**Mundarija**

[KIRISH 5](#__RefHeading___Toc1008_1119060251)

[**I. BOB.WLAN TARMOQLARIDA XAVFSIZLIKNING NAZARIY ASOSLARI 7**](#__RefHeading___Toc1010_1119060251)

[1.1 WLAN tarmoqlarining asosiy tuzilishi va ishlash printsipi. 7](#__RefHeading___Toc1012_1119060251)

[1.2 WLAN tarmoqlari xavfsizligi tahdidlar 12](#__RefHeading___Toc1014_1119060251)

[**II. BOB. WLAN Xavfsizligini Ta’minlash va Tahlil Usullari 15**](#__RefHeading___Toc1016_1119060251)

[2.1.WLAN tarmog’ini Cisco packet tracer orqali qurish 15](#__RefHeading___Toc1018_1119060251)

[XULOSA 41](#__RefHeading___Toc1020_1119060251)

[FOYDALANILGAN ADABIYOTLAR RO’YXATI 42](#__RefHeading___Toc1022_1119060251)

# KIRISH

Bugungi kunda axborot texnologiyalari va kompyuter tarmoqlari har bir sohada keng qo‘llanilmoqda va ularning rivojlanishi zamonaviy dunyoning ajralmas qismiga aylangan. O‘zbekiston Respublikasida ham axborot-kommunikatsiya texnologiyalarini joriy etish va rivojlantirish bo‘yicha bir qator ijobiy o‘zgarishlar amalga oshirilmoqda.

O‘zbekistonda yuritilayotgan raqamli iqtisodiyot siyosati zamirida ham yangi texnologiyalarni rivojlantirish maqsadi ko‘zda tutilmoqda. Davlatimiz rahbarining 2020-yil 28-apreldagi “Raqamli iqtisodiyot va elektron hukumatni keng joriy etish chora-tadbirlari to‘g‘risida”gi qaroriga muvofiq, raqamli iqtisodiyot bilan shug‘ullanadigan yaxlit tizim yaratildi. “Elektron hukumat”, iqtisodiyot tarmoqlari va qishloq xo‘jaligini raqamlashtirish, IT parklarini tashkil etish va boshqarish kabi vazifalar to‘liq Raqamli texnologiyalar vazirligi vakolatiga o‘tdi.

WLAN (Wireless Local Area Network) tarmoqlari, simsiz aloqani ta'minlovchi va foydalanuvchilarga ma'lumot uzatish imkoniyatini beruvchi tarmoqlar bo'lib, zamonaviy hayotda keng qo'llaniladi. Bu tarmoqlar, uyda, ofislarda, jamoat joylarida va boshqa ko'plab joylarda internetga ulanish uchun ishlatiladi.WLAN tarmoqlarida xavfsizlik masalalari, asosan, shifrlash, autentifikatsiya, ma'lumotlarni himoya qilish, va tizimga kirishning noaniqligi kabi masalalarni o'z ichiga oladi. Wi-Fi tarmoqlarida keng tarqalgan X.509 sertifikatlari, WPA (Wi-Fi Protected Access), WEP (Wired Equivalent Privacy) va WPA2 kabi xavfsizlik protokollari tarmoqni himoya qilishda qo'llaniladi, ammo ular ham o'z zaif tomonlariga ega. Shu sababli, WLAN tarmoqlarida xavfsizlikni ta'minlashda so'nggi texnologiyalar va usullarni qo'llash muhimdir. Ushbu kurs ishida WLAN tarmoqlarining xavfsizligini oshirish va uning zaifliklarini tahlil qilish masalalari ko'rib chiqiladi.

O‘zbekiston Respublikasida kompyuter tarmoqlari va axborot texnologiyalarini rivojlantirish borasida bir qator muhim qarorlar qabul qilingan. Masalan, 2002-yil 30-maydagi PF-3080-son Farmonida axborot-kommunikatsiya texnologiyalarini rivojlantirish, kompyuterlashtirish jarayonini joriy etish bo‘yicha chora-tadbirlar belgilangan. Shuningdek, 2012-yil 23-oktabrdagi PQ-1836-son Qarorda axborotlashtirish sohasidagi boshqaruvni takomillashtirish va yangi tashkilotlarni tuzish ko‘zda tutilgan. O‘z navbatida, 2023-yil 24-maydagi PQ-162-son Qarorida raqamli xizmatlarning sifatini oshirish va soha transformatsiyasiga oid yangi chora-tadbirlar ishlab chiqilgan.

**Mavzuning maqsadi va vazifalari:** WLAN tarmoqlari haqida umumiy ma'lumot bo'limida tarmoqlar qanday ishlashi, ularning asosiy komponentlari va arxitekturasi haqida tushunchalar beriladi. Tarmoqni tashkil etishda qo'llaniladigan texnologiyalar, usullar va protokollar haqida qisqacha ma'lumotlar keltiriladi.

**Kurs ishi tuzilmasining tavsifi:**

**WLAN tarmoqlari haqida umumiy ma'lumot** bo'limida tarmoqlar qanday ishlashini, ularning asosiy komponentlari va arxitekturasini tushuntiruvchi bo'lim kiritiladi. Bu bo'limda WLAN tarmoqlarining qanday tashkil etilishi, asosiy elementlari (routerlar, access point’lar, foydalanuvchi qurilmalari) va tarmoq arxitekturasi haqida umumiy ma'lumot beriladi.

**Mavzuning dolzarbligi:** WLAN (Wireless Local Area Network) tarmoqlarining dolzarbligi zamonaviy kiberxavfsizlik va axborot texnologiyalarining rivojlanishi bilan yanada oshmoqda. Bugungi kunda simsiz internetga ulanish keng tarqalgan va jamoat joylarida, ofisda, uyda, kafe, restoranlar va boshqa ko'plab joylarda Wi-Fi tarmoqlari faol ishlatilmoqda. Mobil qurilmalar, noutbuklar, smartfonlar va boshqa qurilmalar orqali tarmoqka ulanish osonlashgani sayin, simsiz tarmoqlar hayotimizning ajralmas qismiga aylanmoqda. Shuningdek, korxonalar va tashkilotlar o'zlarining ichki tarmoqlarini simsiz tarmoq orqali tashkil etib, ishlovchilariga yuqori tezlikda internetga kirish imkoniyatini taqdim etmoqda.

**Kurs ishi tarkibi:** Kurs ishi kirish qismi, ikki bob, xulosa va ilmiy-amaliy tavsiyalar hamda foydalangan adabiyotlar ro‘yxatidan iborat.

# I. BOB.WLAN TARMOQLARIDA XAVFSIZLIKNING NAZARIY ASOSLARI

## **1.1 WLAN tarmoqlarining asosiy tuzilishi va ishlash printsipi.**

Simsiz tarmoq xavfsizligi (WLAN) - bu simsiz kompyuter tarmoqlarini ruxsatsiz kirish va buzilishlardan himoya qilish uchun ularni loyihalash, amalga oshirish va xavfsizlikni ta'minlashni o'z ichiga olgan tarmoq xavfsizligining kichik to'plami. U simsiz tarmoqlar va ularning resurslarining maxfiyligi, yaxlitligi va mavjudligini saqlashga qaratilgan strategiyalarni o'z ichiga oladi. Tegishli xavfsizlik strategiyalarini samarali amalga oshirish ushlash, ma'lumotlarni o'g'irlash va xizmat ko'rsatishni rad etish hujumlari kabi tahdidlarning oldini oladi. Uning ishlash prinsipi quyidagilarga asoslanadi:

**Shifrlash (Encryption)**

* Ma'lumotlarni uzatish jarayonida shifrlash algoritmlari qo'llaniladi, bu esa ma'lumotlarni faqat ruxsat etilgan qurilmalar tomonidan o'qiladigan holga keltiradi.
* **WPA2** yoki **WPA3** kabi xavfsizlik protokollari shifrlash uchun ishlatiladi.

Masalan, AES (Advanced Encryption Standard) algoritmi WPA2/WPA3 protokollarida keng qo'llaniladi.

**Autentifikatsiya (Authentication)**

* Tarmoqdan foydalanish uchun foydalanuvchi yoki qurilmaning kimligini tasdiqlash talab qilinadi. Bu jarayon tarmoq parolini kiritish yoki ikki faktorli autentifikatsiya orqali amalga oshiriladi.

**Kirishni boshqarish (Access Control)**

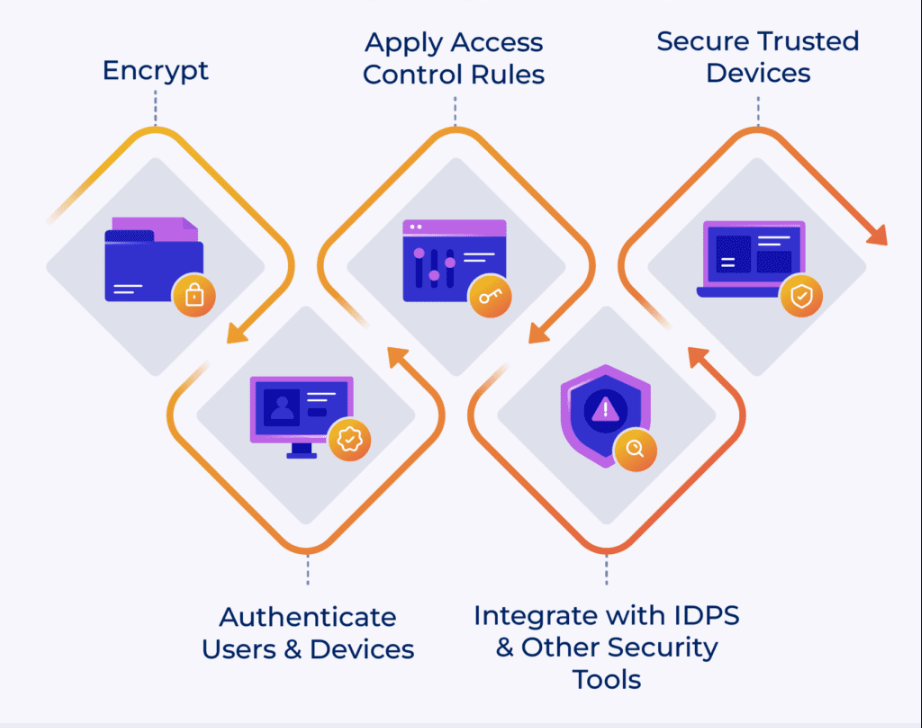
* Tarmoq faqat ruxsat etilgan qurilmalar uchun ochiq bo‘ladi. Masalan, **MAC manzillarni filtrlash** yoki foydalanuvchilarni identifikatsiyalash orqali tarmoqni boshqarish.

**Xavfsiz qurilmalar (Secure devices)**

* Har qanday tarmoqqa ulanadigan ishonchli qurilmalarni aniqlashni o'z ichiga oladi va boshqa o'rnatilgan xavfsizlik vositalarida har qanday siyosatni o'rnatadi.

**IDPS va boshqa vositalar bilan integratsiya (Integrate with IDPS and other tools)**

* Tarmoqdagi shubhali harakatlar va xavfsizlik buzilishlarini ushlang va bloklash.

*1.1.1-rasm WLAN xavfsizligining ishlashi*

**Simli ekvivalent maxfiylik (WEP)**

1997 yilda ishlab chiqilgan WEP shifrlash va kirishni cheklash yordamida simsiz tarmoqlarni himoya qilish uchun mo'ljallangan. Biroq, uning xavfsiz bo'lmagan RC4 shifrlash va umumiy kalit autentifikatsiyasiga tayanishi tarmoqlarni hujumga qarshi himoyasiz holga keltirdi. WEP dastlab simli tarmoqlarga o'xshash shifrlashni ta'minlagan bo'lsa-da, uning kamchiliklari xakerlar tomonidan keng tarqalgan bo'lib, uni eskirgan. Protokolning to'xtatilishi WPA (Wi-Fi himoyalangan kirish) kabi yanada mustahkam muqobillarni yaratdi. Kamchiliklariga qaramay, WEP ning soddaligi va keng qo'llanilishi dastlab e'tiborni tortdi, biroq uning o'ziga xos zaif tomonlari oxir-oqibat simsiz xavfsizlik standartlarini doimiy ravishda yangilab turish muhimligini ta'kidlab, uning afzalliklariga soya soldi.

**Wi-Fi himoyalangan kirish (WPA)**

2003-yilda ishga tushirilgan WPA WEPning kamchiliklarini bartaraf etib, samarali davomchisi sifatida paydo bo'ldi. WPA kalitlarni boshqarish va yaxlitlik tekshiruvlarini yaxshilash uchun vaqtinchalik kalit yaxlitlik protokoli (TKIP) shifrlashdan foydalanadi. U ikkita rejimga ega: uy tarmoqlari uchun WPA-Personal va RADIUS serverlaridan foydalanadigan korxonalar uchun WPA-Korxona.

WPA-ning 128-bitli shifrlashi WEP-ning zaifroq shifrlash standartlariga nisbatan yaxshilangan himoyani ta'minlaydi; ammo, u hali ham WPA2 dan nisbatan zaifroq bo'lib, potentsial kamchiliklar va muvofiqlik qiyinchiliklariga olib keladi. Bundan tashqari, WPA-ni qabul qilish eski uskunaga ega bo'lgan foydalanuvchilar uchun muammo tug'diradigan apparat o'zgarishlarini talab qilishi mumkin.

**Wi-Fi himoyalangan kirish II (WPA2)**

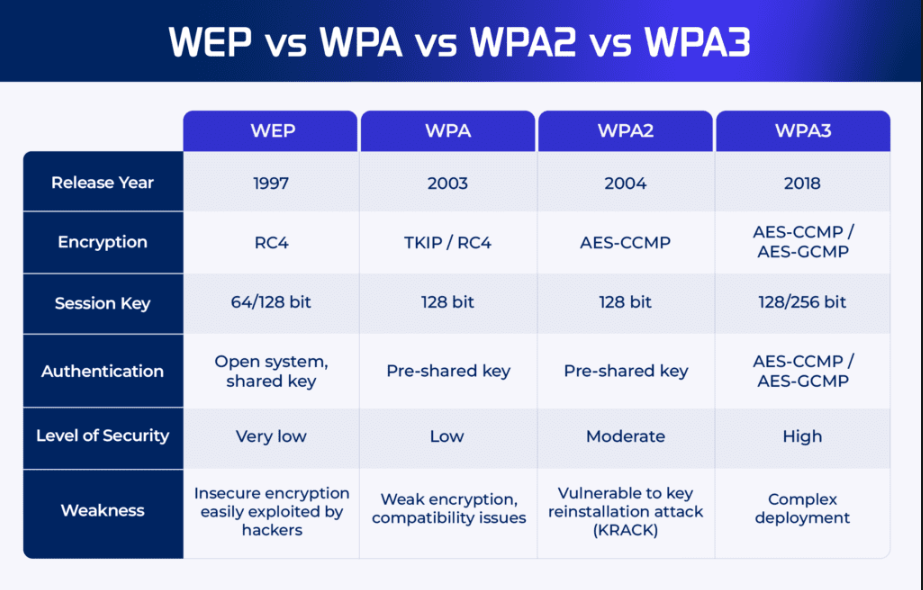
2004-yilda chiqarilgan WPA2 kuchli xavfsizlikni ta'minlash uchun AES shifrlash texnikasidan foydalanadigan eng mashhur simsiz xavfsizlik standartidir. Uning WPA-ga nisbatan afzalliklari yaxshi boshqaruv va hujumlarga nisbatan zaiflikni o'z ichiga oladi. WPA2 sanoat standarti sifatida keng miqyosda qabul qilingan bo'lib, qurilmalarning o'zaro ishlashini ta'minlaydi.

Biroq, kalitlarni qayta o'rnatish hujumi (KRACK) kabi zaifliklar xavfsizlikka xavf tug'diradi. Aksariyat uy tarmoqlari uchun mos bo'lsa-da, murakkab hujumlar keng tarqalgan korxona sozlamalarida qiyinchiliklar paydo bo'ladi. Bundan tashqari, WPA2 bilan mos kelmaydigan eski qurilmalar yangilanishlarni talab qilishi mumkin. Ushbu muammolarga qaramay, WPA2 simsiz tarmoq xavfsizligi uchun muhim bo'lib qolmoqda, ammo o'sib borayotgan tahdidlar va zaif tomonlarni bartaraf etishga urinishlar davom etmoqda.

**Wi-Fi himoyalangan kirish III (WPA3)**

2018-yilda ishga tushirilgan WPA3 Wi-Fi Easy Connect orqali kattaroq shifrlashni, lug‘atning qo‘pol kuch hujumlaridan himoya qilishni va qurilmaning sodda konfiguratsiyasini ta’minlaydi. Ushbu yaxshilanishlarga qaramay, keng tarqalgan qabul qilish sust. WPA3 uchta turda taqdim etiladi: uyda foydalanish uchun WPA3-Personal, tashkiliy sozlamalar uchun WPA3-Enterprise va parol bilan himoyalanmagan tarmoqlar uchun Wi-Fi Enhanced Open.

U umumiy tarmoq xavfsizligini kuchaytirsa-da, kamchiliklarga joylashtirishning murakkabligi, foydalanuvchilarning past qabul qilinishi va eski qurilmalar va uskunalar bilan moslik muammolari kiradi. Uning afzalliklariga qaramay, WPA3-nito'liq miqyosda joylashtirish hali amalga oshirilmagan, bu eski xavfsizlik protokollaridan zamonaviyroq standartga sekin o'tishdan dalolat beradi.

*1.1.2-rasm WLAN tarmoq xavfsizligining 4 protokoli*

**4 turdagi Wi-Fi tarmog'i xavfsizlik qurilmalari -** Wi-Fi tarmog'i xavfsizligi qurilmalarining to'rtta toifasi mavjud: faol, passiv, profilaktik va UTM. Faol qurilmalar trafikni boshqaradi, passiv qurilmalar tahdidlarni aniqlaydi, profilaktik qurilmalar zaif tomonlarni tekshiradi va UTM tizimlari to'liq himoyani ta'minlash uchun bir nechta xavfsizlik tadbirlarini birlashtiradi.

1. **Faol qurilma (Active Device) -** Simli hamkasblariga o'xshash ishlashi bilan birga, faol qurilmalar simsiz muhit uchun mo'ljallangan. Bularga xavfsizlik devori, antivirus va kontentni filtrlash qurilmalari kiradi. Xavfsizlik devorlari kiruvchi va chiquvchi simsiz trafikni filtrlaydi, kiruvchi kirishni oldini oladi va zararli paketlarni aniqlaydi. Antivirus skanerlari doimiy ravishda simsiz ulanishlarni zararli dastur tahdidlari uchun tekshiradi.
2. **Passiv qurilma (Passive Device) -** Intrusionni aniqlash qurilmalari kabi passiv qurilmalar shubhali faoliyat uchun tarmoq trafigini kuzatish orqali simsiz tarmoq xavfsizligini yaxshilaydi. Ular ruxsatsiz kirish urinishlari yoki zararli dasturlarni uzatish kabi potentsial xavflarni aniqlash uchun ma'lumotlar tendentsiyalari va anormalliklarni tekshiradi. Bunday holatlarni aniqlash va hisobot berish orqali ushbu qurilmalar tarmoq menejerlariga xavfsizlik xatarlarini kamaytirish va tarmoq xavfsizligini ta'minlash bo'yicha zudlik bilan choralar ko'rish imkonini beruvchi hayotiy tushunchalarni beradi.
3. **Profilaktik qurilma (Preventive Device) -** Penetratsiyani tekshirish vositalari va zaiflikni baholash asboblari kabi profilaktik qurilmalar xavfsizlikning mumkin bo'lgan kamchiliklarini faol izlash orqali simsiz tarmoq xavfsizligini yaxshilaydi. Ushbu qurilmalar tarmoq infratuzilmasini to'liq tekshirib, tajovuzkorlar foydalanishi mumkin bo'lgan kamchiliklarni aniqlaydi. Profilaktik qurilmalar tarmoqni kibertahdidlarga qarshi mustahkamlaydi, bu esa xavfsizlik kamchiliklarini ulardan foydalanishdan oldin aniqlash va tuzatish orqali xavfsizlikni buzish ehtimolini kamaytiradi.
4. **Yagona tahdidlarni boshqarish tizimi (UTM) -** UTM tizimlari ko'plab xavfsizlik funktsiyalarini bitta apparat qurilmasiga birlashtirib, simsiz tarmoqlarni himoya qiladi. Tarmoq perimetrida joylashgan ushbu qurilmalar zararli dasturlardan, noqonuniy infiltratsiyadan va boshqa xavfsizlik tahdidlaridan keng qamrovli himoyani ta'minlovchi shlyuz vazifasini bajaradi.

## **1.2 WLAN tarmoqlari xavfsizligi tahdidlar**

**WLAN tarmoqlarining xavfsiligining asosiy 5 ta tahdidlari bor**

**DNS-kesh bilan zaharlanish (DNS-Cache Poisoning)**

* DNS keshini zaharlash xaker qonuniy veb-sayt manzilini firibgar bilan almashtirganda sodir bo'ladi, bu esa tashrif buyuruvchilarni bilmasdan zararli sayt bilan aloqa qilishiga olib keladi. Bu ma'lumotlarning o'g'irlanishi yoki xizmat ko'rsatishning rad etilishiga olib kelishi mumkin.
* **Xavfsizlik strategiyalari:**DNS serverlarini boshqarish, ochiq portlar orqali so'rovlarni cheklash va o'rnatilgan xavfsizlik bilan DNS dasturiy ta'minotini qabul qilish DNS bilan zaharlanish hujumlari xavfini kamaytirishga yordam beradi.

**Yovuz egizak hujumlar** (**Evil Twin Attacks**)

* Yovuz egizak hujumlar qonuniy tarmoqlarni taqlid qilib, ommaviy Wi-Fi kamchiliklaridan foydalanadi. Xakerlar soxta Wi-Fi ulanish nuqtalarini yaratib, odamlarni beixtiyor ulanishga undaydi.
* **Xavfsizlik strategiyalari:**O'zingizni himoya qilish uchun xavfsiz bo'lmagan Wi-Fi tarmog'idan qoching va o'rniga parol bilan himoyalangan shaxsiy ulanish nuqtalaridan foydalaning, ogohlantirish bildirishnomalarini kuzatib boring, avtomatik ulanish xususiyatlarini o'chirib qo'ying, umumiy Wi-Fi tarmog'ida shaxsiy hisoblarga kirishdan saqlaning, ko'p faktorli autentifikatsiyadan foydalaning, tashrif buyuring.

**IP-spoofing**

1. IP-spoofing, xaker paketning asl IP-manzilini soxta manzilga almashtirganda sodir bo'ladi va ko'pincha qonuniy manba sifatida o'zini namoyon qiladi. Bu aldamchi usul shaxsni o'g'irlash kabi jinoiy maqsadlarda qo'llanilishi mumkin.
2. **Xavfsizlik strategiyalari:** Ba'zi usullar orasida g'alati faoliyat uchun tarmoqlarni kuzatish, identifikatsiyani tekshirishning kuchli usullaridan foydalanish, xavfsizlik devori himoyasi, IPv6 ga o'tish, kirish va chiqish filtrini amalga oshirish va chuqur paketli tekshiruvdan (DPI) foydalanish kiradi.

**Piggybacking**

1. Wi-Fi tarmoqlarida piggybacking shifrlanmagan signallardan foydalanish orqali internetga kiruvchi kirishni o'z ichiga oladi. Wi-Fi squatting sifatida ham tanilgan ushbu faoliyat tarmoq xavfsizligini xavf ostiga qo'yadi va internetga ulanishni sekinlashtirishi mumkin.
2. **Xavfsizlik strategiyalari:** Piggybacking qurboni bo'lmaslik uchun Wi-Fi tarmoqlarini kuchli parollar bilan himoya qiling, noodatiy harakatlarga e'tibor bering va umumiy Wi-Fi tarmoqlarida shifrlash uchun virtual xususiy tarmoqdan (VPN) foydalanish haqida o'ylang.

**Yelkada serfing (Shoulder Surfing)**

1. Siz jamoat joylarida elektron gadjetlardan foydalanayotganingizda, kimdir muhim ma'lumotlarni o'g'irlaganida elkama-syorfing paydo bo'ladi. Hujumchilar shaxsiy ma'lumotlarni o'g'irlash yoki moliyaviy jinoyat sodir etish uchun kredit karta raqamlari va parollar kabi nozik ma'lumotlarni olishga intiladi.
2. **Xavfsizlik strategiyalari:** Yelkama-syorfingni oldini olish uchun qiyin, noyob parollardan foydalaning, hisoblar bo'ylab parollarni takrorlashdan saqlaning, ikki faktorli autentifikatsiyadan foydalaning va umumiy Wi-Fi tarmoqlariga ulanishda virtual xususiy tarmoqdan (VPN) foydalaning.

***1.3.4-rasm WLAN tarmog’idagi asosiy 5 ta xavfsizlik tahdidlari***

# II. BOB. WLAN Xavfsizligini Ta’minlash va Tahlil Usullari

## **2.1.WLAN tarmog’ini Cisco packet tracer orqali qurish**

**Maqsadlar**

Ushbu faoliyatda biz simsiz uy routerini va WLC-ga asoslangan tarmoqni sozlaymiz. Biz WPA2-PSK va WPA2-Korxona xavfsizligini amalga oshiramiz. Bu ishni quyidagi qadamlar bilan bajaramiz.

1. Turli qurilmalarga Wi-Fi ulanishini ta'minlash uchun uy routerini sozlaymiz.
2. Uy routerida WPA2-PSK xavfsizligini sozlaymiz.
3. WLC-da interfeyslarni sozlaymiz.
4. WLC-da WLAN-larni sozlaymiz.
5. WLAN-da WPA2-PSK xavfsizligini sozlang va xostlarni WLAN-ga ulaymiz.
6. WPA2-Enteprise-ni WLAN-da sozlang va xostlarni WLAN-ga ulaymiz.

**Ulanishni tekshiring WLAN ulanishi.**

*2.1.1-rasm. WLAN tarmog’ini qurish*

**Manzillar jadvali**

| Device-qurilmalar | Interface | IP Address |
| --- | --- | --- |
| Home Wireless Router | Internet | DHCP |
| LAN | 192.168.6.1/27 |
| RTR-1 | G0/0/0.2 | 192.168.2.1/24 |
| G0/0/0.5 | 192.168.5.1/24 |
| G0/0/0.100 | 192.168.100.1/24 |
| G0/0/1 | 10.6.0.1/24 |
| SW1 | VLAN 200 | 192.168.100.100/24 |
| LAP-1 | G0 | DHCP |
| WLC-1 | Management | 192.168.100.254/24 |
| RADIUS Server | NIC | 10.6.0.254/24 |
| Home Admin | NIC | DHCP |
| Enterprise Admin | NIC | 192.168.100.200/24 |
| Web Server | NIC | 203.0.113.78/24 |
| DNS Server | NIC | 10.100.100.252 |
| Laptop | NIC | DHCP |
| Tablet PC | Wireless0 | DHCP |
| Smartphone | Wireless0 | DHCP |
| Wireless Host 1 | Wireless0 | DHCP |
| Wireless Host 2 | Wireless0 | DHCP |

**WLAN ma’lumotlari**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| WLAN | SSID | Authentication | Username | Password |
| Home Network | HomeSSID | WPA2-Personal | N/A | Cisco123 |
| WLAN VLAN 2 | SSID-2 | WPA-2 Personal | N/A | Cisco123 |
| WLAN VLAN 5 | SSID-5 | WPA-2 Enterprise | userWLAN5 | userW5pass |

Vazifani 2 ta qismga bo’lamiz:

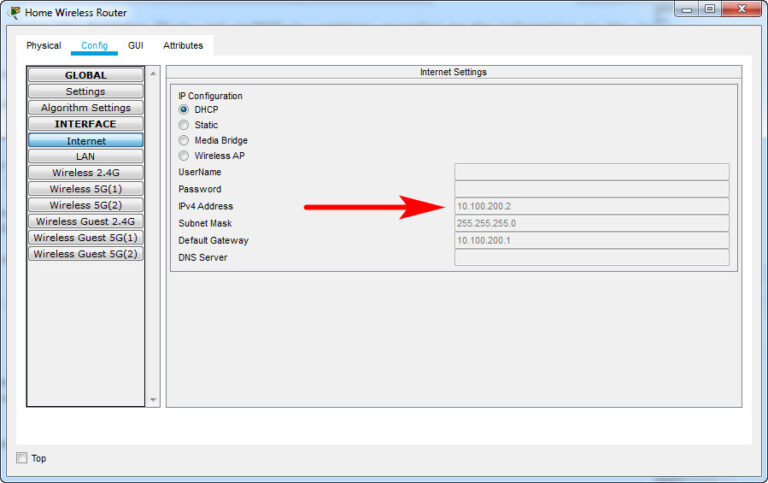
1. Uy routerini sozlash.

#### WLC Controllerning sozlash.

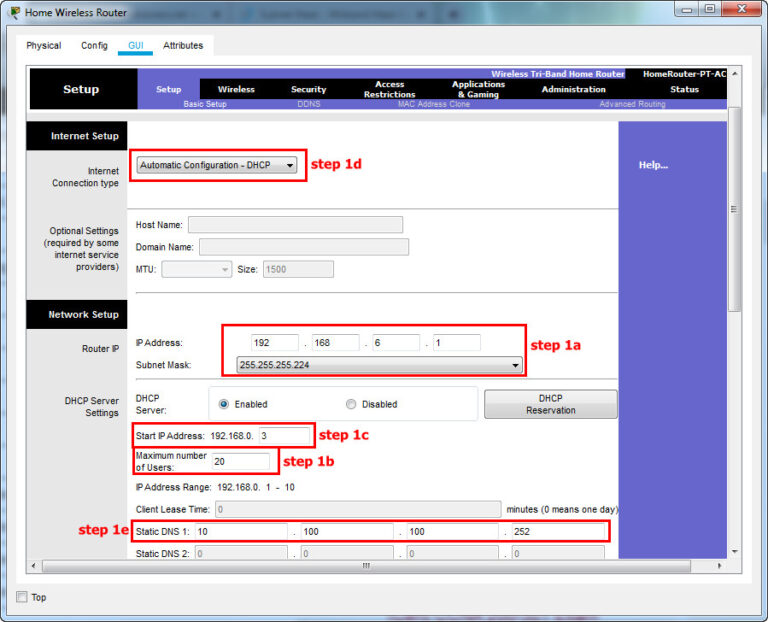
**1-qismni boshlaymiz.**

1-qadam.

1. Home Wireless Router GUI-ni oching va manzillar jadvalidagi ma'lumotlarga muvofiq router IP va DHCP sozlamalarini o'zgartiring.
2. Router tomonidan maksimal **20** ta manzilni chiqarishga ruxsat beramiz.
3. DHCP serverini LAN tarmog'ining .3 IP manzilidan boshlash uchun sozlaymiz.
4. Routerning internet interfeysini uning IP manzilini DHCP orqali olish uchun sozlaymiz (2.2-rasmdagidek).

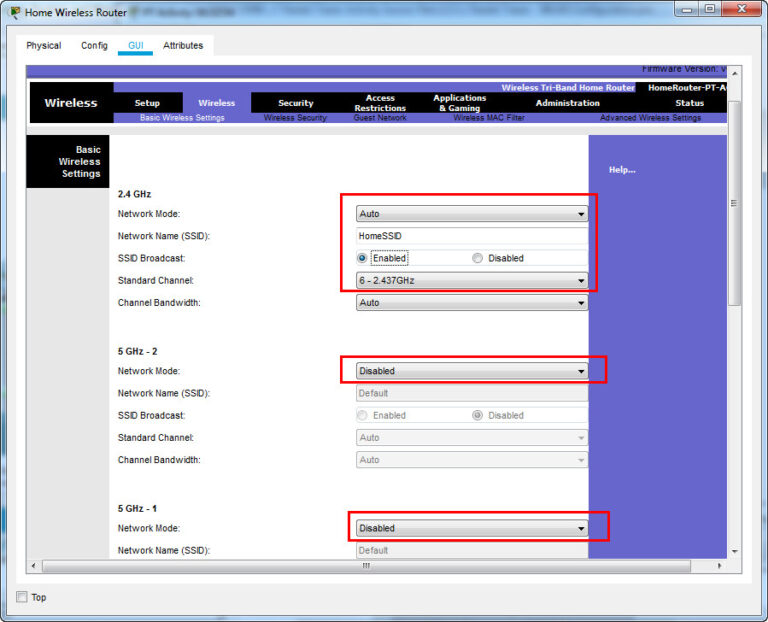
 *2.1.2-rasm.* Home Wireless Router sozlash.

1. Statik DNS serverini manzillar jadvalidagi manzilga sozlaymiz.

*2.1.3-rasm. Home Wireless Router Setup ni sozlaymiz.*

##### **2-qadam: WLANni sozlash.**

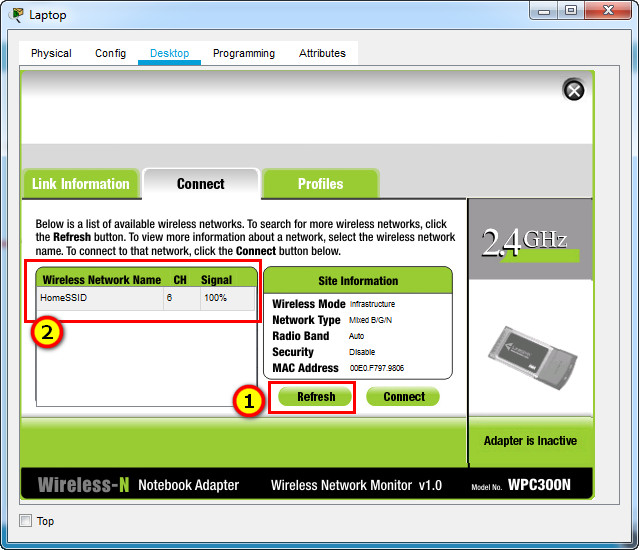
Tarmoq 2,4 gigagertsli simsiz LAN interfeysidan foydalanadi. Simsiz LAN ma'lumotlar jadvalida ko'rsatilgan SSID bilan interfeysni sozlaymiz.

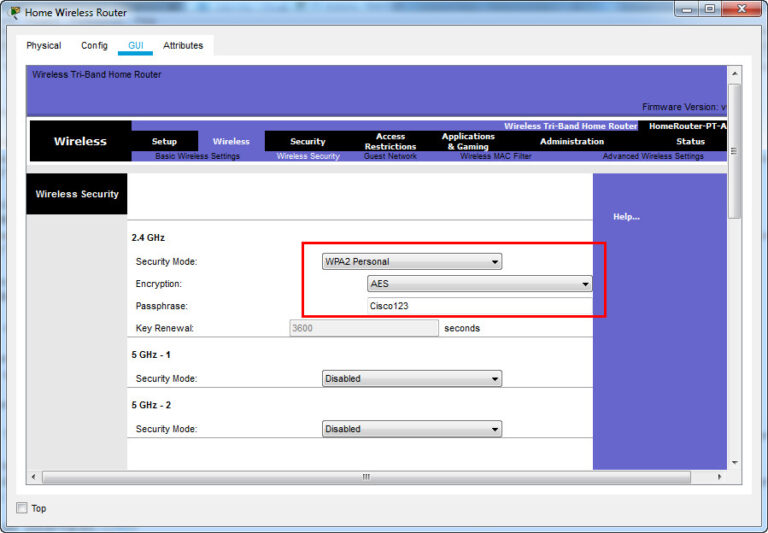
*2.1.4-rasm. Home Wireless Router wireless ni sozlash.*

##### **3-qadam: Xavfsizlikni sozlaymiz.**

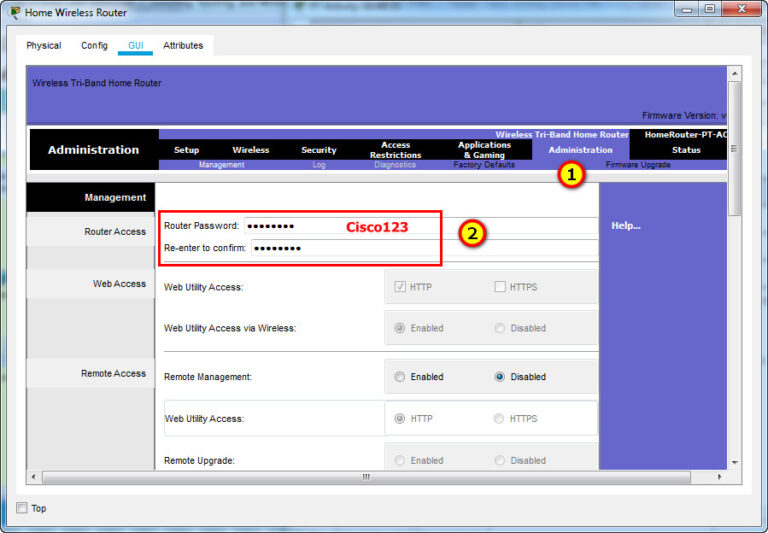
Simsiz LAN xavfsizligini sozlang. **WPA2 Personal**va Simsiz LAN ma'lumotlar jadvalida ko'rsatilgan parol iborasidan foydalanamiz.

Uydagi barcha simsiz hostlar SSID-ni ko'ra olishiga ishonch hosil qiling. Buni ko'rish uchun: **Laptop** –> **PC Wireless** –> **Connect**

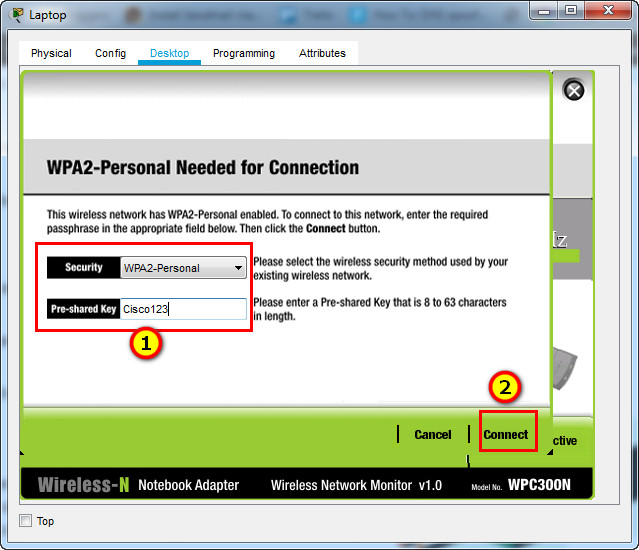
*2.1.5-rasm. Home Wireless Router wireless ni sozlash.*

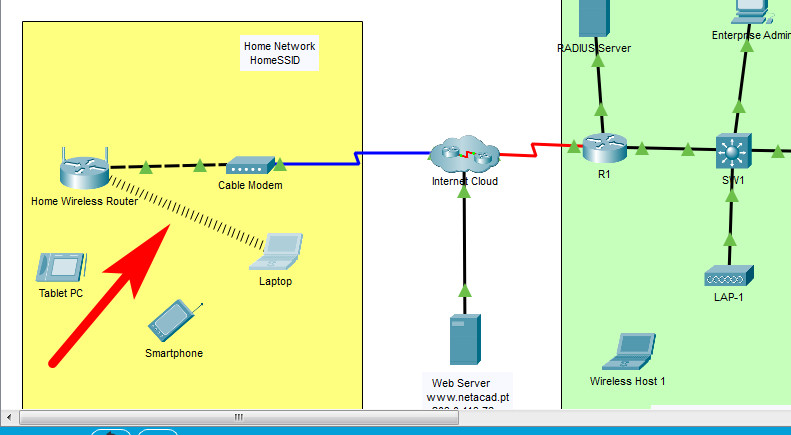
*2.1.6-rasm. Home Wireless Router wireless ni sozlash.*

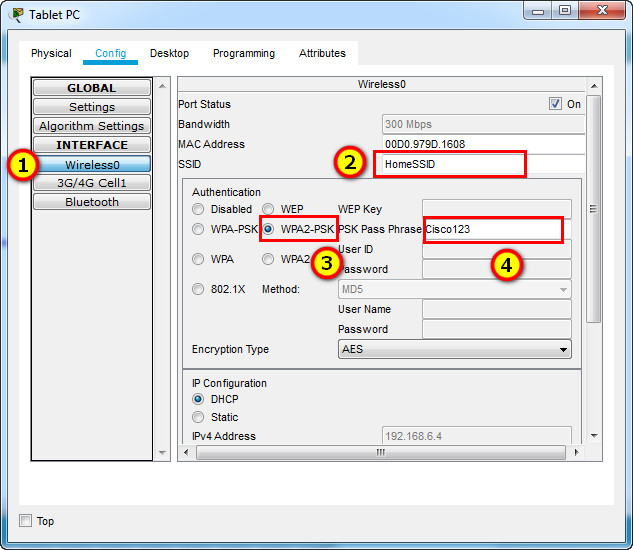
Simsiz LAN ma'lumotlar jadvalida ko'rsatilgan qiymatga standart parolni o'zgartirish orqali marshrutizatorni himoyalaymiz.

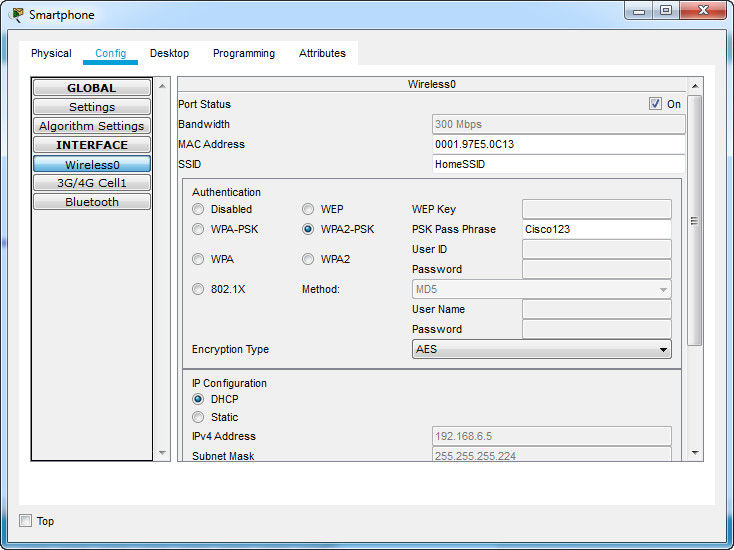
*2.1.7-rasm. Home Wireless Router xavfsizligni sozlash*

##### **4-qadam: Tarmoqqa ulanish.**

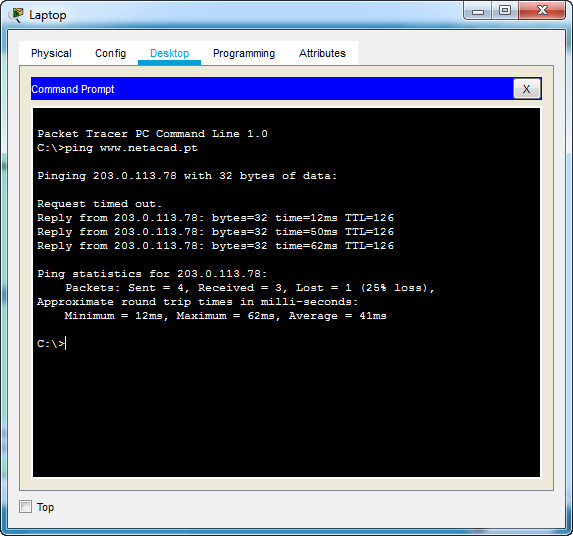
 *2.7-rasm. Noutbuk orqali ulanish.*

***2.1.8-rasm. Ulangan qurilmalarni ko’rinishi.***

***2.1.9-rasm. Planshet orqali ulanish.***

***2.1.10-rasm. Smartphone orqali ulanish.***

**Kompyuter orqali ulanganimiz tekshirish uchun ping orqali tekshirib ko’ramiz.**

***2.1.11-rasm. Ping bilan*** [*www.netacad.pt*](http://www.netacad.pt/) ***ga so’rov yuborib ko’ryapmiz***

****2-qism. WLC Controllerning sozlaymiz****

**Simsiz LAN kontrollerni ikkita WLAN bilan sozlaymiz. Bitta WLAN WPA2-PSK autentifikatsiyasidan foydalanamiz. Boshqasi WLAN WPA2-Enterprise autentifikatsiyasidan foydalanadi. Shuningdek, biz WLC-ni SNMP serveridan foydalanish uchun sozlaysiz va simsiz boshqaruv tarmog'i tomonidan foydalaniladigan DHCP doirasini sozlaymiz.**

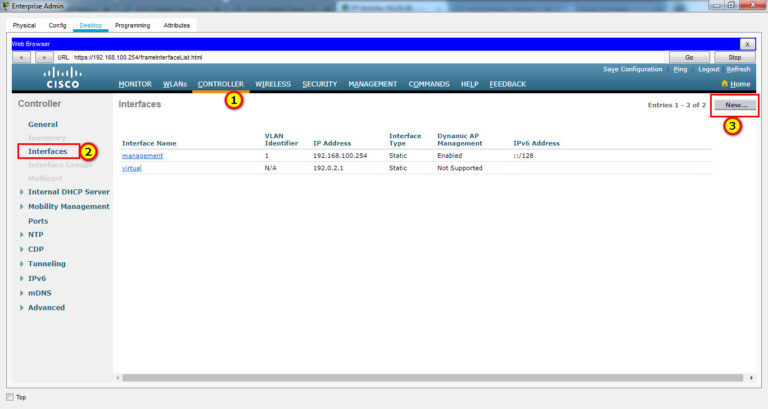
##### **1-qadam: VLAN interfeyslarini sozlash.**

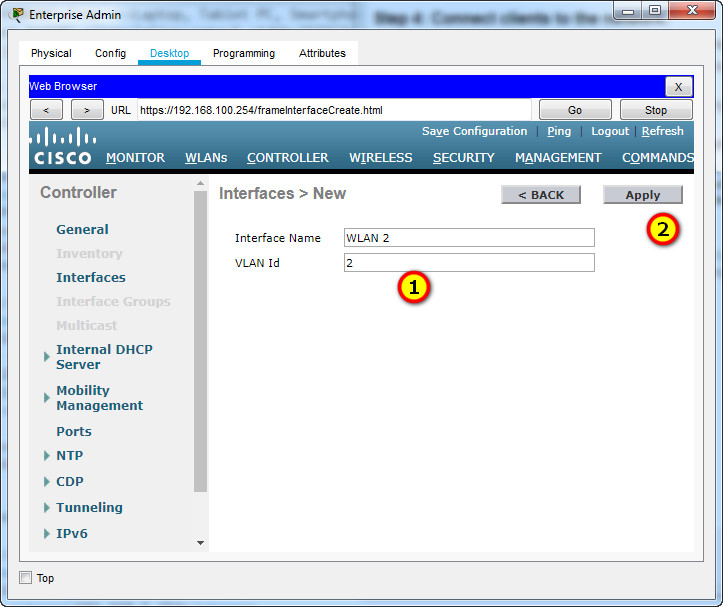
1. **Korxona boshqaruvchisidan veb-brauzer orqali WLC-1 boshqaruv interfeysiga o'ting. WLC-1 tizimiga kirish uchun foydalanuvchi nomi sifatida admin va parol sifatida Cisco123 dan foydalaning. Enterprise Admin PC**

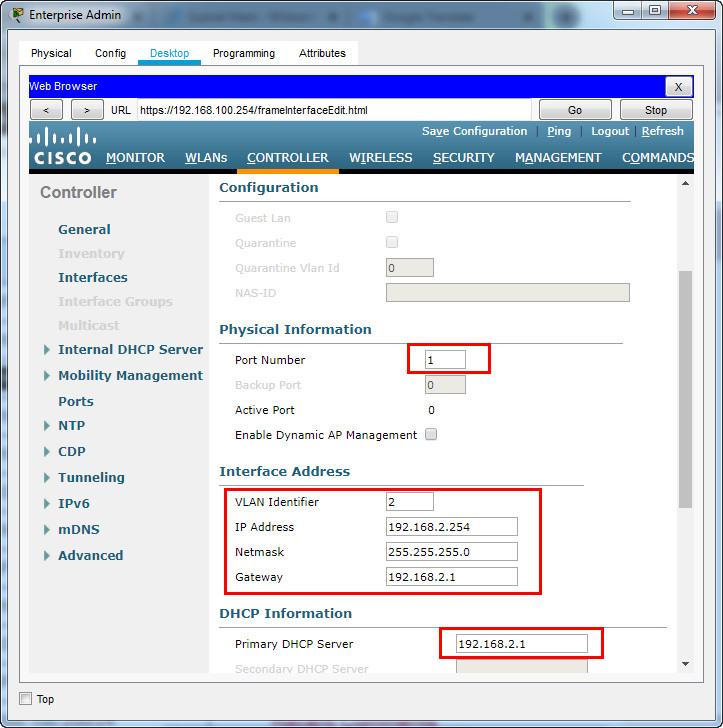
***2.1.12-rasm. Enterprise Admin PC.***

1. **Birinchi WLAN uchun interfeysni sozlash.**

Nomi: **WLAN 2**  
VLAN identifikatori: **2**  
Port raqami: **1**  
Interfeys IP manzili: **192.168.2.254**  
Tarmoq maskasi: **255.255.255.0**  
Shlyuz: **RTR-1 G0/0/0.2 manzili**  
Asosiy DHCP serveri: **Gateway manzili**

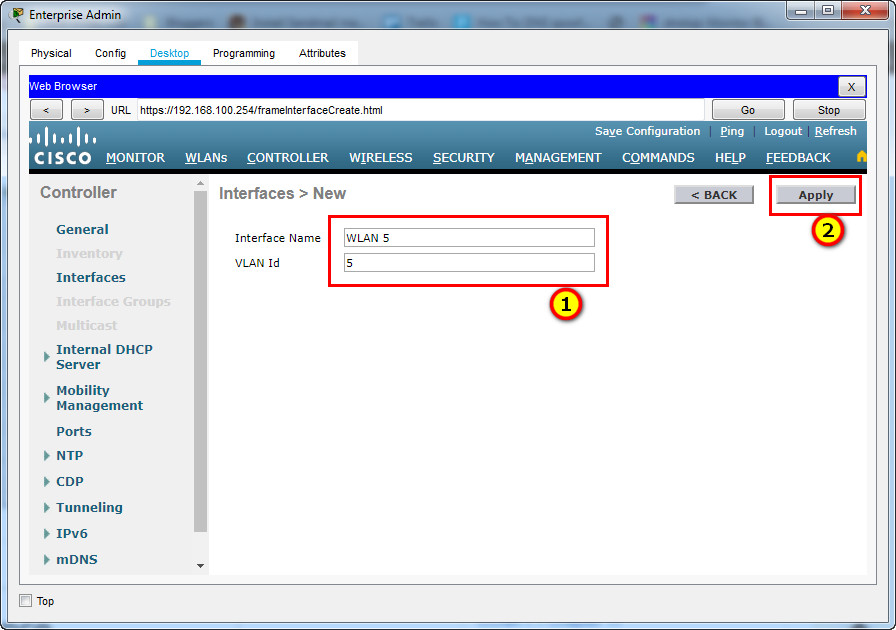
***2.1.13-rasm***

***2.1.14-rasm***

***2.1.15-rasm. Birinchi WLAN uchun interfeysni sozlash.***

**c) Ikkinchi WLAN uchun interfeysni sozlash.**

**Nomi: WLAN 5  
VLAN identifikatori: 5  
Port raqami: 1  
Interfeys IP-manzili: 192.168.5.254  
Tarmoq maskasi: 255.255.255.0  
Gateway: RTR-1 interfeysi G0/0/0.5 manzili  
Asosiy DHCP serveri: Gateway manzili**

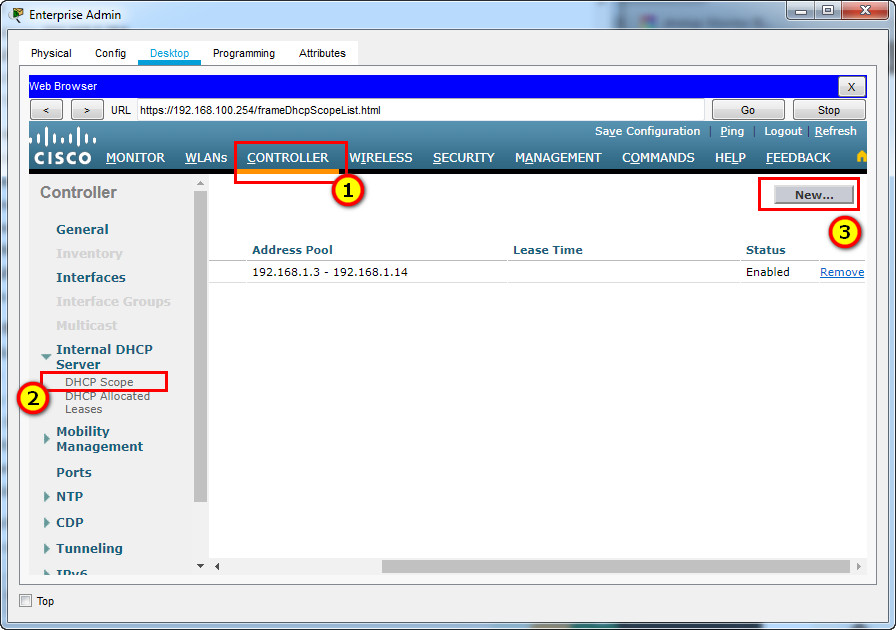
***2.1.16-rasm***

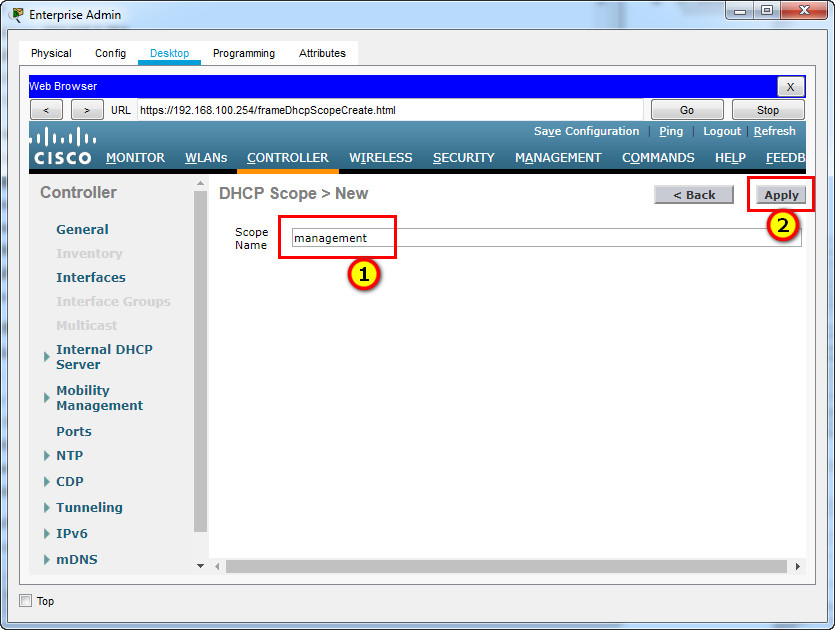
***2.1.17-rasm. Ikkinchi WLAN uchun interfeysni sozlash***

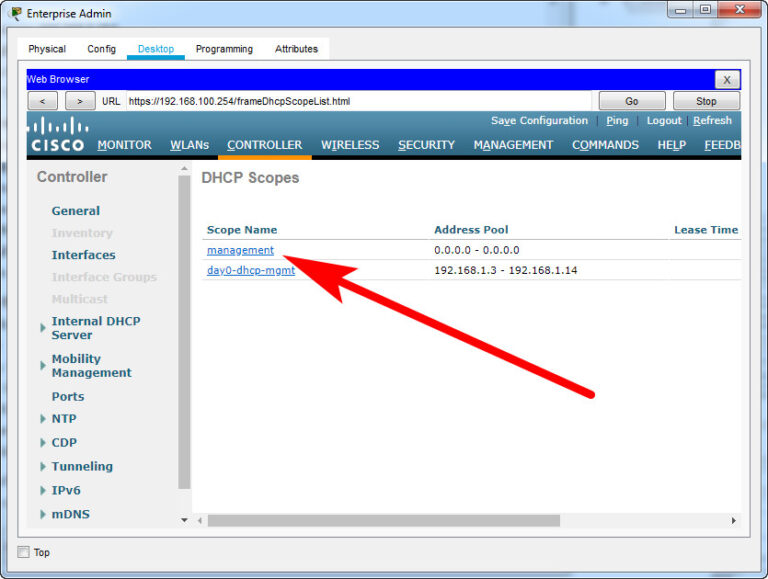
**2-qadam: Simsiz boshqaruv tarmog'i uchun DHCP doirasini sozlash**

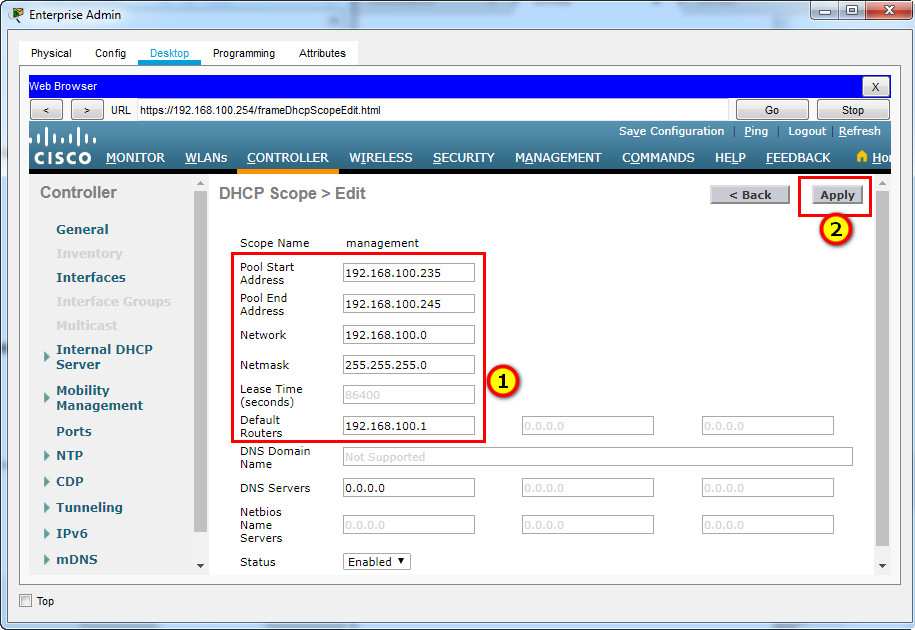
**Ichki DHCP qamrovini quyidagi tarzda sozlaymiz va yoqamiz:**

Qo‘llanish sohasi nomi: **boshqarish**  
Pool Start Manzil: **192.168.100.235**  
Pool End Manzil: **192.168.100.245**  
Tarmoq: **192.168.100.0**  
Netmask: **255.255.255.0**  
Standart Routerlar: **192.168.100.1**

***2.1.18-rasm.***

***2.1.19-rasm.***

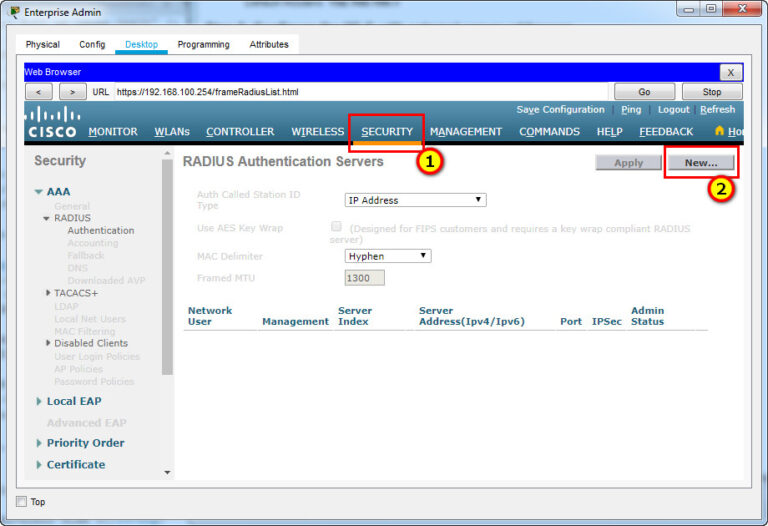
***2.1.20-rasm.***

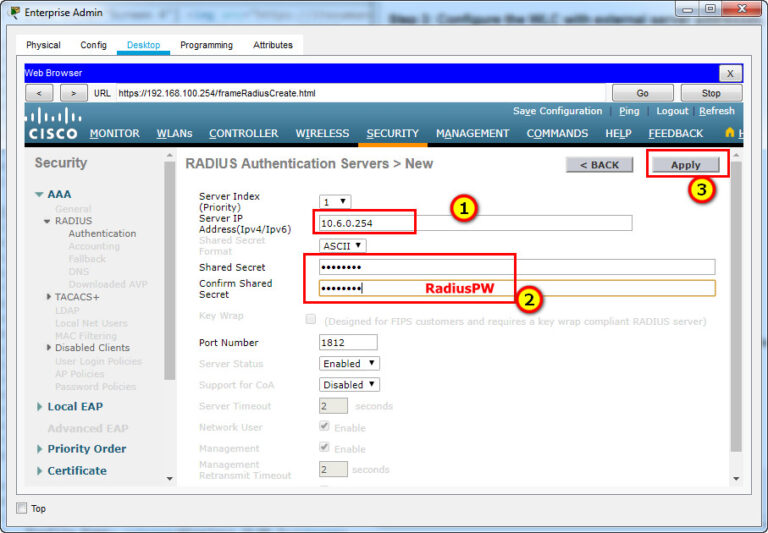
***2.1.20-rasm.Ichki DHCP qamrovini sozlash va yoqish***

##### **3-qadam: WLC-ni tashqi server manzillari bilan sozlang.**

**RADIUS** server ma'lumotlarini quyidagicha sozlaymiz.

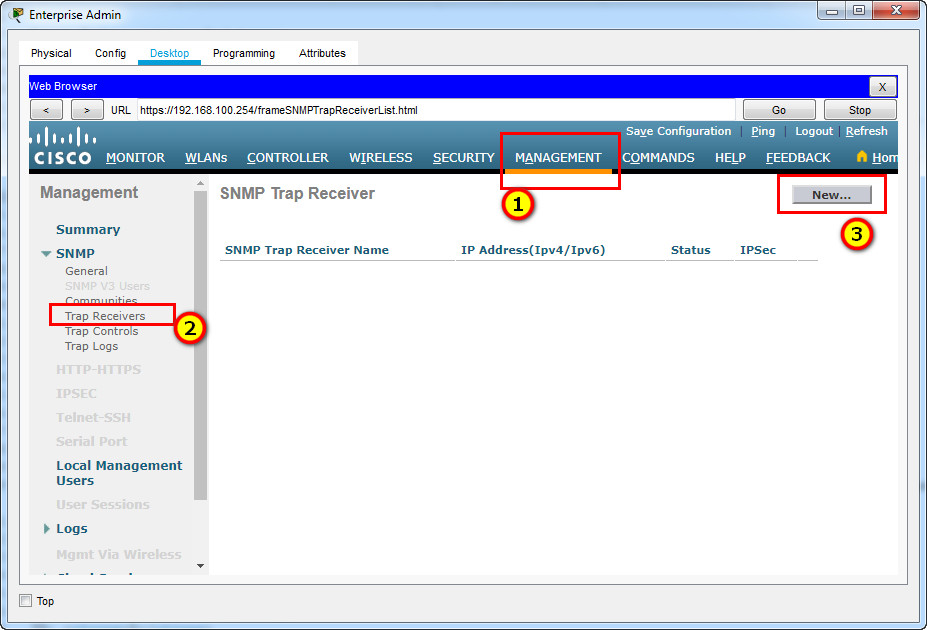
Sever indeksi: **1**  
Sever manzili: **10.6.0.254**  
Umumiy parol: **RadiusPW**

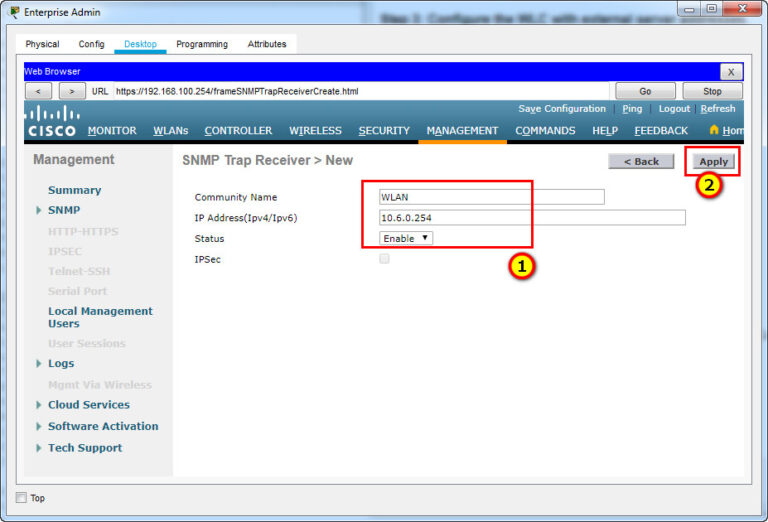
***2.1.21-rasm.***

***2.1.22-rasm. RADIUS server ma'lumotlarini sozlash***

**WLC-ni jurnallar ma'lumotlarini SNMP serveriga yuborish uchun sozlash**

Hamjamiyat nomi: **WLAN**  
IP manzili: **10.6.0.254**

***2.1.23-rasm***

***2.1.24-rasm***

**4-qadam: WLAN-larni yaratish.**

Birinchi WLAN-ni yaratamiz:

Profil nomi: **Simsiz VLAN 2**  
WLAN SSID: **SSID-2**  
ID: **2**  
Interfeys: **WLAN 2**  
Xavfsizlik: **WPA2-PSK**  
Parol: **Cisco123**

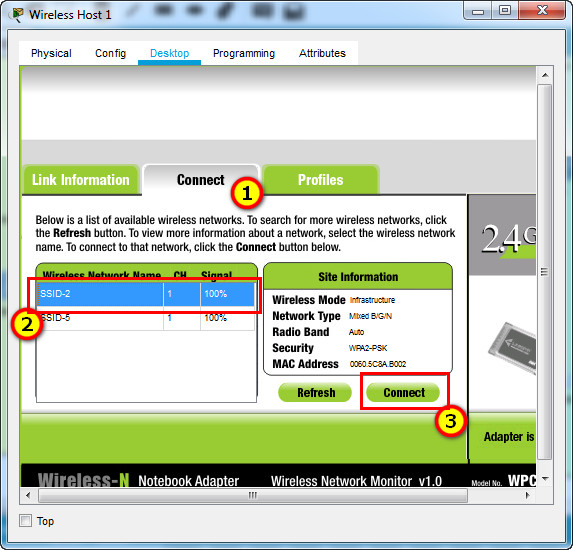
**Ikkinchi WLAN-ni yarating:**

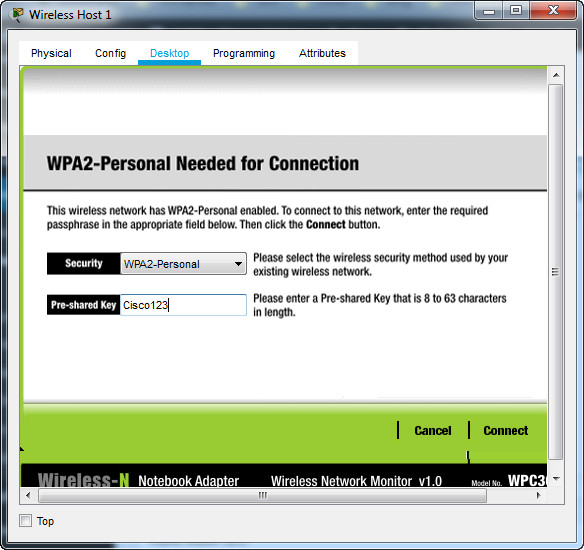
Profil nomi: **Simsiz VLAN 5**  
WLAN SSID: **SSID-5**  
Interfeys: **WLAN** 5  
ID: **5**  
Xavfsizlik: **802.1x – WPA2-Enterprise**

**Bu qadamlarni 1-qadamga qarab ko’rsak bo’ladi.**  
Autentifikatsiya qilish uchun RADIUS serveridan foydalanish uchun WLANni sozlaymiz. **FlexConnect** sozlamalarini 4a-qadamda bajarilganidek o'rnatamiz.

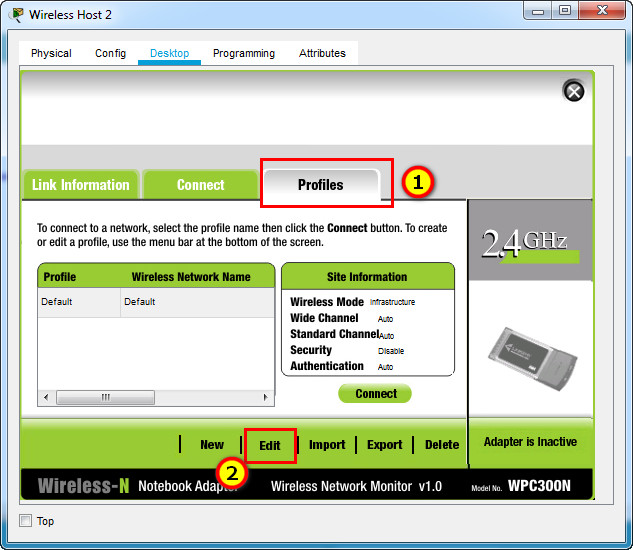
##### **5-qadam: WLAN-larga ulanish uchun xostlarni sozlash**

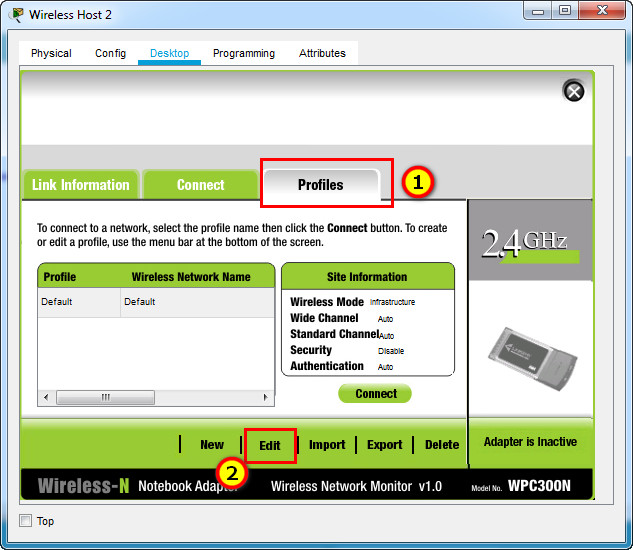
**Simsiz Xost 1 Simsiz VLAN 2 ga ulanishi kerak.**

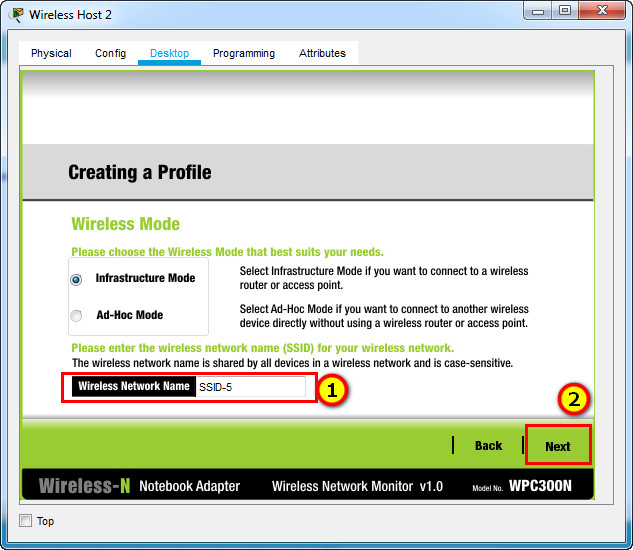
***2.1.25-rasm***

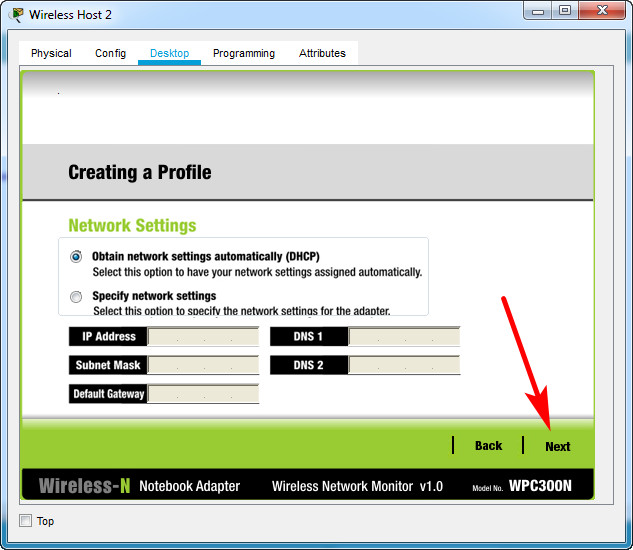
***2.1.26-rasm***

**Wireless Host 2 Wireless VLAN 5 ga WLAN maʼlumotlar jadvalidagi hisobga olish maʼlumotlari yordamida ulanishi kerak.**

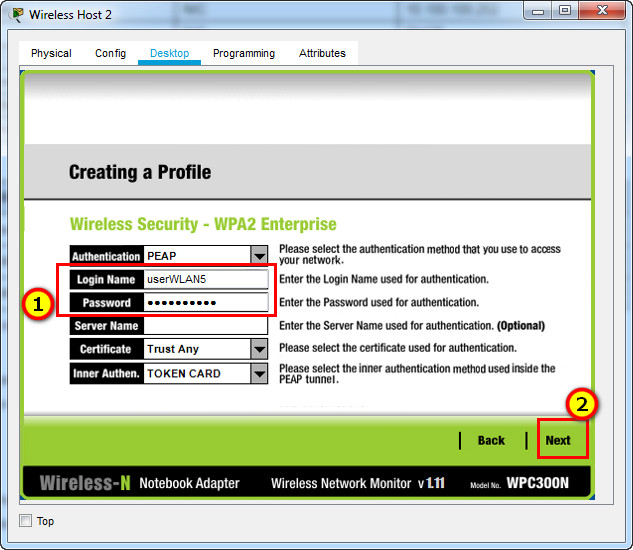
***2.1.27-rasm***

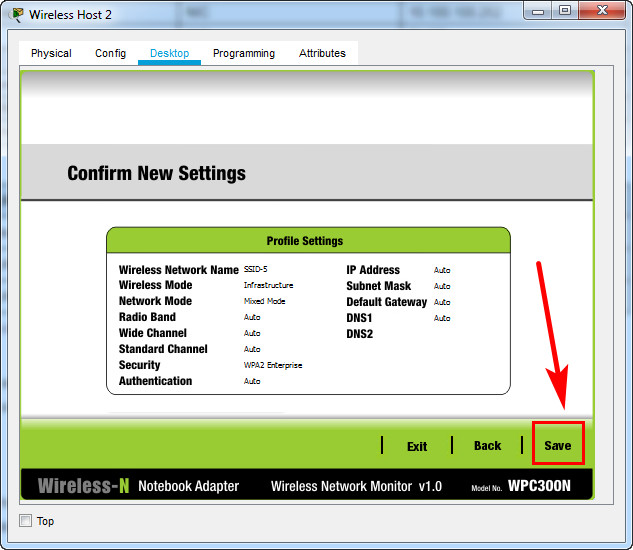
***2.1.28-rasm***

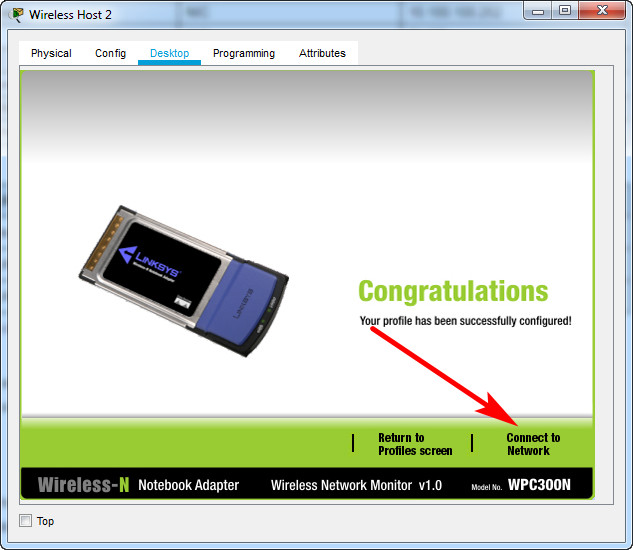
***2.1.29-rasm***

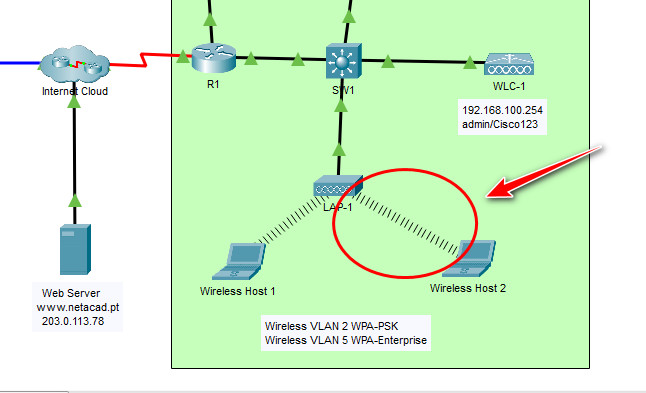
***2.1.30-rasm***

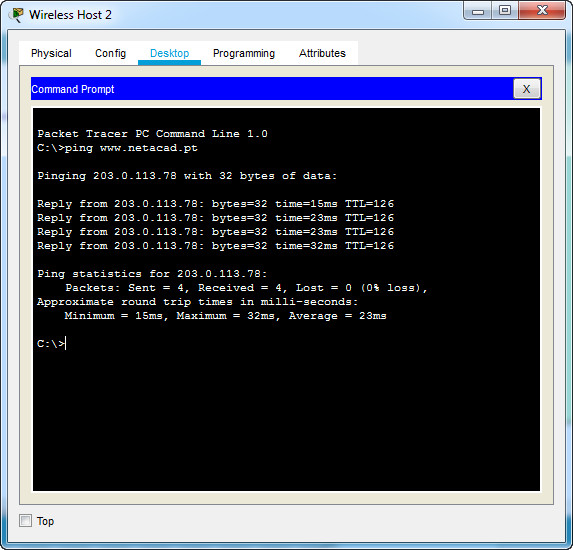
***2.1.31-rasm***

***2.1.32-rasm***

***2.1.33-rasm***

***2.1.34-rasm***

***2.1.35-rasm. Qurilmalar ulanganini ko’rishimiz mumkin.***

***2.1.36-rasm.Ping bilan*** [*www.netacad.pt*](http://www.netacad.pt/) ***ga so’rov yuborib ko’ryapmiz va ishlayotganini ko’rishimiz mumkin.***

## **XULOSA**

WLAN tarmoqlari zamonaviy aloqa tizimlarining ajralmas qismi bo'lib, ko'plab uylar, ofislar va boshqa muassasalarda ishlatiladi. Biroq, bu tarmoqlar o'zining o'ziga xos xavfsizlik muammolari bilan ham yuzma-yuz keladi. Asosiy xavflar, tarmoq orqali ma'lumotlarning o'zgarishi, ushlab qolish, yoki noto'g'ri qo'llanilgan shifrlash tizimlaridan kelib chiqishi mumkin.

WLAN xavfsizligi uchun eng muhim omillar orasida shifrlash protokollari, autentifikatsiya usullari va tizimlar o'rtasidagi o'zaro aloqalar xavfsizligini ta'minlash kiradi. Bunga WEP (Wired Equivalent Privacy), WPA (Wi-Fi Protected Access) va WPA2 kabi shifrlash protokollari kiradi. WEP protokoli eski va osonlik bilan buzilishi mumkin, shuning uchun WPA2 yoki WPA3 kabi zamonaviy va xavfsiz shifrlash tizimlaridan foydalanish tavsiya etiladi.

WLAN tarmoqlarida xavfsizlikni ta'minlash uchun tarmoq administratorlari tomonidan tarmoqni himoya qilish, foydalanuvchi autentifikatsiyasini kuchaytirish, tarmoqning kuchli parollarini belgilash va routerlarni soxta tarmoqlardan himoya qilish kabi bir qator choralarga e'tibor qaratilishi kerak.

Shuningdek, WLAN tarmoqlarida xavfsizlikni ta'minlash uchun antivirus dasturlaridan foydalanish, tarmoq trafikini doimiy ravishda monitoring qilish, xavfsizlik tahlillarini amalga oshirish va Wi-Fi tarmoqlarining zaif joylarini aniqlash zarur.

Umuman olganda, WLAN tarmog'ining xavfsizligi yuqori darajada ta'minlanishi uchun barcha foydalanuvchilar va tarmoq administratorlari tomonidan ehtiyotkorlik va ilg'or xavfsizlik texnologiyalaridan foydalanish zarur.

## **FOYDALANILGAN ADABIYOTLAR RO’YXATI**

1. Coleman, D. D., & Westcott, D. A. (2007). CWSP Certified Wireless Security Professional Official Study Guide. Wiley Publishing.
2. Gast, M. S. (2014). 802.11 Wireless Networks: The Definitive Guide. O'Reilly Media.
3. Nichols, R. K., & Lekkas, P. C. (2004). Wireless Security: Models, Threats, and Solutions. McGraw-Hill.
4. Sanders, C. (2017). Practical Packet Analysis: Using Wireshark to Solve Real-World Network Problems. No Starch Press.
5. Beaver, K., & Davis, P. T. (2011). Hacking Wireless Networks For Dummies. Wiley Publishing.
6. Xu, X., & Zhang, L. (2018). A Survey of WLAN Security. IEEE Communications Surveys & Tutorials, 20(4), 2836-2858.
7. **Yang, Y., & Liu, X. (2020). Vulnerability Analysis of WPA3 Protocol. Journal of Information Security and Applications, 53, 102415.**
8. Zhao, M., & Yang, Y. (2019). WLAN Security: Understanding WPA, WPA2, and WPA3. ACM Computing Surveys, 52(4), 1-34.
9. **Musaev M.M. “Kompyuter tizimlari va tarmoqlari”. Toshkent.: “Aloqachi” nashriyoti, 2013 yil. 8 bob. 394 bet. – Oliy o‘quv yurtlari uchun qo‘llanma**
10. **"Axborot texnologiyalari va kommunikatsiyalar" jurnali 0156**

**INTERNET SAYTLARI**

1. [https://www.wi-fi.org](https://www.wi-fi.org/)
2. https://owasp.org
3. [https://www.cisco.com](https://www.cisco.com/)
4. <https://explained.uz/>
5. <https://youtu.be/y-vhW7XNZGA?si=QCkQGbmmtkGnZsat>
6. <https://github.com/Beksult0n/WLAN_network_security>