ՀՀ ԿՐԹՈՒԹՅԱՆ,ԳԻՏՈՒԹՅԱՆ,ՄՇԱԿՈՒՅԹԻ ԵՎ ՍՊՈՐՏԻ ՆԱԽԱՐԱՐՈՒԹՅՈՒՆ

«Երևանի Լեոյի անվան հ. 65 ավագ դպրոց» ՊՈԱԿ

Թեմա՝ WLAN (WIRELESS LOCAL AREA NETWORK) ՏԵԽՆՈԼՈԳԻԱՆ, ՈՐՊԵՍ ՈՒՍՈՒՄՆԱԿԱՆ ՀԱՍՏԱՏՈՒԹՅՈՒՆՆԵՐԻ ՆԵՐՔԻՆ ԱՆԼԱՐ ՑԱՆՑԵՐԻ ԱՊԱՀՈՎՄԱՆ ՄԻՋՈՑ

ՀԵՏԱԶՈՏԱԿԱՆ ԱՇԽԱՏԱՆՔ

«Զորաշենի միջնակարգ դպրոց»ՊՈԱԿ-ի մաթեմատիկայի ուսուցիչ՝

Ա.Ջ.Երվանդյան

ԳՅՈՒՄՐԻ 2023

ՀԱՄԱՌՈՏԱԳԻՐ

Հայերեն՝ <<WLAN (WIRELESS LOCAL AREA NETWORK) ՏԵԽՆՈԼՈԳԻԱՆ, ՈՐՊԵՍ ՈՒՍՈՒՄՆԱԿԱՆ ՀԱՍՏԱՏՈՒԹՅՈՒՆՆԵՐԻ ՆԵՐՔԻՆ ԱՆԼԱՐ ՑԱՆՑԵՐԻ ԱՊԱՀՈՎՄԱՆ ՄԻՋՈՑ>>

Անգլերեն՝ <<WLAN TECHNOLOGY (WIRELESS LOCAL AREA NETWORK), AS MEANS OF PROVIDING INTERNAL WIRELESS NETWORKS OF EDUCATIONAL INSTITUTIONS>>

Ռուսերեն՝ <<ТЕХНОЛОГИЯ WLAN (WIRELESS LOCAL AREA NETWORK), КАК СРЕДСТВА ОБЕСПЕЧЕНИЯ ВНУТРЕННИХ БЕСПРОВОДНЫХ СЕТЕЙ УЧЕБНЫХ ЗАВЕДЕНИЙ>>

Շարադրանք

Աշխատանքը նվիրված է WLAN (WIRELESS LOCAL AREA NETWORK) Տեխնոլոգիան, որպես ուսումնական հաստատություններ ներքին անլար ցանցերի ապահովման միջոց։Այս աշխատանիքի արդյունքները կարող են կիրառվել շատ այլ ուսումնական հաստատություններում։

Բովանդակություն

Ներածություն

Հետազոտական աշխատանքի արդիականությունը: Ժամանակակից աշխարհում լայնորեն տարածվում են ցանցային տեխնոլոգիաները, որոնք իրենց կիրառությունն են գտնում տարբեր գործընթացներում: Այսօր անհնարին է պատկերացնել որևէ հաղորդակցություն առանց ցանցային տեխնոլոգիաների կիրառման: Մի կողմից օրեցօր աճում են ցանցային ենթակառուցվածքները, մյուս կողմից էլ աճող ցանցային ենթակառուցվածքները իրենց հերթին բերում են հսակայական հաղորդալարերի օգտագործման, ինչն արդյունավետության տեսանկյունից հիմնախնդրային է: Այս ամենին օգնության են գալիս WLAN տեխնոլոգիաները, որոնք տեղեկույթը փոխանցում են մի կետից մյուսն առանց հաղորդալարերի օգտագործման:

Արդի կրթական համակարգը նույնպես անմասն չէ այս փոփոխություններից: Մասնավորապես, կրթական գործընթացներում աճում են հեռավար տեխնոլոգիաների կիրառման հնարավորություններն ու անհրաժեշտություն է առաջանում ուսումնական գործընթացում կիրառել անլար միացմամբ սարքավորումներ (նոութբուք, սմարթֆոն, պլանշետ և այլն): Ինչն էլ իր հերթին խնդիր է առաջադրում նախագծել անլար ցանցային ենթակառուցվածքներ, որոնք հանարվորություն կտան դասավանդողներին ու սովորողներին կիրառելու հեռավար ուսուցման համակարգերը ամենօրյա գործունեության մեջ: Վերը նշված հանգամանքներն էլ հիմնավորում են մեր թեմայի արդիականությունը:

Աշխատանքի **նպատակն է** նախագծել Cisco Packet Tracer ցանցային սիմուլյատորի միջավայրում ուսումնական հաստատության անլար լոկալ ցանց:

Հետազոտական աշխատանքի առաջադիր խնդիրներն են.

1. ուսումնասիրել անլար լոկալ ցանցերի տեխնոլոգիաներն ու ստանդարտները
2. նկարագրել անլար լոկալ ցանցերի ենթակառուցվածքների կոմպոնոնտները
3. բացահայտել անլար լոկալ ցանցերում ալիքների վերահսկման մեխանիզմները
4. նկարագրել անլար լոկալ ցանցերի անվտանգության ապահովման մեխանիզմները

5. նախագծել ուսումնական հաստատության անլար լոկալ ցանց Cisco Packet Tracer միջավայրում։

Աշխատանքի կառուցվածքը: Աշխատանքը կազմված է ներածությունից, երեք գլուխներից՝ իրենց համապատասխան պարագրաֆներով, եզրակացությունից, օգտագործված գրականության ցանկից։ Աշխատանքը շարադրված է 34 համակարգչային էջի վրա։

ԳԼՈՒԽ 1.WLAN տեխնոլոգիայի ընդհանուր նկարագիրը

1.1 Անլար ցանցերի տեսակներն ու անլար տեխնոլոգիաները

Անլար ցանցերը հիմնված են էլեկտրատեխնիկայի և էլեկտրոնիկայի ճարտարագետների ինստիտուտի (IEEE) ստանդարտների վրա և կարող են բաժանվել չորս հիմնական տեսակներիWPAN, WLAN, WMAN և WWAN:

Անլար անհատական ցանցերը (WPAN) օգտագործում են ցածր հզորության հաղորդիչներ՝ մոտ գործող ցանցերի համար, սովորաբար 20-ից մինչև 30 ոտնաչափ (6-ից 9 մետր): Bluetooth-ի և ZigBee-ի վրա հիմնված սարքերը սովորաբար օգտագործվում են WPAN-ում: WPAN-ը հիմնված է 802.15 ստանդարտի և 2.4 GHz հաճախականության վրա:

Անլար լոկալ ցանցեր (WLAN) - հաղորդիչներ է օգտագործում միջին չափի ցանց ապահովելու համար, սովորաբար մինչև 100 մետրի հասնող: Անլար տեղական ցանցերը հարմար են տանը, գրասենյակում և նույնիսկ դպրոցում օգտագործելու համար: WLAN ցանցերը հիմնված են 802.11 ստանդարտի և 2,4 ԳՀց կամ 5 ԳՀց հաճախականության վրա:

Անլար MAN (WMAN) - օգտագործում է հաղորդիչները մեծ աշխարհագրական գոտում անլար կապի ծառայություններ մատուցելու համար: WMAN-ը հարմար է մայրաքաղաքի կամ կոնկրետ տարածքի անլար հասանելիության ապահովման համար: WMAN-ն օգտագործում է որոշակի լիցենզավորված հաճախականություններ

Անլար գլոբալ ցանցեր (WWANs) - օգտագործում է հաղորդիչները լայնածավալ աշխարհագրական տարածքում՝ ծածկույթի ապահովման համար: WWAN-ը հարմար է ազգային և գլոբալ հաղորդակցության համար: WWAN-ը նաև օգտագործում է որոշակի լիցենզավորված հաճախականություններ:

Անլար տեխնոլոգիաներ

Անլար տեխնոլոգիաներում տվյալների ուղարկման և ընդունման համար օգտագործվում են ռադիոհաճախականությունների չլիցենզավորված շերտեր:

Չլիցենզավորված շերտերը հասանելի են բոլոր նրանց, ովքեր օգտագործում են անլար երթուղիչ ունեցող և անլար տեխնոլոգիա ապահովող սարք:

Bluetooth - IEEE 802.15 WPAN ստանդարտ, որն օգտագործում է սարքերի կցորդման գործընթացը, մինչև 100 մ հեռավորության վրա կապի համար (300 ոտնաչափ): Այն կարելի է գտնել «խելացի տուն» սարքերում, ձայնային միացումներում, մեքենաներում և այլ սարքերում, որոնք միացում են պահանջում կարճ հեռավորության վրա: Գոյություն ունեն Bluetooth –ի երկու տեսակ՝Bluetooth Low Energy (BLE) - ապահովում է մի քանի ցանցային տեխնոլոգիաներ, ներառյալ բջջային տոպոլոգիան լայնածավալ ցանցային սարքերի համար:

Bluetooth Basic Rate/Enhanced Rate (BR/EDR) - ապահովում է «կետ-կետ» տոպոլոգիա և օպտիմիզացված է ձայնի հոսքային հաղորդման համար:

WiMAX (միկրոալիքային հասանելիության համաշխարհային Համատեղելիություն) - WiMAX-ը DSL-ի և մալուխի հետ մրցակցող լայնաշերտ լարային ինտերնետ կապերի այլընտրանք է: Այնուամենայնիվ, այն սովորաբար օգտագործվում է այն տարածքներում, որոնք դեռևս միացված չեն DSL-ին կամ մալուխային մատակարարին: Սա IEEE 802.16 WWAN ստանդարտ է, որը ապահովում է մինչև 30 մղոն (50 կմ) հեռավորության վրա բարձր արագությամբ անլար լայնաշերտ հասանելիություն: WiMAX ցանցը գործում է Wi-Fi ցանցի նման, բայց ավելի բարձր արագությամբ, մեծ հեռավորություններով և ավելի մեծ թվով օգտագործողների համար: Այն օգտագործում է WiMAX աշտարակների ցանցը, որը նման է բջջային հեռախոսակապի ցանցի աշտարակներին: WiMAX հաղորդիչները և բջջային հաղորդիչները կարող են համատեղ օգտագործել մեկ աշտարակի տարածություն:

Բջջային լայնաշերտ կապ. - 4G/5G բջջային կապերը՝ անլար բջջային ցանցեր են, որոնք հիմնականում օգտագործվում են բջջային հեռախոսների կողմից, սակայն կարող են օգտագործվել մեքենաներում, պլանշետներում և նոութբուքներում: Բջջային ցանցերը բազմակի հասանելիություն ունեցող ցանցեր են, որոնց միջոցով իրականացվում է ինչպես տվյալների, այնպես էլ ձայնի փոխանցում: Բջջային կայքը

ստեղծվում է բջջային աշտարակի կողմից, որն այդ շրջանում ազդանշաններ է փոխանցում: Միակցվող բջջային կայքերը ձևավորում են բջջային ցանց: Բջջային ցանցերի երկու տեսակներն են բջջային կապի Գլոբալ համակարգը (GSM) և Բազմականգառի հասանելիությունը՝ կոդային բաժանմամբ (CDMA): GSM-ը ճանաչում է գտել ամբողջ աշխարհում, իսկ CDMA հիմնականում օգտագործվում է ԱՄՆ-ում:

4-րդ սերնդի GSM ցանցը (4G) հանդիսանում է ընթացիկ շարժական ցանց: 4G-ն ապահովում է արագություն, որը 10 անգամ ավելի բարձր է, քան նախորդ 3G ցանցերում: Նոր 5G-ն խոստանում է 100 անգամ ավելի բարձր արագություն ապահովել, քան 4G-ն և ցանցին միացնել ավելի շատ սարքեր, քան երևէ:

Արբանյակային լայնաշերտ կապ՝ ապահովում է ցանցային հասանելիություն հեռավոր օբյեկտներին՝ ուղղորդված արբանյակային ալեհավաքի օգտագործման միջոցով, որը կենտրոնացած է Երկրի ուղեծրում որոշակի գեոստացիոնար արբանյակի վրա: Որպես կանոն, այս տեխնոլոգիան տարբերվում է ավելի բարձր արժեքով և պահանջում է ապահովել ուղիղ տեսանելիություն: Սովորաբար այն ավելի թանկ է և պահանջում է հստակ ակնարկ: Որպես կանոն, այն օգտագործվում է գյուղական տներում և ձեռնարկություններում, որտեղ չկա մալուխ և DSL:

1.2 802.11 ստանդարտներն ու ռադիոհաճախականությունները

Անլար կապի աշխարհը հսկայական է: Այնուամենայնիվ, որոշակի մասնագիտական հմտությունների համար, մենք ուզում ենք կենտրոնանալ Wi-Fi - կոնկրետ ասպեկտների վրա: Ավելի լավ է սկսել IEEE 802.11 WLAN ստանդարտներից: Այս ստանդարտները սահմանում են, թե ինչպես են ռադիոհաճախականությունները օգտագործվում անլար ալիքների համար: Ստանդարտների մեծ մասում նշված է, որ

անլար սարքերն ունեն մեկ ալեհավաք՝ նշված ռադիոհաճախականության (2.4ԳՀց կամ 5ԳՀց) վրա անլար ազդանշանների փոխանցման և ընդունման համար: Նոր չափանիշներից որոշները, որոնք փոխանցում և ընդունում են ավելի բարձր արագությամբ, պահանջում են, որ մուտքի կետերը (AP) և անլար հաճախորդները ունենան մի քանի ալեհավաքներ, որոնք օգտագործում են բազմակի մուտքի և բազմակի ելքի տեխնոլոգիա (MIMO): MIMO-ն օգտագործում է մի քանի ալեհավաքներ որպես հաղորդիչ և ընդունիչ՝ կապի առանձնահատկությունները բարելավելու նպատակկով: Տեխնոլոգիան ապահովում է մինչև չորս ալեհավաք:

Վերջին տարիներին մշակվել են IEEE 802.11 ստանդարտի մի շարք իրագործումներ, որոնք ցուցադրվում են նկարում: Աղյուսակում նշված են այդ ստանդարտները:

Աղյուսակ 1.

IEEE WLAN ստանդարտներ	Ռադիոհաճախականություն, ՌՀ	Նկարագրություն
802.11	2,4 ԳՀց	• մինչև 2 Մբ/վ արագություն
802.11a	5 ԳՀց	• մինչև 5 Մբ/վ արագություն • ծածկույթի փոքր տարածք • քիչ արդյունավետ է շինարարական կառուցվածք ներթափանցելիս • համատեղելի չէ 802.11 b-ի և 802.11 g-ի հետ
802.11b	2,4 ԳՀց	• մինչև 11Մբ/վ արագություն • ծածկույթի ավեի մեծ տարածք կամ 802.11a • ավելի լավ է ներթափանցում շինարարական կառուցվածքմեր
802.11g	2,4 ԳՀց	• մինչև 54 Մբ/վ արագություն • 802.11 b-ի հետ հակադարձ համատեղելիությունը նվազեցված թողունակությամբ

Աղյուսակ 1.

IEEE WLAN ստանդարտներ	Ռադիոհաճախականություն, ՌՀ	Նկարագրություն
802.11n	2,4 ԳՀց և 5 ԳՀց	• տվյալների փոխանցման արագությունը տատանվում է 150-ից մինչև 600 Մբիթ / վ-ից մինչև 70 մ (230 ֆուտ) • Մուտքի կետերի եւ անլար հաճախորդների համար պահանջվում են մի քանի ալեհավաքներ, որոնք օգտագործում են MIMO տեխնոլոգիան • Այս ստանդարտը ունի հակառակ համատեղելիությունը 802.11 a/b / g ստանդարտների սարքերի հետ՝ տվյալների փոխանցման արագության սահմանափակմամբ
802.11ac	5 ԳՀց	• ապահովում է տվյալների փոխանցման արագությունը 450 Մբիթ / վ-ից մինչև 1,3 Գբիթ / վ (1300 Մբիթ/վ) MIMO տեխնոլոգիայի օգտագործմամբ • Ապահովում է մինչև 8 ալեհավաք • հակառակ համատեղելիություն 802.11 a / n սարքերի հետ, տվյալների փոխանցման արագության սահմանափակմամբ
802.11ax	2,4 ԳՀց և 5 ԳՀց	• թողարկվել է 2019 թվականին՝ վերջին ստանդարտն է • նաև հայտնի է որպես բարձր արդյունավետ անլար (HEW) • տվյալների փոխանցման ավելի բարձր արագություն • ալիքի թողունակության հնարավորությունների բարձրացում • ապահովում է մեծ թվով միացված սարքեր • էներգիայի սպառման օպտիմալացում

Ռադիոհաճախականություն: Բոլոր անլար սարքերը աշխատում են էլեկտրամագնիսական սպեկտրի ռադիոալիքների տիրույթում: WLAN ցանցերն աշխատում են 2,4 ԳՀց հաճախականությունների տիրույթում և 5 ԳՀց տիրույթում: Անլար LAN սարքերը ունեն հաղորդիչներ և ընդունիչներ, որոնք հարմարեցված են ռադիո ալիքների տիրույթի կոնկրետ հաճախականությունների վրա, ինչպես ցույց է

տրված նկարում: Մասնավորապես, 802.11 անլար LAN ստանդարտի համար առանձնանում են հետեւյալ հաճախականությունները՝

- 2.4 ԳՀց (UHF) - 802.11b/g/n/ax
- 5 ԳՀց (SHF) - 802.11a/n/ac/ax

1.3 Անլար ցանցային ադապտորներն ու երթուղիչները

Անլար ցանցային ադապտերներ: Անլար տեղակայման համար պահանջվում է առնվազն երկու սարք, որոնք ունեն ռադիոհաղորդիչ և ռադիոընդունիչ, որոնք կազմաձևվված են նույն ռադիոհաճախականություններին:

- Վերջնակետային սարքեր՝ հագեցած անլար ցանցային ադապտերների կողմից
- Ցանցային սարք, ինչպիսիք են անլար երթուղղիչը կամ անլար մուտքի կետը

Անլար կապի համար նոութբուքները, պլանշետները, սմարթֆոնները և նույնիսկ նորագույն մեքենաները հագեցած են ներկառուցված անլար ցանցային քարտերով, որոնք ներառում են ռադիոհաղորդիչ/ընդունիչ: Սակայն, եթե սարքը չունի ներկառուցված անլար ցանցային ադապտեր, դուք կարող եք օգտագործել անլար USB ադապտեր, ինչպես ցույց է տրված նկարում:

Շատ անլար սարքեր չունեն տեսանելի ալեհավաքներ. Դրանք ներդրված են սմարթֆոններում, նոութբուքներում և անլար տնային երթուղիչներում:

Տնային անլար երթուղիչ: Ենթակառուցվածքի սարքի տեսակը, որի հետ վերջնական սարքը կապվում և վավերացվում է, կախված է WLAN-ի չափից և պահանջներից:

Օրինակ, տնային օգտագործողը սովորաբար կապում է անլար սարքերը փոքր անլար երթուղիչի հետ, ինչպես ցույց է տրված նկարում: Անլար երթուղիչը ծառայում է որպես:

- **Մուտքի կետ** - ապահովում է 802.11 a/b/g/n/ac անլար մուտք
- **Կարգավորիչ** - ապահովում է քառաստիճան լիարժեք Ethernet-կարգավորիչ 10/100/1000-ը՝ լարային սարքերի միացման համար

- **Երթուղիչ** - ապահովում է կանխադրված դարպաս՝ ինտերնետի նման այլ ցանցային ենթակառուցվածքներին միանալու համար.

Անլար երթուղիչը սովորաբար օգտագործվում է որպես փոքր ձեռնարկությունների կամ բնակելի տարածքների անլար մուտքի սարք: Անլար երթուղիչը հայտարարում է իր անլար ծառայությունների մասին՝ ուղարկելով ազդանշաններ, որոնք պարունակում են ընդհանուր ծառայությունների id (SSID): Սարքերը հայտնաբերում են SSID-ն և փորձում է միացնել ու վավերացնել այն՝ լոկալ ցանց և ինտերնետ մուտք գործելու համար:

Անլար երթուղիչները նաև ապահովում են ընդարձակ առանձնահատկություններ, ինչպիսիք են բարձր արագությամբ մուտքը, հոսքային վիդեո ապահովում, IPv6 հասցեավորում, սպասարկման որակ (QoS), սպասարկող ծրագրային կարգավորումներ և USB պորտեր տպիչների կամ շարժական կրիչների միացման համար:

Բացի այդ, տնային օգտագործողները, ովքեր ցանկանում են ընդլայնել իրենց ցանցային ծառայությունները, կարող են իրականացնել Wi-Fi տիրույթի ընդլայնում: Սարքը կարող է միացված լինել անլար կապի ընդլայնիչին, ինչը մեծացնում է անլար երթուղիչի հետ տվյալների փոխանակման արագությունը:

1.4 Անլար հասանելիության կետերն (Acces Point) և դրանց կատեգորիաները

Անլար մուտքի կետերը:

Չնայած նրան, որ ընդլայնիչների կարգավորումները բավականին հեշտ են, լավագույն լուծումը կլինի մեկ այլ անլար մուտքի կետի տեղադրումը: Անլար հաճախորդները օգտագործում են իրենց անլար ցանցային ադապտերները՝ իրենց SSID ID-ն հայտարարած մոտակա մուտքի կետերը հայտնաբերելու համար: Այնուհետև հաճախորդները փորձում են կապվել և վավերացվել AP-ի հետ:

Վավերականությունը անցնելուց հետո անլար ցանցի օգտատերերը մուտքի իրավունք են ստանում ցանցի ռեսուրսներին։

AP կատեգորիաներ

Մուտքի կետերը կարող են լինել ինքնավար և կառավարվող։

Ինքնավար մուտքի կետեր

Սրանք ինքնավար սարքեր են, որոնք կազմաձևված են՝ հրամանի տող ինտերֆեյսի կամ գրաֆիկական ինտերֆեյսի միջոցով, ինչպես ցույց է տրված նկարում: Ինքնավար AP-ն օգտակար է այն իրավիճակներում, երբ կազմակերպությունում պահանջվում է միայն AP զույգ։ Տնային երթուղիչը առանձին մուտքի կետի օրինակ է, քանի որ մուտքի կետի ամբողջ կոնֆիգուրացիան գտնվում է սարքի վրա։ Անլար ցանցի ռեսուրսների նկատմամբ պահանջարկի մեծացմամբ կարող է առաջանալ հասանելիության կետերի մեծ քանակության անհրաժեշտություն։ Յուրաքանչյուր մուտքի կետ կաշխատի անկախ այլ մուտքի կետերից, և յուրաքանչյուր մուտքի կետ կպահանջի ձեռքով կարգավորումներ և վերահսկում: Շատ մուտքի կետերի կարգավորման դեպքում, սա բավականին դժվար կլիներ։

AP՝ վերահսկչի վրա հիմնված

Այս սարքերը չեն պահանջում նախնական կարգավորում և հաճախ կոչվում են հեշտացված մուտքի կետեր (LAP): LAP-ն օգտագործում է հեշտացված մուտքի կետի արձանագրությունը (LWAPP) WLAN (WLC) վերահսկիչի հետ կապի համար, ինչպես ցույց է տրված ստորև նկարում: Վերահսկիչի կողմից կառավարվող մուտքի կետերը խորհուրդ է տրվում օգտագործել այն դեպքերում, երբ ցանցը պահանջում է բազմաթիվ մուտքի կետեր: Շատ AP-ների ավելացման պատճառով, յուրաքանչյուր AP ավտոմատ կերպով կարգավորվում և վերահսկվում է WLC-ի կողմից։

Ուշադրություն դարձրեք նկարին, որ WLC-ն ունի չորս պորտեր, որոնք միացված են կարգավորիչի ենթակառուցվածքին։ Այս չորս պորտերը կազմաձևված են որպես ալիքի ագրեգացման խումբ (LAG)՝ դրանք միասին միավորելու համար։ Ճիշտ այնպես, ինչպես աշխատում է EtherChannel-ը, LAG ապահովում է ծանրաբեռնվածությամ

բաշխում: Կարգավորիչի վրա գտնվող բոլոր պորտերը, որոնք կապված են WLC-ի հետ, պետք է տրանկինգ լինեն և կազմաձևվեն միացված EtherChannel հետ: Սակայն, LAG չի աշխատում ճիշտ այնպես, ինչպես EtherChannel-ը: WLC-ն չի ապահովում պորտերի ագրեգացման արձանագրություն (PaGP) կամ ալիքների ագրեգացման կառավարման արձանագրությունը (LACP):

Առաջին գլխի ամփոփում

Առաջին գլխում ուսումնասիրվում է WLAN x ստանդարտները, ինչպես նաև անլար երթուղիչների տեսակներն ու հասանելիության կետերի կատեգորիաները:

տեխնոլոգիայի հիմնարար գաղափարները: Ներկայացվում է անլար ցանցերի տեսակներն ու 802.11

ԳԼՈՒԽ 2. Անլար լոկալ ցանցերի աշխատանքի սկզբունքները

2.1 Անլար լոկալ ցանցերի տոպոլոգիաների 802.11 ռեժիմները

WLAN ցանցերը կարող են օգտագործել ցանցի տարբեր տոպոլոգիաներ: 802.11 ստանդարտը սահմանում է անլար ցանցի երկու հիմնական եղանակները՝ Ad hoc ռեժիմը և ենթակառուցվածքների ռեժիմը: Մոդեմը նույնպես ռեժիմ է, որը երբեմն օգտագործվում է արագ անլար մուտքի ապահովման համար:

Ad hoc ռեժիմ - Ad hoc ռեժիմն օգտագործվում է, երբ երկու սարքերը անլար ցանցում միացված են նույն կարգով (P2P), առանց մուտքի կետերի կամ անլար երթուղղիչների օգտագործման: Օրինակ կարող են ծառայել անլար հաճախորդները, որոնք ուղղակիորեն կապված են միմյանց Bluetooth-ի կամ Wi-Fi Direct-ի միջոցով: IEEE 802.11 ստանդարտը վերաբերում է հատուկ ցանցին որպես ծառայությունների անկախ բազային հավաքածու (IBSS):

Ենթակառուցվածքային ռեժիմն այն է, երբ անլար հաճախորդները միանում են անլար երթուղղիչի կամ մուտքի կետի միջոցով, օրինակ, WLAN-ում: Մուտքի կետերը միանում են ցանցային ենթակառուցվածքներին, օգտագործելով լարային բաշխման համակարգը, օրինակ, Ethernet-ը:

Բջջային հեռախոսի օգտագործումը, որպես ինտերնետ հասանելիության կետ - տվյալներին բջջային հասանելիություն ունեցող սմարթֆոնը կամ պլանշետը՝ միացված է անձնական մուտքի կետ ստեղծելու համար: Անլար մուտքի կետը, որպես կանոն, ժամանակավոր կարճաժամկետ լուծում է, որի շնորհիվ սմարթֆոնը կարող է ապահովել Wi-Fi-երթուղիչի անլար կապի ծառայություններ:

2.2 CAPWAP տեխնոլոգիայի աշխատանքի սկզբունքը

CAPWAP-ը ստանդարտ IEEE արձանագրություն է, որը թույլ է տալիս WLC-ին կառավարել բազմակի մուտքի կետերը և WLAN-ը: CAPWAP-ը նաև

պատասխանատու է AP-ի և WLC-ի միջև հաճախորդների տրաֆիկի տեղափոխման համար:

CAPWAP-ը հիմնված է LWAPP-ի վրա, սակայն ավելացնում է լրացուցիչ անվտանգություն՝ դեյտագրամմ (DTLS) տրանսպորտային մակարդակի պաշտպանությամբ: CAPWAP-ը թունելներ է ստեղծում օգտագործողի դեյտագրամմների (UDP) արձանագրության պորտերում: CAPWAP-ը կարող է աշխատել ինչպես IPv4-ի, այնպես էլ IPv6-ի միջոցով, ինչպես ցույց է տրված նկարում, սակայն լռելյայն օգտագործում է IPv4-ը:

IPv4-ը և IPv6-ը կարող են օգտագործել 5246 և 5247 UDP պորտերը: Սակայն, CAPWAP թունելները շրջանակի վերնագրում օգտագործում են տարբեր IP-արձանագրություններ: IPv4-ն օգտագործում է 17 IP արձանագրություն, և IPv6-ն օգտագործում է 136 IP արձանագրություն:

2.3 Անլար ցանցերում ալիքների վերահսկումը

Հաճախականության ալիքի հագեցվածությունը:

Անլար լոկալ ցանցի սարքերն ունեն հաղորդիչներ և ընդունիչներ, որոնք համապատասխանեցված են ռադիոալիքների տիրույթի կոնկրետ հաճախականություններին: Սովորաբար, որպես միջակայքեր՝ առանձնանում են հաճախականությունները: Նման միջակայքերը, ապա բաժանվում են փոքր միջակայքերի՝ ալիքների:

Եթե կոնկրետ ալիքի պահանջարկը շատ բարձր է, այդ ալիքը, ամենայն հավանականությամբ, կդառնա գերհագեցած: Անլար ցանցի միջավայրի հագեցվածությունը նվազեցնում է տվյալների փոխանակման որակը: Վերջին մի քանի տարիների ընթացքում մշակվել են հատուկ հնարքներ, որոնք թույլ են տալիս բարելավել տվյալների փոխանակման որակը և նվազեցնել հագեցվածությունը: Այս մեթոդները նվազեցնում են ալիքի հագեցվածությունը, օգտագործելով ալիքները ավելի արդյունավետ կերպով:

Ուղղակի հաջորդականությամբ սպեկտրը (DSSS) – Սա մոդուլյացիայի մեթոդ է, որը նախատեսված է ավելի լայն հաճախականությամբ ազդանշանի տարածման համար: Սպեկտրի ընդլայնման մեթոդները մշակվել են պատերազմի ժամանակ, որպեսզի թշնամիներն ավելի դժվար լինի որսալ կամ կոծկել հաղորդակցական ազդանշանը: Սրան հասնում են ազդանշանի տարածման ավելի լայն հաճախականությամբ, որը արդյունավետ քողարկում է նկատելի ազդանշանը, ինչպես ցույց է տրված նկարում: Պատշաճ կերպով կազմաձևված ընդունիչը կարող է փոխել DSSS մոդուլյացիան և վերականգնել լռելյայն ազդանշանը: DSSS-ն օգտագործվում է 802.11 b սարքերի կողմից՝ նույն 2.4 ԳՀց հաճախականությունը օգտագործող այլ սարքերից խուսափելու նպատակով:

Հաճախականությունների թռիչքային վերակառուցմամբ տարածվող սպեկտրը (FHSS) - Այն հիմնված է կապի համար ընդլայնված սպեկտրի մեթոդների վրա: FHSS-ա օգտագործման ժամանակ՝ ուղարկողը և ստացողը պետք է սինխրոնացված լինեն, որպեսզի «իմանան», թե ինչ ալիք պիտի փոխանցեն: Ալիքների միջև ազդանշանի փոխանցման այս գործընթացը ապահովում է ալիքների ավելի արդյունավետ օգտագործումը, ինչը նվազեցնում է դրանց գերբեռնվածությունը: FHSS-ն օգտագործվել է 802.11 բնօրինակ ստանդարտում: 900 ՄՀց հաճախականությամբ աշխատող շարժական ռացիաներն ու ռադիոհեռախոսները նույնպես օգտագործում են FHSS-ը, մինչդեռ Bluetooth-ն ապավինում է այս տեխնոլոգիայի տատանումներից մեկին:

Մուլտիսպեկտավորում՝ օրթոգոնալ հաճախականությունների բաժանումով (OFDM) - սա մուլտիսպեկտավորման ենթաբազմություն է՝ հաճախականությունների բաժանմամբ, որի մեկ ալիքը օգտագործում է հարակից հաճախականություններում մի քանի ենթաալիք: OFDM համակարգում ենթալալիքները ճշգրիտ օրթոգոնալ են միմյանց նկատմամբ, ինչը թույլ է տալիս ենթաալիքներին վերաճածկվել՝ առանց փոխադարձ խոչընդոտների: OFDM-ն օգտագործվում է բազմաթիվ կապի համակարգերի կողմից, ներառյալ 802.11 a/g/n/ac ստանդարտը: Նոր 802.11 ax

ստանդարտը օգտագործում է OFDM-ի մի տեսակ, որը կոչվում է օրթոգոնալ բազմակի հասանելիություն, հաճախականությունների բաժանմամբ (OFDMA):

Ալիքի ընտրություն:

WLAN ցանցերի համար, որոնց համար պահանջվում է մի քանի մուտքի կետ, խորհուրդ է տրվում օգտագործել չհատվող ալիքները: Օրինակ, 802.11 b/g/n ստանդարտները գործում են 2,4 ԳՀց-ից մինչև 2,5 ԳՀց հաճախականությունների տիրույթում: 2,4 ԳՀց խումբը բաժանված է մի քանի ալիքների: Յուրաքանչյուր ալիքին հատկացվել է 22 ՄՀց շերտ, և այն առանձնացված է հաջորդ ալիքից մինչև 5 ՄՀց: 802.11 b ստանդարտը սահմանում է 11 ալիք Հյուսիսային Ամերիկայի համար, ինչպես ցույց է տրված նկարում (13-ը Եվրոպայում և 14-ը Ճապոնիայում):Նշում: Ինտերնետում գտնեք 2.4 ԳՀց ալիքներ, տարբեր երկրներում տատանումների վերաբերյալ ավելի ծատ ինֆորմացիա իմանալու համար: Պատկերում ցույց է տրված 11 ալիք, 22 ՄՀց լայնությամբ, հեռավորությունը յուրաքանչյուրի միջև 5 ՄՀց է: Սպեկտրը գտնվում է 2,2 ԳՀց-ի և 2,5 ԳՀց-ի միջև:Հյուսիսային Ամերիկայում 2,4 ԳՀց փակվող ալիքները:Խոչընդոտները տեղի են ունենում, երբ ազդանշանը փակում է մեկ այլ ազդանշանի համար նախատեսված ալիքը՝ առաջացնելով հնարավոր աղավաղումներ: 2,4 ԳՀց WLAN-ի համար լավագույն պրակտիկան, որոնք պահանջում են մի քանի AP-ներ, կայանում է նրանում, որ օգտագործվեն չօգտագործվող ալիքները, թեև ժամանակակից AP-ների մեծ մասը դա կանի ավտոմատ կերպով: Եթե կան երեք հարևան մուտքի կետեր, օգտագործեք 1, 6 և 11 ալիքները:

2.4. Անլար լոկալ ցանցերի վտանգներն և անվտանգության ապահովման մեխանիզմները

Wi-Fi անլար ցանցերի վրա հարձակումների մի քանի տեսակ կա՝ տվյալների հասանելիություն ստանալու նպատակով

- Ներքին վտանգներ,

- Արտաքին վտանգներ։

Արտաքին հարձակումները կատարվում են առանց ներքին աշխատակիցների մասնակցության։ Արտաքին հարձակումների հիմնական հատկանիշները ներառում են համակարգի սկանավորման օգտագործումը և տեղեկատվության հավաքումը։

Արտաքին հարձակումները կարելի է բաժանել կառուցվածքային հարձակումների և առանց կառուցվածք հարձակումների՝

Արտաքին կառուցվածքային հարձակումներ: Համակարգված հարձակումները սովորաբար նախաձեռնվում են որոշակի ցանցից և նախապես մշակված նպատակներ ունեն, որոնց վրա նախատեսվում է ազդեցություն ունենալ ոչնչացման, վնասի և այլնի միջոցով։ Այս դեպքում հարձակվողները սովորաբար ունեն լայն գիտելիքներ ցանցերի նախագծման, անվտանգության համակարգերի շրջանցման, ներառյալ IDS շրջանցման (Intrusion Detection Systems) և ունեն առաջադեմ հաքերային գործիքներ։ Իրենց զինանոցում կան նոր տեխնիկ ցանցային հարձակումների զարգացման համար անհրաժեշտ գիտելիքներ և գոյություն ունեցող հաքերային գործիքակազմը իրենց խնդիրներին համապատասխանեցնելու հնարավորություն։ Որոշ դեպքերում ընկերության ներքին աշխատակիցները, որոնք ունեն մուտքի իրավունք, կարող են օգնել հարձակվողներին։

Արտաքին առանց կառուցվածքի հարձակումներ: Նման հարձակումները սովորաբար նախաձեռնվում են անփորձ հաքերների կողմից։ Այս մոտեցման դեպքում հարձակվողն օգտագործում է պարզ հաքերային գործիքակազմը կամ համացանցում առկա սցենարները՝ ցանցային հարձակման համար։ Հարձակվողի գիտելիքների մակարդակը սովորաբար ցածր է լուրջ վտանգ ստեղծելու համար։ Հաճախ դրանք պարզապես ձանձրացող երիտասարդներ են, որոնք փնտրում են համբավ ձեռք բերելու հնրավորություն՝ կորպորատիվ կայքեր կոտրելու միջոցով։

Արտաքին հեռավոր հարձակումները։ Նման հարձակումները սովորաբար ուղղված են այն ծառայություններին, որոնք կազմակերպությունն առաջարկում է բաց և հրապարակային։

- Հեռավոր հարձակումները, որոնք ուղղված են ներքին օգտագործողների համար մատչելի ծառայություններին: Սովորաբար նման հարձակումները տեղի են ունենում, նման ներքին ծառայությունները պաշտանելու համար նախատեսված միջցանցային էկրանների բացակայության պատճառով:

- Հեռավոր հարձակումները, որոնք ուղղված են կորպորատիվ ցանցի մուտքի կետերի տեղադրությանը (անլար մուտքի ցանցեր, պորտեր, մոդեմներ):

- Հարձակումներ, ինչպես օրինակ՝ Ծառայության մերժում (DoS), սերվերների վրա պրոցեսորների ծանրաբեռնվածություն ստեղծելու համար և այլն, որպեսզի ձևավորվի մի իրավիճակ, երբ լիազորված օգտվողները չեն կարող օգտվել ծառայություններից:

- Իսկության համակարգերի գաղտնաբառերը կոտրելու փորձեր:

Արտաքին լոկալ հարձակումներ (հարձակումներ ներսից): Նման հարձակումները սովորաբար սկսվում են, երբ բաց է մուտքը դեպի համակարգչային տարածք, և կարելի է մուտք գործել ցանկացած համակարգ:

Ներքին հարձակումներ: հաճախ նախաձեռնվում են դժգոհ կամ նեղացած նախկին կամ գործող աշխատակիցների կամ արտահաստիքային անձնակազմի կողմից: Ներքին հարձակվողներն ունեն համակարգի հասանելիության այս կամ այն ձևը և սովորաբար փորձում են թաքցնել հարձակումը և այն ներկայացնել որպես սովորական աշխատանքային գործընթաց: Օրինակ, անհավատարիմ աշխատակից ունի մուտքի հնարավորություն դեպի ներքին ցանցի որևէ ռեսուրսներ: Նա կարող է ունենալ նույնիսկ որոշ վարչական իրավունքներ ցանցում: Այստեղ լավագույն մոտեցումներից մեկն այն է, որ IDS (կամ IPS) ներխուժման հայտնաբերման համակարգը տեղակայվի և այն կոնֆիգուրացիան, որը համակարգը սկանավորում է ինչպես արտաքին, այնպես էլ ներքին հարձակումների ժամանակ: Հարձակման բոլոր ձևերը պետք է ներառվեն ամսագրի մեջ, և դրանք պետք է ստուգվեն, հասկացվեն և հետագայում նման հարձակումներից պաշտպանվելու միջոցներ ձեռնարկեն

Այսօրվա դրությամբ գոյություն ունեն անլար ցանցերի պաշտպանության հետևյալ մեխանիզմները՝

- Ցանցի սահմանի վերահսկում։ Դա կատարվում է ռադիոազդանշանի տարածման գոտու սահմանափակման միջոցով, ինչը թույլ է տալիս լուծել 2 խնդիր՝ նվազեցնել ռադիոընդունիչի հայտնաբերման հավանականությունը և նվազեցնել այն հեռավորությունը, որից չարագործը կարող է իրականացնել ակտիվ կամ պասիվ հարձակումներ։

- Թաքնված SSID (անգլ. ServiceSetIDentifier) (թաքնված անլար ցանցի ID)

- Նույնականացում IEEE 802.11X

- Նույնականացում ըստ MAC-հասցեների (ցուցակներ MAC-հասցեների սև և սպիտակ)

- Փաթեթի կառուցվածքի կոնֆիգուրացիա (ոչ ստանդարտ փաթեթի կառուցվածքը)

- WEP, հիմնված RC4 վրա,

- WPA, հիմնված AES վրա,

- անլար ցանցի սեգմենտի կոնֆիգուրացիայի օպտիմալացում։

Այսպիսով, որպեսզի հնարավոր լինի օգտվել անլար ցանցերի առավելություններից, դրանք պետք է պաշտպանվեն։ Անպաշտպան անլար ցանցերը հաքերների և այլ չարագործների համար բացում են գրեթե անսահմանափակ հասանելիություն կորպորատիվ ցանցին։

2.5 Անլար լոկալ ցանցերի նախագծման առանձնահատկությունները

Անլար ցանցերի ծանրաբեռնվածությունը օրեցօր աճում է։ Դրան նպաստում են մի շարք գործոններ՝

- Բջջային սարքերի քանակի և օգտագործման ինտենսիվության ավելացում

- Բջջային ծառայությունների և հավելվածների հայտնիության աճը, որը պահանջում է փոխանցման մեծ արագություն

- Անլար լոկալ ցանցերի օգտագործումը բջջային ցանցերի բեռնաթափման համար

Անլար լոկալ ցանցի և նրա օգտատերերի արագ աճող տրաֆիկի պլանավորված թողունակության անհամապատասխանությունը հանգեցնում է ցանցի բնութագրերի զգալի վատթարացման, նրա օգտատերերի դժգոհության և uzxcvb խալ եզրակացությունների այն մասին, որ Wi-Fi ցանցը չի կարող հաղթահարել մեծ ծանրաբեռնվածությունը: Սակայն նախագծման պարզ սկզբունքների պահպանումը թույլ կտա ապահովել Wi-Fi անլար ցանցի բավարար թողունակություն՝ մեկ վայրում հազարավոր օգտատերերի սպասարկման համար, ինչպես ցույց են տալիս հաջող նախագծերի օրինակները:

2.6 Անլար լոկալ ցանցերի նախագծման մեթոդներն ու ցանցերի ներկայացվող պահանջները

WLAN անլար լոկալ ցանցի պլանավորումը դրա ներդրման նախագծի իրականացման կարեւոր փուլն է, որը թույլ է տալիս ապահովել ցանցի օգտատերերի պահանջների կատարումը նրա բնութագրերին:

Այսօր կան պլանավորման երեք ամենատարածված տեսակ:

Առաջին տեսակը հաճախ անվանում են «նախնական նախագծային հետազոտություն», «ռադիո հետախուզում»: Արտասահմանյան գրականության մեջ նրան համապատասխանում է «sitesurvey», «RF site survey» տերմինը: Պահանջում է մեկնել մասնագիտացված սարքավորումներով զինված փորձագետի տեղակայման վայր՝չափումների և տարբեր թեստերի անցկացման համար: Այն ավելի ծախսատար է, բաց և ավելի արդյունավետ, քանի որ թույլ է տալիս կատարել իրական չափումներ պահանջվող հատկանիշներով իրական օգտագործվող սարքավորումների իրական կիրառման պայմաններում:

Անլար ցանցի պլանավորման երկրորդ մեթոդը նրա ռադիոկապի հաշվարկն է: Այս մեթոդը հիմնված է հաճախորդի կողմից ստացված ելակետային տվյալների

հիման վրա անլար ցանցի բնութագրերի հաշվարկման կանխատեսման վրա: Բնութագրերի կանխատեսումը կատարվում է մաթեմատիկական մոդելի օգնությամբ: Պատվիրատուն պետք է ձևակերպի անլար ցանցի բնութագրերին ներկայացվող պահանջները, տրամադրի շենքի գծագրերը կամ մասշտաբային տեղանքի սխեման, նշի պատերի հաստությունը և նյութը, սյուները, ծածկերը, օգտատերերի կուտակման վայրերը, օգտատերերին անհրաժեշտ ծառայությունները և հավելվածները: Տեղադրման վայրի մասին տեղեկատվությունը մշակվում է փորձագետի կողմից և ներմուծվում է մասնագիտացված ծրագրային ապահովում, որը թույլ է տալիս կատարել անլար ցանցի հիմնական բնութագրերի հաշվարկ և առաջարկել մուտքի կետերի նախնական տեղաբաշխում պատվիրատուի պահանջների կատարման համար՝ հիմնված տեսական հաշվարկի տվյալների վրա:

Պլանավորման երրորդ տեսակը կարելի է անվանել «աչքի չափով», «ողջամտությամբ»*:* Անլար ցանցերում փորձաքննության բացակայությունը չի խանգարում նման «պլանավորողներին» 50-100 մետր շրջաններով ծածկել շինության սխեման և այն անվանել «պլանավորում»: Այս մոտեցումը առավել արագ է և ծախսատար չէ, բայց ուղեկցվում է օգտվողների մեծ հիասթափությամբ: Հաշվի չառնելով ցանցի սարքավորումների առանձնահատկությունները և կիրառման վայրը, նման մեթոդը հանգեցնում է պլանավորման մեծ սխալների և չպետք է կիրառվի նույնիսկ անլար ցանցի ստեղծման նախագծի բյուջետային գնահատման համար: Խնդիրների ստեղծման վտանգը և նույնիսկ նախագծի ամբողջական ձախողման վտանգը չափազանց մեծ է: Նույնիսկ ժամանակակից ռադիոժամետերի հարմարվողական կարգավորումների համակարգերը թույլ չեն տա ուղղել պլանավորման այս մեթոդի սխալները:

Աղյուսակ.2 Լոկալ ցանցերի պլանավորման երեք տեսակների համեմատություն՝

Պլանավորման խնդիրը	1-ին մեթոդ Ռադիո հետախուզում, նախանախագծային հետազոտություն (RF site survey)	2-րդ մեթոդ Ռադիոծածկույթի հաշվարկ	3-րդ մեթոդ «Ողջամտությամբ»
Հաշվի առնել տեղադրման վայրի առանձնահատկությունները	+	Սահմանափակ, մոտավոր	–
Սահմանել պահանջվող մուտքի կետերի թիվը	+	+	–
Ստուգել մուտքի կետերի տեղադրման վայրերը, ընտրել համապատասխան ալեհավաքներ	+	–	–
Բացահայտել միջամտության աղբյուրները և նվազագույնի հասցնել դրանց ազդեցությունը	+	–	–
Փորձարկել տարբեր օգտատերերի սարքերի բնութագրերը	+	–	–
Ստուգել հաճախորդների անլար ռոումինգը	+	–	–

Որոշել օգտագործվող հաճախականության ալիքները և ճառագայթման հզորությունը	+	+	–
Առավել ամբողջական հաշվի առնել օգտվողների բոլոր պահանջները և կիրառման առանձնահատկությունները	+	**Սահմանափակ, մոտավոր**	–

Սարքավորումներին ներկայացվող պահանջները՝

- Ստանդարտի ապահովում 801.11n
- MIMO-ի ապահովում
- 300 Մբիթ/վ անլար կապի առավելագույն արագությունը
- Կենտրոնացված / կառավարվող ճարտարապետություն

Եզրակացություններ՝ այս բաժնում առաջադրանք է դրվել հետագա նախագծման համար: Անլար ցանցի ներդրման ծրագրվող օգուտը՝ շարժունակության բարձրացումը և աշխատակիցների արտադրողականության ավելացումը, աշխատուժի արդյունավետ օգտագործման, ինչպես նաև գրասենյակային տարածքի հաշվին, ավելի արդյունավետ կդառնա տեղեկատվության օպերատիվ կառավարումը:

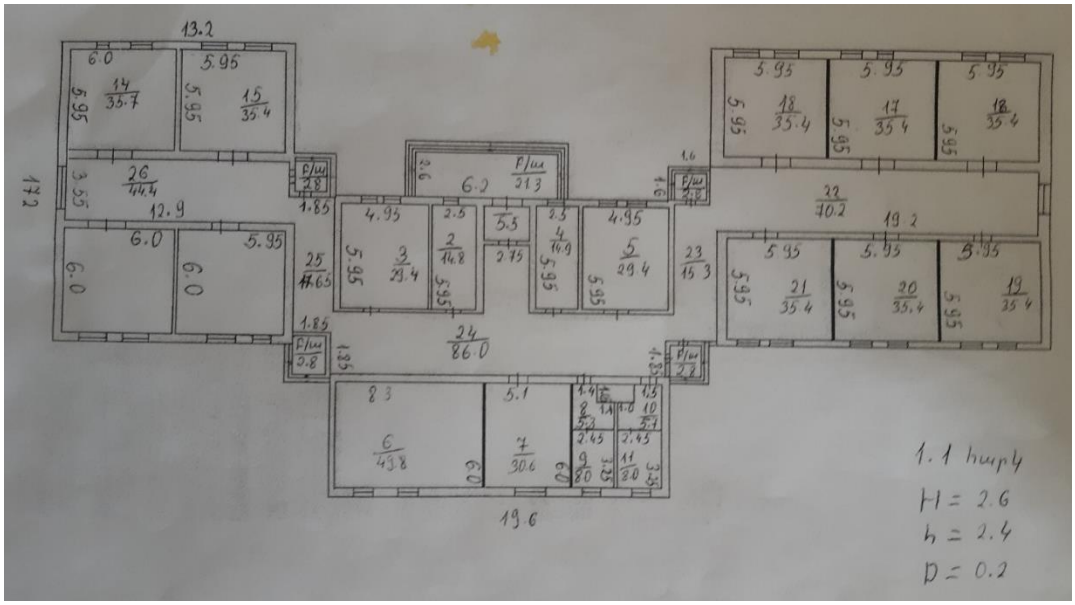
Երկրորդ գլխի ամփոփում

Երկրորդ գլխում ուսումնասիրվում է անլար լոկալ ցանցերի տոպոլոգիաների 802,11 ռեժիմները, ալիքների վերահսկման ու ալիքների ճիշտ ընտրության մեխանիզմներ։ Ներկայացվում է անլար ցանցերում առկա վտանգների և անվտանգության ապահովման ձևերն ու մեթոդները։ Այս գլխում ուսումնասիրվում է նաև անլար լոկալ ցանցերի նախագծման առանձնահատկություններն ու մեթոդները։

ԳԼՈՒԽ 3. Ուսումնական հաստատության անվար լոկալ ցանցի նախագծումը

3.1 Ցանցի ֆիզիկական տոպոլոգիայի նկարագրությունը:

Աշխատանքի շրաջանակներում նախագծվել է Արագածաոտնի մարզի, Կարին համայնքի միջնակարգ դպրոցի անվար լոկալ ցանցը՝ ելնելով դպրոցի հատակագծի պայմաններից՝



Նկ. 1 Կարին համայնքի միջնակարգ դպրոցի հատակագիծը

Նկ 2. Կարին համայքնի դպրոցի արբանյակային նկարը

Համակարգիչների բաշխումներն ըստ սենյակների բերված է աղյուսակ 3-ում:

Աղյուսակ.3

1-ին հարկ	**Սենյակի համար**								
	Դասասենյակ 1	*Դասասենյակ 2*	*Դասասենյակ 5*	*Տնօրենի սենյակ*	*Հաշվապահության սենյակ*	*Դասասենյակ 6*	*Դասասենյակ 7*	*Դասասենյակ 8*	*Դասասենյակ 9*
	Սարքավորումների քանակը								
	1	*1*	*1*	*3*	*1*	*4*	*3*	*1*	*1*

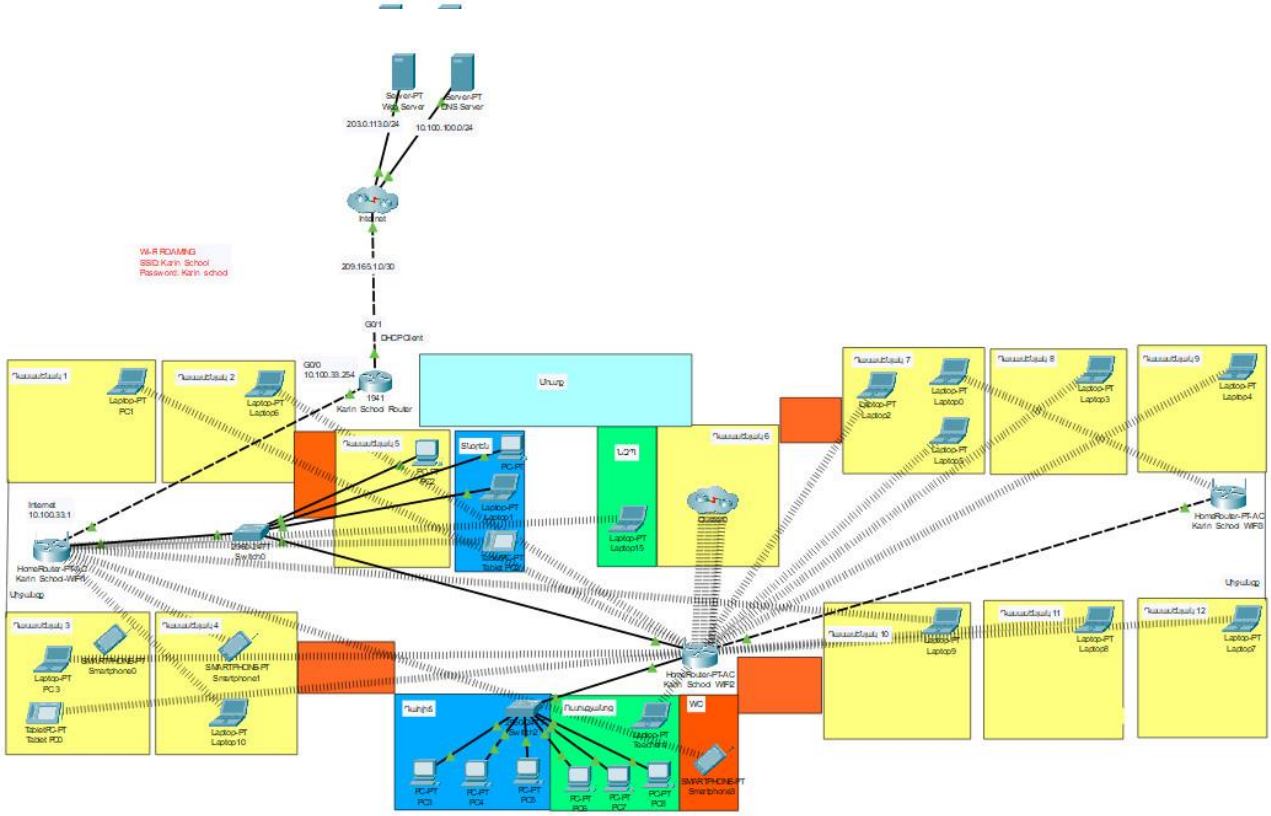
Միջանցք

1-ին հարկ	*Դասասենյակ 3*	*Դասասենյակ 4*	*Դահլիճ*	*Ուսուցչանոց*	*Դասասենյակ 10*	*Դասասենյակ 11*	*Դասասենյակ 12*
	Սարքավորումների քանակը						
	3	*2*	*3*	*3*	*1*	*1*	*1*

Մեր խնդիրն է նախագծել համակարգչային ցանցը և օպտիմալացնել նրա կառավարումը:

Շատ կարևոր է լավ նախագծել ցանցը և ընտրել համապատասխան սարքեր, որպեսզի առավել արդյունավետ դարձնել ցանցի սպասարկումը:

Ցանցի հիերարխիկ նախագծումը ներառում է ցանցի բաժանումը դիսկրետ շերտերի: Յուրաքանչյուր շերտ ապահովում է որոշակի գործառույթներ, որոնք կատարում են իրենց դերը ընդհանուր ցանցի շրջանակներում: Առանձնացնելով տարբեր գործառույթներ, որոնք գոյություն ունեն ցանցում, ցանցի դիզայնը դառնում է մոդուլային, որը հեշտացնում է պատկերացումը ցանցի մասին և նրա օգտագործումը:



Նկ 3. Նախագծված լոկալ ցանցի տոպոլոգիան Packet Tracer միջավայրում

Ելնելով դպրոցի ենթակառուցվածքի առանձնահատկություններից ընտրվեծ է 3 հատ անլար երթուղիչներ, որոնք տեղադրվել են դպրոցի կոնկրետ տեղամասերում և կարգաբերվել են միմյանց հետ չհատվող 1,6 և 11 ալիքիների ընտրությամբ և 2.412 ԳՀց հաճախականության տակ:

3.2 Նախագծված ցանցի հիմնական կարգաբերումները

Խնդրի դրվածքին համապատասխան Cisco Packet Tracer սիմուլյատորի օգնությամբ, կառուցվել է ցանցի հիերարխիկ մոդելը իր ողջ կարգավորումներով:

Մոդելի կառուցման ընթացքում, ցանցում օգտագործվել են ստորև ներկայացված սարքավորումները:

Cisco switch 2950 (24 port) – 1 հատ, որին միացված բոլոր սարքավորումները գտնվում եմ միևնույն VLAN-ի ներսում:

Cisco router 1941 երթուղիչ – 3 հատ, որոնցից 1 հատը, որպես դպրոցի եզրային երթուղիչ, որը հանդիսանում է DHCP կլիենտ և ստանում է ավտոմատ կերպով IP հասցե պրովայդերի կողմից, իսկ դեպի ներքին ցանց տանող ինտերֆեյսը կարգաբերված է ստատիկ հասցեով:

Մյուս երկուսը տեղադրված Internet Cloud տեղամասում, որը մոդելավորվել է որպես պրովայդերի ներքին ցանց և դրանց վրա իրականացվել է EIGRP երթուղավորման դինամիկ արձանագրության կարգաբերումները:

Cisco Wireless Tri-Band Home Router անլար երթուղիչ - 3 հատ, որոնք կարգաբերված են միմյանց հետ չհատվող ալիքների՝ 1, 6, 11 ընտրությամբ:

DNS SERVER դոմեյնային ծառայության տրամադրման համար:

WEB SERVER գլոբալ ցանց մուտք ապահովելու համար:

Օգտատերերի սարքավորումներ տարբեր քանակությամբ՝ նոութբուքեր, սմարթֆոններ, պլանշետներ, որոնք ավտոմատ կերպով ստանում են համապատասխան կարգաբերումները և ունեն հասանելիություն դեպի ինտերնետ դպրոցի ողջ տարածքում:

Եզրային երթուղիչի՝ **Karin_School Router**-ի կարգաբերումները ներկայացված են ստորև՝

```
hostname Karin_School
license udi pid CISCO1941/K9 sn FTX1524U285-
interface GigabitEthernet0/0
```

ip address 10.100.33.254 255.255.255.0

duplex auto

speed auto

interface GigabitEthernet0/1 // դեպի պրովայդեր տանող պորտը

ip address dhcp

duplex auto

speed auto

interface Vlan1

no ip address

shutdown

router eigrp 1

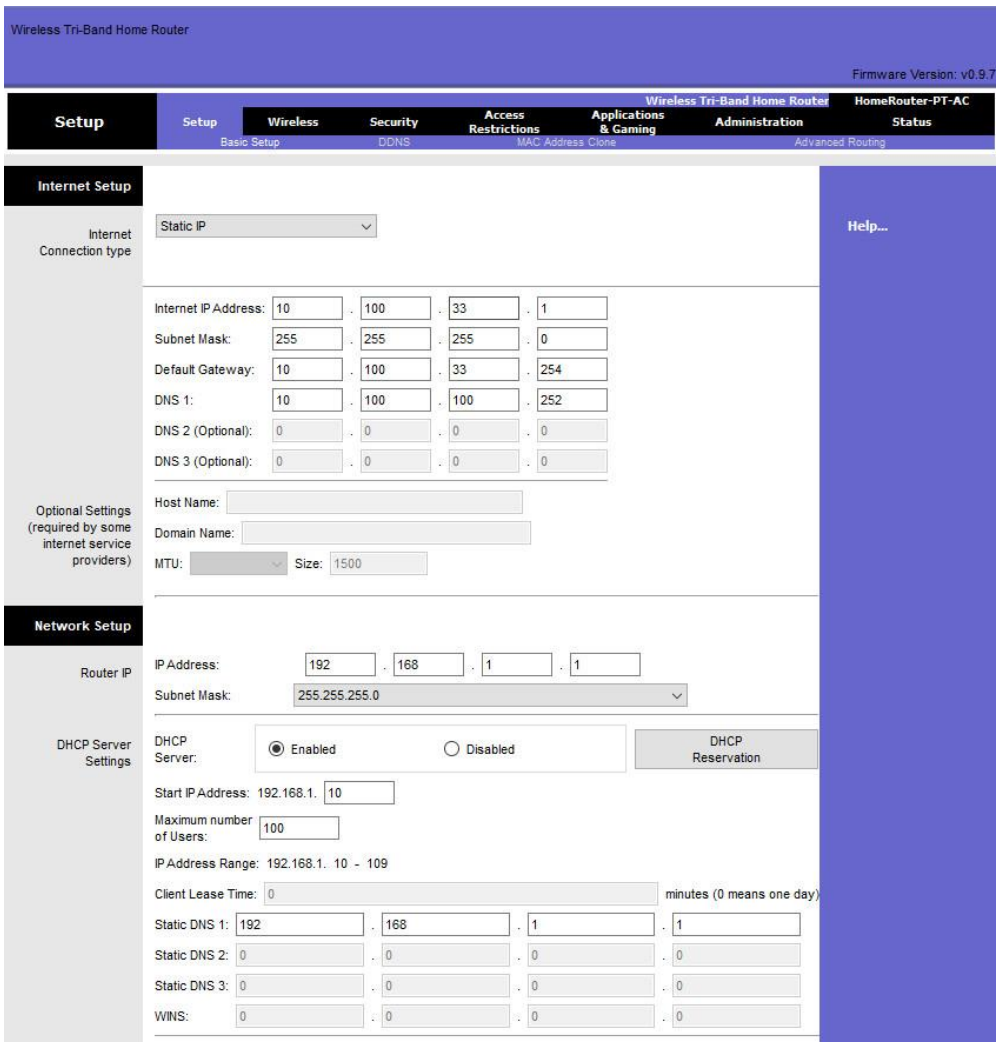
passive-interface GigabitEthernet0/0

network 209.165.1.0

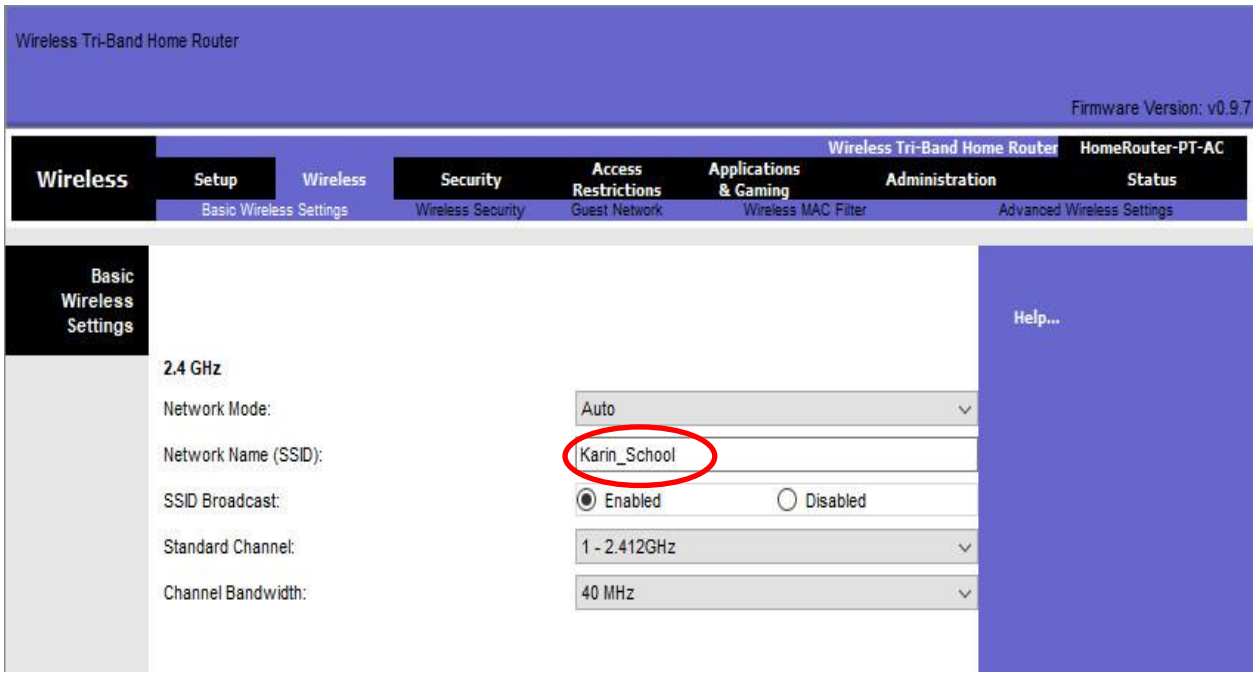
network 10.100.33.0 0.0.0.255

ip classless

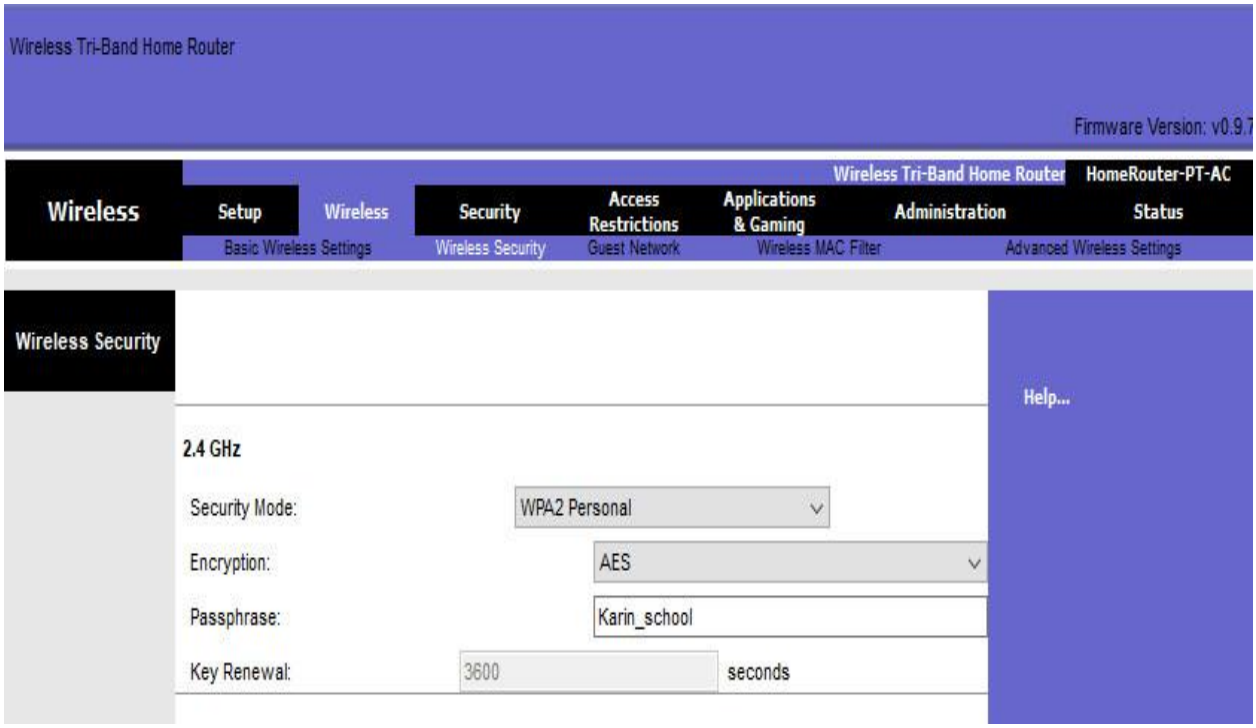
Cisco Wireless Tri-Band Home Router անլար երթուղիչներից մեկի **Karin_School-WIFI**1 կարգաբերումները ներկայացված է ստորև՝



Նկ. 4.WAN և LAN պորտերի կարգաբերումները



Նկ. 5. Անլար ցանցի ալիքի և հաճախականության ընտրության կարգաբերումները:



Նկ.6.Անլար ցանցի անվտանգության կարգաբերումները

Երրորդ գլխի ամփոփում

Երրորդ գլխում նկարագրված է Cisco Packet Tracer միջավայրում դպրոցի անլար լոկալ ցանցի նախագծման գործընթացը: Ցանցը նախագծվել է Արագածոտնի մարզի Կարին համայքի միջնակարգ դպրոցի հատակագծի հիման վրա:

Եզրակացություն

1. Ուսումնասիրվել են անլար լոկալ ցանցերի տեխնոլոգիաներն ու ստանդարտները: Հիմնավորվել է, որ ժամանակակից անլար լոկալ ցանցերում լայնորեն կիրառվում են IEEE 802.11x ստանդարտները

2. Նկարագրվել են անլար լոկալ ցանցերի ենթակառուցվածքների բաղադրիչները: Մասնավորապես վերլուծվել են տարբեր հաճախականությամբ ռադիոալիքների տեղաբաշխման արդյունավետությունը՝ ըստ տեղակայման կոորդինատների, հաճախականությունների և այլն:

3.Բացահայտվել են անլար լոկալ ցանցերում ալիքների վերահսկման մեխանիզմները: Հիմնավորվել են, թե ի՞նչ հաճախականությամբ է անհրաժեշտ կագաբերել տվյալ անլար երթուղիչը ցանցն առավել վերահսկելի դարձնելու համար:

4. Նախագծվել է ուսումնական հաստատության անլար լոկալ ցանց:

Օգտագործված գրականության ցանկ

1. Э.Таненбаум, Д. Уэзеролл: Компьютерные сети. Пятое издание, Питер 2019.
2. В. Олифер, Н. Олифер Компьютерные сети. Издательский дом «Питер», 978-5-4461-1426-9, 2020
3. Microsoft Corporation. Компьютерные сети. Пер. с англ. — М.: Издательско-торговый дом «Русская Редакция», 2000. — 552 стр.
4. Cisco CCNA. Учебная программа 1 и 2. Вспомогательное руководство. Москва, СанктПетербург, Киев, 2008. Третье издание, исправленное и дополненное.
5. CiscoSystems inc. CCNAv7 online course. 2020.
6. Пролетарский А.В., Баскаков И.В., Чирков Д.Н. Беспроводные сети Wi-Fi. М.: Интуит, 2007. — 177 с.
7. Рошан П., Лиэри Д. Основы построения беспроводных локальных сетей стандарта 802.11Пер. с англ. — М.: Вильямс, 2004. — 304 с.