Arhitektura CISCO bežične LAN mreže

Kovač, Matej

SVEUČILIŠTE U ZAGREBU
FAKULTET PROMETNIH ZNANOSTI

Matej Kovač

ARHITEKTURA CISCO BEŽIČNE LAN MREŽE

ZAVRŠNI RAD

Zagreb, 2022.

SVEUČILIŠTE U ZAGREBU
FAKULTET PROMETNIH ZNANOSTI
ODBOR ZA ZAVRŠNI RAD

Zagreb, 4. svibnja 2022.

Zavod: **Zavod za informacijsko komunikacijski promet**
Predmet: **Arhitektura telekomunikacijske mreže**

ZAVRŠNI ZADATAK br. 6774

Pristupnik: **Matej Kovač (0035218181)**
Studij: Promet
Smjer: Informacijsko-komunikacijski promet

Zadatak: **Arhitektura CISCO bežične LAN mreže**

Opis zadatka:

U radu je potrebno opisati osnovne principe i obilježja rada bežične LAN mreže. Zatim, opisati arhitekturu CISCO bežične LAN mreže i njezine implementacijske modele. Analizirati sigurnosne značajke CISCO bežične LAN mreže.

Mentor:

doc. dr. sc. Ivan Forenbacher

Predsjednik povjerenstva za završni ispit:

SVEUČILIŠTE U ZAGREBU
FAKULTET PROMETNIH ZNANOSTI

ZAVRŠNI RAD

Arhitektura CISCO bežične LAN mreže

Architecture of CISCO Wireless LAN Network

Mentor: doc. dr. sc. Ivan Forenbacher

Student: Matej Kovač
JMBAG: 0035218181

Zagreb, rujan 2022

SAŽETAK

Većina današnjih terminalnih uređaja (prijenosnih računala, mobilnih telefona i sličnih uređaja) za pretraživanje i usluge koje zahtijeva korisnik koristi bežične LAN mreže. Bežične LAN mreže su *de facto* postale standard za povezivanje istih. Privlače sve veći broj korisnika zbog jednostavne implementacije, istovremeno osiguravajući nominalnu brzinu prijenosa. Veće nominalne brzine prijenosa olakšavaju pristup informacijama i reduciranje samih troškova mreže. Bežične mreže imaju puno prednosti, no najveći nedostatak koji stvara mnoge probleme je sigurnost. Nositelj informacije u bežičnim mrežama su radiofrekvencijski valovi, a medij kojim se prenose je zrak. Informacija koja se prenosi ne ostaje unutar objekta na području koje pokriva bežična mreža te je češće meta napada. Kako bi se detektirale i spriječile takve vrste napada, razvijeni su i koriste se razni sigurnosni oblici. Ovaj rad opisuje opće karakteristike bežične mreže kroz primjer CISCO bežične LAN mreže. Opisane su vrste arhitektura koje se mogu primijeniti u izradi bežične mreže, sigurnosni protokoli, kao i osnovna načela prijenosa signala i oprema potrebna za uspostavljanje mreže takvog tipa.

KLJUČNE RIJEČI: CISCO bežična LAN mreža; arhitektura; informacije; sigurnosni protokoli; oprema

SUMMARY

Most of today's terminal devices (laptops, mobile phones and similar devices) use wireless LAN networks for searching and services required by the user. Wireless LAN networks have become *de facto* the standard for connecting that type of device. They are attracting an increasing number of users due to their simple implementation, while providing a nominal transmission speed. Higher nominal transmission speeds facilitate access to information and reduce network costs. Wireless networks have many advantages, but the biggest disadvantage that creates many problems is security. The carrier of information in wireless networks are radio frequency waves and the medium through which they are transmitted is air. The information that is transmitted does not stay inside the object in the area covered by the wireless network and it is more often the target of attacks. In order to detect and prevent such types of attacks, various forms of security have been developed and are used. This paper describes the general characteristics of a wireless network through the example of a CISCO wireless LAN network. The types of architectures that can be applied in the creation of a wireless network, security protocols, as well as the basic principles of signal transmission and the equipment required to establish a network of this type are described.

KEY WORDS: CISCO wireless LAN network; architecture; information; security protocols; equipment.

SADRŽAJ

1. Uvod

Velika većina korisničkih uređaja spojena je na neku lokalnu mrežu (engl. *Local Area Network* – LAN). Korištenje tehnike bežičnog pristupa mreži (engl. *Wireless Local Area Network* – WLAN), odnosno LAN mreži postao je sastavni dio svakodnevnice. Bežična LAN mreža omogućuje upravljanje raznim uređajima bez potrebe za fizičkom interakcijom s uređajem. WLAN se preporučuje ponajviše korisnicima mobilnih terminalnih uređaja kako bi se riješila problematika povećanog mobilnog podatkovnog prometa. Ovaj rad opisuje strukturu CISCO bežične mreže, postupke kojima se uspostavlja takva mreža, kao i osnovne karakteristike općenito WLAN mreže. Rad je podijeljen u 7 poglavlja:

1. Uvod
2. Principi rada bežične LAN mreže
3. Obilježja arhitekture bežične LAN mreže
4. Arhitektura CISCO bežične LAN mreže
5. Implementacijski modeli CISCO bežične LAN mreže
6. Sigurnost CISCO bežične LAN mreže
7. Zaključak

U drugom poglavlju opisani su osnovni principi na kojima se temelji rad bežičnih mreža. Prikazana je podjela elektromagnetskog (EM) zračenja te je dan uvid u radiofrekvencijske (RF) valove, koji predstavljaju temelj za prijenos informacije u bežičnim mrežama. Bežični pristup ponajviše se koristi u 2,4 i 5 GHz pojasu, koji je također obuhvaćen, kao i modulacijske tehnike koje se koriste za učinkovitiji prijenos podataka.

Mrežni elementi potrebni za uspostavljanje bežične mreže i njihove karakteristike kao i načini uspostave mreže dio su trećeg poglavlja. Uz mrežne elemente opisani su i glavni infrastrukturni dijelovi i načini rada mreže.

Četvrto poglavlje prikazuje arhitekturu CISCO bežične mreže oblike i glavne karakteristike svakog oblika u kojem se može uspostaviti. Arhitektura je podijeljena u tri glavne grupe: arhitektura autonomne pristupne točke (engl. *Autonomous AP*), *cloud based AP* i *split–MAC* arhitektura. (Tu sam se malo pogubila jer ne znam koje su to tri. Probaj to napraviti kao dolje niže gdje opisuješ 6.pogl. Nemoj se bojati koristiti dvotočku)

Peto poglavlje pokazuje korake potrebne za uspostavu CISCO bežične mreže. U navedenom poglavlju naglašene su dodatne funkcionalnosti te načini rada pristupne točke i kontrolera.

Sigurnost kao jedan od najvažnijih čimbenika za korisnike CISCO mreže predstavljena je u šestom poglavlju. Metode su grupirane u dvije skupine: metode provjere autentičnosti klijenta te metode privatnosti i integriteta.

2. Principi rada bežične LAN mreže

Bežična mreža, poznatija pod nazivom WLAN, definira se kao komunikacijska mreža u kojoj se podaci, između najmanje dva ili više uređaja, prenose putem EM valova, točnije putem radio valova. WLAN ima različit doseg pokrivanja ovisno o tipu prostora i radijusu pokrivanja lokalne mreže, koji ovisi o tipu prijenosnog medija (koaksijalni kabel, upletena parica ili optičko vlakno). U zatvorenim prostorima poput zgrada radijus pokrivanja varira u rasponu od 30 do 50 metara, dok za otvorene prostore iznosi više od 100 metara [1].

Bežična mreža koristi se ponajviše unutar jednog objekta, poput poslovne ili stambene zgrade te industrijskog postrojenja. Ukratko, bežična mreža se postavlja na lokacijama gdje se očekuje velika fluktuacija ljudi, a gdje je istovremeno teško izvedivo provesti ožičenje ili je ono ekonomski neisplativo na određenom području [1]. Većina WLAN mreža funkcionira u industrijskom, znanstvenom i medicinskom pojasu (engl. *industrial, scientific and medical band* – ISM) [2].

2.1. Karakteristike bežične LAN mreže

Kao što uvod u poglavlje opisuje, prijenos podataka u bežičnoj mreži temelji se na radio valovima. Frekvencija radiovalova izražava se u MHz, a njihove valne duljine variraju u rasponu od jednog do nekoliko stotina metara. EM val sastoji se od električnog i magnetskog polja koja su međusobno okomita te su okomita na smjer širenja vala. Skup svih EM valova naziva se elektromagnetski spektar, a dijeli se na ionizirajuće (gama zračenje, rendgensko zračenje i ultraljubičasto zračenje) i neionizirajuće zračenje (vidljiva svjetlost, infracrveno, mikrovalno i radiovalno zračenje te zračenje ekstremno niskih frekvencija i jako niskih frekvencija) [3]. Prikaz elektromagnetskog spektra i njegovih dijelova ilustriran je Tablicom 1.

Tablica 1. Elektromagnetski spektar

ELEKTROMAGNETSKI SPEKTAR			
NEIONIZIRAJUĆE ZRAČENJE		IONIZIRAJUĆE ZRAČENJE	
Vrlo niske frekvencije	$0 – 10^2$ Hz	Ultraljubičasto zračenje	$10^{16} – 10^{19}$ Hz
Niske frekvencije	$10^2 – 10^5$ Hz	Rendgensko zračenje	$10^{19} – 10^{22}$ Hz
Radiovalovi	$10^5 – 10^{12}$ Hz	Gama zračenje	$10^{22} –$
Mikrovalovi	$10^9 – 10^{12}$ Hz		
Infracrveno zračenje	$10^{12} – 10^{14}$ Hz		
Vidljiva svjetlost	$10^{14} – 10^{16}$ Hz		

Izvor:[3]

Količina informacija, odnosno veličina podataka koji radio valovi mogu prenositi ovisi o dostupnom frekvencijskom pojasu. Radioval, odnosno signal se na odašiljanoj strani prvo modulira kako bi se prilagodio karakteristikama medija kojim se prenosi i time bio otporniji na smetnje. Svaki signal prenosi se na samo jednoj frekvenciji kako bi se izbjegle smetnje, tj. interferencije budući da se unutar jednog prostora može se prenositi više signala. Prijemnik zaprima pojedini signal, demodulira ga, odnosno izdvaja informaciju važnu za korisnika [2].

Na početku poglavlja spomenuto je da većina WLAN mreža djeluje u ISM frekvencijskom pojasu. ISM pojas označava dio radio spektra koji je međunarodno rezerviran za industrijske, znanstvene i medicinske svrhe. Prema [2] ISM kategorizira frekvencije u tri grupe:

- 902 MHz – 928 MHz,
- 2,4 GHz – 2,4835 GHz i
- 5,728 GHz – 5,750 GHz.

Među navedenima najkorištenija je druga grupa frekvencija. Drugi frekvencijski pojas u kojem bežična mreža može djelovati je nelicencirani pojas. Nelicencirani pojas ne zahtijeva dozvolu i naknadu za korištenje. Karakteristike poput maksimalne dozvoljene izlazne snage, točno definirana frekvencija korištenja, kao i mogućnost uporabe nelicenciranog pojasa razlikuju se ovisno o državi i njenim propisima [2].

Bežična je mreža specifična po tome što se, osim izobličenja signala, kao smetnje javljaju i problemi poput gubitka snage EM vala (engl. *Path. loss*) koje se javlja tijekom propagacije signala od izvora do odredišta [2]. Slabljenje EM vala propagacijom kroz slobodni prostor prema izvoru [3] računa se pomoću formule (1):

$$P = \frac{P_{Tx}}{4\pi d^2} \cdot \frac{\lambda^2}{4\pi} \tag{1}$$

pri čemu oznake imaju sljedeće značenje:

- P_{TX} – snaga predajnika
- λ – valna duljina koja se može dodatno izraziti kao omjer brzine svjetlosti i frekvencije vala.
- d – udaljenost između dviju antena izražena u metrima.

Kada je riječ o urbanim područjima prema [3], tada se moraju uzeti u obzir i dobitci antena te se snaga izračunava pomoću formule (2):

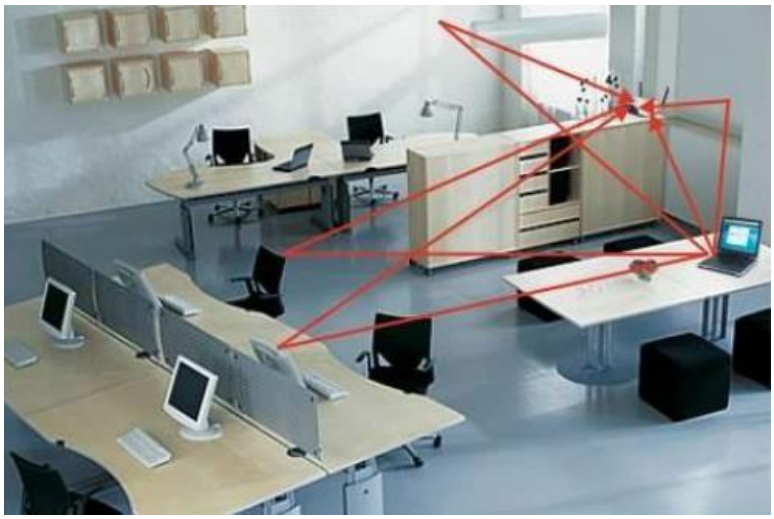
$$P = \frac{P_{Tx}}{4\pi d^2} \cdot \frac{\lambda^2}{4\pi} \cdot G_{Tx} \cdot G_{Rx} \tag{2}$$

gdje oznake znače sljedeće:

- P_{TX} – snaga predajnika
- λ – valna duljina koja se može dodatno izraziti kao omjer brzine svjetlosti i frekvencije vala

- d – udaljenost između dviju antena izražena u metrima.
- G_{TX} – dobitak predajnika,
- G_{RX} – dobitak prijamnika odnosno prijemne antene.

Višestazno propagiranje (engl. *Multipath propagation*) također je jedna od smetnji koji se javljaju u bežičnim mrežama. Tijekom propagacije EM valovi se reflektiraju od različite materijalne tvari što rezultira kasnijim dolaskom na odredište. Odredište na taj način prima zakašnjele inačice signala što pridonosi intersimbolnoj interferenciji i povećanju kašnjenja. Intersimbolna interferencija prepoznaje se po tome što štetno proširuje trajanje simbola tijekom prijema zbog čega se simboli međusobno ometaju [5]. Vištestazno propagiranje u uredskom prostoru prikazano je na Slici 1.



Slika 1. Vištestazna propagacija u WLAN mreži unutar jednog ureda,

Izvor:[5]

Uz navedene negativne smetnje koje se javljaju u bežičnim mrežama je i iščezavanje signala (engl. *Shadow fading*) čiji je uzrok zasjenjenje. Stupanj zasjenjenja ovisi o dielektričnim karakteristikama materijala kroz koji EM val prolazi [2]. Interferencija s drugim izvorima može izazvati velike smetnje pri prijenosu signala. Uređaji koji odašilju signale na istoj frekvenciji mogu si međusobno smetati [4].

Kao primjer može se promatrati predajnik u jednoj bežičnoj mreži i mobilni terminalni uređaj koji odašilje signale prema prijemniku u drugoj bežičnoj mreži, pri čemu oba uređaja za predaju signala koriste istu frekvenciju. Signali se u tom slučaju mogu pomiješati što će posljedično izazvati komunikacijske smetnje [4].

Navedene smetnje te problemi koji se uzrokuju mogu se izbjeći na više načina. Višestazno propagiranje može se spriječiti korištenjem visoko direkcionalnih antena, ali budući da su korisnici WLAN mreža najvećim dijelom korisnici mobilnih terminalnih uređaja, navedeno rješenje nije prikladno za mobilne komunikacije. Drugi način kako spriječiti

intersimbolnu interferenciju, a samim time i višestazno propagiranje, je produžiti trajanje simbola tako što se tok koji prenosi podatke podijeli na više istovremenih tokova manje brzine. Podjela toka dovodi do smanjenja broja simbola koju pristižu na prijemnu stranu u jednoj sekundi te povećava trajanje simbola [5].

Najveći izazov u bežičnim mrežama predstavlja interferencija zbog utjecanja na kvalitetu prijenosa i ograničavanja. Razlikuju se dvije vrste interferencije, interferencija po istom i po susjednom kanalu. Interferencija po istom kanalu znači da pristupne točke na koje su spojeni terminalni uređaji koriste isti kanal. Međusobna komunikacija terminalnih uređaja odvija se po pravilu „slušaj dok drugi govore“. Interferencija po susjednom kanalu opisuje se kao istovremena komunikacija terminalnih uređaja unutar preklapajućih kanala, a same pristupne točke koriste susjedne, odnosno preklapajuće kanale [5].

2.2. Tehnike proširenog spektra

Tehnika proširenog spektra (engl. *Spread spectrum*) prvotno je razvijena i korištena od strane američke vojske sa ciljem smanjenja mogućnosti prisluškivanja te kako bi signal kojim se prenose informacije bio što otporniji na smetnje opisane u prethodnom dijelu rada. Navedena tehnika izvodi se na način da se koristi niz pseudo slučajnih brojeva u binarnom obliku. Oblik takvog niza sličan je sinusoidnom obliku šuma. Koristan signal, odnosno signal koji sadrži informaciju množi se sa pseudo slučajnim nizom brojeva. Posljedica takvog postupka dovodi do sljedećih pojava:

- Spektar snage se proširuje na veće, tj. šire frekvencijsko područje u odnosu na osnovno frekvencijsko područje (engl. *Bandwidth*).
- Druga pozitivna posljedica je to što signal poprima oblik šuma i ostaje unutar šuma komunikacijskog kanala zbog čega ga je jako teško presresti i modificirati [2].

Prošireni korisni signal vraća se na prvotnu frekvencijsku širinu dok se istovremeno smetnje proširuju. Na taj način gustoća spektra šuma u originalnom, tj. osnovnom pojasu se smanjuje. Nakon filtriranja iznos šuma je sveden na male vrijednosti te se na prijemnoj strani preneseni signal sažima i, koristeći pseudo slučajni niz brojeva, dekodira. Mala gustoća snage i upotreba signala proširenog spektra omogućuje većem broju korisnika korištenje istog medija za prijenos signala, a da pri tome ne smetaju jedni drugima. Razlikuju se tri tehnike koje se pri tome koriste:

- *Direct-Sequence Spread Spectrum* (DSSS),
- *Frequency Hopping Spread Spectrum* (FHSS) i
- *Hybrid System* (DS/FFH) koji predstavlja kombinaciju prvih dviju tehnika [2].

DSSS tehnika poznata je i pod nazivom DS-CDMA (engl. *Direct Sequence code division multiple access*) i koristi se u većini standarda. ISM frekvencijski pojas dijeli se na 13 kanala pri čemu svaki peti kanal koristi DSSS, a kanali su međusobno razmaknuti za 25 MHz kako bi

se izbjegla interferencija. Unutar pojasa moguć je istovremeni prijenos podataka trima korisnicima. Moguće brzine prijenosa korištenjem navedene tehnike su 1, 2.5, 5 i 11 Mbps [2].

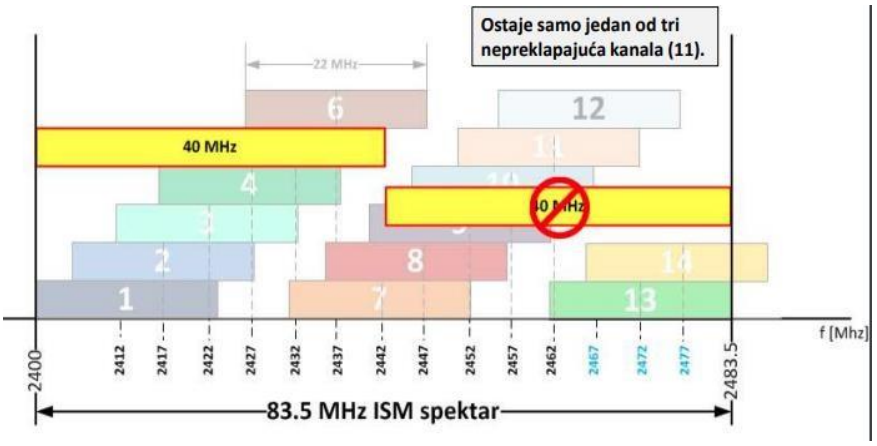
FHSS modulacijska tehnika je poznata pod nazivom *Frequency-Hopping Code Division Multiple Access* (FH-CDMA). U navedenoj tehnici se određuju frekvencijski skokovi unutar spektra. Frekvencijski skokovi mogu se izraziti kao izrazito brze frekvencijske promjene gdje u trenutku promjene frekvencije se događa prijenos podataka. Predajnik emitira podatke, u određenom trenutku se prebacuje na drugu frekvenciju te šalje drugi niz podataka. Predajnik i prijemnik moraju biti sinkronizirani kako ne bi došlo do gubitka podataka te se na taj način održava logički kanal [2].

Vrijeme tijekom kojeg se podatak nalazi u određenom kanalu naziva se vremenski odsječak (engl. *Time slot*) i minimalna vrijednost mu iznosi 625 μs. U slučaju da nastane interferencija na jednoj od frekvencija prelazi se na drugu frekvenciju i podaci se ponovno šalju. FHSS sustav onemogućuje preslušavanje i jamči visoku razinu sigurnosti tijekom prijenosa. Navedeno omogućuje većem broju bežičnih mreža rad unutar istog geografskog područja bez međusobnog smetanja [2].

2.3. Svojstva bežične LAN mreže u 2,4 i 5 GHz pojasu

U prethodnom poglavlju rada rečeno je da bežične mreže mogu raditi na frekvencijama od 2,4 i 5 GHz u licenciranom ISM ili nelicenciranom pojasu. Nelicencirani je pojas dio spektra Nacionalne informacijske infrastrukture bez odobrenja. U 2,4 GHz definirano je 14 kanala širine 22 MHz, pri čemu postoji mogućnost proširenja širine kanala na 40 MHz spajanjem pojedinih kanala. Broj kanala koji su na raspolaganju ovisi o državi, tj. regiji gdje se koristi. Kanali su međusobno razmaknuti za 5 MHz pri čemu se svaki idući kanal preklapa 75% s prethodnim kanalom [5].

Glavni razlog preklapanja je mala raspoloživost frekvencijskog spektra koji se koristi. Kako bi se izbjegla interferencija, omogućeno je korištenje maksimalno tri kanala i to su kanali: 1, 6 i 11. U slučaju da se širina kanala proširi na 40 MHz, uzimajući u obzir razmak između kanala u iznosu od 3 MHz, frekvencijski pojas od 2,4 GHz ne bi bio dovoljan za implementaciju više od jednog takvog kanala. Kanal od 40 MHz nastaje spajanjem osam kanala širine 22 MHz. Preporuča se kućnim ili poslovnim korisnicima za čije potrebe je dovoljna jedna pristupna točka uz napomenu da u njihovom okruženju ne postoji velik broj drugih pristupnih točaka [5]. U pozadini Slike 2. prikazan je raspored kanala u 2,4 GHz pojasu, a sama slika prikazuje kako kanali širine 40 MHz djeluju na sami pojas.



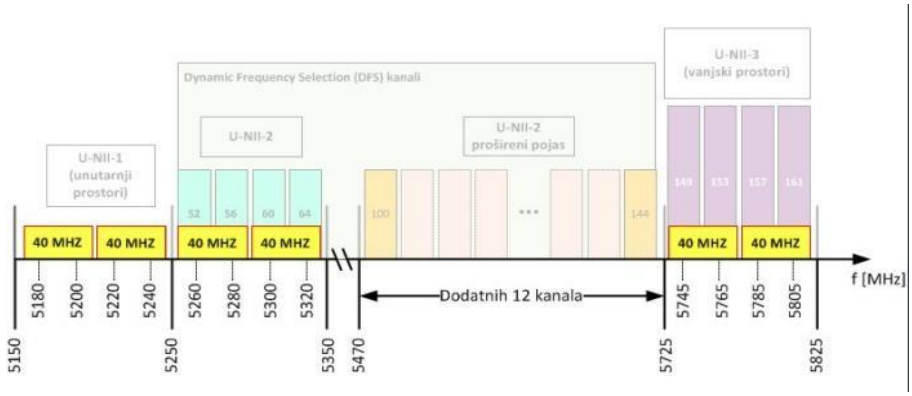
Slika 2. Utjecaj kanala širine 40 MHz na 2.4 GHz spektar

Izvor:[5]

Specifikacije radio prijamnika za nelicencirane Nacionalne informacijske infrastrukture (U-NII) definiraju raspored 25 kanala za nelicenciranu uporabu u frekvencijskom pojasu od 5 GHz. Kao i kod 2,4 GHz pojasa ukupan broj dostupnih kanala ovisi o državi, odnosno regiji u kojoj se koristi. Kanali su širine 20 MHz te su im centralne frekvencije udaljene 20 MHz. Prema [5] 20 kanala je numerirano sa specifičnim brojem te su podijeljeni u četiri skupine:

- U-NII-1,
- U-NII-2,
- U-NII-2 prošireni (engl. *Extended*) i
- U-NII-3.

Za razliku od 2,4 GHz pojasa, kanali širine 40 MHz se ne preklapaju, već se mogu slobodnije koristiti te ih je moguće spojiti do širine od 160 MHz [5]. Kao i Slika 2., tako i Slika 3. u svojoj pozadini prikazuje raspored kanala u 5 GHz pojasu, a sama slika ilustrira kako 40 MHz kanali utječu na 5 GHz pojas te mogućnost spajanja kanala u kanala širine 80 i 160 MHz [5].



Slika 3. Utjecaj konfiguracije kanala širine u 5 GHz pojasu

Izvor:[5]

Prijenos signala između predajnika i prijamnika moguće je poboljšati na neki od sljedećih načina. Jedan od najjednostavnijih je načina postaviti pristupnu točku na otvoreni prostor gdje je utjecaj zapreka sveden na najnižu razinu, pri čemu je generalno važno izbjegavati tvari koje blokiraju signal. U slučaju da pristupna točka sadrži *dual-band* opciju, prijenos podataka može se prebaciti na 5 GHz pojas zbog ranije navedenih prednosti. U slučaju da pristupna točka radi u 2,4 GHz pojasu, poželjnije je koristiti interferenciju po istom kanalu [5].

U područjima s visokom koncentracijom ljudi potrebno je koristiti kanale širine 22 MHz kako bi se izbjegla interferencija po susjednom kanalu. Ako pristupna točka ima ugrađene dvije antene za bolji prijenos signala, preporuča se okretanje jedne antene okomito, a drugu horizontalno pri čemu dolazi do usklađivanja polarizacije i terminalnog uređaja. U 5 GHz pojasu preporuča se korištenje DFS (engl. *Dynamic Frequency Selection*) koji omogućuje podjelu 5 GHz pojasa među uređajima koji koriste taj spektar [5]. Polarizacija se definira kao smjer titranja električnog polja, a može biti vertikalna, horizontalna i kružna [3].

3. Obilježja arhitekture bežične LAN mreže

Arhitektura bežične mreže sastoji se od prijemnika, antene, pristupne točke (engl. *Access point* – AP) i bežičnog medija kojim se prenose signali u kojima su sadržani podaci. Navedeni dijelovi međusobno djeluju s ciljem ostvarivanja zajedničke funkcije. Prijemnik se još naziva i *transceiver* (engl. *transmitter/receiver*) i predstavlja uređaj kojim upravljaju korisnici. Antena je sadržana u predajniku i prijemniku te je odgovorna za odašiljanje i prijem signala [5].

Uspostava bežične mreže zahtijeva posjedovanje vanjske antene, pristupne točke koja je sastavni dio bežičnog usmjerivača, bežičnog adaptera te jednog ili više klijenata. Bežični adapter često se izvodi u obliku mrežne kartice koja je jedan od glavnih dijelova terminalnih uređaja. Bežični usmjerivač (engl. *Wireless router*) definira se kao mrežni element čija je zadaća pronalazak optimalnih puteva za prijenos podataka od izvora do odredišta [6].

Većina današnjih prospojnika (engl. *Switch*) koji omogućuju povezivanje više klijenata odnosno računala u LAN mreži u sebi ujedno sadrže i usmjernike [6]. Budući da je svakom uređaju na mreži dodijeljena jedinstvena IP adresa, prilikom prelaska iz privatne LAN mreže na javnu WAN mrežu (engl. *Wide Area Network*) bežični usmjerivači koristeći NAT (engl. *Network Address Translation*) protokol konvertiraju privatnu adresu u javnu i prosljeđuju podatke. Isto vrijedi i u obrnutom slučaju [7].

3.1. Temeljni uređaji bežične LAN mreže

Preduvjet koji treba biti ispunjen kako bi korisnici mogli pristupiti bežičnoj mreži je da uređaj sadrži bežični adapter nakon čega se korisnik može spojiti na pristupnu točku [6].

Pristupna točka uređaj je koji pruža korisnicima mogućnost spajanja na ostatak žičane infrastrukture koristeći tehniku bežičnog pristupa. Pristupna točka definirana je mrežnim nazivom (engl. *Service Set IDentifier* – SSID) kojeg korisnik mora unijeti na svome uređaju tijekom postupka povezivanja [5].

Gledano iz perspektive sigurnosti, pristupna točka može biti otvorenog i zatvorenog tipa. Pristupna točka otvorenog tipa znači da korisnik nije obavezan unijeti identifikacijske podatke, tj. odgovarajuću šifru kako bi se spojio na mrežu. Takve pristupne točke koriste se u većim gradovima, restoranima, kafićima, hotelima, zračnim lukama i drugim sličnim mjestima gdje nije potrebno unositi šifru, već je dovoljno samo prihvatiti uvjete propisane od strane pružatelja usluga [8].

Pristupna točka zatvorenog tipa zahtijeva od korisnika unošenje šifre, tj. lozinke kako bi mogao pristupiti mreži. Navedeni tip pristupnih točki koristi se u stambenim i poslovnim zgradama, raznim organizacijama pri čemu se koriste određeni tipovi zaštite poput WEP, WPA i drugih [2]. Tipovi zaštite dodatno su pojašnjeni u šestom poglavlju. Prema [8] razlikuju se četiri načina rada pristupnih točaka:

- *Root Mode* – osnovni način rada u kojem AP predstavlja središnju pristupnu točku koja je žičano povezana na ostatak mreže i na koju se bežično povezuju ostali klijenti.
- *Client Mode* – jedan AP ima ulogu klijenta koji se spaja na drugi AP uređaj pri čemu AP koji ima ulogu klijenta ne može primati druge klijente jer se ponaša kao bežični adapter, odnosno predstavlja mrežnu karticu.
- *Bridge Mode* – AP uređaj u funkciji je mosta koji spaja dvije ili više mreža pri čemu isto kao i u *client modu* nije u mogućnosti primati ostale klijente.
- *Repeater Mode* – način rada u kojem jedan AP ponavlja signal nekog drugog AP-a unutar istog geografskog područja. Preuzima promet od svojih klijenata i prosljeđuje ga drugom AP-u [2],[8].

Antena je element bežične mreže kojim se zaprimaju signali, a koji je implementiran u pristupnu točku ili bežičnu karticu. U slučaju da ista nije implementirana na uređaju, postoji za to predviđeni priključak. Ograničavajući faktor kod ugrađenih antena je domet, odnosno radijus pokrivanja nekog područja. Kako bi područje pokrivanja signalom bilo veće, potrebno je koristiti vanjske antene te primijeniti jedan od prethodno navedenih načina za poboljšanje prijenosa signala. Povećanje fokusa signala koji se prenosi istodobno uzrokuje povećanje osjetljivost prijamnika (engl. *Receiver sensitivity*) i snage samog signala [2].

Snaga kojom zrači pojedina antena izražava se u decibelima što predstavlja logaritamski omjer signal/šum na ulazu i izlazu, iz čega se može zaključiti da povećanje signala uzrokuje povećanje osjetljivosti kako je prethodno rečeno [2]. Antene se prema [5] mogu kategorizirati u sljedeće skupine:

- Omni-direkcionalne antene – u većini se slučajeva koriste za unutarnje prostore. Zrače relativno istom snagom, ovisno o dobitku antene, u svim smjerovima prostorije.
- Polu-direkcionalne antene – zrače više-manje usmjereno u jednom smjeru. Često se koriste kada se AP nalazi u *bridge* načinu rada za premošćivanje bežičnih mreža.
- Visoko-direkcionalne antene – služe se *point-to-point* vezama za velike udaljenosti. Signali se usmjeravaju isključivo u jednom smjeru. Izvedene su u oblik parabole. Kao i polu-direkcionalne antene primjenjuju se u premošćivanju bežičnih mreža.
- *Diversity* antene – sadrže veći broj antena koje zajedno djeluju sa ciljem osiguravanja veće kvalitete prijenosa. Razlikuju se *dual* i *tri band* antene. *Dual band* antene imaju opciju istodobnog prijenosa signala u 2,4 GHz i 5 GHz pojasu, dok *tri band* nude mogućnost prijenosa jednog signala u 2,4 GHz pojasu i dva signala u 5 GHz pojasu. Pristupna točka sa *diversity* antenom i 4 gigabitna LAN ulaza prikazana je na Slici 4.

Slika 4. Pristupna točka sa *diversity* antenama

Izvor:[9]

Kako bi se spojili na bežičnu mrežu, klijenti moraju u svojim terminalnim uređajima, poput mobitela, prijenosnih i stolnih računala, imati bežičnu mrežnu karticu. Bežična mrežna kartica može biti implementirana u sâm uređaj ili se izvodi kao USB kartica namijenjena za sva računala koja sadrže USB ulaz [2].

3.2. Topologija bežične LAN mreže

Topologiju bežične mreže čini osnovni skup usluga (engl. *Basic Service Set* – BSS), neovisni skup usluga (engl. *Independent Basic Service Set* – IBSS), prošireni skup usluga (engl. *Extended Service Set* – ESS), distribucijski sustav usluga (engl. *Distribution System* – DS) i korisnici, tj. njihovi terminalni uređaji (engl. *Station* – STA) [10].

Osnovni skup usluga infrastrukturno gledano sastoji se od pristupne točke. Pristupna točka nudi skup osnovnih usluga koristeći jedan kanal i to samo na području koje obuhvaća njen radijus pokrivanja. Pristupna točka i svi korisnici moraju koristiti isti kanal za komunikaciju. Korištenje istog kanala predstavlja preduvjet koji treba biti ispunjen kako bi se komunikacija pravilno odvijala. Geografsko područje koje jedna pristupna točka pokriva, odnosno unutar kojeg se prenose signali naziva se ćelija (engl. *Basic service area* – BSA) [10].

Slično kao kod uspostavljanja veze u mobilnim komunikacijama pristupna točka odašilje signal prema terminalnim uređajima korisnika [10]. Pristupna točka povezana je na žičani LAN te nudi opciju premošćivanja kada jedan uređaj, odnosno stanica započinje komunikaciju sa drugim uređajem ili stanicom ili čvorom na DS [11].

U poglavlju 3.1 rečeno je da je pristupna točka određena SSID-jem, no to predstavlja samo simbolički naziv kako bi korisnik prepoznao pristupnu točku. Pristupna je točka zapravo određena jedinstvenim identifikatorom (engl. *basic service set identifier – BSSID*) koji se bazira na fizičkoj adresi radio sučelja bežične točke. Može se reći da je pristupna točka za korisnike

određena SSID-jem, dok je za korisničke uređaje određena BSSID-jem. Kada se korisnik želi spojiti na određenu pristupnu točku, prvo što mora učiniti je poslati zahtjev za pridruživanjem pristupnoj točki. Pristupna točka zaprima zahtjev te ga ovisno o korisničkim ovlastima zaprima ili odbija [10].

Neovisni skup usluga ne zahtijeva postojanje infrastrukture. Slično kao u osnovnom skupu usluga, pristupna točka oglašava svoje postojanje pri čemu jedan od uređaja preuzima ulogu voditelja i oglašava ime mreže, frekvenciju i ostale parametre. Bilo koji drugi uređaj se tada ovisno o potrebi može pridružiti. Opisani skup usluga treba biti ustrojen na improviziran i distribuiran način. Broj uređaja koje podržava kreće se u rasponu od osam do deset [10]. Ponekad se za istu koristi naziv *Ad-hoc* bežična mreža [11].

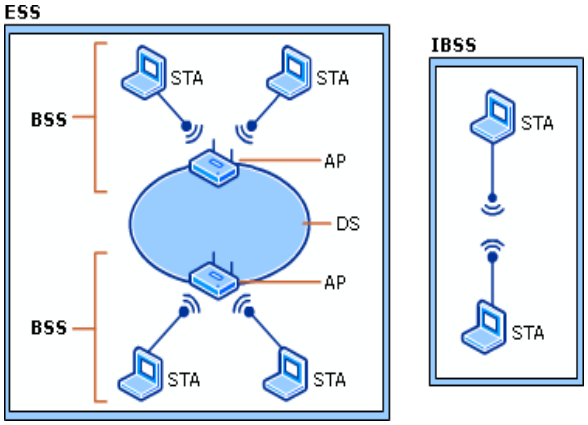
Prošireni skup usluga koristeći prospojničku infrastrukturu omogućuje međusobno povezivanje pristupnih točaka koje se nalaze na različitim lokacijama poput kata bolnice, hotela i sličnih ustanova. Temelji se na principu da svaka pristupna točka unutar nekog područja npr. kata bolnice ima jednak SSID, ali različit BSSID što omogućuje korisniku da neprestano koristi usluge bežične mreže i kada se nalazi na nekom području pokrivanja jedne od nekoliko pristupnih točaka. Korisnik kada napusti jedno područje pokrivanja automatski se spaja na drugo područje pokrivanja. Prelazak sa jedne pristupne točke na drugu naziva se prelaženje (engl. *Roaming*) [10].

Važno je naglasiti da svaka pristupna točka nudi vlastiti skup osnovnih usluga na svom kanalu u svrhu sprječavanja interferencija. Prilikom prelaska sa jedne pristupne točke na drugu korisnik, tj. terminalni uređaj mora prvo skenirati dostupne kanale s ciljem pronalaska nove pristupne točke na koju se može priključiti [10]. Sve pristupne točke povezane su na istu žičanu infrastrukturu [11].

Distribucijski sustav usluga omogućuje korisnicima koji su spojeni na pristupnu točku komunikaciju sa drugim uređajima koji nisu spojeni na istu pristupnu točku. Pristupna točka mapira virtualne lokalne mreže (engl. *Virtual LAN* –VLAN) u SSID. Kako bi se više VLAN-ova mapiralo u više SSID potrebno je pristupnu točku povezati linkom do prospojnika koji je

povezan na VLAN. Kada pristupna točka koristi više SSID-a, ona usmjerava pojedini VLAN putem zraka i zatim preko istog kanala do klijenata [11].

Klijenti moraju koristiti odgovarajući SSID koji je mapiran na odgovarajući VLAN. Pristupna točka može podržavati veći broj logičkih veza pri čemu svaka veza pokriva isto područje djelovanja što može predstavljati problem budući da svi korisnici koriste iste resurse poput sklopovske podrške, antena i slično [11]. Odnos između BSS-a, ESS-a i IBSS-a prikazan je Slikom 5 koja ujedno predstavlja arhitekturu bežične mreže.



Slika 5. Arhitektura bežične mreže

Izvor:[11]

Mesh topologija koristi se u slučajevima kada se želi osigurati dostupnost bežične mreže na većem geografskom prostoru gdje nije praktično provoditi Ethernet kabliranje do svake pristupne točke. U *mesh* topologiji promet se premošćuje od jedne do druge pristupne točke pri čemu su pristupne točke međusobno povezane u seriju i svaka koristi različit kanal. Svaka pristupna točka u *mesh* topologiji može koristiti dvostruke kanale za različite raspone frekvencija po pojedinom kanalu [10].

U praksi jedan kanal se koristi za BSS na koji se klijenti mogu povezati. Promet koji se prenosi *mesh* mrežom se premošćuje od jedne do druge pristupne točke sve do žičane LAN infrastrukture. Opisana mreža se može uspostaviti u zatvorenom ili otvorenom prostoru i nudi mogućnost pokretanja vlastitog dinamičkog protokola za usmjeravanje [10].

Osim opisanih topologija razlikuju se još i topologija mosta i ponavljača što je vezano uz načine rada pristupne točke što je opisano u prethodnom dijelu rada. U topologiji mosta most radne grupe (engl. *Workgroup bridge* – WGB) povezuje žični mrežni adapter uređaja sa bežičnom mrežom. WGB postaje bežični klijent BSS-a i djeluje kao vanjski bežični mrežni adapter za uređaj koji ne posjeduje mrežni adapter. Jedan klijent je povezan bežično na AP, dok drugi se prvo povezuje na WGB pa zatim na AP. Prema [10] razlikuju se 2 tipa WGB-a:

- Univerzalni most radne grupe (engl. *Universal workgroup bridge* –uWGB) koji podržava premošćivanje samo jednog uređaja na bežičnu mrežu.
- WGB implementacija pod nadležnošću CISCO-a te nudi opciju premošćivavanja više žičanih uređaja na bežičnu mrežu.

3.3. Načini rada bežične LAN mreže

Bežična mreža može raditi na dva načina, prema [5] razlikuju se:

- Infrastrukturni način
- *Ad–hoc* način.

U infrastrukturnom načinu korisnički uređaji razmjenjuju podatke odnosno komuniciraju pri čemu pristupna točka predstavlja posrednika između krajnjih uređaja [5]. Kako bi stanici, tj. terminalnom uređaju korisnika bila omogućena komunikacija prvo što je potrebno je spajanje stanice na pristupnu točku. Broj terminalnih uređaja koji se može priključiti na jednu pristupnu točku ovisi o različitim faktorima kao što su udaljenost, primijenjeni standard te postavke mreže [2].

U slučajevima kada je broj korisnika spojenih na jednu pristupnu točku veći od preporučenog izvedbene karakteristike mreže se smanjuju. BSS nudi mogućnost pokrivanja područja ovisno o vrsti prostora. Za zatvorene prostore radijus pokrivanja iznosi od 10 do 30 metara dok je za otvorene prostore znatno veći [2].

Ad–hoc način rada ne zahtjeva postojanje mrežne infrastrukture već korisnički uređaju komuniciraju jedni sa drugima. Svaki korisnički uređaj pojedinačno vodi brigu o brzini prijenosa, komutaciji i ostalim parametrima [5]. Uklanjanjem potrebe za pristupnim točkama korisnicima je omogućena izrada i korištenje mreže bez mrežne infrastrukture što uzrokuje ograničenost dometa pa se tako korisnici moraju nalaziti u području pokrivanja koje je definirano radijusom pokrivanja. U slučaju da se želi povećati područje pokrivanja tada se mora koristiti infrastrukturni način [2].

4. Arhitektura CISCO bežične LAN mreže

Arhitektura CISCO bežične LAN mreže ovisi: u kojem okruženju se stvara mreža, odnosno kako će se njome upravljati i postavljati, na koji način se rješavaju problemi na mreži, kontroliranje rada pristupnih točaka te tok prometa kroz mrežu. Razlikuju se prema [10] tri glavne arhitekture:

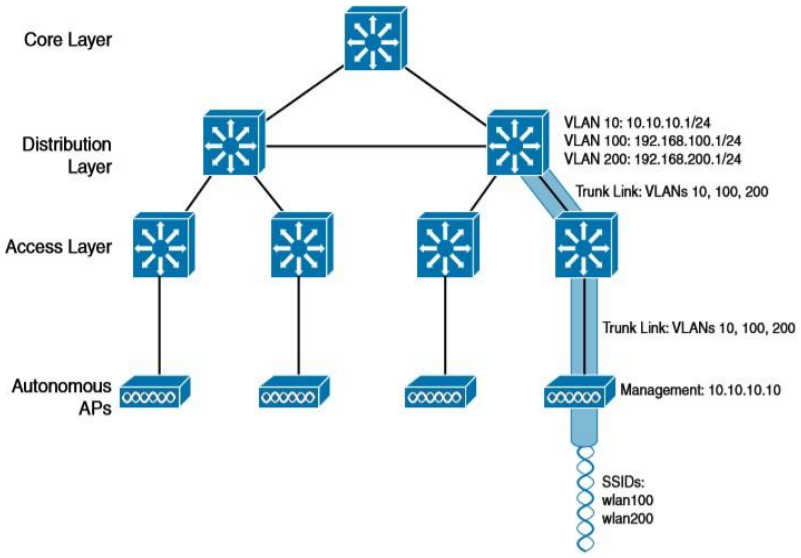
- Arhitektura autonomne pristupne točke (engl. *Autonomus AP arhitecture*),
- *Cloud-based AP* arhitektura i
- *Split-MAC* arhitektura.

4.1. Arhitektura autonomne pristupne točke

Autonomna pristupna točka omogućuje korisnicima jedan ili više skupova osnovnih usluga pri čemu je svaki skup samostalan. Takva vrsta pristupne točke predstavlja most koji povezuje identifikatore bežičnog seta usluga sa žičanim virtualnim LAN-ovima na pristupnom sloju (engl. *Access layer*). Korištenje iste autonomne pristupne točke korisnicima daje opciju međusobne komunikacije bez potrebe za povezivanjem na žičani dio mreže. Arhitektura izrađena od takve vrste pristupnih točaka nudi kraće i jednostavnije putanje između žičnog i bežičnog dijela mreže [10].

Kako bi pojedina autonomna pristupna točka postala dio CISCO bežične LAN mreže, ista se prvo mora povezati vezama s prospojnicima na pristupnom sloju koji se povezuju na prospojnike distribucijskog sloja. Glavna je karakteristika ovakve arhitekture što pristupna točka vrši VLAN mapiranje budući da je povezana s distribucijskim prospojnikom pomoću *trunk* veze. Nakon povezivanja pristupne točke s distribucijskim slojem, pristupnoj se točki mora dodijeliti IP adresa za upravljanje. IP adresa za upravljanje pruža korisnicima opciju udaljenog upravljanja pa tako korisnik može samostalno postaviti SSID, VLAN, frekvencijske parametre poput kanala i snage prijenosa. Za održavanje cjelokupne mreže potrebno je postaviti i održavati svaku autonomnu pristupnu točku ili se može primijeniti platforma poput Cisco Prime Infrastructure ili Cisco DNA Center [10].

U slučaju da se veličina mreže poveća, podaci za upravljanje koje pojedini VLAN treba proslijediti do autonomne pristupne točke putuju sve duže do odredišta te mrežna konfiguracija i učinkovitost postaju sve kompleksniji. Dodavanje novog VLAN-a predstavlja ne tako jednostavan proces budući da je potrebno konfigurirati svaki prospojnik na pojedinom sloju i svaku pojedinu pristupnu točku. Ukoliko postoje redundantne veze između svakog sloja STP protokola na pojedinom prospojniku, prospojnik preuzima glavnu ulogu za sprječavanje nastanka petlji koje povećavaju kompleksnost mreže. Upravo je mogućnost povećanja kompleksnosti mreže razlog zbog kojeg je prelazak korisnika iz jednog područja u drugo ograničen samo na pristupni sloj [10]. Slika 6. prikazuje hijerarhijski raspored jezgri distribucijskog i pristupnog sloja sa odgovarajućim uređajima na svakom sloju [10].



Slika 6. Arhitektura autonomne pristupne točke

Izvor:[10]

4.2. *Cloud based* arhitektura

U prethodnom potpoglavlju opisana je arhitektura autonomne pristupne točke koja zahtijeva dosta upravljanja i konfiguracije. Rastom mreže postupci postavljanja i upravljanja postaju kompleksniji i zahtjevniji. Kako bi se olakšalo upravljanje, moguće je koristiti platformu na centralnoj lokaciji unutar poduzeća. Drugi je opcija korištenje *cloud-based* arhitekture gdje upravljanje pristupnim točkama i konfiguracija bazirana na *cloud* tehnologiji poznatoj pod nazivom Cisco Meraki [10].

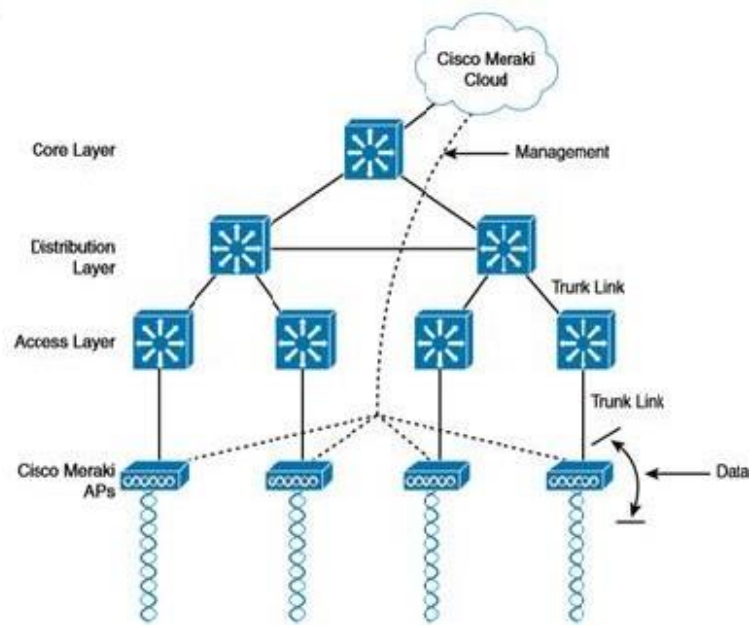
Cisco Meraki temelji se na *cloud* tehnologiji i uvelike olakšava centralizirano upravljanje mrežama koje su uspostavljene pomoću Meraki proizvoda. Umrežavanjem Meraki proizvoda korisniku je putem nadzorne ploče omogućeno konfiguriranje i upravljanje pristupnim točkama, promatranje performansi i aktivnosti CISCO bežične LAN mreže te generiranje izvješća na temelju dobivenih podataka. Cisco Meraki nakon registracije korisnika i pokretanja autonomne pristupne točke omogućuje automatsko konfiguriranje o čemu korisnik dobiva obavijest [10].

Nadogradnja kao proces vrlo je olakšana u odnosu na ostale arhitekture jer se izvodi dijeljenjem koda nadogradnje svim pristupnim točkama u mreži. Cisco Meraki prikuplja podatke iz svih pristupnih točaka u mreži koje analizira i na temelju rezultata analize donosi odluke. Podaci u ovom tipu arhitekture putuju isključivo između klijenata, a ne do oblaka (engl. *Cloud*) i obratno [10].

Oblak dijeli upravljačke podatke do pristupnog dijela mreže. Razlikuju se dvije različite rute: ruta za prijenos podataka i ruta za prijenos podataka odgovornih za upravljanje prometom. Sukladno tome razlikuju se dvije funkcije:

- Kontrolna ravnina – koristi se za upravljanje prometnom odgovornim za kontrolu, postavljanje, upravljanje i nadzor same pristupne točke.
- Podatkovna ravnina – sadrži funkcije vezane za promet koji generira krajnji korisnik i koji prolazi kroz sve pristupne točke [10].

Slika 7. prikazuje *cloud-based* arhitekturu u čijem se jezgrinome dijelu nalazi program Cisco Meraki. Kontrolna ravnina dio je distribucijskog i jezgrinog dijela dok se podatkovna razina nalazi između pristupne točke i prospojnika na pristupnom sloju.



Slika 7. *Cloud-based* arhitektura

Izvor:[10]

4.3. *Split-MAC* arhitektura

Upravljanje autonomnim pristupnim točkama vrlo je zahtjevan posao. Mrežni administrator ima zadaću konfigurirati svaku pojedinačnu pristupnu točku. Svaka autonomna pristupna točka upravlja svojom sigurnosnom politikom pri čemu ne postoji centralizirana točka koja razdvaja žični od bežičnog dijela mreže. To znači da ne postoji idealno mjesto za promatranje performansi mreže. Kako bi se izbjegli problemi uzrokovani distribuiranim autonomnim pristupnim točkama, funkcije pojedine pristupne točke su prema [10] podijeljene u dva dijela, odnosno grupe:

- Funkcije upravljanja – nisu sastavni dio upravljanja okvirima putem RF kanala i njima se upravlja pomoću centralizirane platforme.

- Procesi u stvarnom vremenu – odnose se na slanje i zaprimanje 802.11 okvira. Uključuju kontrolu pristupa mediju (engl. *Media access control*) koja omogućuje komunikaciju s klijentima i dio su sklopovske opreme pristupne točke.

Nakon što se provede postupak podijele funkcija autonomnog sustava, sklopovski dio pristupne točke (engl. *Lightweight access point* – LAP) odgovoran je za stvarno-vremenske procese. Funkcije upravljanja su tada izvedene od strane bežičnog LAN kontrolera (engl. *Wireless LAN controller* – WLC) koji istovremeno provjerava i nadzire rad LAP-ova te na taj način LAP postaje ovisna o WLC-u po pitanju autorizacije korisnika, upravljanje sigurnosnim postavkama i slično. Podjela funkcija autonomne pristupne točke i segmenti koji prilikom toga nastaju čine *split-MAC* arhitekturu. Svaka lagana pristupna točka tada se mora povezati s WLC-om kako bi mogla posluživati klijente [10].

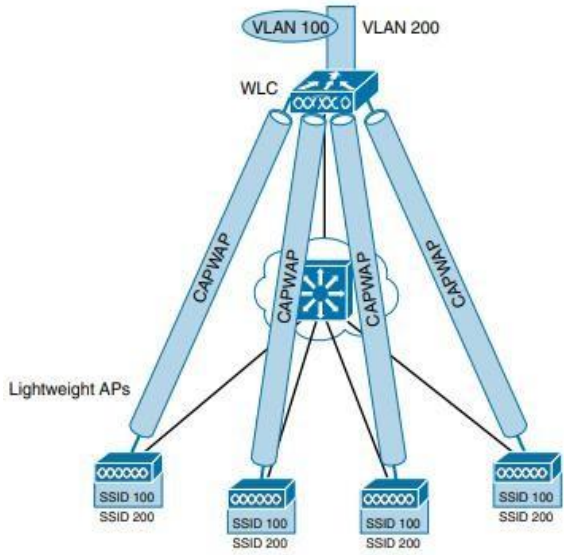
U svrhu pružanja kompletnih funkcija koje je imala autonomna pristupna točka, WLC i LAP povezani su *Control and Provisioning of Wireless Access Points* (CAPWAP) protokolom. CAPWAP protokol enkapsulira podatke između LAP-a i WLC-a unutar novo formiranog IP paketa te pruža opciju da LAP i WLC budu geografski i logički odvojeni. CAPWAP čine dva odvojena tunela:

- CAPWAP kontrolne poruke (engl. *CAPWAP control messages*) – prenose podatke vezane za konfiguraciju pristupne točke i upravljanje njenim radom. Sami podaci su autentificirani i šifrirani te na taj način samo odgovarajući WLC kontrolira LAP, tj. pristupnu točku.
- CAPWAP podaci (engl. *CAPWAP data*) – prenosi podatke podatkovnim tunelom do korisnika, no prema početnoj pretpostavci podaci nisu šifrirani. U slučaju da je dostupno šifriranje koristi se DTLS (engl. *Datagram Transport Layer Security*) [10].

Svaki LAP i WLC međusobno se autentificiraju, odnosno provjeravaju pomoću digitalnog certifikata. U tu svrhu za CISCO bežičnu LAN mrežu koristi se X.509 certifikat koji je ugrađen u svaki uređaj. Certificiranje provjerava ispravnost svakog uređaja prije nego se isti doda u mrežu te štiti korisnika od upada neovlaštene pristupne točke u mrežu. Uspostavljanjem CAPWAP tunela između WLC-a i LAP-a dolazi do proširenja spektara mogućnosti WLC-a, a prema [10] to su sljedeće aktivnosti:

- Dinamička dodjela kanala,
- Optimizacija snage prijenosa,
- Samopopravljiva bežična pokrivenost,
- Fleksibilno prelaženje klijenta iz jednog područja u drugo,
- Dinamičko balansiranje opterećenja klijenta,
- RF nadzor,
- Upravljanje sigurnošću i
- Bežični sustav zaštite od upada.

Slika 8. prikazuje povezivanje više LAP-ova s jednim WLC-om pri čemu je svaki LAP povezan jednim CAPWAP tunelom sa WLC-om.



Slika 8. *Split-MAC* arhitektura

Izvor:[10]

Koncept *split-MAC* može se primijeniti na različitim arhitekturama ovisno o položaju WLC-a u mreži. Tako WLC se prema [10] razlikuje sljedeće koncepte:

- *Centralized WLC deployment/unified* koncept – WLC je smješten na centralnom mjestu u mreži čime se maksimizira broj pridruženih pristupnih točaka. Promet usmjeren od središta mreže prema korisniku i obratno se prenosi putem CAPWAP tunela. Navedeni koncept olakšava primjenu i implementaciju sigurnosnih pravila koja imaju utjecaj na sve korisnike te podržava maksimalno 6000 pristupnih točaka.
- *Cloud-based WLC deployment* – predstavlja model gdje je WLC smješten unutar podatkovnog centra u privatnom *cloud*-u. WLC se primjenjuje u obliku virtualnog stroja (engl. *Virtual machine*) te podržava najviše 3000 pristupnih točaka.
- *Embedded WLC deployment* – koristi se za manja područja poput kampusa ili distribuiranih podružnica. WLC je ugrađen u sklopovsku podršku za prospajanje pri čemu pristupne točke ne moraju nužno biti povezane na prospojnike koji u sebi sadržavaju WLC, već se mogu naknadno povezati na WLC. Obično podržavaju do 200 pristupnih točaka.
- *Mobility Express WLC deployment* – podržava do 100 uređaja. WLC je integriran u pristupnu točku i koristi se u malim okruženjima [10]. Tablicom 2. uspoređeni su pojedini načini rada ovisno o položaju WLC-a, broju pristupnih točaka i klijenata te području uporabe.

Tablica 2. Usporedba WLC modela.

WLC Model	Položaj WLC-a	Broj AP-a	Broj klijenata	Područja uporabe
Unified	Centraliziran	6000	64000	Velika poduzeća
Cloud	Podatkovni centar	3000	32000	Privatni cloud
Embedded	Pristupni prospojnici	200	4000	Manji kampusi
Mobility Express	Pristupna točka	100	2000	Lokacija podružnice

Izvor:[10]

CISCO pristupne točke mogu raditi na dva različita načina autonomni i *lightweight* način, ovisno o potrebi. Prema [10] WLC također nudi opciju konfiguriranja *lightweight* pristupne točke za rad posebne namjene u jednom od načina:

- Lokalni način rada – *lightweight* način rada pristupne točke koji omogućuje jedan ili više BSS-ova na određenom kanalu istodobno skenirajući ostale kanale i njihove performanse.
- Monitor način rada – predajnik pristupne točke ne odašilje signale dok se prijemnik ponaša kao namjenski senzor i utvrđuje položaj stanice, detektira lažne pristupne točke.
- *FlexConnect* – pristupna točka koja se nalazi na udaljenoj lokaciji može lokalno preusmjeriti promet između SSID-a te VLAN-a ako je njegov CAPWAP tunel do WLC-a neaktivan i ako je konfiguriran za to.
- *Sniffer* – primarna je zadaća pristupne točke je prikupljanje prometa, tj. podataka od ostalih izvora te prosljeđivanje istih do računala. Računala pomoću programskog softvera dalje analiziraju prikupljeni promet.
- Detektor lažnih podataka – pristupne točke zadužene su za detektiranje lažnih uređaja uspoređujući MAC adresu na žičanom i bežičnom dijelu mreže. U slučaju da se ista pojavljuje u oba dijela riječ je o lažnom uređaju.
- *Bridge* – koristi se za povezivanje dviju udaljenih lokacija ili mreža pri čemu pristupna točka ima ulogu namjenskog mosta.
- *Flex+Bridge* – postiže se omogućavanjem opcije *FlexConnect* na mrežnoj pristupnoj točki.
- *SE-Connect* – pristupna točka posvećena je analizi frekvencijskog spektra na bežičnim kanalima. Jedan od softvera koji se pri tome koristi je Cisco Spectrum Expert.

5. Implementacijski modeli CISCO bežične LAN mreže

Prvi korak pri implementaciji CISCO bežične LAN mreže je odabir načina rada pristupne točke, odnosno hoće li pristupna točka biti autonomna ili će se sastojati od *lightweight* pristupne točke i WLC-a [10]. Karakteristike svakog načina rada odnosno autonomne i *lightweight* pristupne točke te WLC-a opisani su u potpoglavljima 4.1. i 4.3. stoga se neće opet navoditi sve karakteristike, već će se ukratko iznijeti značajke bitne za uspostavu bežične mreže.

Autonomne pristupne točke su samostalni uređaji koji mapiraju svaki VLAN u WLAN i BSS te sadrži jedno sučelje za žičani dio mreže odnosno za žičani Ethernet i podržava upravljanje sesijom na temelju preglednika korištenjem HTTP ili HTTPS protokola [10].

Lightweight pristupna točka također sadrži jedno Ethernet sučelje te, kako bi potpuno bila funkcionalna, se mora povezati sa WLC-om. U ovom slučaju WLC vrši VLAN mapiranje za distribuiranje prometa dalje u žični dio mreže. Drugim riječima, promet putuje dosta posrednički od pristupne točke prema WLC-u. Pristupnoj točki potrebna je pristupna veza za povezivanje na mrežnu infrastrukturu i njezin završetak na kraju CAPWAP tunela koji povezuje WLC i AP [10].

Pristupnu točku, nakon što joj se dodijeli IP adresa i postane sposobna za rad, potrebno je povezati sa terminalnim uređajem korištenjem Telneta. U slučaju autonomne pristupne točke koristi se HTTP ili HTTPS protokol dok je u slučaju *lightweight* pristupne točke potrebno prvo konfigurirati i povezati pristupnu točku s WLC-om. Konfiguracija i povezivanje WLC-a odvija se putem grafičkog korisničkog sučelja (engl. *Graphical user interface* – GUI) internetske stranice ili pomoću SSH sesije, odnosno komandnog sučelja (engl. *Command line interface* – CLI) [10].

Oba načina od korisnika zahtijevaju unošenje autentifikacijskih podataka te nakon uspješne verifikacije nude opcije praćenja konfiguriranja i otklanjanja pogrešnih aktivnosti. WLC se sastoji od fizičkih portova koji su prema [10] grupirani u sljedeće skupine:

- *Service port* – koristi se za obnovu sustava i početno pokretanje sustava.
- *Distribution system port* – odgovoran je za upravljački promet te prenosi sav promet koji dolazi i odlazi iz priključka. Najčešće je povezan s prospojnikom pomoću *trunk* veze.
- *Console port* – koristi se za potrebe *out of band* upravljanje.
- *Redundacy port* – povezuje se sa dodatnim kontrolerom za visoku dostupnost operacija.

Logička interna sučelja u WLC-u moraju biti konfigurirana s IP adresom, maskom podmreže, zadanim pristupnikom i protokolom za automatsku dodjelu IP adrese (*Dynamic Host Configuration Protocol* – DHCP). Svako logičko sučelje tada ima dodijeljen fizički priključak i VLAN ID. Logička interna sučelja se, kao i kontrolni priključci, prema [10] mogu kategorizirati na:

- *Managment interface* – zaduženo za upravljanje prometom (odnosi se na upravljački promet protokola poput SSH, SNMP, HTTPS), komunikaciju između WLC-a te definira CAPWAP tunele između WLC-a i pristupne točke. Orijentirano je prema komutiranoj mreži u kojoj se nalaze korisnici i pristupne točke.
- *Redundacy managment* – sučelje u kojem se nalazi upravljačka adresa redundantnog WLC-a koji je dio para kontrolera visokih dostupnosti. Aktivni WLC koristi sučelje za upravljanje adresom dok WLC koji se nalazi u stanju pripravnosti koristi adresu *redundacy managmenta*.
- *Service port interface* – koristi se za određeni skup operacija orijentiranih prema klijentu poput autentifikacije klijenta na internet pregledniku zbog čega ga je potrebno konfigurirati jedinstvenom adresom koja se ne može usmjeravati. *Service port interface* povezano je sa *service portom*.
- *Dynamic interface* – povezuje VLAN s odgovarajućim WLAN-om. Dinamičko sučelje mora biti konfigurirano s vlastitom IP adresom.

Uspostava bežične LAN mreže može se promatrati na dva načina: bežično i žično. Iz bežične perspektive nakon konfiguracije pristupna točka oglašava svoj SSID prema klijentima kako bi se mogli povezati, dok u žičnom dijelu VLAN se povezuje na jedno od dinamičkih sučelja. WLAN predstavlja poveznicu između SSID-a i VLAN-a Slično kao i VLAN, WLAN također omogućuje podjelu korisnika i prometa kojeg oni generiraju u logičke mreže.

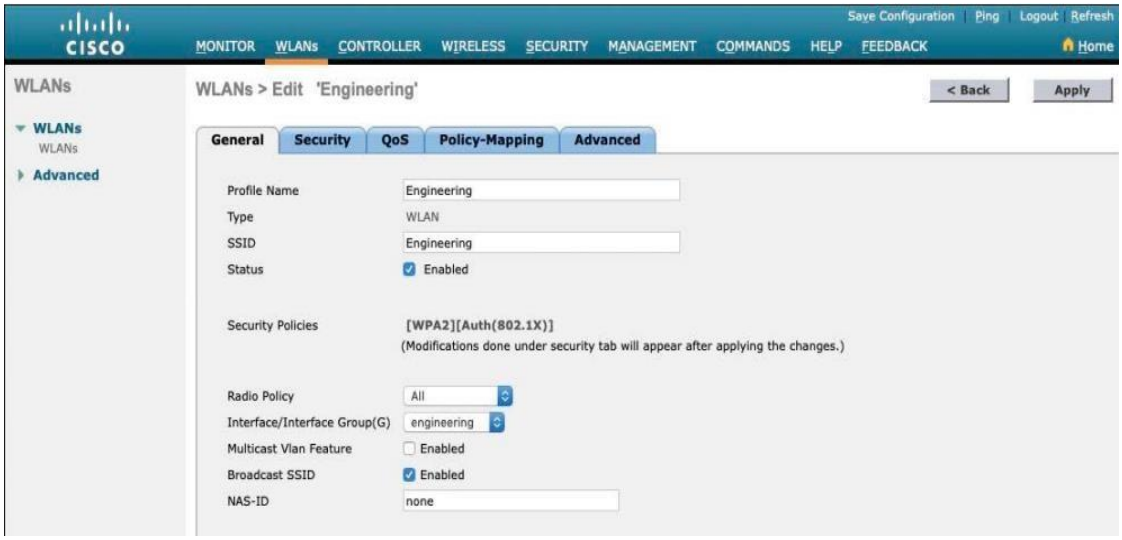
Korisnici ne mogu prijeći iz jednog WLAN-a u drugi osim ako prelazak nije definiran unutar žičanog dijela mreže, odnosno između VLAN-ova stoga je vrlo važno prije kreiranja novog WLAN-a voditi računa o broju uređaja i primjeni istog. CISCO WLAN sadržava ograničenja kojih se potrebno pridržavati prilikom izrade, a prema [10] to su:

- CISCO upravljači podržavaju maksimalno 512 WLAN-ova pri čemu samo 16 ih može biti konfigurirano na jednu pristupnu točku
- Oglašavanje pojedinog WLAN-a smanjuje vrijeme predviđeno za emitiranje, tj. prijenos podataka.

Beacons označava uređaj koji omogućuje prijenos podataka do terminalnih uređaja unutar određenog prostornog raspona [12]. Svaka pristupna točka oglašava *beacon* upravljačke podatke kako bi oglasila postojanje BSS-a. Budući da je WLAN povezan sa BSS-om, svaki WLAN mora biti oglašavan prema terminalnim uređajima zajedno sa pripadajućim *beaconsima*. U slučaju da je stvoreno previše WLAN-ova, vrijeme koje je predviđeno za emitiranje, odnosno prijenos će biti kraće. Smanjenje vremena predviđenog za prijenos na korisničkoj strani će se manifestirati dužim vremenom potrebnim za prijenos podataka. Kako bi se izbjegao opisani problem, potrebno je ograničiti maksimalni broj WLAN-ova na pet [10].

Prilikom stvaranja WLAN-a najvažniji parametri o kojima treba voditi brigu su SSID niz, sučelje WLC-a, VLAN broj te sigurnost, o čemu će više biti riječi u idućem poglavlju.

Svaki korak konfiguracije se izvodi se putem sesije internet preglednika koja je povezana s upravljačkom adresom WLC-a. Nakon što se definiraju sučelja, pristupna točka i WLC, korisnik se autentificira putem internet sučelja te može započeti sa izradom CISCO bežične LAN mreže [10]. Slika 9. prikazuje sučelje koje se prikazuje korisniku zajedno sa parametrima koje može definirati poput SSID-a, kvalitete usluge (engl. *Quality of service* – QOS) i slično.



Slika 9. Sučelje za izradu WLAN-a

Izvor:[10]

U opciji Općenito (engl. *General*) korisnik može provjeriti status bežične mreže, je li aktivna ili ne, te na kojim frekvencijama će biti dostupna. Zatim se bežična mreža povezuje sa sučeljima definiranim na WLC-u. *Broadcast SSID* omogućuje pristupnoj točki oglašavanje vlastitog SSID-a. Opcija Sigurnost (engl. *Security*) nudi odabir vrste „zaštite“ koji će bežična mreža imati (WPA, WPA2 ili neki drugi model) odnosno način autentifikacije klijenta. Prozor QOS nudi projektantu CISCO bežične LAN mreže opciju definiranja kvalitete usluge koja će biti ponuđena korisnicima. Prema [10] razlikuju se četri razine usluge:

- Platinasta (engl. *Platinum*) – za usluge prijenosa glasa,
- Zlatna (engl. *Gold*) – u svrhu prijenosa videa,
- Srebrna (engl. *Silver*) – koji nudi *best effort* usluge i
- Brončana (engl. *Bronze*).

Prozor Napredno nudi opciju postavljanja naprednih postavki CISCO bežične LAN mreže. *Client Exclusion* definira nakon kojeg vremena se korisnik mora reautentificirati. Prema zadanim postavkama ta vrijednost iznosi 30 minuta. Nakon što projektant odabere parametre treba potvrditi unesene vrijednosti čime se finalizira izrada bežične mreže [10].

6. Sigurnost CISCO bežične LAN mreže

Mreže temeljene na 802.11 standardu, a među njima i CISCO bežična LAN mreža su vrlo često meta napada i neovlaštenih upada. Kako bi korisnik mogao koristiti bežičnu mrežu, mora biti autentificiran od strane pristupne točke. Postupkom autentifikacije bežična mreža ostvaruje kontrolu nad pristupom. Postoji nekoliko metoda autentifikacije pri čemu neke od njih zahtijevaju samo tekstualni niz. Autentifikacijeske metode koje zahtijevaju tekstualni niz koriste se samo u slučajevima kada se autentificiraju pouzdani klijenti i pouzdane pristupne točke [10].

Najveći nedostatak takvih metoda je sigurnost budući da u slučaju gubitka ili krađe terminalnog uređaja neovlašteni korisnik može pristupiti mreži. Osim gubitka ili krađe uređaja navedena metoda je nesigurna zbog mogućeg povezivanja na lažne pristupne točke. Budući da se korisnici i uređaji automatski povezuju na mreže za koje već znaju da su pouzdane, lažna pristupna točka može emitirati SSID pouzdane pristupne točke i na taj način presretati komunikaciju [10].

Presretanjem komunikacije od i prema klijentu onemogućen je normalan rad mrežnih operacija koje je korisnik zatražio. Takve vrste napada moguće je izbjeći autentifikacijom pristupne točke od strane klijenta prije nego je sam klijent autentificiran na pristupnoj točki. U svrhu osiguranja privatnosti podataka sami podaci se moraju šifrirati prije prijenosa medijem [10].

Bežične mreže podržavaju jednu autentifikacijsku i enkripcijsku metodu, stoga svi klijenti u mreži moraju koristiti tu metodu nakon pridruživanja. Klijenti se ne mogu međusobno prisluškivati jer su pristupna točka i klijent jedina dva uređaja koja imaju zajedničke ključeve za šifriranje odnosno enkripciju za prijenos podataka. Unatoč šifriranju podataka i dalje postoji mogućnosti modifikacije podataka na putu prema odredištu što će prijemnik teško primijetiti. U tu svrhu se koristi provjera integriteta poruke MIC (engl. *Message integrity check*) [10].

6.1. Metode provjere autentičnosti klijenta

Za provedbu autentifikacije klijenata u procesu povezivanja na bežičnu mrežu može se koristiti više metoda, no u ovom radu obuhvatit će se samo najkorištenije metode. Svaka metoda s vremenom je evoluirala te su uklonjeni sigurnosni nedostatci i unaprijeđeni sami uređaji koji čine bežičnu mrežu [10].

Otvorena autentifikacija (engl. *Open autentification*) jedan je od prvih primjenjivanih načina autentifikacije. Prva verzija standarada 802.11 nudila je dva načina autentifikacije otvorenu autentifikaciju i WEP. Otvorena autentifikacija omogućuje otvoren pristup bežičnoj mreži te korisnik mora poslati zahtjev za autentifikacijom prije nego li bude u mogućnosti koristiti mrežu. Slanje autentifikacijskog zahtjeva provodi se putem mrežne stranice na kojoj

korisnik mora prihvatiti uvjete prije nego se spoji na bežičnu mrežu. Većina današnjih operacijskih sustava upozorava korisnika da podaci neće biti zaštićeni prilikom prijenosa [10].

WEP način autentifikacije za razliku od otvorenog načina omogućuje enkripciju podataka između klijenta i pristupne točke. Algoritam šifriranja koji koristi WEP metoda šifrira svaki bežični paket te ga na taj način čini nevidljivim za presretače. Isti algoritam dekriptira podatke na prijemnoj strani te koristi niz bitova koji se nazivaju WEP ključ kako bi prijenos podataka bio siguran. Predajnik i prijemnik moraju imati identičan ključ kako bi prijemnik dešifrirao ono što je predajnik poslao. U slučaju da klijent ne koristi odgovarajući WEP ključ, povezivanje s pristupnom točkom bit će onemogućeno [10].

Pristupna točka šalje nasumični izazovni izraz nakon čega klijent odgovara. Takav način autentifikacije u kojem pristupna točka postavlja pitanje, a korisnik mora dati valjan odgovor kako bi bio autentificiran zove se izazovno odgovorna autentifikacija. Pristupna točka uspoređuje odgovor klijenta s odgovorom u pohranjenim u svojim postavkama. Ovisno o tome jesu li ključevi identični korisniku se dopušta ili odbija pristup. WEP ključevi su duljine 40 ili 104 bita prikazani u obliku heksadekadskog niza u rasponu od 10 ili 26 znamenki. Ratifikacijom 802.11i amandmana WEP se službeno smatrao zastarjelim i više se ne preporuča njegovo korištenje [10].

802.1x/EAP predstavlja prilagodljiviji i skalabilniji autentifikacijiski okvir. WEP metoda kategorizirana je kao slaba vrsta autentifikacije, što je dovelo do razvoja EAP metode. EAP definira skup uobičajenih metoda koje su međusobno jedinstvene i drugačije, ali sve koriste EAP okvir. EAP se može integrirati s IEEE 802.1x kontrolnim standardom čime je korisniku dozvoljeno povezivanje sa pristupnom točkom, ali prijenos podataka u bilo koji drugi dio mreže će biti onemogućen dok proces autentifikacije ne bude u potpunosti završen. EAP metoda se sastoji od tri čimbenika:

- *Supplicant* – uređaj koji zahtjeva pristup mreži.
- *Authenticator* – mrežni uređaj koji omogućuje pristup mreži najčešće je riječ o WLC-u.
- *Autehentication* – server je uređaj koji zaprima autentifikacijske podatke korisnika i na temelju toga prihvaća ili odbija pristup mreži [10].

Lightweight EAP (LEAP) je metoda razvijena od strane CISCO-a za provjeru autentičnosti. Klijent i autentifikacijski server razmjenjuju šifrirane izazovne poruke čime se ostvaruje obostrana autentifikacija. Opisani proces izvodi se sve dok je enkripcija poruka uspješna. LEAP metoda razvijena je kao odgovor na WEP nedostatak, no pokazalo se da je takav način izazovno odgovorne autentifikacije ranjiv te se ne preporučuje za korištenje [10].

EAP Flexible Authentication by Secure Tunneling (EAP-FAST) jedna je od metoda također razvijena od strane CISCO-a. Vjerodajnice za provjeru autentičnosti zaštićene su prosljeđivanjem vjerodajnica za pristup (engl. *Protected access credential* – PAC). PAC je oblik dijeljenja podatka generiranog od strane pristupne točke. Izvodi se u tri faze:

- Faza 0 (engl. *Phaze 0*) – u kojoj se vjerodajnica generira i instalira na klijentu.

- Faza 1 (engl. *Phaze 1*) – nakon međusobne autentifikacije klijent i pristupna točka pregovaraju o *Transport Layer Security* (TLS) tunelu.
- Faza 2 (engl. *Phaze 2*) – moguće je u svrhu dodatne sigurnosti korisnika dodatno autentificirati kroz TLS tunel [10].

Zaštićeni EAP (PEAP) metoda je koja koristi unutarnju i vanjsku autentifikaciju. Pristupna točka predstavlja digitalni certifikat koji se sastoji od standardnog oblika podataka. Podaci identificiraju vlasnika i verificirani su od treće strane te se koriste za provjeru autentičnosti kod podnositelja zahtjeva za vanjsku autentifikaciju [10].

Treća se strana definira kao certifikat autoritet i poznat je pristupnoj točki i podnositelju zahtjeva te se koristi za prosljeđivanje javnog ključa i dešifriranje poruka poslanih iz pristupne točke [10]. Ako je podnositelj zahtijeva zadovoljan identitetom pristupne točke između njih se uspostavlja TLS tunel koji se koristi za razmjenu enkripcijskog ključa. Klijent nema niti samostalno koristi certifikat te mora biti autentificiran pomoću TLS tunela [10].

EAP Transport Layer Security (EAPTLS) zahtijeva certifikate na svakoj pristupnoj točki i klijentu odnosno klijentskom uređaju. Koristeći navedenu metodu pristupna točka i podnositelj zahtjeva razmjenjuju certifikate i međusobno se autentificiraju. EAPTLS se smatra jednom od najsigurnijih i najdostupnijih metoda bežične autentifikacije [10].

Kada je potrebno instalirati certifikate na većem broju uređaja koristi se sustav (*Public Key Infrastructure* – PKI) koji bi mogao sigurno i učinkovito isporučiti certifikate te ih opozvati kada klijent ili korisnik više ne bi trebao imati pristup mreži što obično za sobom povlači i procese postavljanja ili izgradnje autentifikacijskih centara [10].

6.2. Bežične metode privatnosti i integriteta

Izvorni 802.11 standard koristio je isključivo WEP metodu za zaštitu podataka. WEP je kao metoda postao kompromitiran te se ne preporučuje njegova uporaba. Nekorištenje WEP-a dovelo je do razvoja novih metoda koje će osigurati cjelovitost i privatnost podataka tijekom prijenosa medijem. Prema [10] to su sljedeće metode:

- *Temporal key integrity protocol* (TKIP) metoda – sastoji se od sigurnosne značajke MIC, vremenske oznake, MAC adrese pošiljatelja, brojača TKIP sekvenci, algoritma za miješanje ključeva i duljeg vektora inicijalizacije.
- *Counter/CBC-MAC Protocol* (CCMP) – sastoji se od dva algoritma, *Advanced Encryption Standard* (AES) i *Cipher block chaining message authentication code* (CBC-MAC). AES predstavlja svjetski opće prihvaćeni, javno dostupan te najsigurniji algoritam. Kako bi koristili CCMP metodu korisnički uređaj i pristupna točka moraju sadržavati sklopovsku podršku za navedene algoritme.
- *Galois/Counter Mode Protocol* (GCMP) je robusnija metoda u odnosu na CCMP, također se sastoji od dva algoritma, AES-a i *Galois Message Authentication Code*

(GMAC) koji se koristi za provjeru integriteta poruka. Navedena se metoda koristi u WPA 3 [10].

Zaštićeni WI – Fi pristup (WPA) razvijen je od strane Wi-Fi Alliance, neprofitne udruge bežične industrije koja olakšava korisniku konfiguriranje bežične sigurnosti u WLAN-u. Udruga je prema [10] razvila tri verzije WPA pristupa:

- WPA temeljio se na dijelovima 802.11i standarda te je podržavao 802.1x autentifikaciju, TKIP i metodu za dinamičko upravljanje ključem šifriranja.
- WPA2 stupio je na snagu ratificiranjem 802.11 standarda što je postalo njegov temelj. WPA2 osnovu su činili AES i CCMP algoritmi.
- WPA3 predstavljen je 2018. godine kao zamjena za WPA2. WPA3 i nudi jače šifriranje kombinirajući AES i GCMP protokol. *Protected Management Frames* (PMF) osiguravaju upravljanje 802.11 okvirima između pristupne točke i klijenata u svrhu sprječavanja zlonamjernih aktivnosti koje bi ometala rad BSS-a. Tablicom 3. prikazana je usporedba navedenih standarda [10].

Tablica 3. Usporedba načina autentifikacije

Autentifikacija i šifriranje	WPA	WPA2	WPA3*
Autentifikacija sa PSK	Da	Da	Da
Autentifikacija sa 802.1x	Da	Da	Da
Šifriranje i MIC sa TKIP	Da	Ne	Ne
Šifriranje i MIC sa AES i CCMP	Da	Da	Ne
Šifriranje i MIC sa AES i GCMP	Ne	Ne	Da

Izvor:[10]

Iz tablice se vidi da sve verzije WPA podržavaju ili PSK ili 802.1x . Navedeni standardni su poznati pod nazivima osobni i poslovni način rada [10]. U osobnom načinu rada niz ključeva se konfigurira ili dijeli svakom klijentu i pristupnoj točki prije nego se klijenti spoje na bežičnu mrežu. Klijenti i AP-ovi koriste četverosmjernu proceduru rukovanja. Četverosmjerna procedura rukovanja koristi niz unaprijed podijeljenih ključeva i razmjenu ključeva za šifriranje koji se mogu otvoreno razmjenjivati [10].

Poslije završetka procesa pristupna točka može autentificirati klijenta te oni međusobno mogu osigurati poslane podatkovne okvire. Načini WPA i WPA2 i dalje ne mogu spriječiti zlonamjernog korisnika u prisluškivanju. Zlonamjerni korisnik može presresti četverostruko rukovanje između klijenta i pristupne točke te koristiti presreteni rječnik za automatizirano pogađanje PSK-a. U slučaju da je napad uspješno izvršen zlonamjerni korisnik se može predstaviti kao legitimni korisnik.

WPA3 koristeći metodu *Simultaneous Authentication of Equals* (SAE) omogućuje ravnopravan autentifikacijski odnos između klijenta i pristupne točke pri čemu svaki od njih može pokrenuti proces autentifikacije. U slučaju da je lozinka ili ključ kompromitiran WPA3 ima opciju *forward secrecy* čime je onemogućeno napadačima korištenje presretenih ključeva za dešifriranje [10].

7. Zaključak

Bežična LAN mreža je neizostavni dio svakodnevnog života većine ljudi ponajviše iz razloga što korisnicima omogućuju veću mobilnost, brzu i jednostavnu implementaciju. Informacije se u bežičnoj mreži prenose pomoću radiovalova, a sama mreža se sastoji od pristupne točke (koja sadrži antenu) i terminalnih uređaja. CISCO bežična mreža uspostavlja se povezivanjem terminalnog uređaja i pristupne točke koja se ovisno o potrebi pokrivanja prostora može konfigurirati u *root, client, bridge* ili *repeater* načinu rada. Svaka pristupna točka određena je SSID-jem i BSSID-jem. Tehnike proširenog spektra omogućuju većem broju korisnika korištenje istog medija za prijenos signala, a da pri tome ne smetaju jedni drugima što je glavna prednost bežičnih mreža.

Bežične mreže se sastoje od više manjih dijelova međusobno povezanih u smislenu cjelinu pa tako svaka pristupna točka nudi svoj osnovni skup usluga i oglašava se prema terminalnim uređajima u blizini. Pristupna točka povezuje se na prospojničku infrastrukturu i na taj način se proširuje osnovni skup usluga i omogućuje međusobno povezivanje pristupnih točaka koje se nalaze na različitim lokacijama unutar nekog objekta. Na kraju svega, distribucijski sustav kao zadnji dio u bežičnoj mreži povezuje uređaje koji nisu spojeni na istu pristupnu točku.

CISCO bežična mreža ovisno o vrsti pristupne točke razlikuje tri vrste arhitekture. Autonomna pristupna točka arhitektura je koja povezuje korisnika s jednim kanalom, odnosno jednim BSS-om. *Cloud-based* arhitektura se uspostavlja pomoću programa CISCO Meraki. Navedeni program automatski konfigurira svaku pristupnu točku o čemu obavještava korisnika. *Split-MAC* arhitektura dijeli pristupnu točku na dva dijela: WLC i LAC.

LAC je odgovoran za autorizaciju korisnika, upravljanje sigurnosnim postavkama i slično te je upravljan od strane WLC-a. Svaki LAC mora biti povezan CAPWAP tunelom s WLC-om. Od svih navedenih arhitektura *Split-MAC* arhitektura omogućuje najjednostavnije upravljanje i najveću raznolikost po pitanju veličine mreža budući da vrsta WLC-a određuje broj klijenata koji se mogu povezati.

Većina današnjih uređaja svoj rad bazira u 2,4 GHz pojasu čija širina kanala može biti 20 ili 40 MHz. Analiza novijih trendova pokazala je rast korištenja uređaja u 5 GHz pojasu zbog većih kapaciteta i brzina prijenosa. Antena koja je sadržana u pristupnoj točki definira područje rada. S obzirom na način rada, razlikuju se *ad-hoc* i infrastrukturne mreže.

Korisnik se, nakon što se poveže na pristupnu točku, mora autentificirati kako bi mogao koristiti bežične usluge. Postoji više metoda autentifikacije. Danas se najviše koriste PEAP, EAP i EPTLS. Sigurnost često uz sebe veže i pojmove integriteta i cjelovitosti pa se stoga, kako bi se osigurala cjelovitost i integritet poruke, koriste većinom WEP, WEP2 i WEP3 protokoli. Nakon autentifikacije, korisnik (projektant) putem *web* poslužitelja može uspostaviti bežičnu mrežu sa željenim parametrima što je prikazano u poglavlju 5.

Popis literature

[1] Horak R. *Telecommunications and Data Communications Handbook*, Wiley Interscience, 2007.

[2] B. Jeren, P. Pale *WLAN*, Fakultet elektrotehnike i računarstva, Sveučilište u Zagrebu, 2008 Preuzeto s: http://spvp.zesoi.fer.hr/predavanja%202008/WE_skripta.pdf [Pristupljeno: 28.travnja.2022.]

[3] Muštra M. Auditorna predavanja iz kolegija Mobilni komunikacijski sustavi, Fakultet prometnih znanosti Sveučilišta u Zagrebu, 2022. Preuzeto s: https://moodle.srce.hr/2021-2022/course/view.php?id=97607 [Pristupljeno: 30.travnja.2022.]

[4] James F. Kurose, Keith W. Ross: *Computer Networing*, A Top-Down Approach, 2013.

[5] Forenbacher, I.: Auditorna predavanja iz Arhitekture telekomunikacijske mreže, Fakultet Prometnih Znanosti, Zagreb, 2015.

[6] Mrvelj, Š.: Auditorna predavanja iz Tehnologije telekomunikacijske mreže, Fakultet prometnih znanosti, Zagreb, 2014.

[7] Forenbacher, I.: Auditorna predavanja iz kolegija Komutacijski procesi i sustavi, Fakultet Prometnih Znanosti, Zagreb, 2015.

[8] Aries Institute of Technology, Inc.
Preuzeto s: http://www.aries.net/demos/Wireless/chapter04/chapter04_1.html [Pristupljeno: 15. svibnja.2022.]

[9] Conrad Preuzeto s: https://www.conrad.hr/p/edimax-ra21s-wlan-pristupna-tocka-26-gbits-24-ghz-5-ghz-1491082 [Pristupljeno 16.lipnja.2022.]

[10] Odom W., *CCNA 200-301 Official Cert Guide, Volume 1*, Cisco Press, 2020.

[11] Technet.microsoft
Preuzeto s: https://technet.microsoft.com/en-us/library/cc757419(v=ws.10).aspx [Pristupljeno: 25. lipnja 2022.]

[12] Wigmore Ivy *Beacon*
Preuzeto s :https://www.techtarget.com/whatis/definition/beacon-proximity-beacon [Pristupljeno: 12. lipnja 2022.]

Popis kratica

AP (Access Point) pristupna točka
BSS (Basic service set) osnovni skup usluga
BSSID (basic service set identifier) identifikator pristupne točke
CAPWAP (Control and Provisioning of Wireless Access Points) protokol
CCMP (Counter Mode with Cipher Block Chaining Message Authentical Code Protocol)
CLI (Command line interface) komandno sučelje
DFS (Dynamic Frequency Selection) opcija za 5 GHz uređaje
DHCP (Dynamic Host Configuration Protocol) protokol za automatsku dodjelu IP adrese
DS (Distribution System) distribucijski sustav
DSSS (Direct Sequence Spread Spectrum) tehnika proširenog spektra
DS/FFH (Hybrid system) tehnika proširenog spektra
DTLS (Datagram Transport Layer Security) komunikacijski protokol
EAP (Extensible Authentication Protocol) autentifikacijski protokol
EAP FAST(Flexible Authentication via Secure Tunneling) autentifikacijski protokol
EM (electromagnetic) elektromagnetski val, spektar…
ESS (Extended Service Set) proširenI skup usluga
FHSS (Frequency Hopping Spread Spectrum) tehnika proširenog spektra
GMAC (Galois Message Authentication Code)
GUI (Graphical user interface) grafičko sučelje
HTTP (Hypertext Transfer Protocol)
ISM (industrial, scientific and medical band) industrijsko, znanstveno i medicinskim pojas
IBSS (Independent Basic Service Set) neovisni skup usluga
LAN (Local area network) lokalna mreža
LAP (Lightweight access point) lagana pristupna točka
LEAP (Lightweight EAP) autentifikacijska metoda
PEAP (Protected Extensible Authentication Protocol) zaštićeni EAP
PAC (Protected access credential) pristupne vjerodajnice
PMF (Protected Management Frames) zaštićeni upravljački okviri
SAE (Simultaneous Authentication of Equals) metoda korištena od strane WPA 3
SNMP (Simple Network Management Protocol) protokol aplikacijskog sloja u OSI modelu.
SSID (Service set identifier) naziv pristupne točke
STA (Station) terminalni uređaj
U-NII (Unlicensed National Information Infrastructure) nelicencirana nacionalna informacijska infrastruktur**a**
VLAN (Virtual LAN) logička mreža
QOS (Quality of service) kvaliteta usluge
WAN (World area network) širokopojasna mreža
WEP (Wireless Encryption Protocol)
WGB(workout group bridge) most radne grupe
WLAN (Wireless LAN) bežični pristup lokalnoj mreži
WPA (Wi-Fi Protected Access)

Popis slika

Popis tablica

Sveučilište u Zagrebu
Fakultet prometnih znanosti
Vukelićeva 4, 10000 Zagreb

IZJAVA O AKADEMSKOJ ČESTITOSTI I SUGLASNOSTI

Izjavljujem i svojim potpisom potvrđujem da je završni rad isključivo rezultat mojega vlastitog rada koji se temelji na mojim istraživanjima i oslanja se na objavljenu literaturu, a što pokazuju upotrijebljene bilješke i bibliografija. Izjavljujem da nijedan dio rada nije napisan na nedopušten način, odnosno da je prepisan iz necitiranog rada te da nijedan dio rada ne krši bilo čija autorska prava. Izjavljujem, također, da nijedan dio rada nije iskorišten za bilo koji drugi rad u bilo kojoj drugoj visokoškolskoj, znanstvenoj ili obrazovnoj ustanovi.

Svojim potpisom potvrđujem i dajem suglasnost za javnu objavu završnog/diplomskog rada pod naslovom Arhitektura CISCO bežične LAN mreže , u Nacionalni repozitorij završnih i diplomskih radova ZIR.

Student/ica:

U Zagrebu, 04.09.2022.

Matej Kovač
(ime i prezime, *potpis*)