode and processes only the management services of APs. The service data of APs reaches the uplink network without passing through the AC.
- **Application scope**: network reconstruction or construction of large- and medium-sized campus networks

Direct i Tunnel Forwarding



- **Direct forwarding**: AP direktno prosleđuje korisničke (STA) pakete bez ikakve enkapsulacije.
- Uloga AC je (samo) upravljanje AP-ovima
- Prednost: saobraćaj ne prolazi kroz AC, pa je opterećenje AC-a veoma malo.
- Ovaj mod je preporučen za mreže kod kojih je ukupni saobraćaj od strane mogilnih korisnika reda veličine 10 Gbps i više



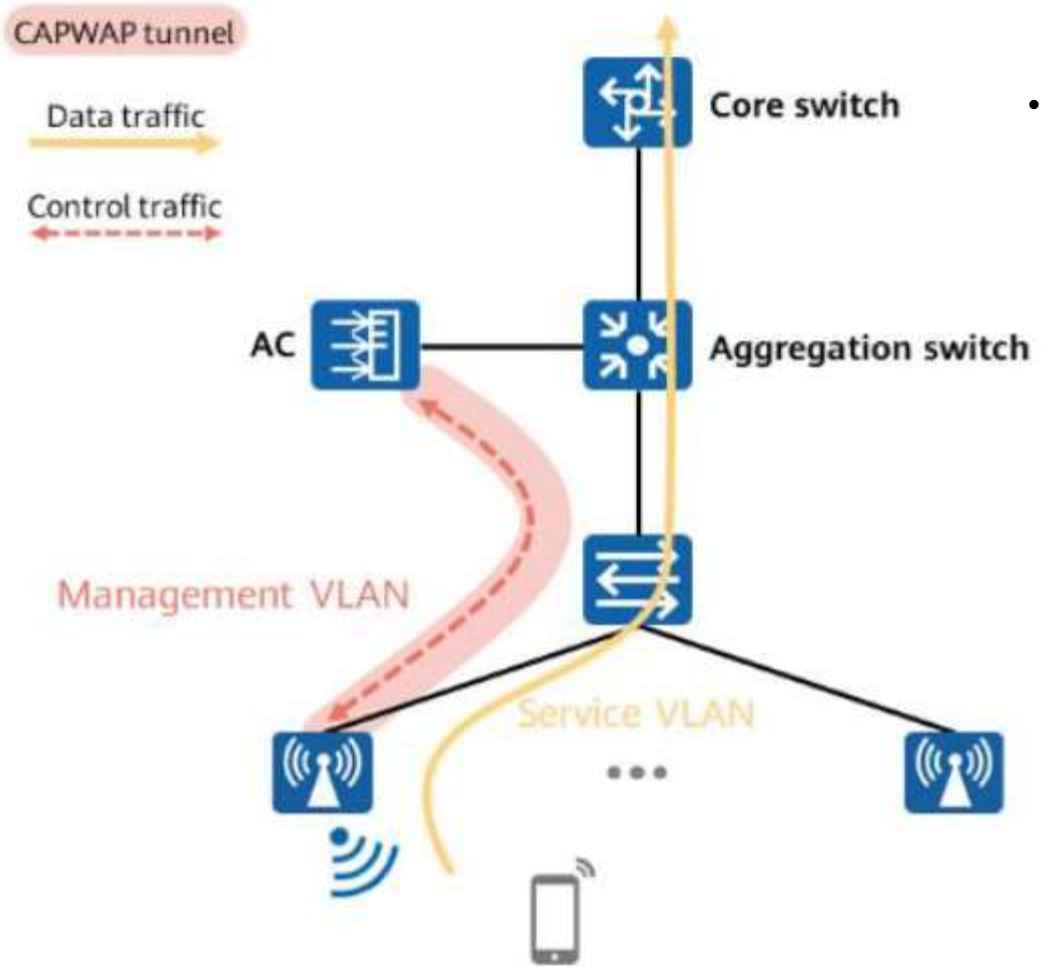
- **Tunel forwarding**: Paketi STA se enkapsuliraju u CAPWAP i šalju preko IP mreže do AC (tuneluju).
- Prednosti: saobraćaj prolazi kroz AC, pa je
  - Bezbednost bolja
  - Moguć roaming ako AP-ovi imaju različite IP mreže.

Mrežni modovi

- In-path/off-path, Layer 2/3 i tunel/direktan mod se mogu kombinovati na različite načine.

Networking	Characteristics
In-path mode + Layer 2 networking + direct forwarding	No data bypassing and high forwarding efficiency
Off-path mode + Layer 2 networking + direct forwarding	No data bypassing and high forwarding efficiency, facilitating WLAN deployment on the live network and deployment of the hot standby (HSB) solution
Off-path mode + Layer 2 networking + tunnel forwarding	Simple data VLAN configuration and Layer 2 tunnels provided by tunnel forwarding for supporting 802.1X authentication, facilitating WLAN deployment on the live network and deployment of the HSB solution.
Off-path mode + Layer 3 networking + tunnel forwarding	Simple data VLAN configuration and Layer 2 tunnels provided by tunnel forwarding for supporting 802.1X authentication, facilitating WLAN deployment on the live network and deployment of the HSB solution.
Off-path mode + Layer 3 networking + direct forwarding	No data bypassing and high forwarding efficiency, facilitating WLAN deployment on the live network and deployment of the HSB solution

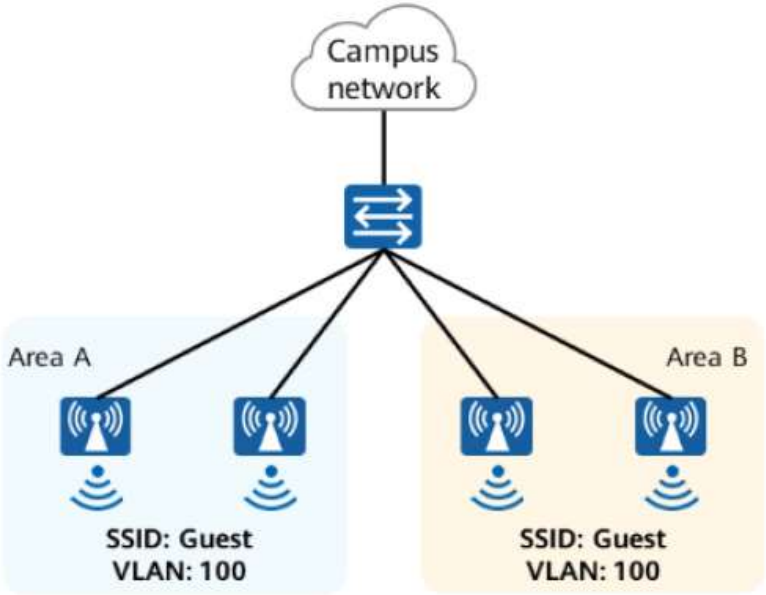
Planiranje VLAN-ova



- VLAN na kom se ostvaruje CAPWAP i VLAN na kom su STA se može razlikovati kod AC + Fit AP arhitekture, bez obira na mod u kom AC i AP rade
- Management VLAN je obično na Native-VLANu sviča! Objašnjenje…

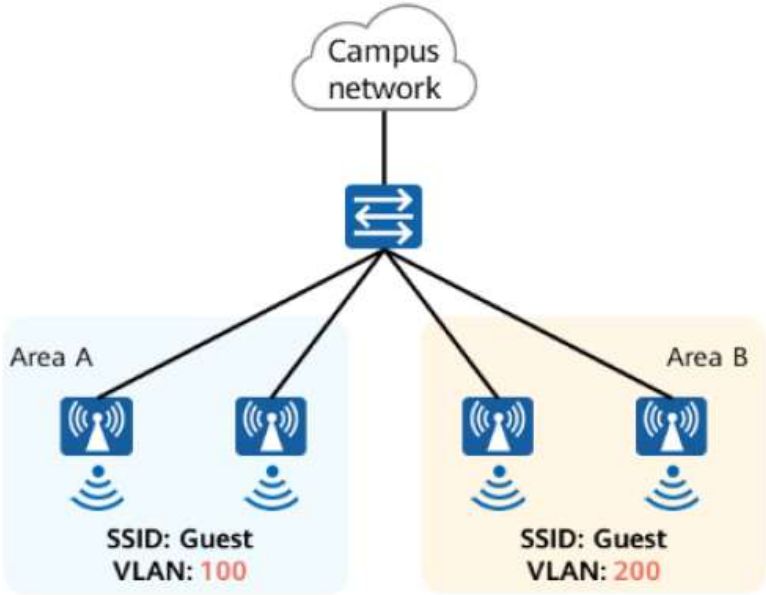
Planiranje IP adresa

SSID:VLAN = 1:1



- Jednostavniji roaming jer je IP adresa STA validna prilikom prelaska.
- Teže za implementaciju na većim mrežama

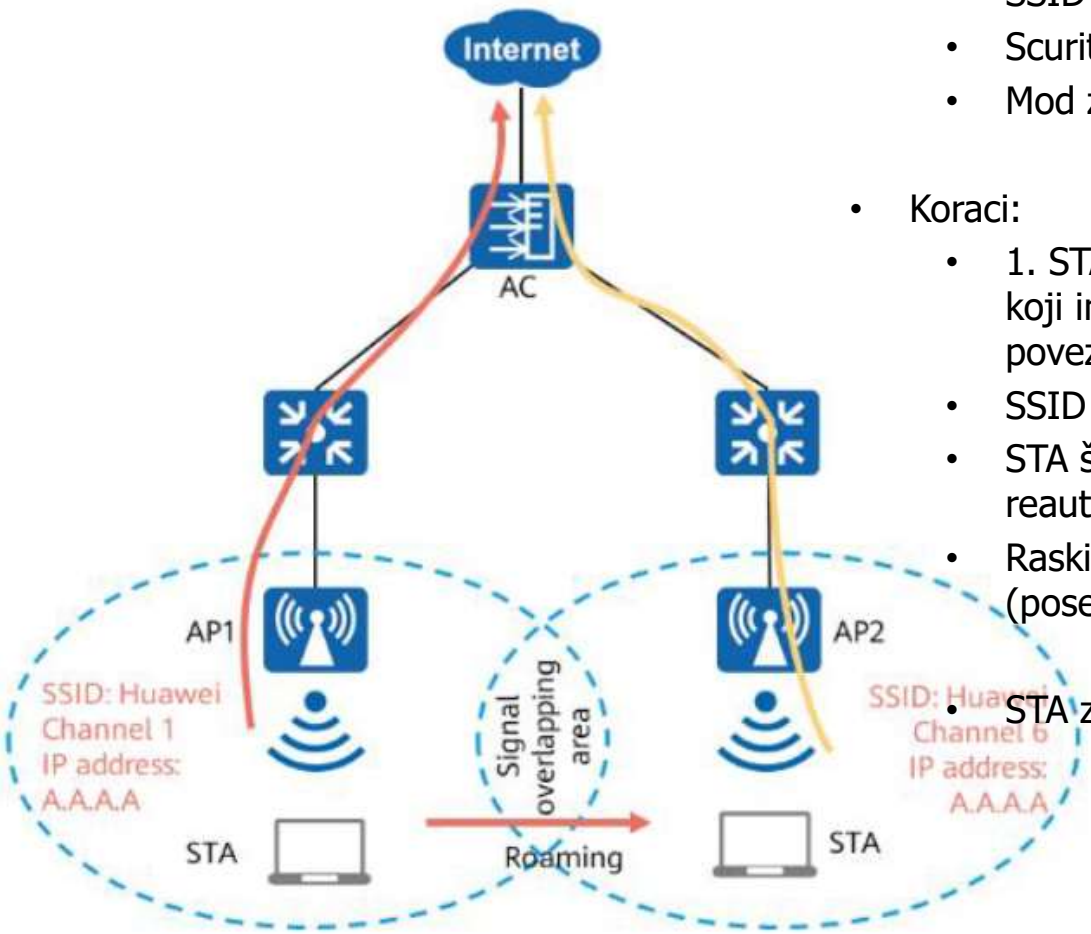
SSID:VLAN = 1:*N*



- Roaming moguć samo u tunel modu
- Jednostavnije za implementaciju na većim mrežama

WLAN ROAMING

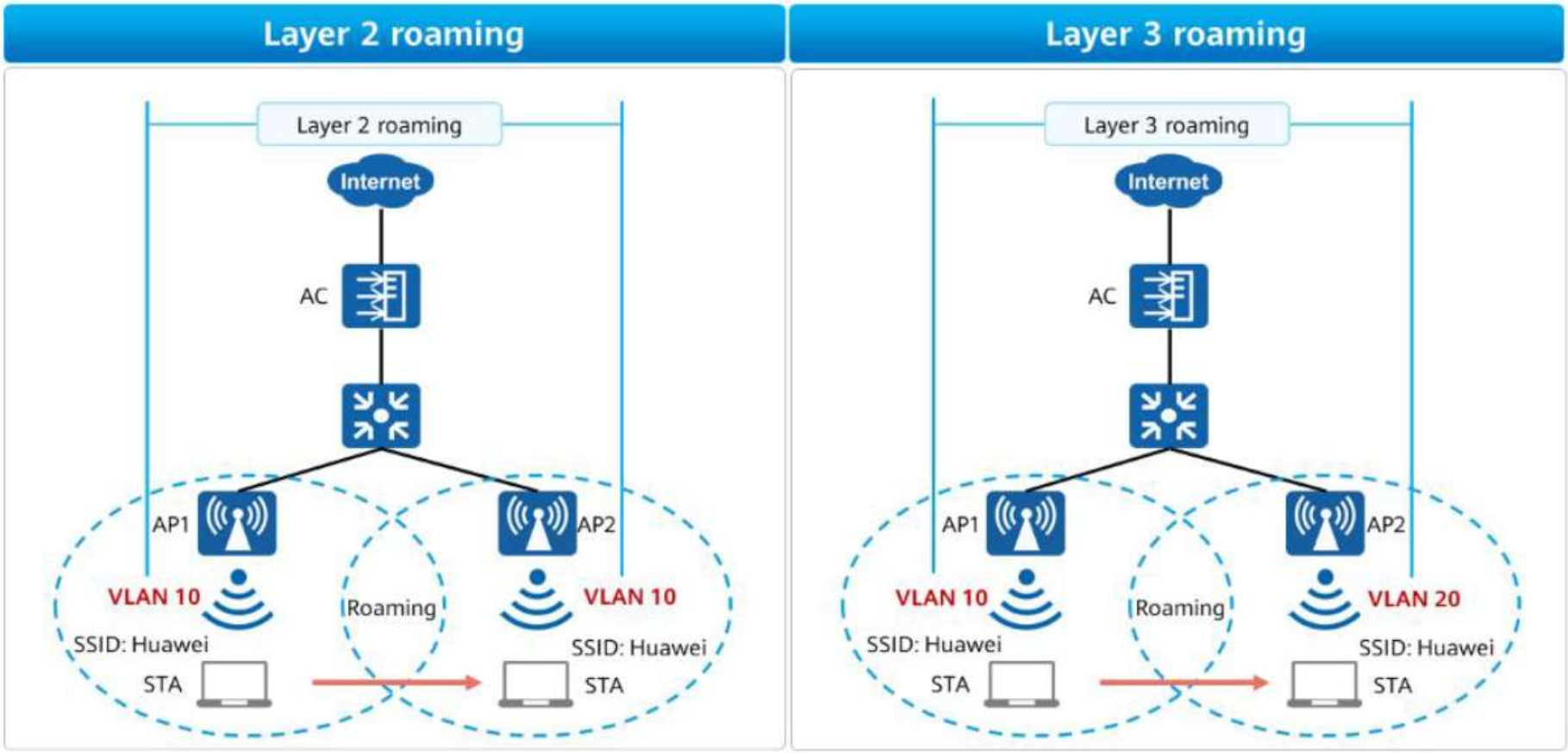
Koncept roaming-a



- WLAN roaming omogućava da STA prelazi sa jednog na drugi AP bez prekida veze i servisa
- Da bi roaming bio moguć:
  - SSID treba da je isti
  - Scurity identičan
  - Mod za utentifikaciju isti

- Koraci:
  - 1. STA detektuje da postoji AP sa istim SSID-jem koji ima jači signal od AP-a na koji je trenutno povezan
  - SSID je isti, BSSID se razlikuje
  - STA šalje zahtev na oba BSSID-a za reautentifikacijom
  - Raskida vezu sa jednim i vrši **reasocijaciju** (poseban 802.11 frejm) na drugi AP.
  - STA zadržava svoju IP!!!

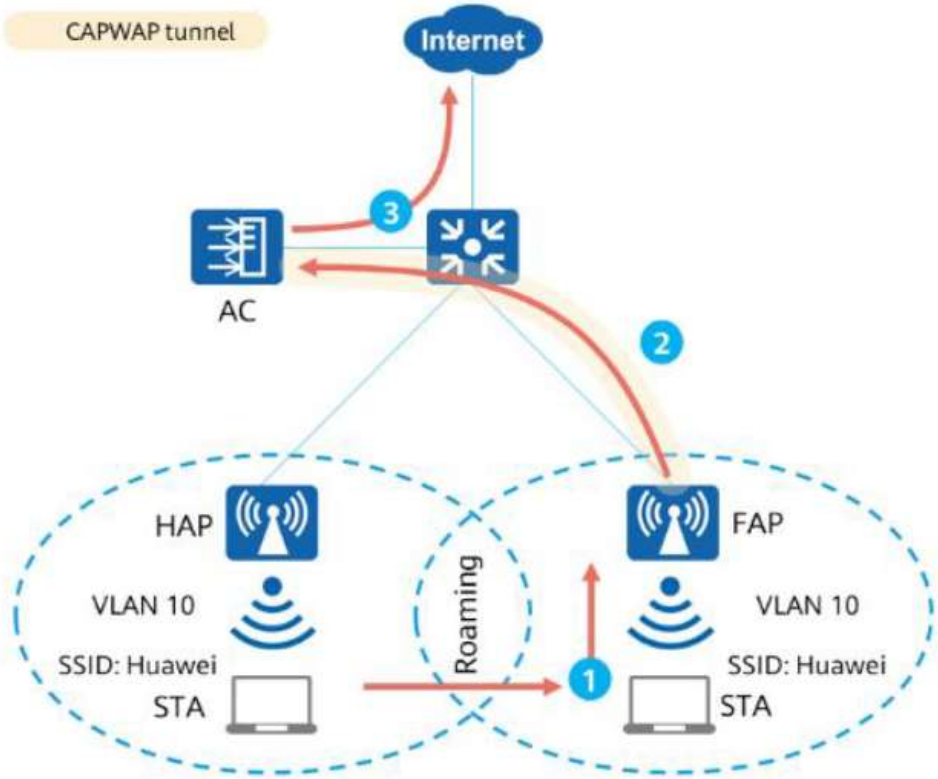
Tipovi roaming-a



- Kod L3 roaminga AC + Fit AP arhitektura mora da bude u tunel modu, bez obzira da li je in, ili off-path

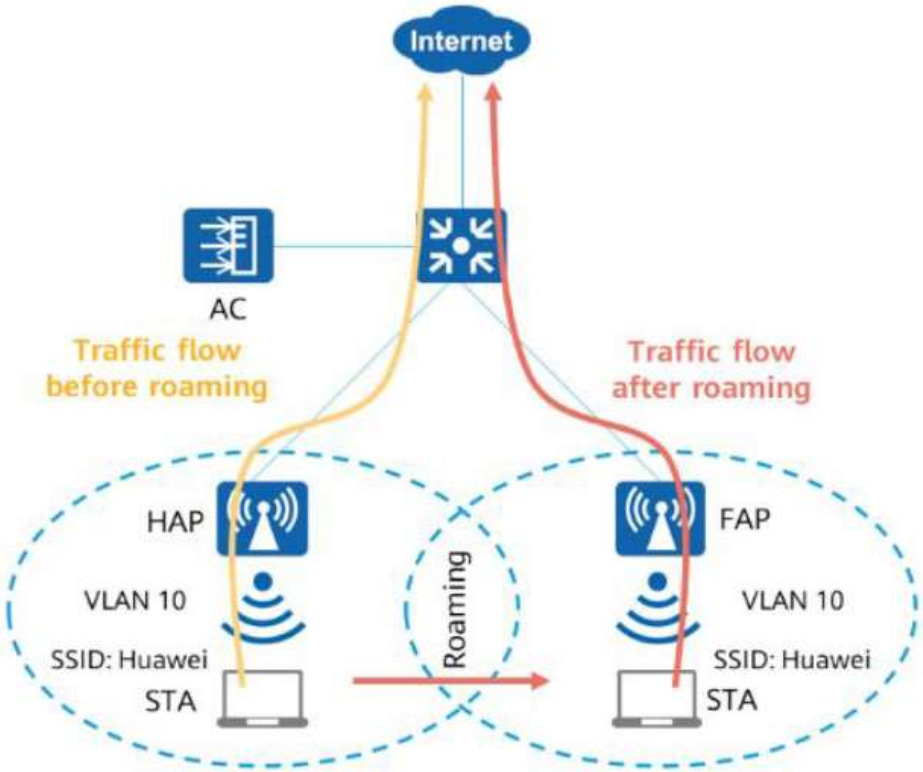
Primer prosleđivanja paketa prilikom rominga

Layer 2 Roaming — Tunnel Forwarding



- Before roaming:
  - The STA sends service packets to the HAP.
  - After receiving the service packets, the HAP sends them to the AC through the CAPWAP tunnel.
  - The AC forwards the service packets to the upper-layer network through the switch.
- After roaming:
  - The STA sends service packets to the FAP.
  - After receiving the service packets, the FAP sends them to the AC through the CAPWAP tunnel.
  - The AC forwards the service packets to the upper-layer network through the switch.

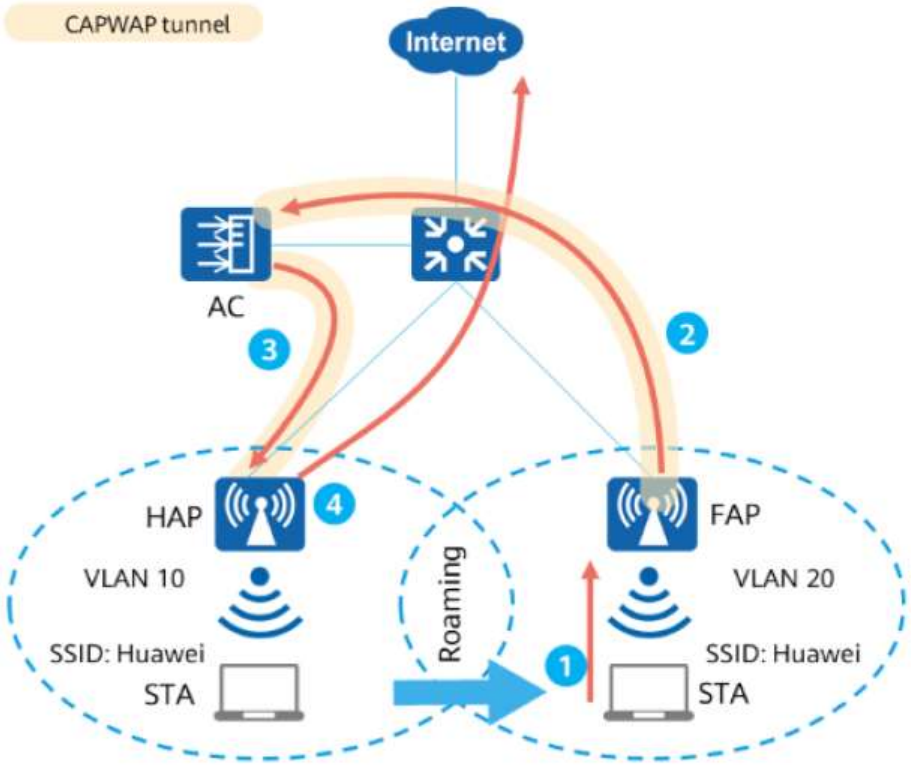
Primer prosleđivanja paketa prilikom rominga (nast.)



- Before roaming:
  - The STA sends service packets to the HAP.
  - After receiving the service packets, the HAP forwards them to the upper-layer network through the gateway (switch).
- After roaming:
  - The STA sends service packets to the FAP.
  - After receiving the service packets, the FAP forwards them to the upper-layer network through the gateway (switch).

Primer prosleđivanja paketa prilikom rominga (nast.)

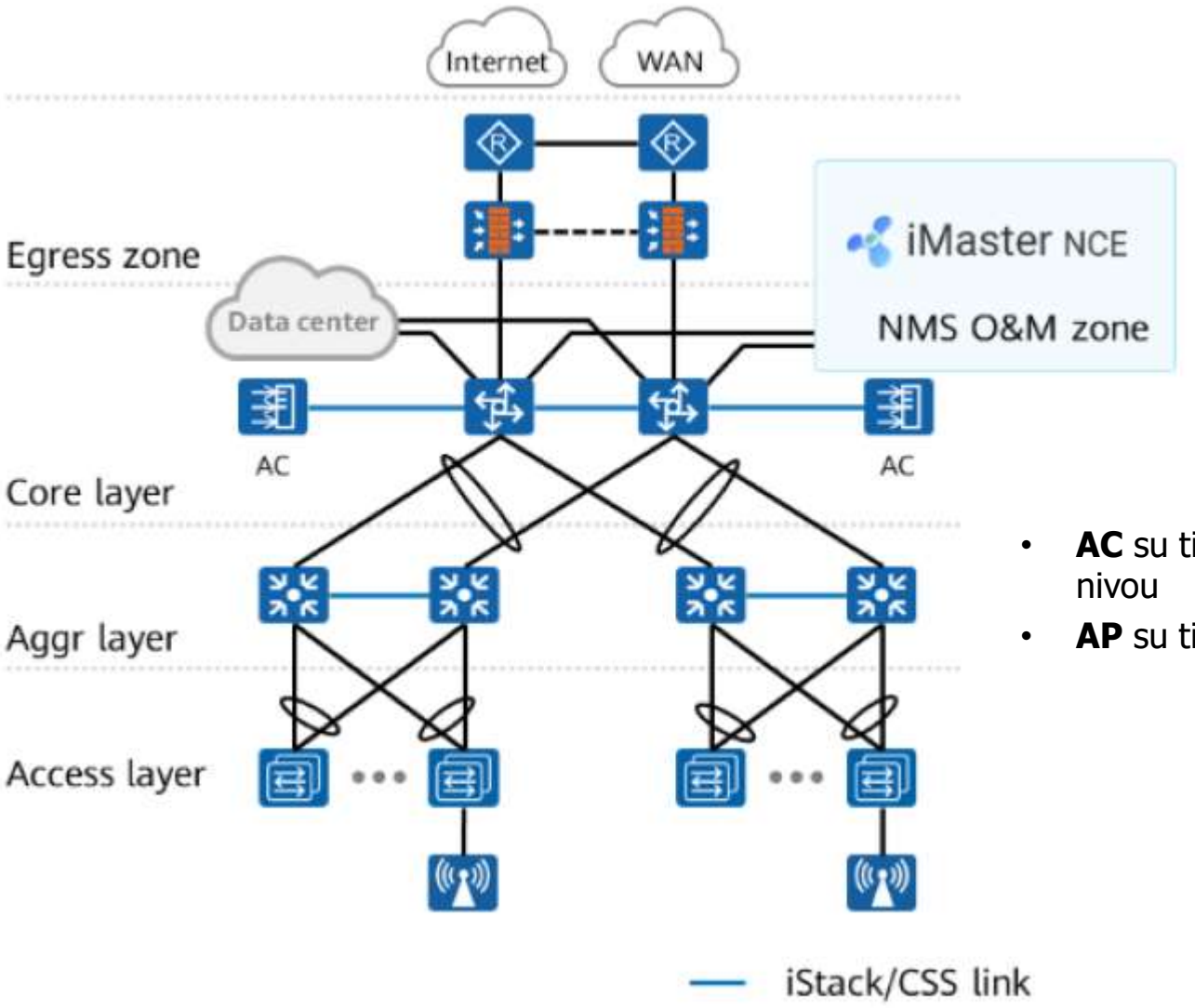
Intra-AC Layer 3 Roaming — Direct Forwarding (HAP as the Home Agent)



- Before roaming:
  - The STA sends service packets to the HAP.
  - After receiving the service packets, the HAP sends them to the HAC through the CAPWAP tunnel.
  - The HAC forwards the service packets to the upper-layer network through the switch.
- After roaming:
  - The STA sends service packets to the FAP.
  - After receiving the service packets, the FAP sends them to the HAC through the CAPWAP tunnel.
  - After receiving the service packets, the HAC sends them to the HAP through the CAPWAP tunnel.
  - The HAP forwards the service packets to the upper-layer network through the switch.

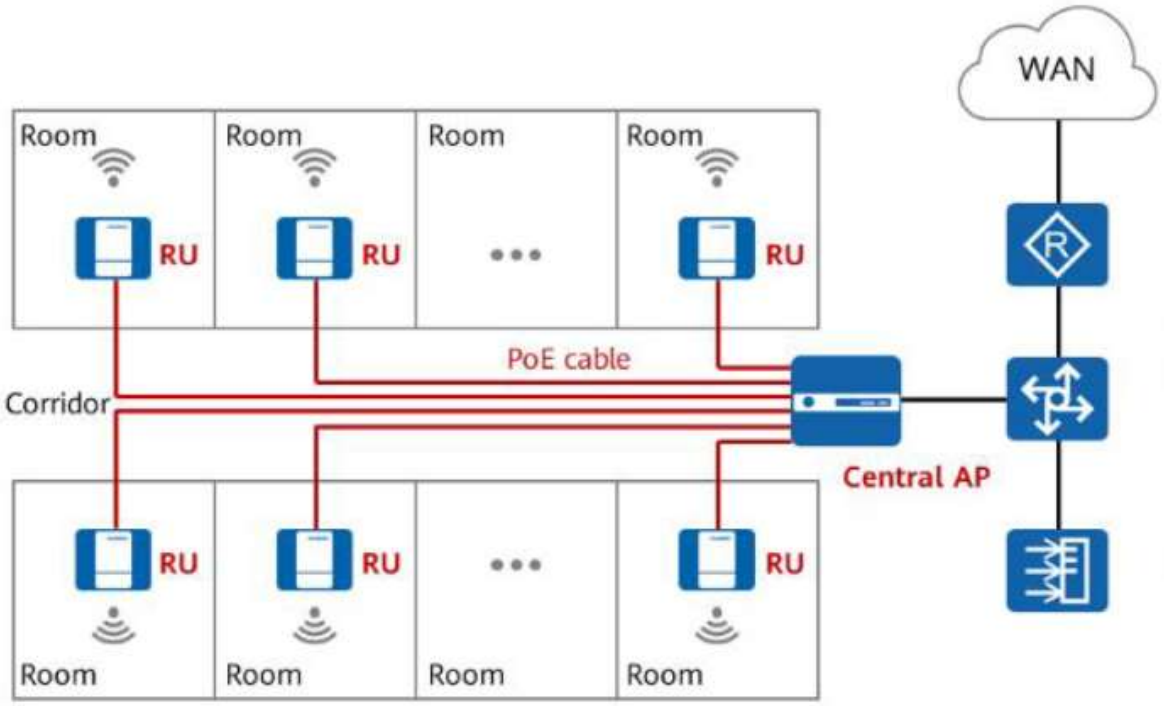
TIPIČNA REŠENJA

Rešenje za velike mreže



- **AC** su tipično na ditributivnom ili core nivou
- **AP** su tipično na access nivou

Agilna bežična topologija



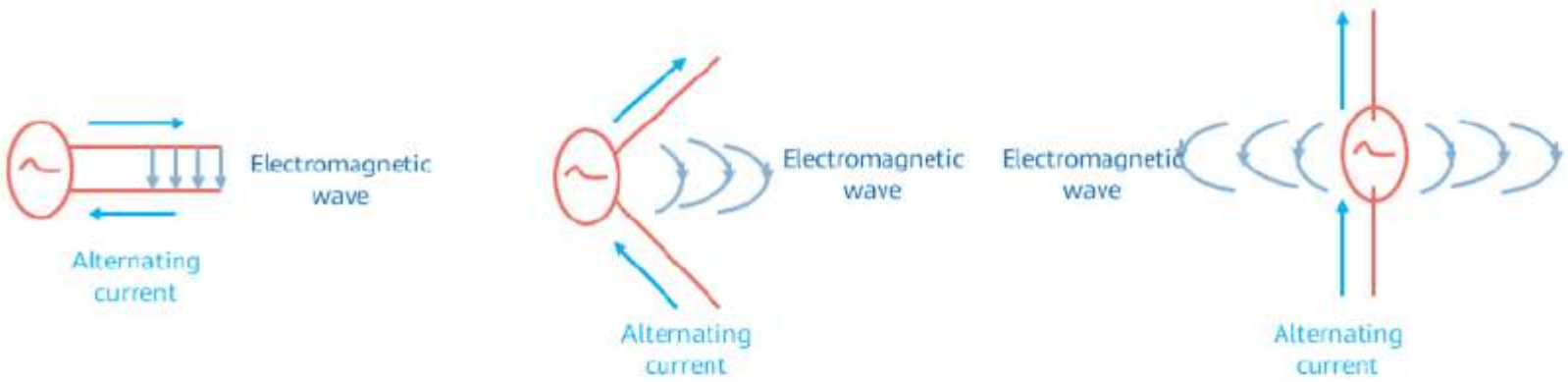
- Ova arhitektura koristi dva tipa uređaja:
  - Jedan AP (Fat AP, centralni)
  - Remote Unit (RU)
- RU je ekstenzija AP-a koji omogućava postavljanje antene na udaljenosti od AP-a i povezivanja te antene ethernet kablom na AP
- RU fizički podseća na AP

- Ovaj scenario je pogodan ukoliko ima puno prostorija odvojenih fizičkim preprekama koje bi inače slabile signal, a nema mnogo korisnika po prostoriji (hoteli i sl.).

ANTENE

Osnovni koncept bežične komunikacije

- Radio talasi su elektromagnetni talasi koji se prostiru kroz prostor.
- Signal radio frekvencije je elektromagnetni talas koji se prostire kroz prostor na frekvencijama između 300 kHz i 300 GHz. Mikrotalasi su talasi (prostiranje, zračenje) frefvencije od 300 MHz do 300 GHz
- Kada su dva provodnika blizu jedan drugom, električno polje je ograničeno i zračenje je malo. Kada su dva provodnika daleko jedan od drugoga električno polje je povećano.



Klasifikacija antena

Antenna classification

- **Po usmerenosti**
  - Omnidirectional – omni antena
  - Directional – usmerena antena
  - Smart antena
- **Po polarizaciji**
  - Jednostruko polarizovana
  - Dvostruko polarizovana
- **Po izgledu**
  - Štap (eng. whip) antena
  - Pločasta (eng. plate) antena
- **Po lokaciji**
  - Eksterna
  - Ugrađena


Directional antenna


Omnidirectional antenna


Whip antenna


Antenna built in a wall plate AP

Primeri eksternih antena:


Ceiling-mount antenna

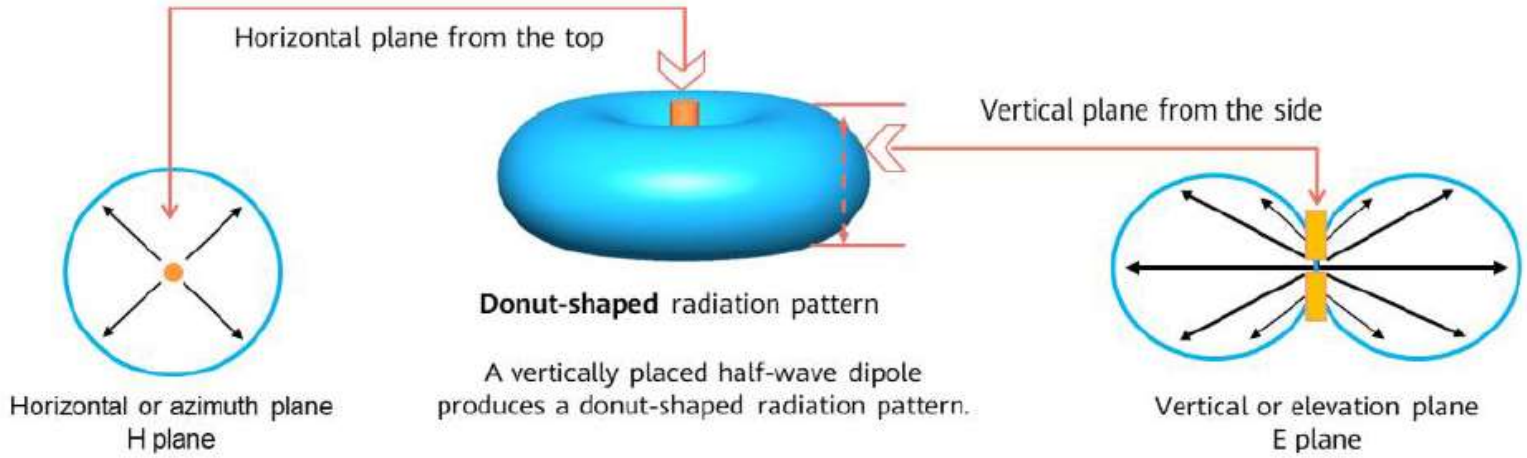

Indoor directional antenna


2.4G&5G outdoor omnidirectional antenna


Outdoor backhaul antenna

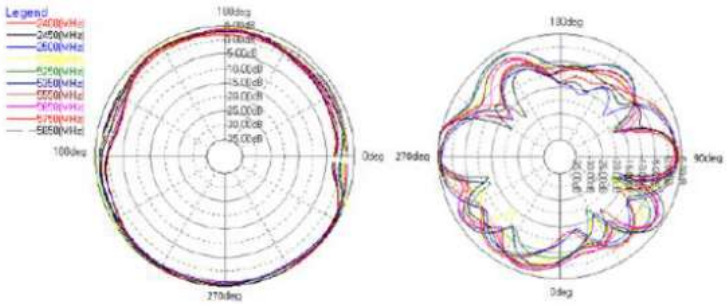

2.4G&5G outdoor directional antenna

Oblast pokrivanja omni- antene



- Pogled odozgo pokazuje da omni antena ima (praktično) podjednak domet u svim pravcima i da je maksimalan domet u horizontalnoj ravni.
- Sposobnost predaje antene i prijema signala je jednaka
- Energija zračenja u pravcu antene je 0.
- Obično se za granice zračenja uzima tačka gde je slabljenje 3 dB

Antenna model: 27011668
Gain: 4 dBi @ 2.4 GHz; 7 dBi @ 5 GHz



Horizontal radiation pattern

Vertical radiation pattern

Snaga antene

- Relativna snaga u logaritamskoj skali se izražava u decibelima (dB) i određuje na sledeći način:

$$P[dB] = 10 \cdot log \frac{A}{B}$$

gde je A snaga čija se vrednos izražava u dB, B referentna snaga.

- Za jačinu signala uzima se jedinica dBm, gde je referentna snaga 1mW:

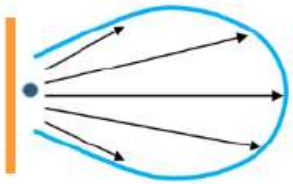
$$P[dB] = 10 \cdot log \frac{P[W]}{1mW}$$

Parameter	Description	Calculation Formula
W	Describes the transmit power of a device.	Device nominal value
dBm	Calculates the wireless link.	10 x log (power value/1 mW)
dB	Describes the relative value of the signal power.	10 x lg (power value A/power value B)

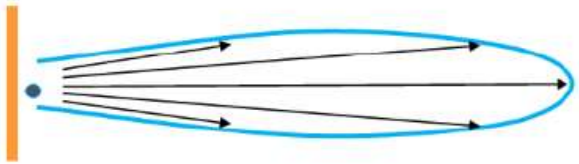
- Primeri (bez kalkulatora):
  - Koliko dBm ima antena od 100mW?
  - Kolika je predajna snaga antene od 13 dBm?
  - Kolika je predajna snaga antene od 23 dBm

Gain antene

- Antene su pasivni elementi => antene ne pojačavaju signal
- Gain (eng. dobit) je odnos snaga elektromagnetnog talasa koji emituje konkretna antena i hipotetička antena koja s uzima za refencu.
- Gain antene je vezan za model i specifikacije antene
- Veći gain znači veći domet u horizontalnoj ravni, ali manji u vertikalnoj (spljošteni oblik krive)



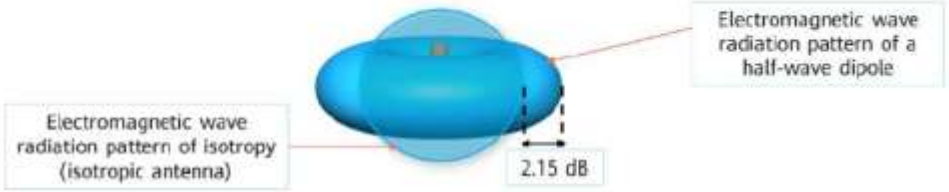
Low gain



High gain

- Gain se izražava u decibelima.
  - Ukoliko se računa u odnosu na idealnu sferu jedinice su dBi
  - Ukoliko se računa u odnosu na idealnu omni antenu jedinice su dBd

Parameter	Description	Calculation Formula
dBi/dBd	Describes the antenna gain, with the reference of an isotropic antenna for dBi and the reference of dipole (half-wave dipole) for dBd.	dBd = dBi + 2.15

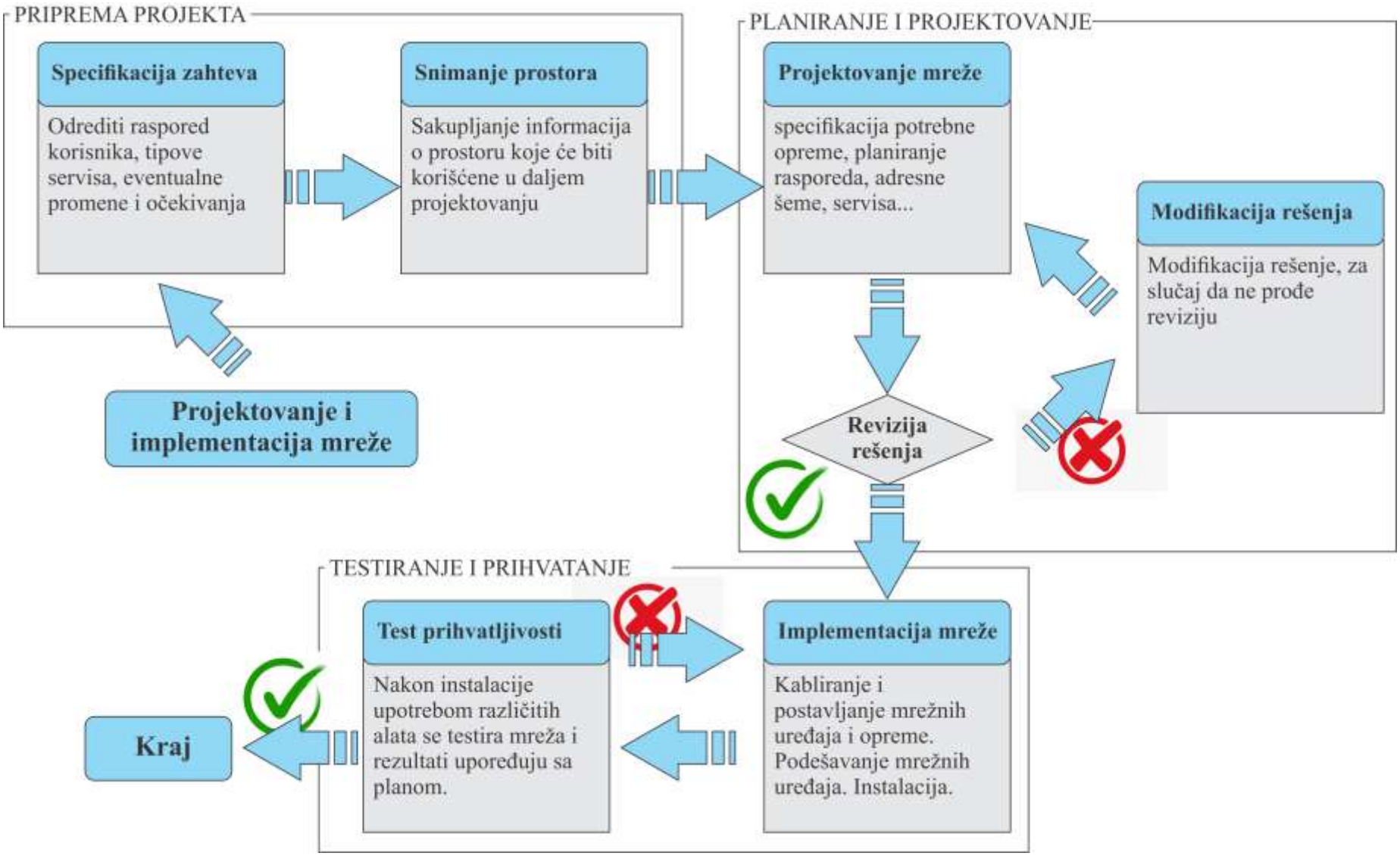


- Tipične vrednosti:
  - Indoor ugrađena antena: 2-3 dBi
  - Outdor eksterna omni antena: 6-8 dBi
  - Outdor usmerena antena: 8-14 dBi

- Pitanje: kolika je razlika u snazi po horizontalnoj razni ako je gain 13 dBd?

PROSTORNO PLANIRANJE

Proces projektovanja mreže

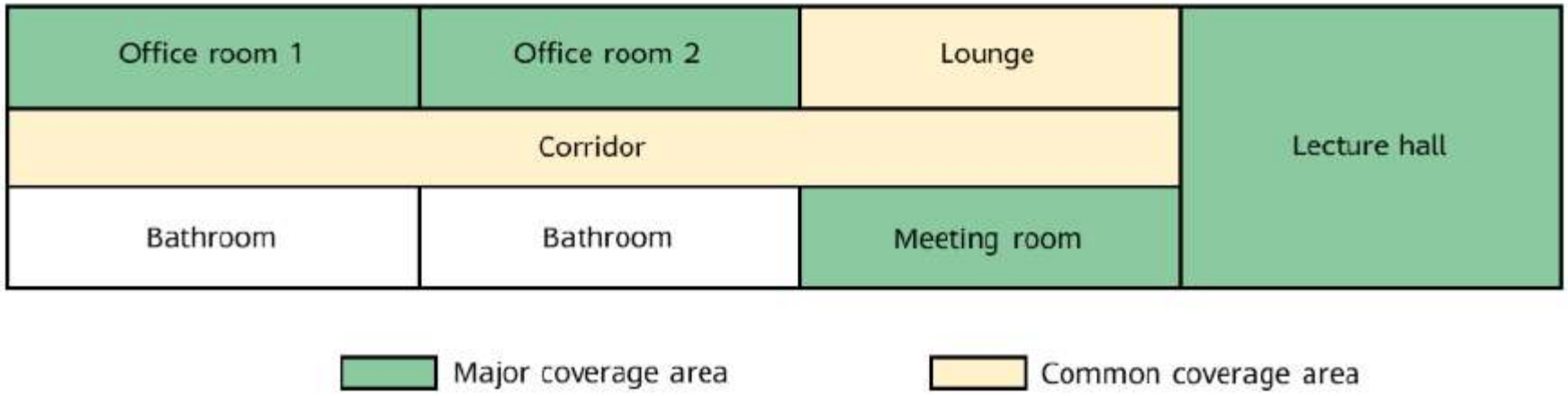


Specifikacija zahteva

Zahtev	Opis	Podrška
Zakonske regulative i dostupnost kanala	Svaka zemlja propisuje regulative koje se tiču upotrebe RF kanala: frekvencije i snage. Npr. 2.4 GHz je dozvoljeno bez posebnih dozvola, ali samo ako je snaga manja od 100mW	
Plan (nacrt) zgrade	Plan je neophodan kako bi se sa klijentom kompetentno razgovaralo o zahtevima i očekivanjima. Treba da sadrži sve mere i rastojanja.	CAD alati
Pokrivenost prostorija WiFi signalom	Treba specificirati (1) ključne oblasti (kao što su kancelarije i sale za sastanke), (2) oblasti nižeg ranga (hodnici i sl.) i oblasti u kojima signal nije potreban	
Jačina signala	Ukoliko korisnik ima specifične zahteve. Npr. od -40 dBm do -65 dBm u kancelarijama i salama za sastanke i više od -75 dBm u hodnicima.	
Broj i raspored uređaja	Broj uređaja	
Tipovi i namena uređaja	Identifikovati uređaje i njihove potrebe: laptop, tablet, mobilni telefon, itd.	Spisak krajnjih uređaja.
Lokacija napajanja	Način na koji će se napajati AP-ovi i mrežna oprema	
Lokacija Svičeva i AC-ova	Lokacija mrežnih uređaja DS sistema na koji će biti povezan WLAN	

Planiranje pokrivanja signalom

Coverage	Field Strength	Typical Area in Common Projects
Major coverage area	–40 dBm to –65 dBm	Dormitory room, library, classroom, hotel room, lobby, meeting room, office, hall, etc.
Common coverage area	> –75 dBm	Corridor, kitchen, storeroom, and dressing room
Special coverage area	N/A	Areas where coverage or installation is limited or not allowed, for the sake of service security, property management, or other reasons



- aaa

Planiranje pokrivanja signalom

Requirement analysis

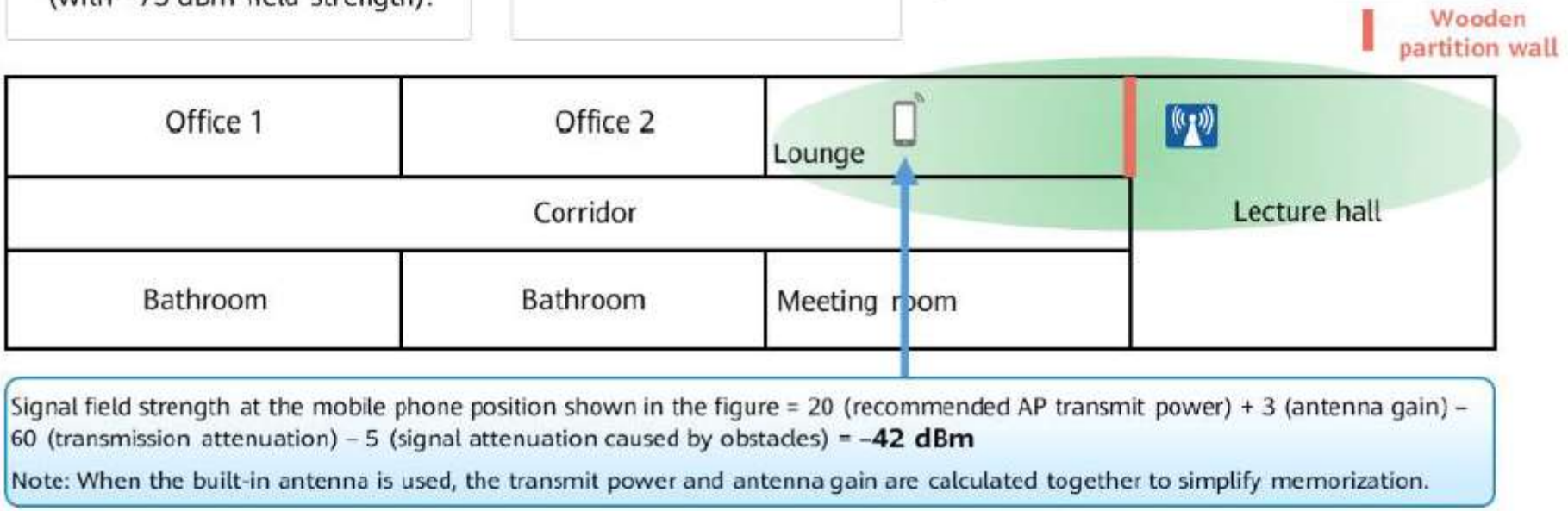
- APs cannot be installed in the lounge.
- APs in the lecture hall are used to provide signal coverage (with –75 dBm field strength).

Site survey

- The signal attenuation value of the wooden partition wall is 5 dBm.

Coverage analysis

- Final signal field strength = AP transmit power + Antenna gain – Transmission attenuation – Signal attenuation caused by obstacles



- aaa

Slabljenje signala

- Coverage distance by a single AP

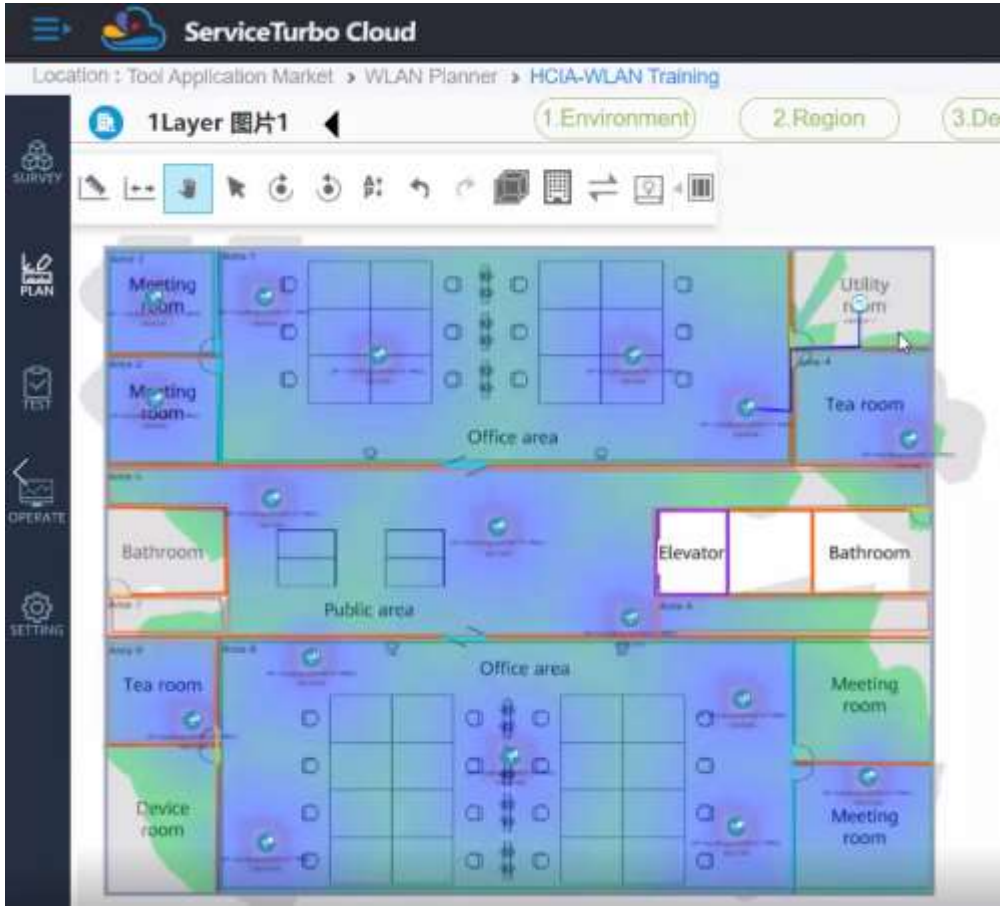
Distance	1 m	2 m	5 m	10 m	20 m	40 m	80 m	100 m
2.4 GHz	46 dB	53.5 dB	63.5 dB	71 dB	78.5 dB	86 dB	93.6 dB	96 dB
5.8 GHz	53 dB	62 dB	74 dB	83 dB	92 dB	101 dB	110.1 dB	113 dB

- Signal attenuation caused by common obstacles

Obstacle	Thickness (mm)	2.4 GHz Signal Attenuation (dB)	5 GHz Signal Attenuation (dB)
Synthetic material	20	2	3
Asbestos	8	3	4
Wood door	40	3	4
Glass window	50	4	7
Heavy colored glass	80	8	10
Brick wall	120	10	20
Brick wall	240	15	25
Armored glass	120	25	35
Concrete	240	25	30
Metal	80	30	35

- Primer određivanja dometa (bez korišćenja kalkulatora):
  - Na kom rastojanju će jačina signala biti -65dBm, ako je predajna snaga AP-a 20mW i gain njegove antene 2 dBi

Alati za planiranje prostornog rasporeda i prihvatanje projekta



- aaa