11 WIRELESS LOCAL AREA NETWORK (WLAN)

**О.Энэрэл 22B1NUM0506**

**МТЭС, Програм хангамж**

**Ажлын зорилго**

Энэ лабораторийн ажлаар бид утасгүй дотоод сүлжээний IEEE 802.11 протоколын талаар судлах болно.

**Үндсэн ойлголт**

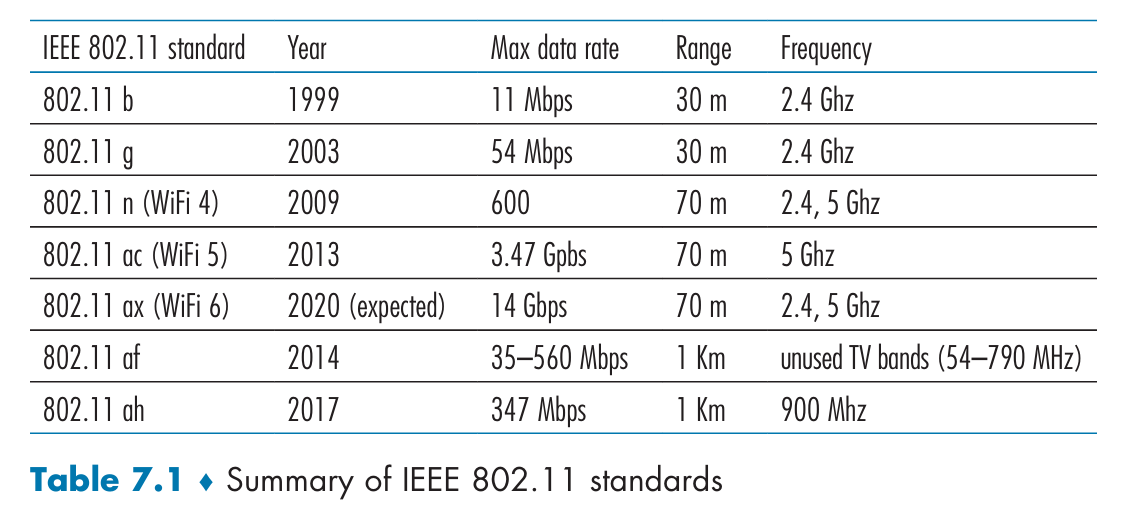
Утасгүй сүлжээ гэдэг нь радио долгион ашиглан төхөөрөмжүүдийг холбодог сүлжээ юм. Бидний өдөр тутам ашигладаг Wi-Fi нь 802.11 стандарт дээр суурилдаг.

Wireless network-ийн элементүүд:

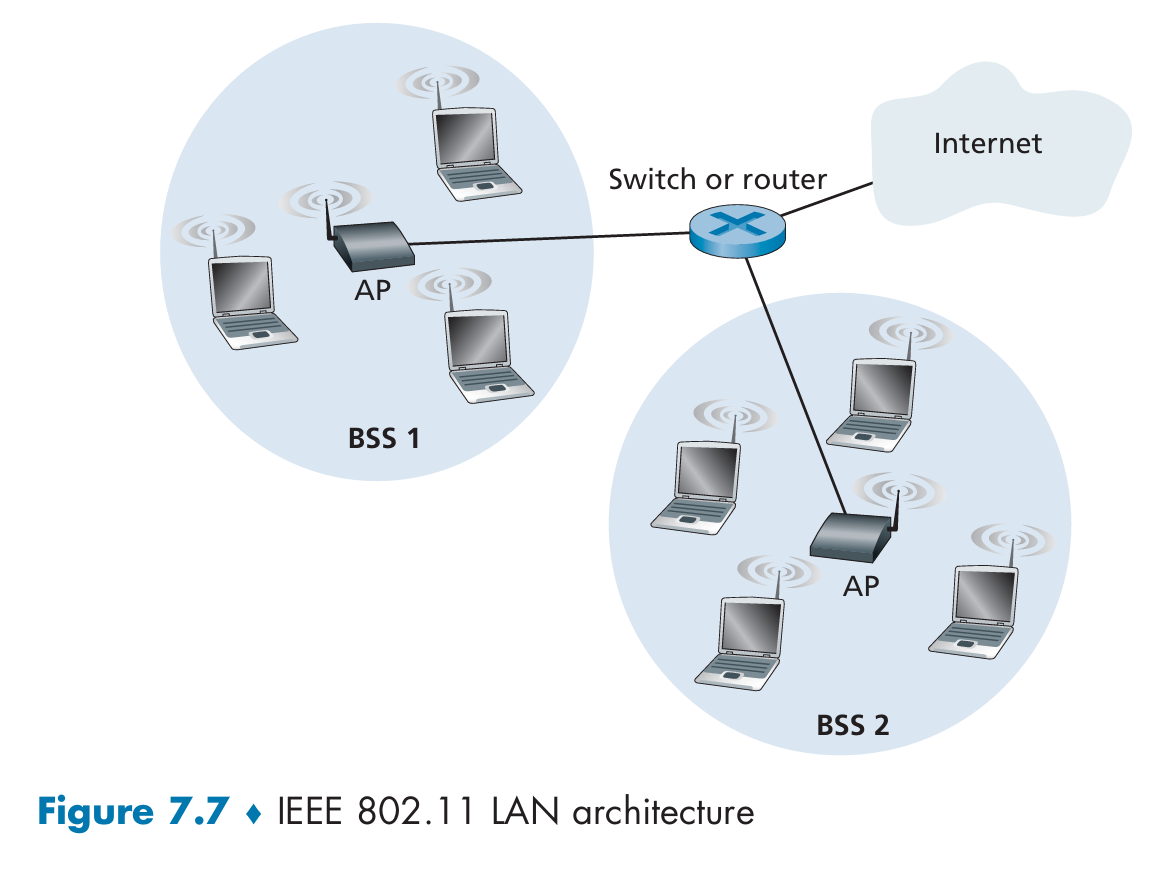
*Wireless hosts:* Утасгүй сүлжээнд холбогдох боломжтой төхөөрөмжүүд. Эдгээр төхөөрөмжүүд нь 802.11 сүлжээний адаптер бүхий MAC хаягтай байдаг.

*Base Station:* Утасгүй сүлжээний төвлөрсөн удирдлагын төхөөрөмж. Access Point (AP) эсвэл Wireless Router хэлбэрээр ажилладаг.

*Wireless links*: Төхөөрөмжүүд болон суурь станцуудын хооронд мэдээлэл дамжуулах радио долгион ашигласан холбоос. 802.11 стандарт нь 2.4 GHz болон 5 GHz зурвас дахь утасгүй холбоог тодорхойлдог. Холбоосын гүйцэтгэл нь дохионы чанар, сувгийн сонголтоос хамаардаг.



* 1. WLAN архитектур



*BSS (Basic Service Set):* Суурь нэгж. Нэг AP болон түүнд холбогдсон төхөөрөмжүүдээс бүрдэнэ.

*SSID (Service Set Identifier):* Сүлжээний нэр.

*Channel (Суваг):* Сүлжээний администратор AP-д тодорхой суваг оноодог (жишээ нь: 2.4 GHz-д 1, 6, 11 дугаар суваг).

IEEE 802.11 фреймийн төрөл

1. Management Frames:  
   Холболт үүсгэх, удирдах.

Subtypes: Beacon, Probe Request/Response, Association Request/Response, Authentication, Deauthentication, г.м.

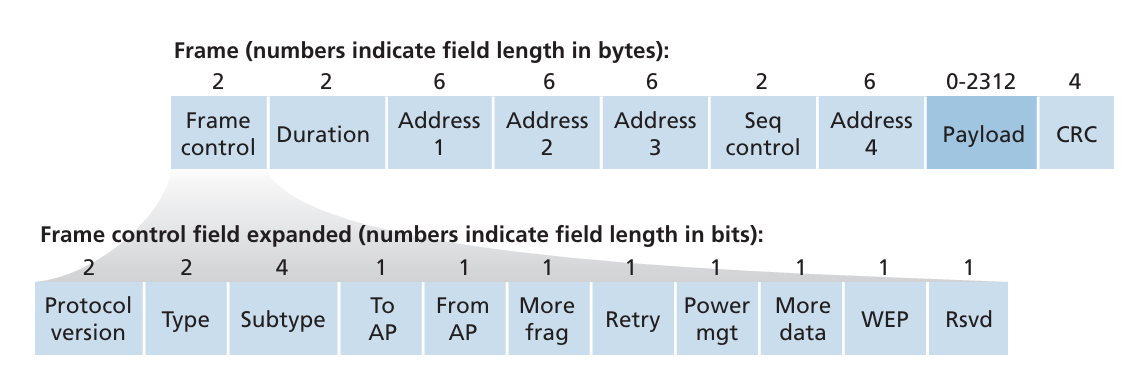
1. Control Frames:  
   Холболтыг хянах:

Subtypes: ACK, RTS (Request to Send), CTS (Clear to Send), PS-Poll (Power Save Poll).

1. Data Frames:  
   Төхөөрөмжүүдийн хооронд бодит өгөгдөл дамжуулдаг.

Subtypes: Data, Null Data ( used for power management), QoS Data (for Quality of Service).

802.11 frame-ийн бүтэц



* Frame Control 2byte：Frame -ийн control мэдээллийг хадгалдаг. Үүнд:
* Protocol Version (2 bits): 802.11 protocol -ийн хувьлбар ихэнхдээ 00 байдаг.
* Type (2 bits): Frame -ийн төрөл
* Subtype (4 bits): main type (e.g., Beacon, ACK).
* Flags
* To DS (1 бит): Frame Distribution Sytem рүү явж буй эсэх.
* From DS (1 бит): DS-ээс ирж буй эсэх.
* More Fragments (1 бит): Илүү хуваагдсан хэсэг байгаа эсэх.
* Retry (1 бит): Дахин дамжуулалтийг заана.
* Power Management (1 бит): power-saving mode..
* More Data (1 бит): Илүү өгөгдөл байгаа эсэх.
* Protected Frame (1 бит): Фрейм шифрлэгдсэн эсэх.
* Order (1 бит): Нарийн дараалал шаардлагатай эсэх.
* Duration/ID (2 байт):
* Өгөгдөл болон менежментийн фреймд: зөөвөрлөгчийн хадгалах хугацааг микросекундээр заана..
* Хяналтын фреймд: Association ID.
* Хаягууд(тус бүр 6 байт):
* Хаяг1: Энэ хаяг нь фреймийг хүлээн авах станцын MAC хаяг байна. Хэрэв утасгүй станц фрейм дамжуулж байвал Address 1 нь тухайн фреймийн очих AP-ийн MAC хаяг байна.
* Хаяг 2: Энэ хаяг нь фреймийг дамжуулж буй станцын MAC хаяг байна. Хэрэв Access Point (AP) фрейм дамжуулж байвал AP-ийн MAC хаяг Address 2 талбарт бичигдэнэ.
* Хаяг 3: Энэ хаяг нь BSS-ээс гадна холбогдсон сүлжээний завсрын төхөөрөмжийн MAC хаяг байна. Жишээ нь, фрейм BSS-ээс гарч, өөр сүлжээ рүү чиглэж байгаа бол Address 3 талбарт тухайн рүтерын интерфейсийн MAC хаяг бичигдэнэ.
* Хаяг 4: WDS горимд ашиглагдана.
* Sequence Control (2 байт):
* Fragment Number (4 бит)
* Sequence Number (12 бит)
* Payload:
* Бодит өгөгдлийг агуулна.
* FCS (Frame Check Sequence) (4 байт):
* CRC нь алдаа илрүүлдэг.

802.11 Сүлжээний Үйл Ажиллагаа

1) Сүлжээг хайх (Scaning)

* Passive Scanning：Beacon Frame ашиглана. Access Point нь үе үе beacon frame илгээж, өөрийн SSID, суваг зэрэг мэдээллийг зарладаг. STA нь эдгээр Beacon Frame-ийг хүлээн авч, ямар сүлжээ байгаа талаар мэдэж авна.
* Active Scanning：STA нь Probe Request фрейм илгээж, боломжит AP-уудаас хариу хүсдэг. AP-ууд Probe Response фреймээр хариулж, STA-д өөрийн мэдээллийг өгдөг.

2) Баталгаажуулалт (Authentication)

STA нь AP-тай холбогдох эрхтэй эсэхийг шалгах.

* STA нь Authentication Request фреймийг AP-д илгээнэ.
* AP нь хүлээн авч, Authentication Response фрейм илгээж, зөвшөөрөх эсвэл татгалзах шийдвэрийг өгнө.

3) Холболт үүсгэх (Association)

STA нь AP-тай албан ёсоор холбогдож, өгөгдөл дамжуулах боломжтой болно.

* STA нь Association Request фреймийг илгээнэ. Энэ нь STA-ийн MAC хаяг болон SSID зэрэг мэдээллийг агуулна.
* AP нь Association Response фрейм илгээж, STA-д Association ID олгож, холболтыг баталгаажуулна.

4) Өгөгдөл дамжуулах

STA болон AP нь хоорондоо өгөгдөл солилцоно.

* Data Frame: Өгөгдөл дамжуулахад ашиглагдана. Фреймийн Address 1, Address 2, Address 3 талбарт хаягууд бичигдэнэ.
* ACK Frame: STA эсвэл AP нь хүлээн авсан фреймийг баталгаажуулж, ACK фрейм илгээнэ.
* ACK фрейм ирээгүй тохиолдолд фреймийг дахин дамжуулна.

5) Алдаа засах

* Фрейм бүр нь FCS гэсэн хэсэгтэй байдаг, энэ нь алдааг илрүүлж, засах боломжийг олгодог.
* CRC ашиглан фреймийн алдааг шалгана.
* Хэрэв алдаа илэрвэл ACK фрейм хүлээн авалгүй дахин дамжуулалт хийнэ.

5) Power Saving

STA нь эрчим хүч хэмнэх горимд шилжих үед ашиглана.

* PS-Poll Frame: STA нь AP-аас хадгалагдсан өгөгдлийг авах хүсэлт илгээнэ.
* Null Data Frame: Эрчим хүч хэмнэх зорилгоор өгөгдөлгүй фрейм илгээж, холболтыг идэвхтэй байлгадаг.

6) Холболт таслах (Deauthentication)

STA эсвэл AP нь холболтыг дуусгах үед ашиглана.

* Deauthentication Frame: Холболтыг таслах шийдвэр гаргасан STA эсвэл AP нь энэ фреймийг илгээж, сүлжээнээс гарах үйлдлийг хийнэ.

802.11 -гийн хоёр үндсэн топологийг:

Infrastructure Mode (Дэд Бүтцийн Горим)

* + STA-ууд нь **Access Point (AP)**-ээр дамжуулан холбогдоно.
  + Ихэнх байгууллага, гэрийн сүлжээнд ашиглагддаг.

Ad-Hoc Mode

* + STA-ууд хоорондоо шууд холбогдоно.
  + AP шаардлагагүй, түр зуурын сүлжээнд тохиромжтой.

Аюулгүй Байдал

* 1. үлжээнд аюулгүй байдлыг хангах хэд хэдэн протоколууд байдаг:

1. WEP : WEP нь RC4 шифрлэлтийг ашиглаж өгөгдлийг хамгаална. Шифрлэх үед IV (Initialization Vector) хэмээх санамсаргүй утгыг ашиглан өгөгдлийг шифрлэнэ. WEP-ийн гол сул тал нь IV нь 24-bit хэмжээтэй тул давтагдах магадлал өндөр байдаг бөгөөд энэ нь шифрлэлтийг эвдэхэд хялбар болгодог.
2. WPA : TKIP нь WEP-ийн сул талыг шийдэх зорилготойгоор бүтээгдсэн. Түлхүүрийг динамикаар сольж, IV-ийн хэмжээг нэмсэн. Message Integrity Check (MIC) механизмаар өгөгдлийн бүрэн бүтэн байдлыг шалгадаг. WEP-ийн сайжруулсан хувилбар. TKIP ашиглана.
3. WPA2:

* AES шифрлэл: Өндөр түвшний шифрлэл ашиглан өгөгдлийг найдвартай хамгаалдаг.
* CCMP: Өгөгдөл шифрлэх, нягтлан шалгах зорилготой.
* Personal болон Enterprise горимтай.

1. WPA3

* SAE: Dragonfly handshake гэгддэг шинэ баталгаажуулалтын протокол. Нууц үг эвдэх халдлагаас хамгаалдаг.
* Өмнөх шифрлэгдсэн өгөгдлийг халдагч тайлж унших боломжгүй болгодог.
* Нээлттэй сүлжээнд шифрлэлгүйгээр аюулгүй холболт үүсгэдэг.

**Туршилт**

1)Туршилтад бид Packet tracer программ дээр дараах топологийн дагуу сүлжээ байгуулна. Ингэхдээ Packet tracer програмын “Physical” хэсгийг идэвхижүүлнэ. Packet tracer дээрх “Grid” цэсрүү орж “City” талбарт X=200, Y=200 гэж тохируулж өг. Мөн ногоон өнгөөр шугам татахаар тохируулаарай. Үүний дараа дараах зурагт үзүүлснээр төхөөрөмжүүдийг байрлуул. PC-үүдэд “WMP300N” модулийг нэмж суурьлуулсан.

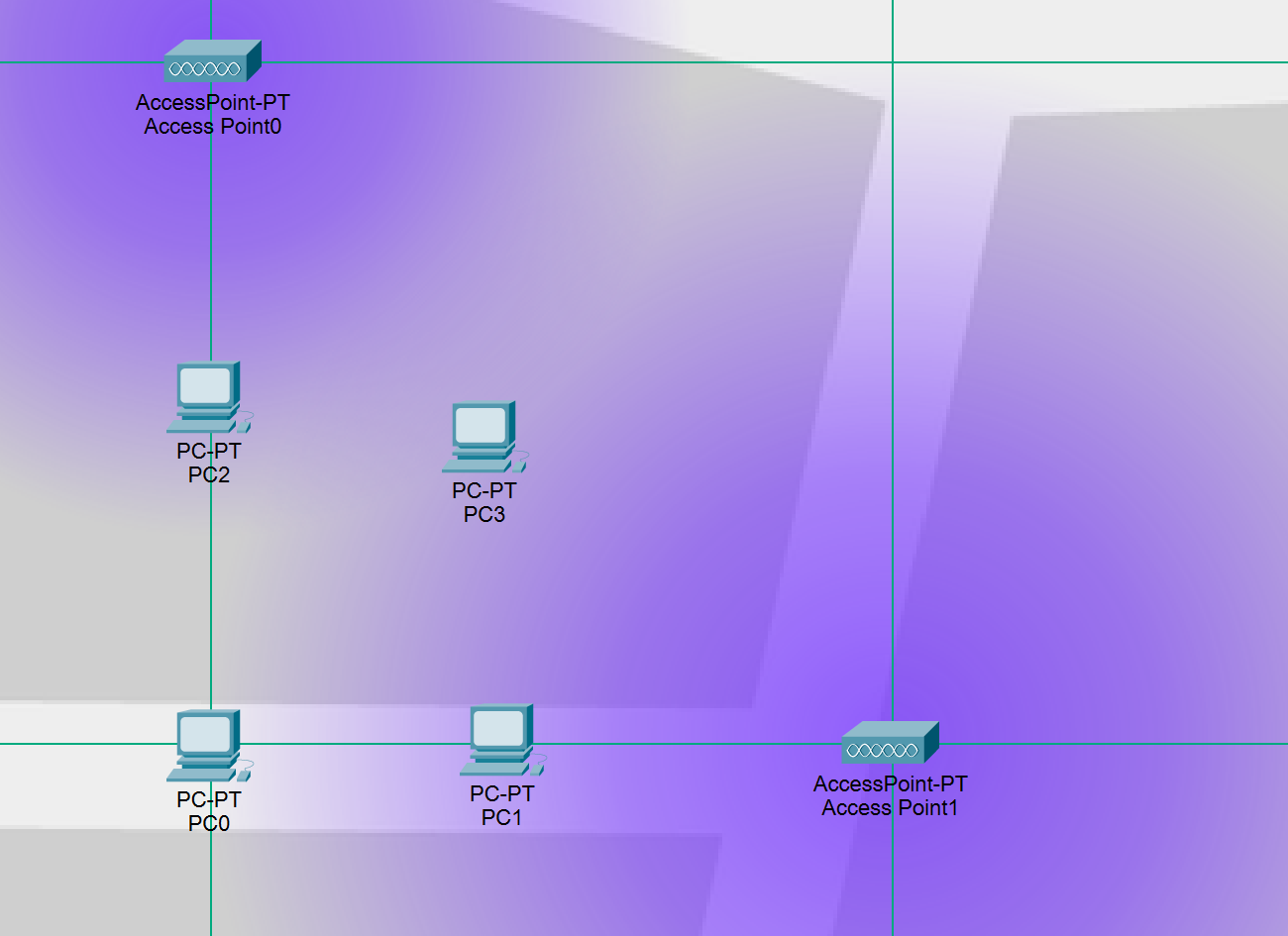


Figure 1 Туршилтын тодологи 1

2) “Access Point0” төхөөрөмжийн Config -> Interface -> Port1-д SSID нь AP0, Authentication нь WPA2-PSK байхаар тохируулж, дараа нь “Access Point1” -ийг SSID нь AP1, Coverage range -ийг 200 метр байхаар тохируулна.

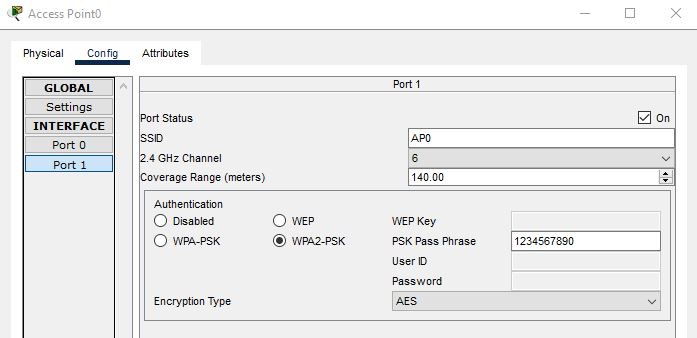


Figure 2AP0

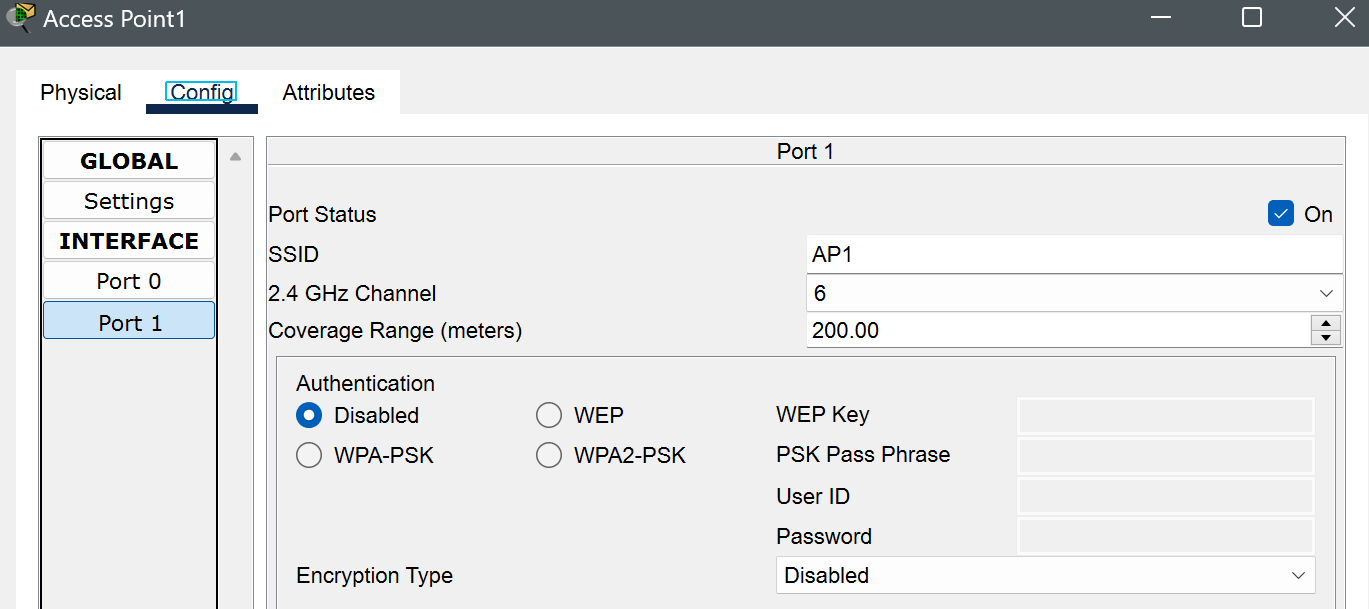


Figure 3 AP1

3) PC0-ийн Desktop -> PC Wireless -> Connect хэсгийг нээхэд Зураг 11.4-д үзүүлсэн цонх харагдана. Refresh товч дарахад холбогдох боломжтой утасгүй сүлжээний холболтын төхөөрөмжүүдийн жагсаалт болон шаардлагатай мэдээллүүд гарч ирнэ. Бүх компьютерүүд дээрх мэдээлүүдийг ажигла.

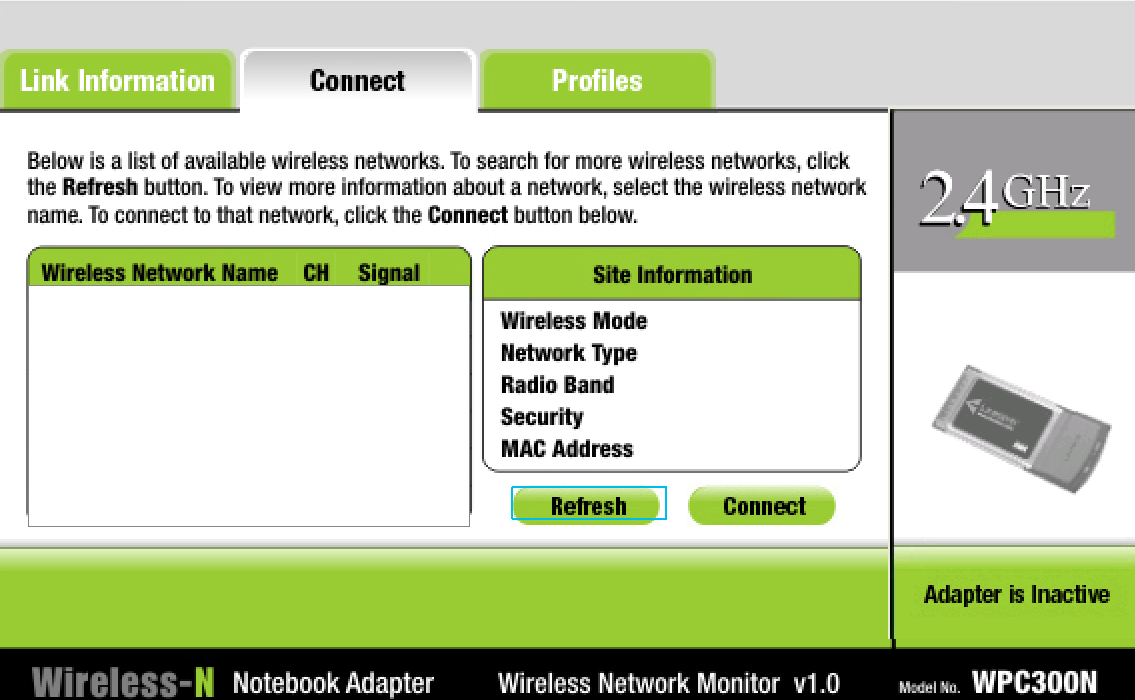


Figure 4 PC0

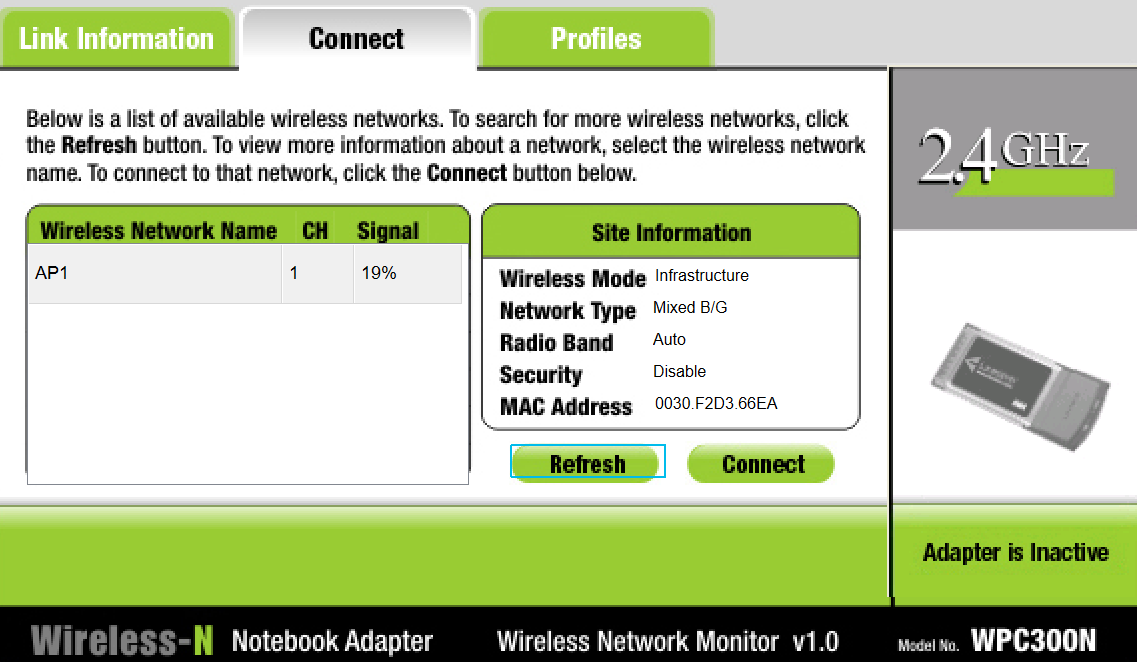


Figure 5 PC1

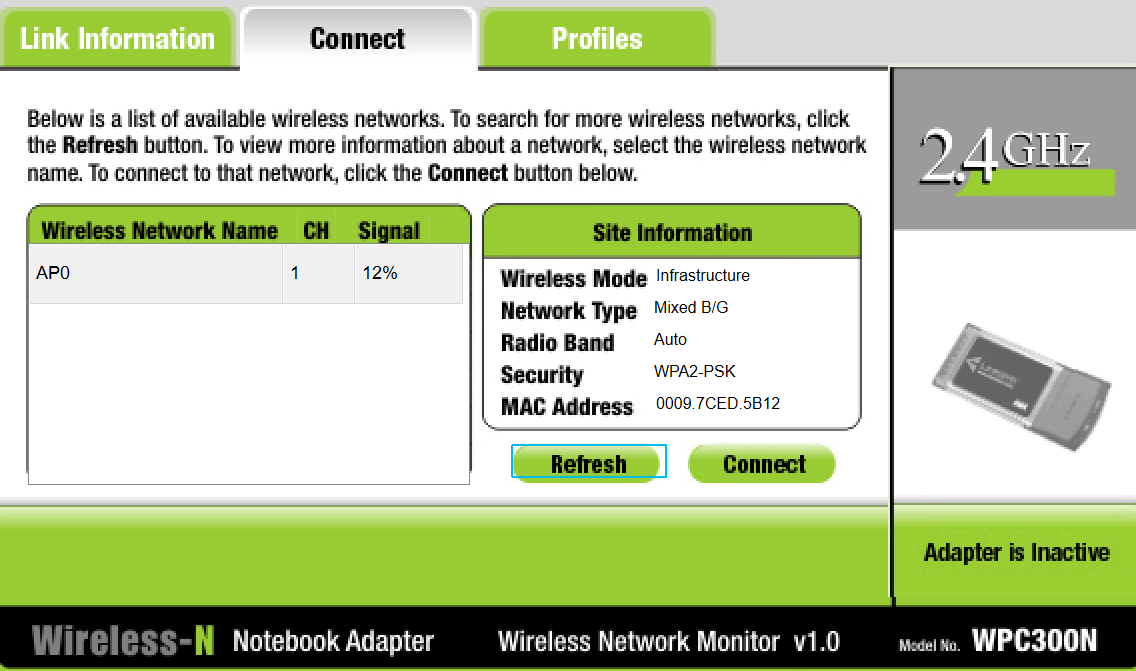


Figure 6 PC2

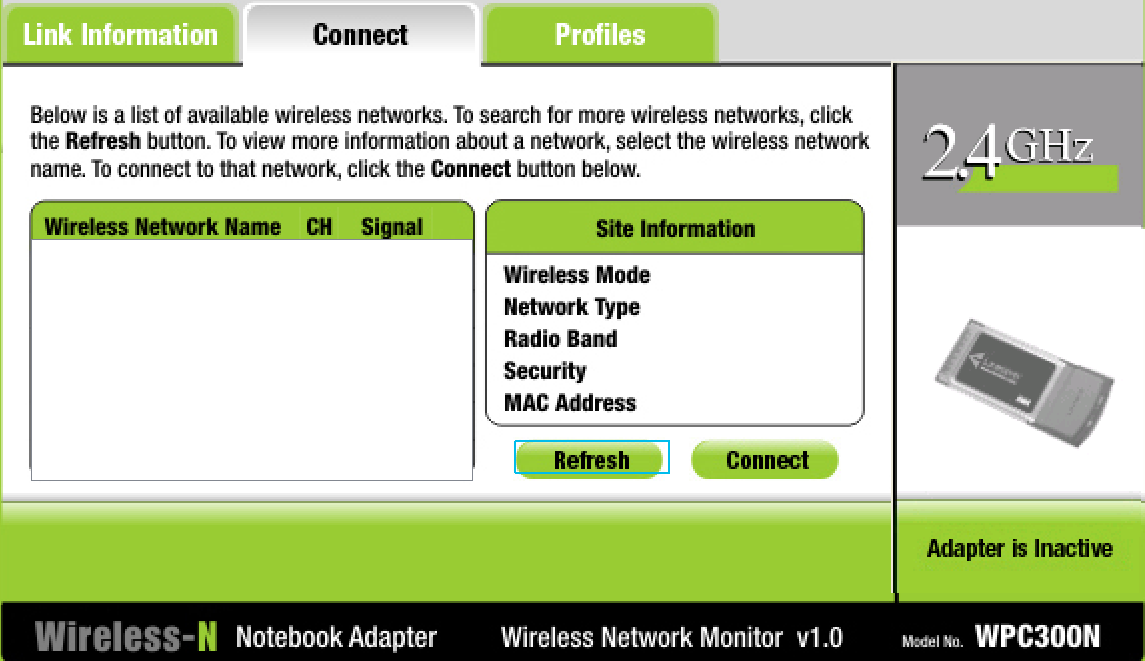


Figure 7 PC3

4) WRT300N төхөөрөмжийг нэмж байрлуулаад Config -> Interface -> Wireless -руу орж SSID-ийг WR0 болгож өөрчил. Үүний дараа компьютерүүд дээрх утасгүй сүлжээний мэдээлэл хэрхэн өөрчлөгдсөн талаар ажигла.

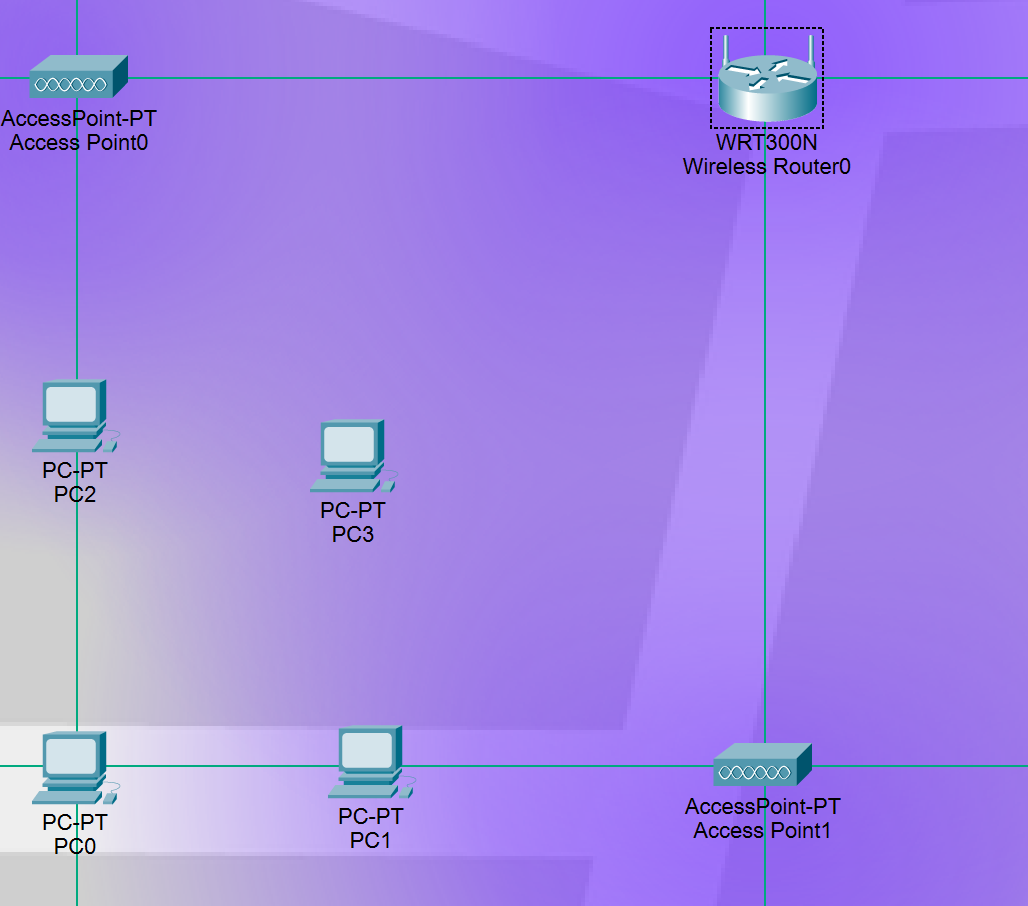


Figure 8 Туршилтын топологи2

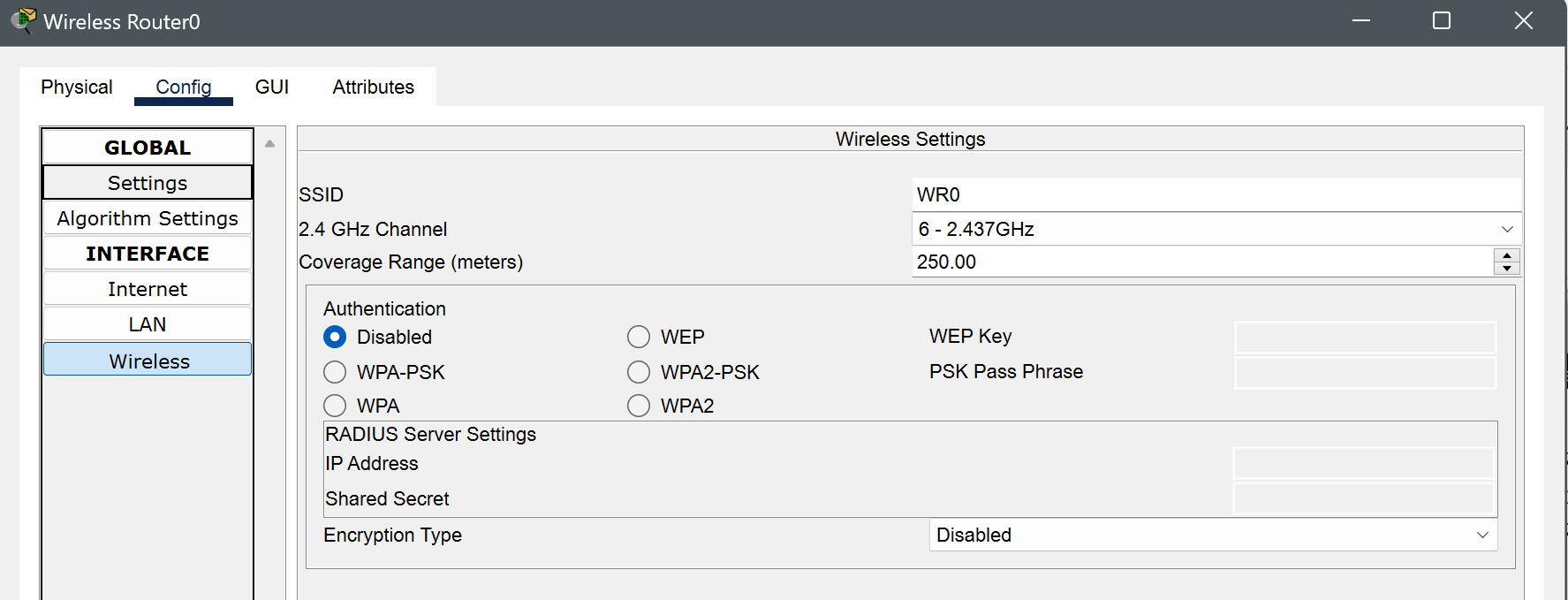


Figure 9WR0

Гарсан өөрчлөлт

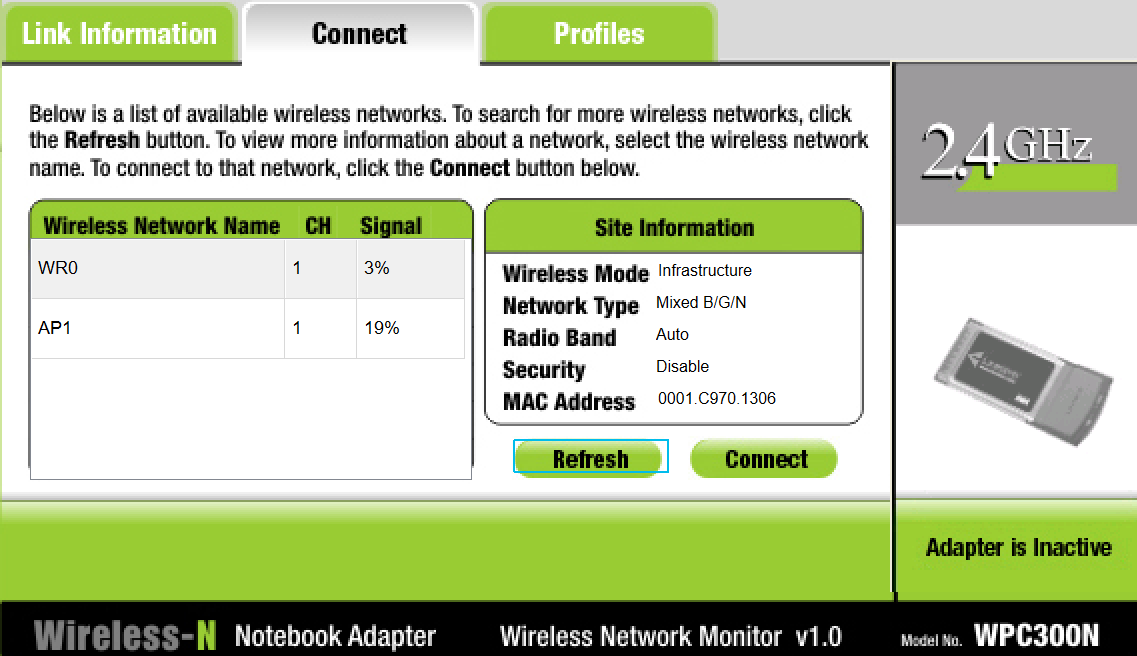


Figure 10 PC1

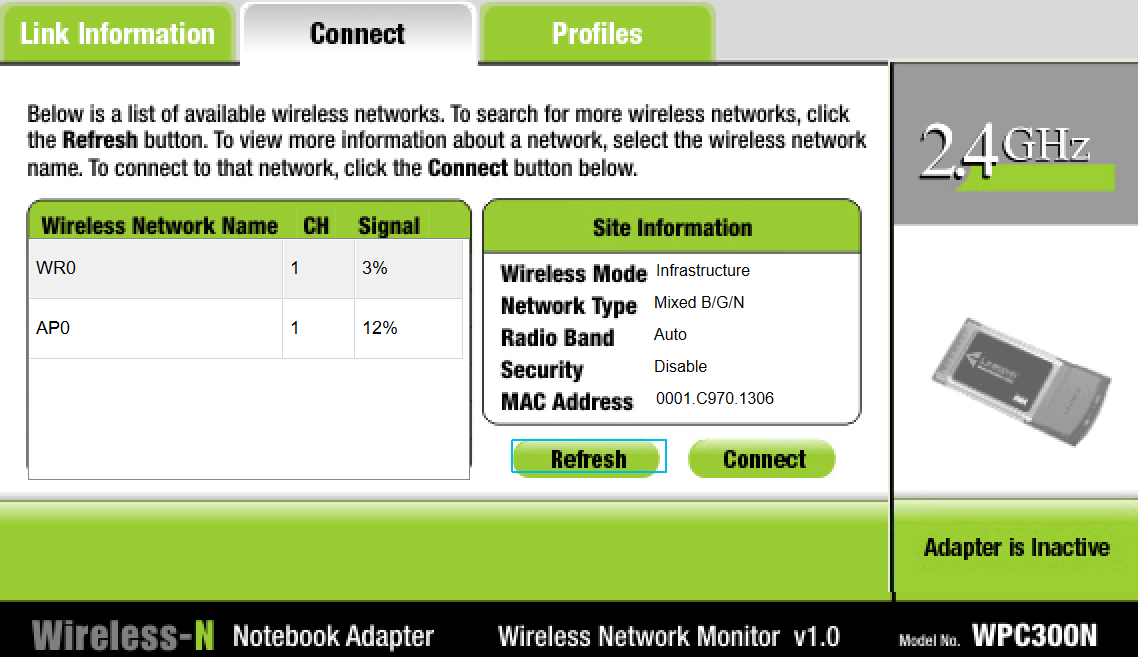


Figure 11PC2

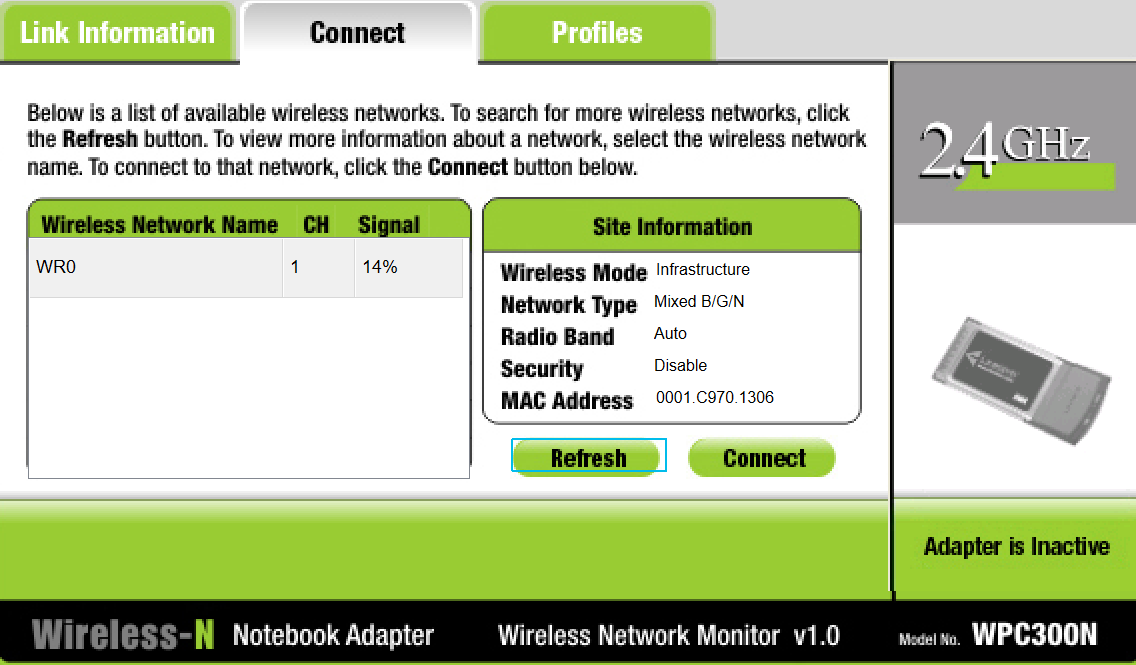


Figure 12 PC3

5) Сүлжээний топологийг үзүүлсэнээр өөрчил.

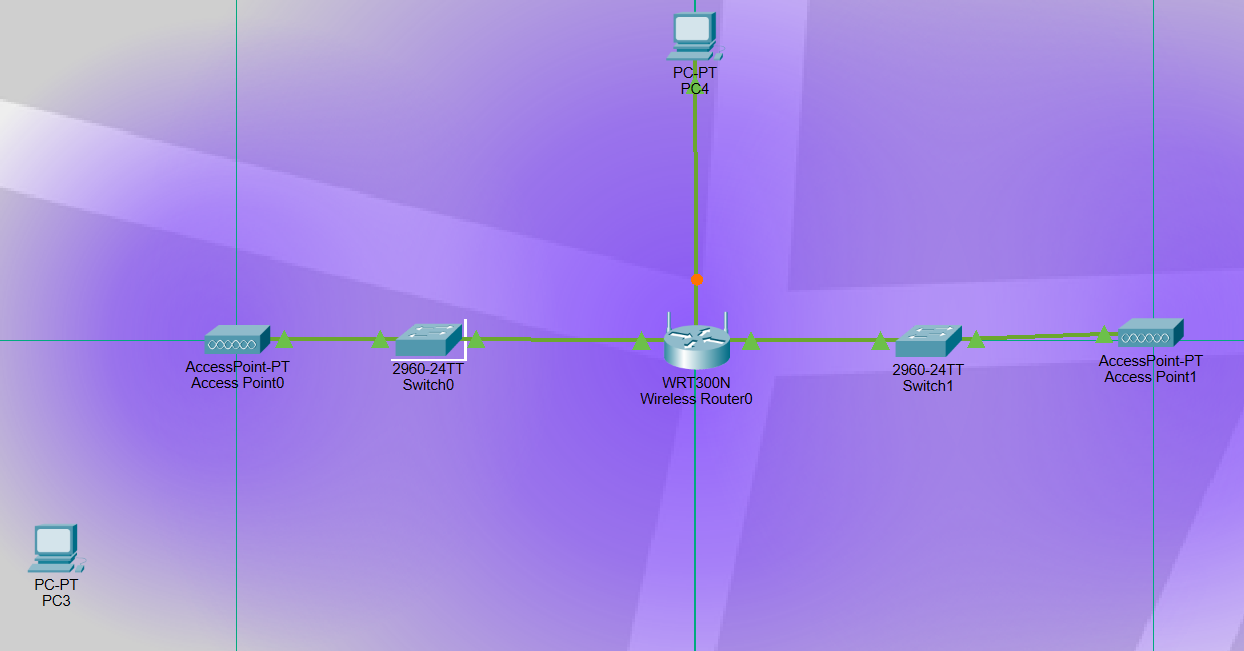


Figure 13туршилтын топологи3

6) Бүх утасгүй сүлжээний холболтын төхөөрөмжүүдийн SSID-ийг NUM болго. Нууц үг буюу authentication нь бүгд ижил байна. Мөн Wireless Router0 -> GUI -> Wireless -> Standard Channel -ийг “6 – 2.437GHz” болгож өөрчлөөд цонхны доор байрлах Save товчийг дарж хадгал.

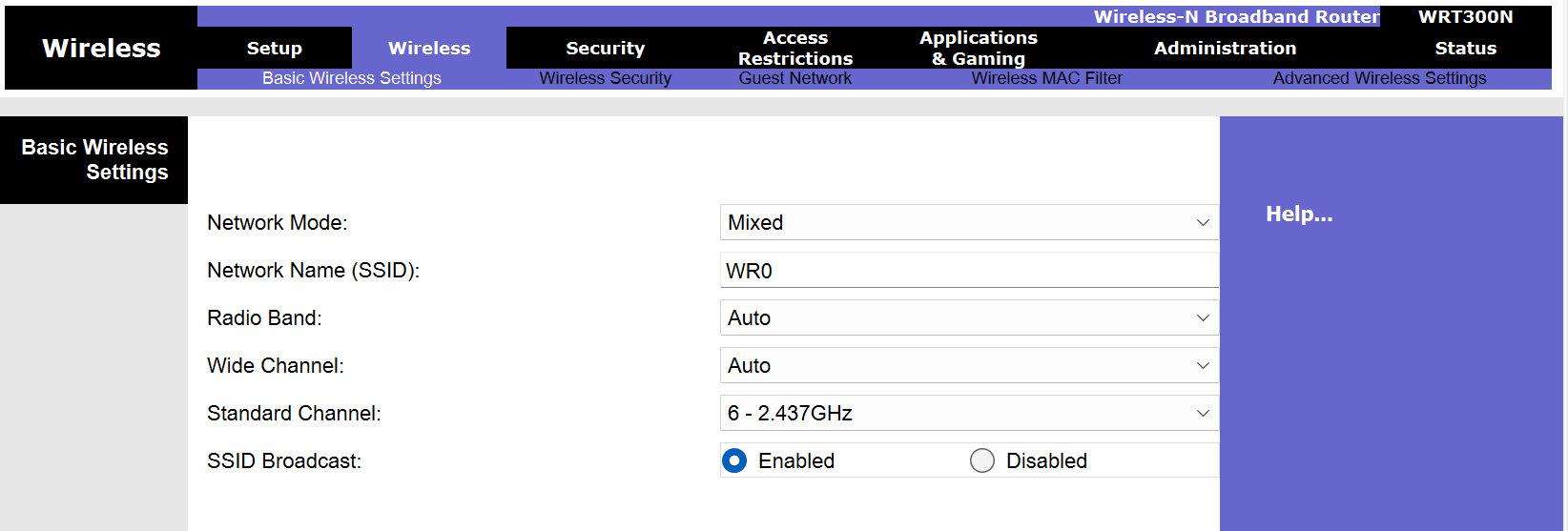


Figure 14 wireless router тохиргоо

7) Бүх PC-үүд DHCP-ээс хаягийн тохируулга хийхээр тохируулаад шалгаарай. PC3-ийг NUM нэртэй утасгүй сүлжээнд холбоод PC4-рүү ICMP пакет явуулж холболтыг шалга.



Figure 15 PC3 request IP address from DHCP Server

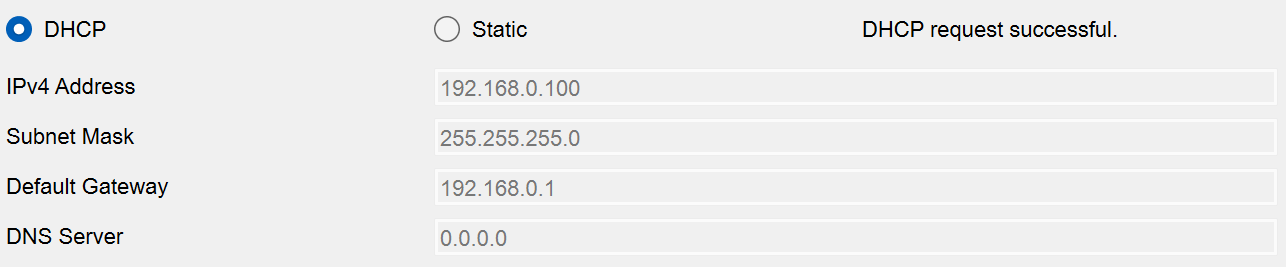


Figure 16 PC4 request IP address from DHCP Server

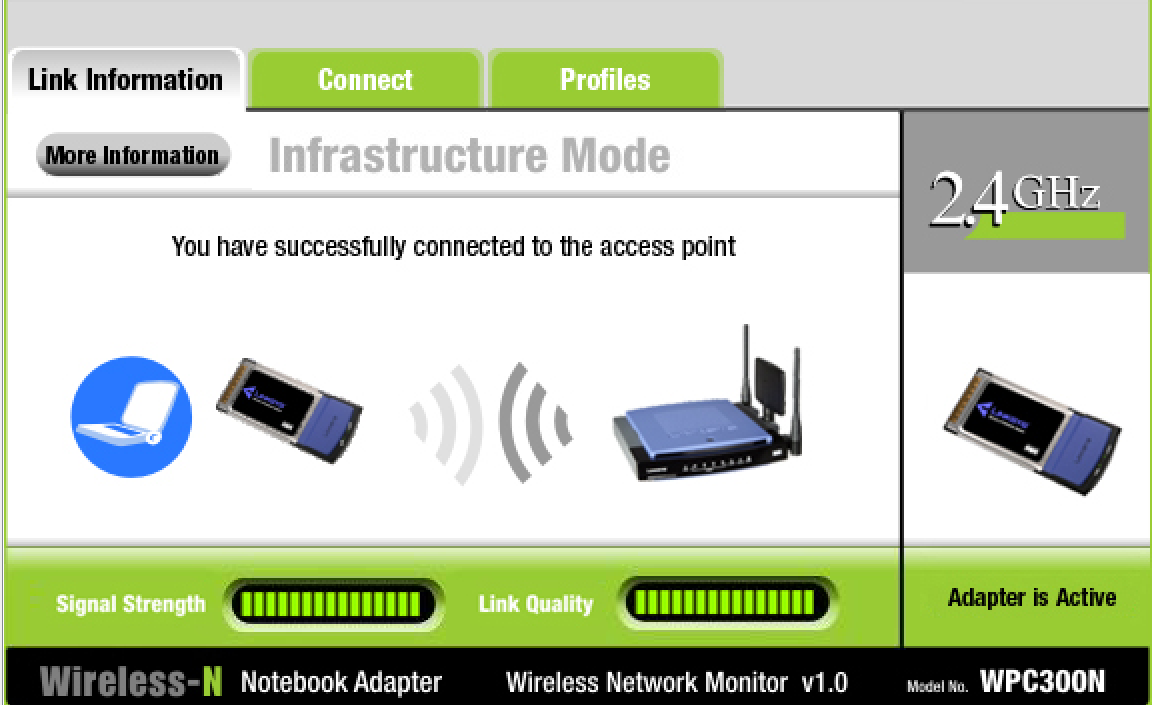


Figure 17 PC wireless сүлжээнд хобогдох

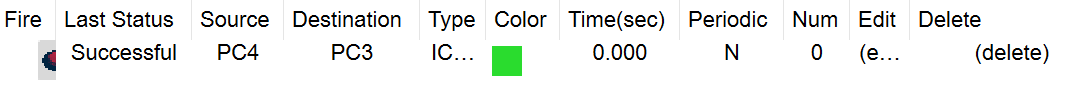


Figure 18 PC3-PC4

8) PC3-ийг Зураг 11.6-д үзүүлсэн 1, 2, 3 байрлалуудад зөөж байрлуулаад PC4-рүү пакет аль замаар хэрхэн дамжиж байгааг ажигла. Ингэхдээ PC3-аас PC4 тасралтгүй ping хийж, хэзээ хэдэн пакет тасалдаж байгааг ажиглаж тайланд оруулна уу.

AP0-ийн зүүн доор байрлуулахад:

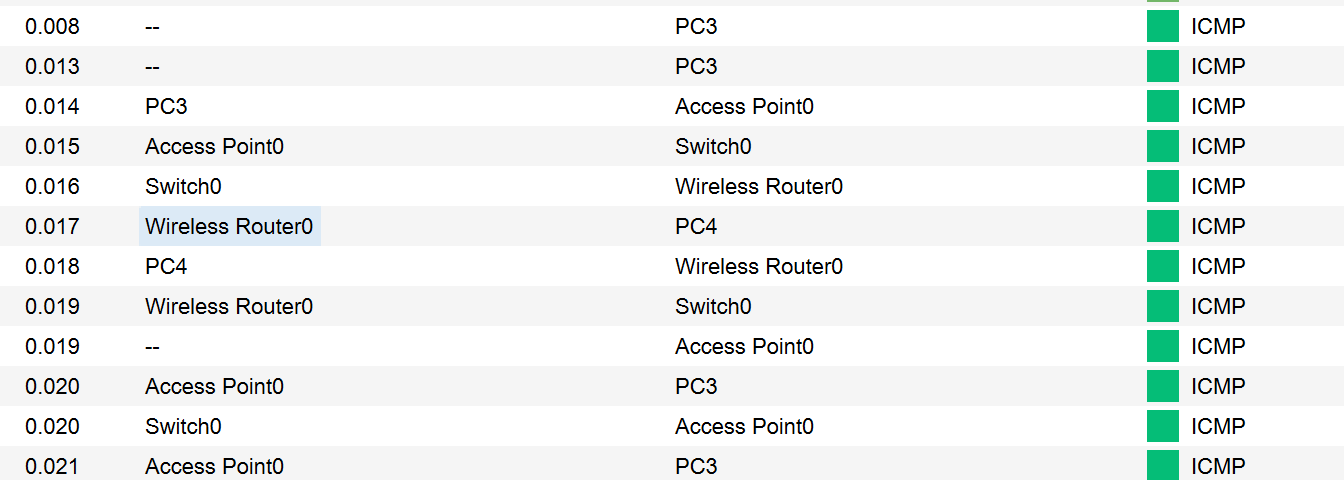


Figure 19 ping1

WR0- ийн доор байрлуулахад

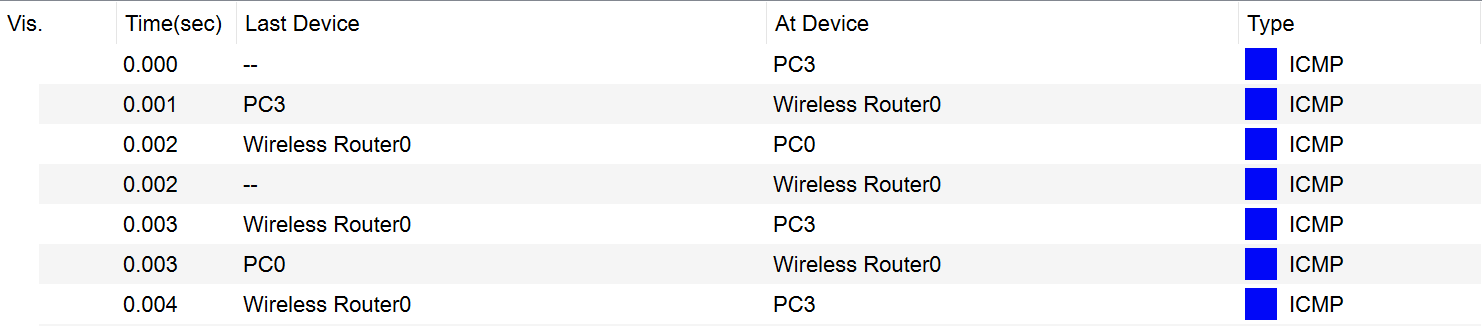


Figure 20 ping2

AP1-ийн баруун доор байрлуулахад

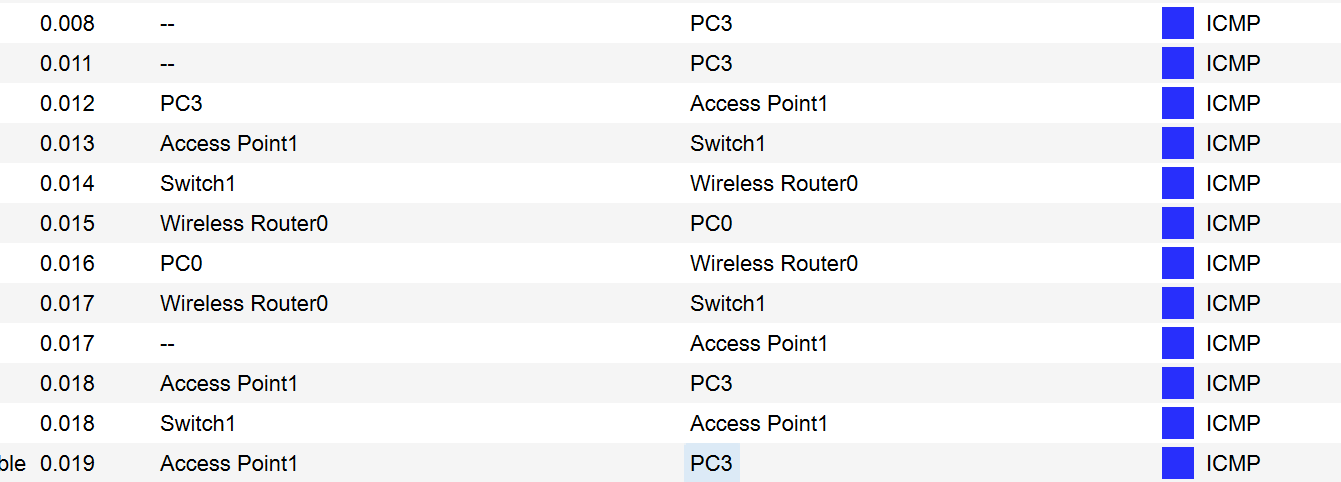


Figure 21 ping3

**Даалгавар1**

Зураг 11.7-д үзүүлсэнээр сүлжээг байгуул. Ингэхдээ дараах байдлаар сүлжээний топологи болон төхөөрөмжүүдийн тохируулна. Үүнд:

Бүх свич ямар нэгэн тохиргоо хийгдэхгүй. Switch1 болон Switch2-уудийг Wireless Router1-ийн Ethernet портод холбоно.

Wireless Router0-ийн Internet портыг свичтэй холбо. PC0 нь Wireless Router0-ийн SSID буюу WR0-рүү, PC1 нь Access Point0-ийн SSID буюу AP0-рүү холбож DHCP-ээс хаягийн тохиргоо хийнэ.

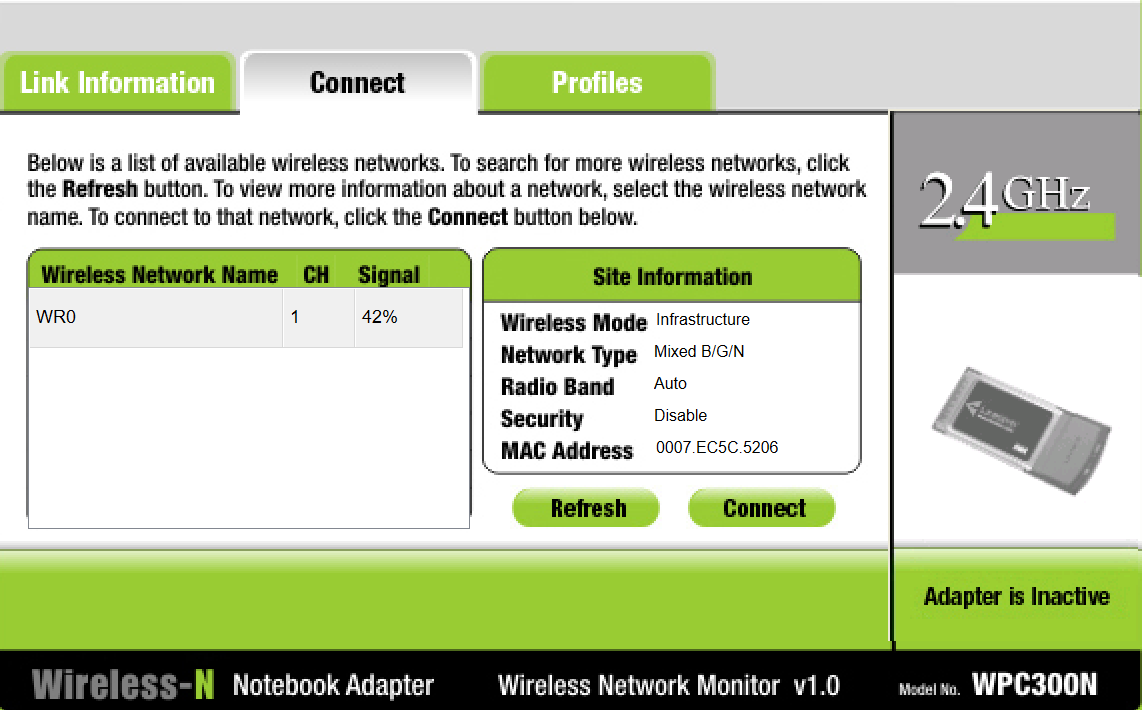


Figure 22 PC0 wireless

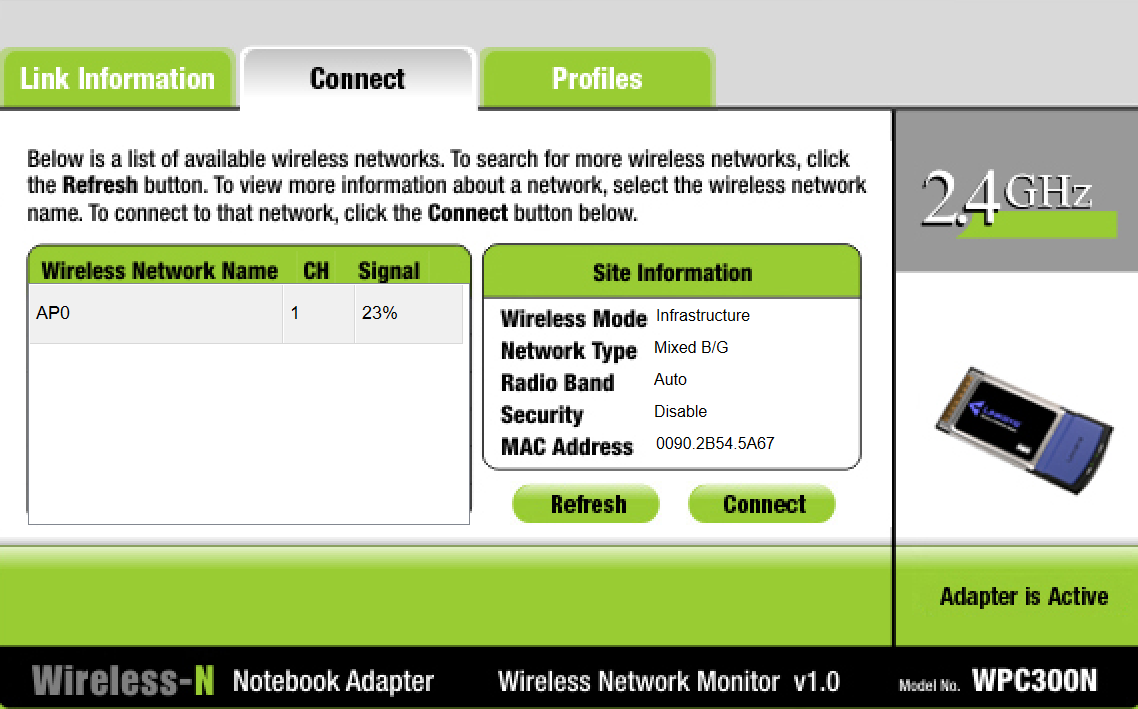


Figure 23PC1 wireless

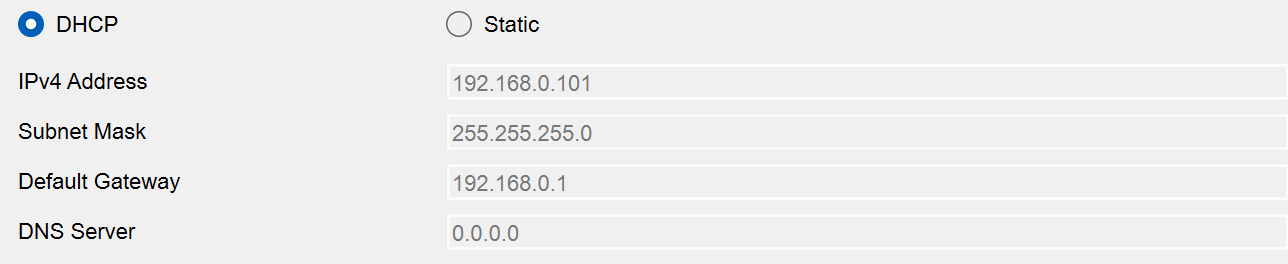


Figure 24 PC0 IP address

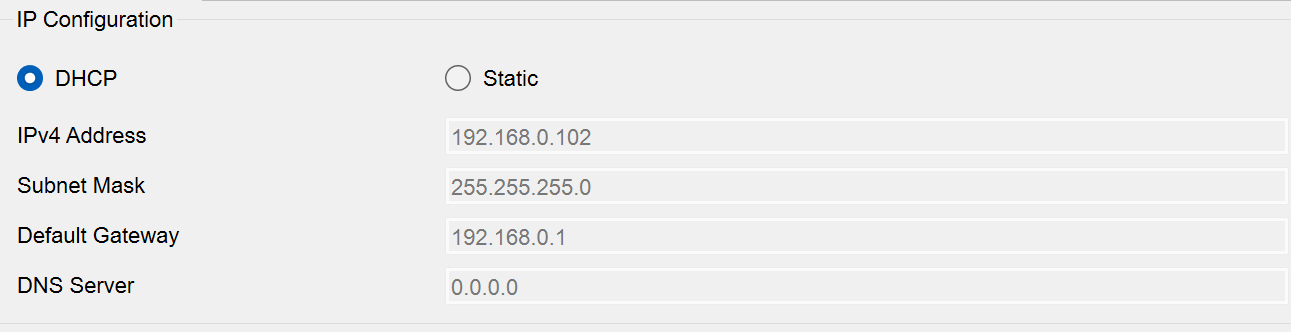


Figure 25 PC1 IP address

PC0-ээс PC1-рүү мессеж дамжуулж холболтыг шалга.

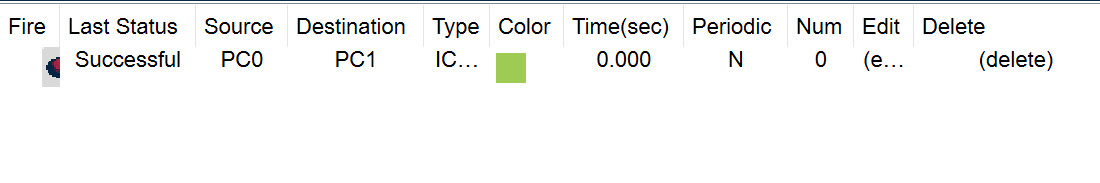
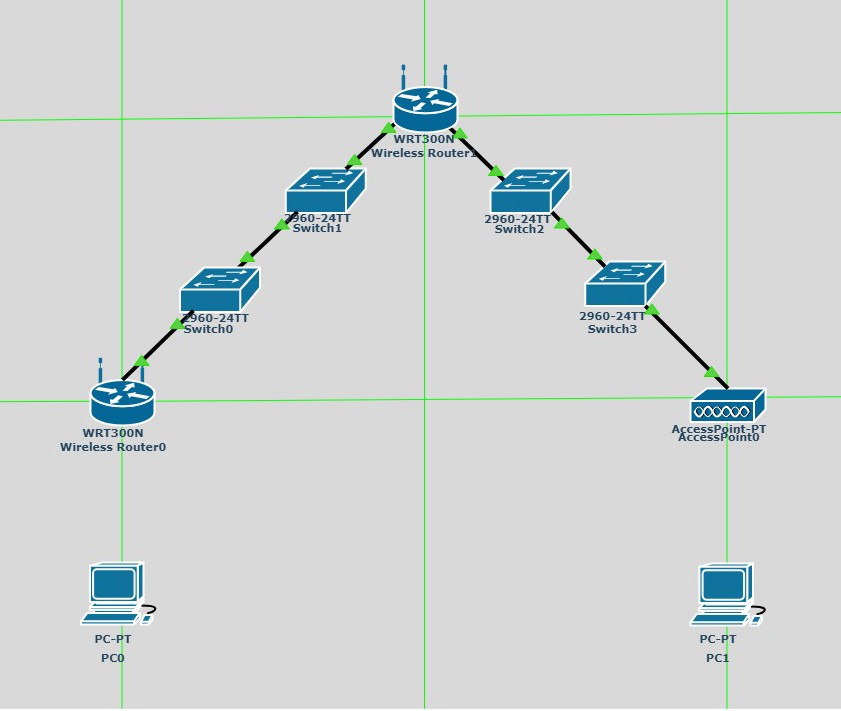


Figure 26 холболт шалгах

Зураг 11.7 Даалгавар №1 топологи

Дараах асуултанд дэлгэрэнгүй хариул.

1. Хоёр PC-үүд аль DHCP сервертэй холбогдсон вэ?

PC0 нь WR0-ийн DHCP server-тэй холбогдсон. PC1 нь AP0-ийн DHCP -тэй холбогдсон.

1. PC0-ээс PC1-рүү дамжуулалт хийх үед PC0-ээс Wireless Router0-руу дамжуулагдсан мессеж, Wireless Router0-аас Wireless Router1-руу дамжуулагдаж байгаа пакетууд хоорондоо ямар ялгаатай байна вэ? Яагаад?

PC0-ээс Wireless Router0:

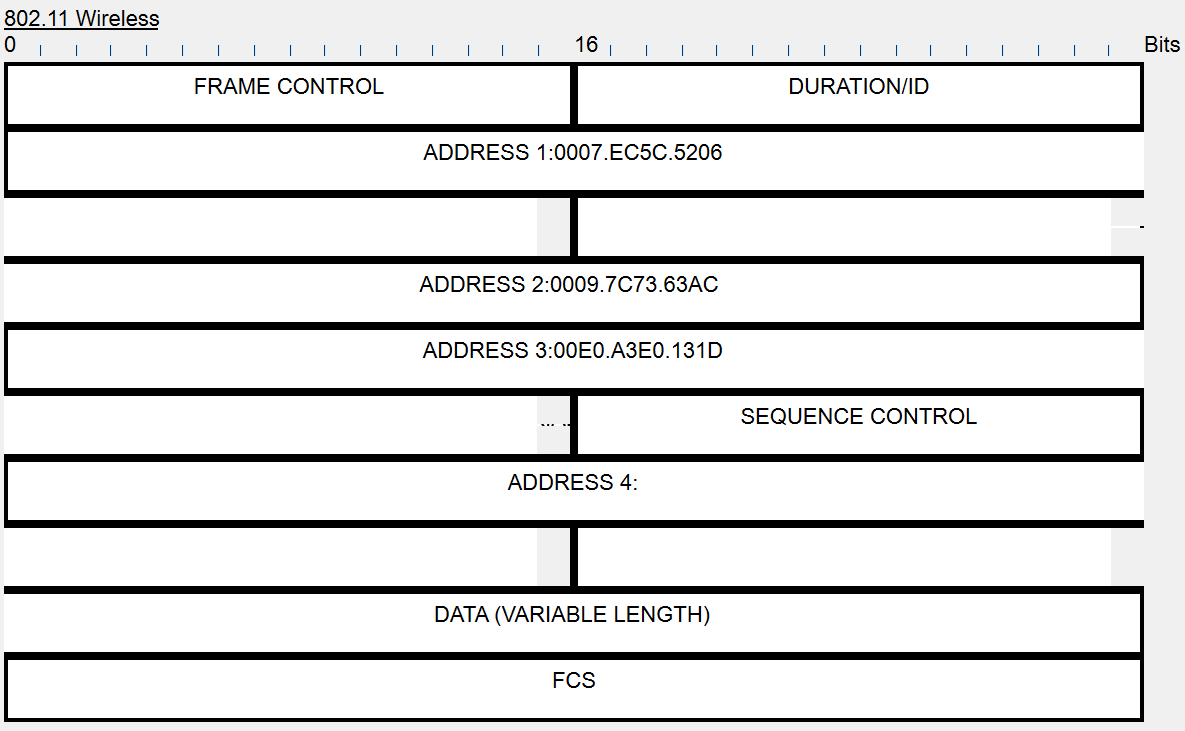


Figure 27 PC0-WR0

Address1: WR0- ийн wireless interface-ийн MAC address тухайлбал хүлээн авагчийн хаяг.

Address2:PC0 -ийн MAC address тухайлбал илгээгчийн хаяг.

Address3: WR0 -ийн switch0-тэй холбогдсон interface-ийн MAC address тухайлбал Intermediate -ийн хаяг.

Wireless Router0-аас Wireless Router1:

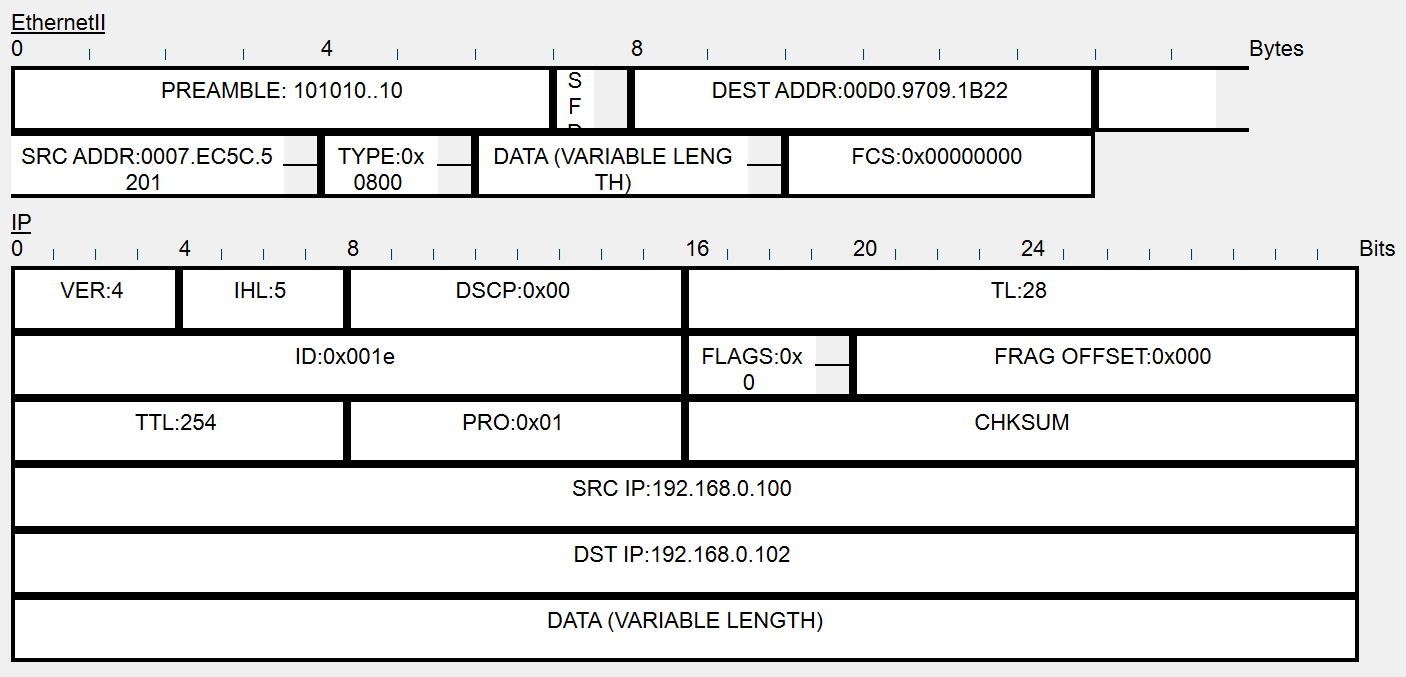
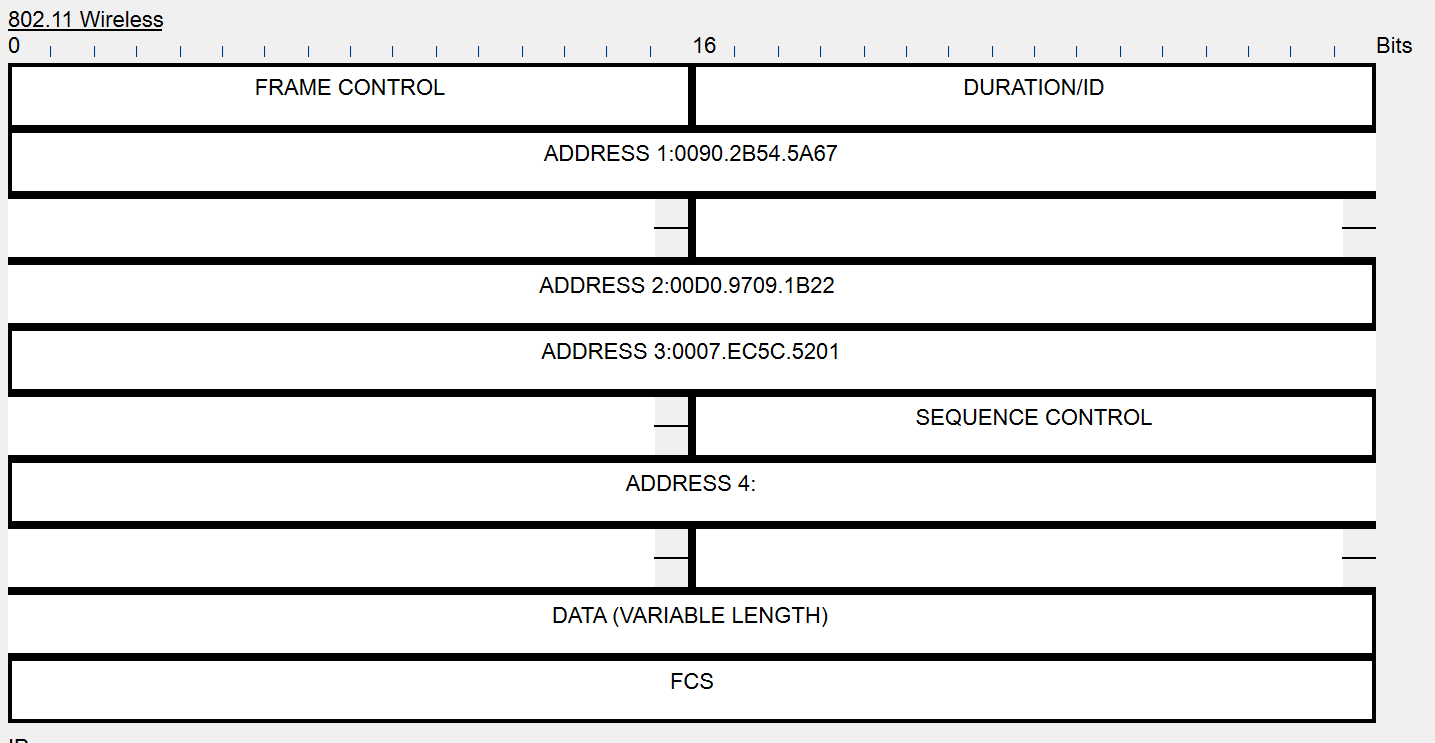


Figure 28WR0-WR1

802.11 wireless frame байгаагүй, IP header-ээс харвал илгээгчийн хаяг нь РС0-ийн хаяг хүлээн авагчийн хаяг РС1 -ийн хаяг байсан.

1. Access Point0 дээр дээрх үйлдэл давтагдаж байна уу?

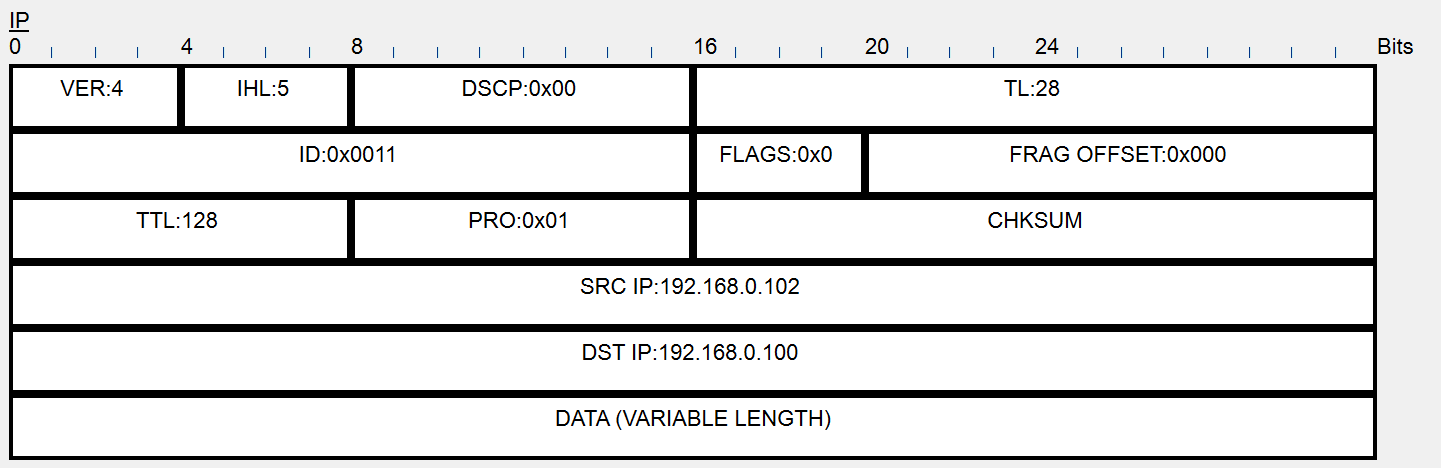
Access Point0 дээр дээрх үйлдэл давтагдаж байна.



Address1: AP0-ийн МАС хаяг

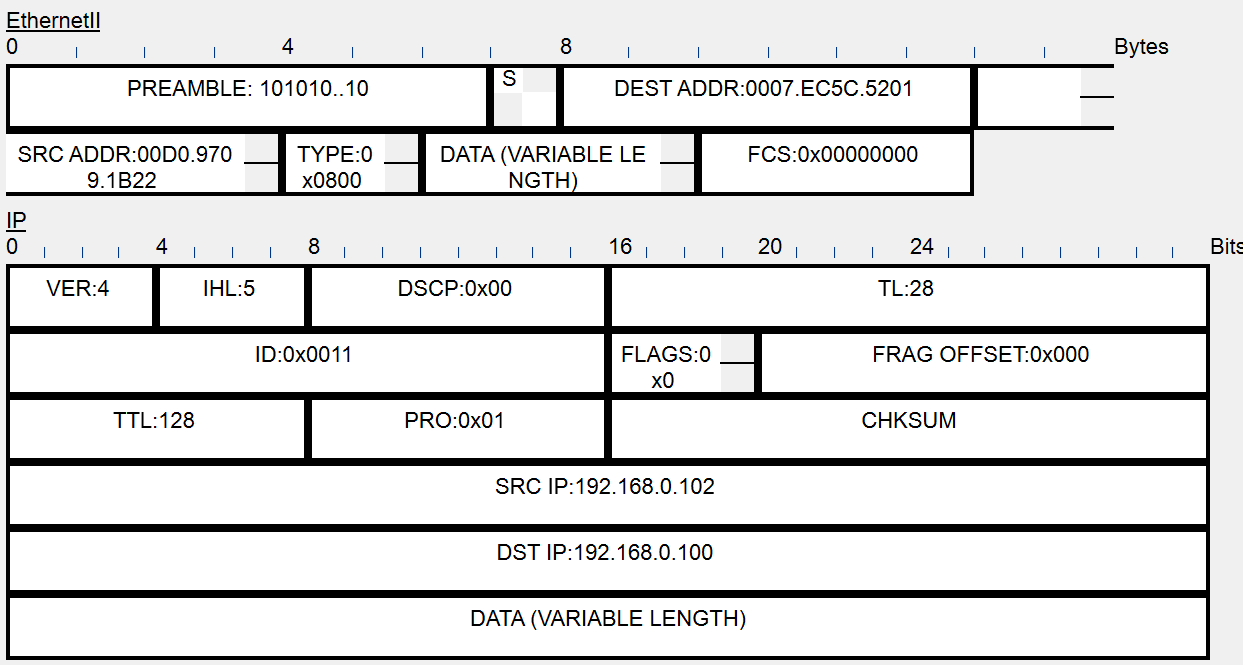
Address2: РС1-ийн МАС хаяг

Address3: WR0-ийн internet port-ийн МАС хаяг



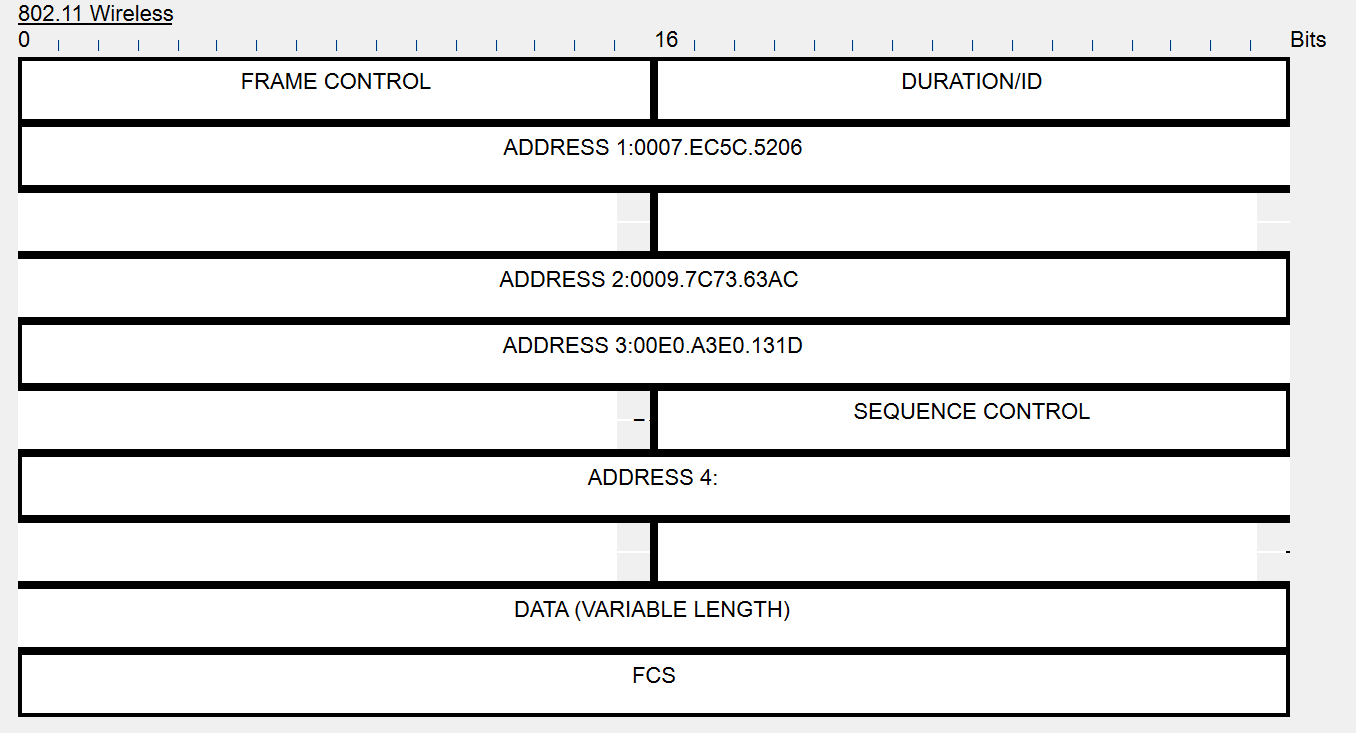
Илгээгчинй хаяг нь РС1 -ийн хаяг байж хүлээн авагчийн хаяг нь РС0-ийн хаяг байна.

1. Wireless Router1 дээр дээрх үйлдэл давтагдаж байна уу?



Илгээгчинй хаяг нь РС1 -ийн хаяг байж хүлээн авагчийн хаяг нь РС0-ийн хаяг байна дээрэх үйлдлийг давтаж байна.

1. PC0-ээс Wireless Router0-руу дамжуулагдсан мессеж хэдэн МАС хаягтай байна вэ?



3 MAC address байна.

**Даалгавар2**

Wireshark программ дээр AirPcap ашиглан бэлдсэн Wireshark\_802\_11.pcap файлыг нээ. Файлыг <http://netconf.num.edu.mn/wiresharkfiles/Lab11_Wireshark_802_11.html> хуудаснаас татаж авна уу. Энэхүү файлд “30 Munroe St” гэсэн SSID-тай төхөөрөмжрүү холбогдсон хостын дараах үйлдлүүдийг бичиж авсан байгаа. Үүнд:

* 1. Хугацааны 24.82 дахь агшинд хост HTTP хүсэлтийг <http://gaia.cs.umass.edu/wireshark-labs/alice.txt> гэсэн домэйн руу илгээсэн. gaia.cs.umass.edu домэйнд харгалзах IP хаяг нь 128.119.245.12 юм.
  2. Хугацааны 32.82 дахь агшинд хост HTTP хүсэлтийг [http://www.cs.umass.edu](http://www.cs.umass.edu/) домэйн буюу 128.119.240.19 хаяг руу илгээсэн.
  3. Хугацааны 49.58 дахь агшинд хост нь “30 Munroe St” төхөөрөмжөөс салж “linksys\_ses\_24086” төхөөрөмжрүү холбогдох оролдлого хийсэн. Гэтэл энэхүү төхөөрөмж нь нууц үгээр хамгаалагдсан учир хост холбогдож чадаагүй болно.
  4. Хугацааны 63.00 дахь агшинд хост дахин “linksys\_ses\_24086”-руу хологдох оролдлого хийсэн ба буцаад “30 Munroe St” төхөөрөмжрүү холбогдсон.

**Дараа нь доорх асуултуудад хариул.**

1. Beacon фрем дэх SSID-ийг илэрхийлсэн хэсгүүдийг дэлгэж тайлбарла. Ямар үед ижил байна вэ?

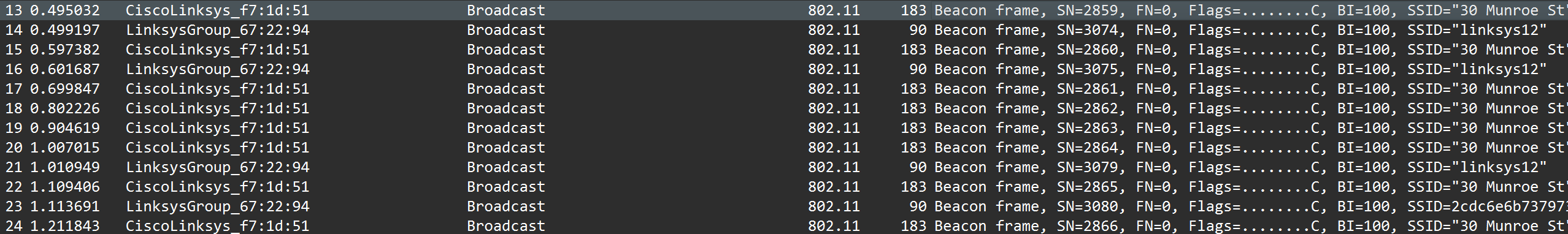


Figure 29 Beacon frame

SSID талбар нь тухайн сүлжээний нэрийг илэрхийлнэ. SSID нь ижил үед sequence number, frame check sequence-ээс өөр талбаруудийн утга ижил байна.

1. Beacon фремүүдийн хоорондох хугацаа утасгүй сүлжээний төхөөрөмж бүрт хэд байсан бэ? MAC хаяг нь ямар байна вэ?

SSID нь “30 Munroe St” ба “linksys\_ses\_24086” үед Beacon фремүүдийн хоорондох хугацаа нь ойролцоогоор 1024 s байсан.

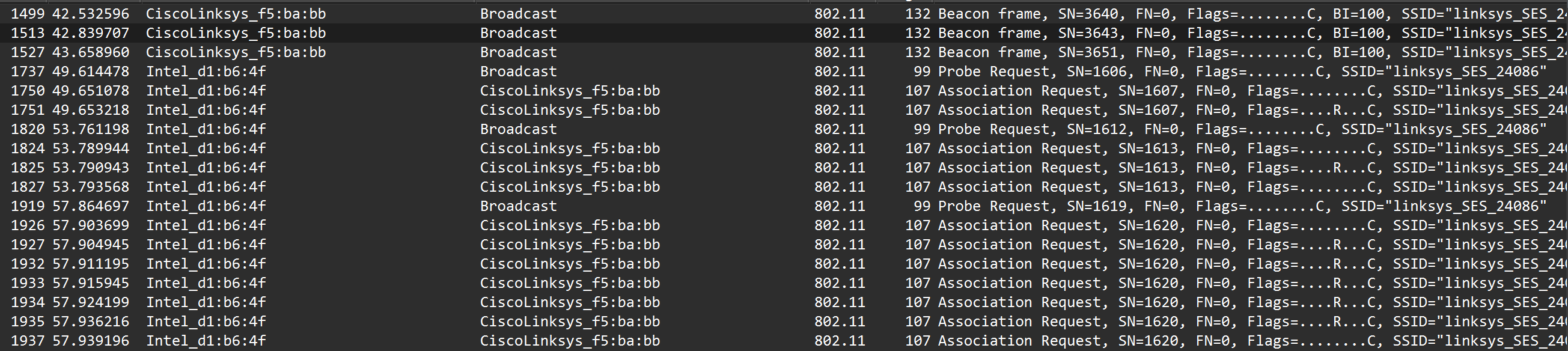


Figure 30 wlan.ssid=="linksys\_SES\_24086"

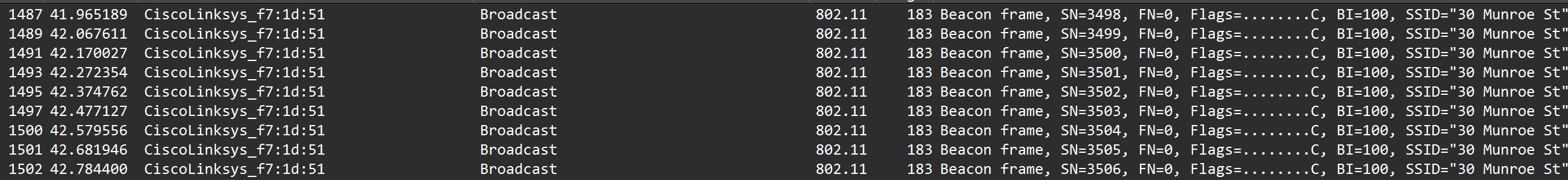


Figure 31 wlan.ssid=="30 Munrou St"

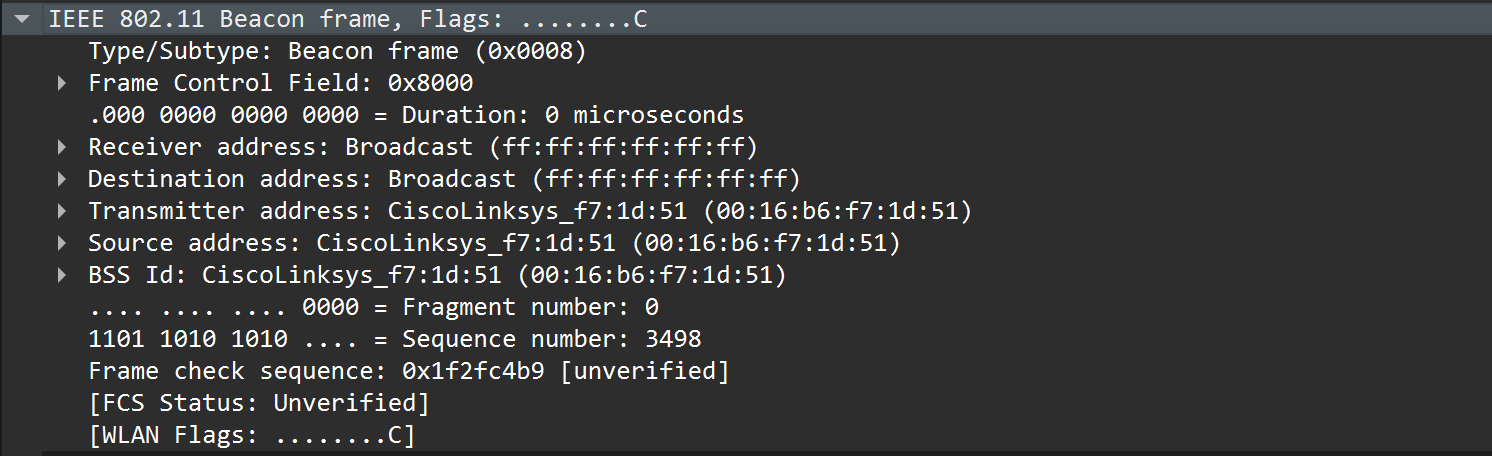


Figure 32 30 Munroe St MAC

Source address: 00:16:b6:f7:1d:51

Destination address: Broadcast

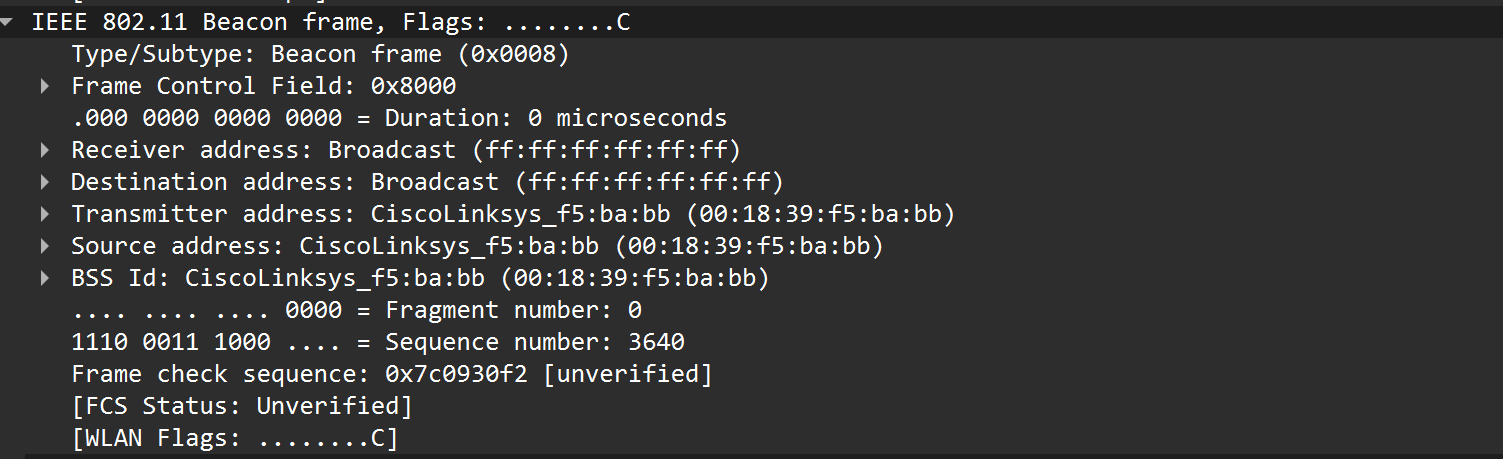


Figure 33 "linksys\_SES\_102486" MAC

Source address: 00:18:39:f5:ba:bb

Destination address: Broadcast

* 1. “30 Munroe St” төхөөрөмжийн beacon фремийн хүлээн авагчийн МАС хаяг ямар байна вэ? Яагаад?

Broadcast байсан, Beacon фрейм нь AP утасгүй сүлжээгээ зарлах зориулалттай.

Энэ нь тухайн сүлжээг ашиглаж болох боломжтойг ойролцоо байгаа бүх төхөөрөмжүүдэд мэдэгдэх үүрэгтэй. 802.11 стандартын дагуу Beacon фреймүүд нь үргэлж Broadcast хаяг руу чиглэгддэг.

* 1. “30 Munroe St” төхөөрөмжийн beacon фремээс харахад дамжууллын хэдэн төрлийн хурдыг дэмжиж байна вэ? Мөн “linksys\_ses\_24086” -ийн дэмжих дамжууллын хурдны тохиргоо хэд байна вэ?

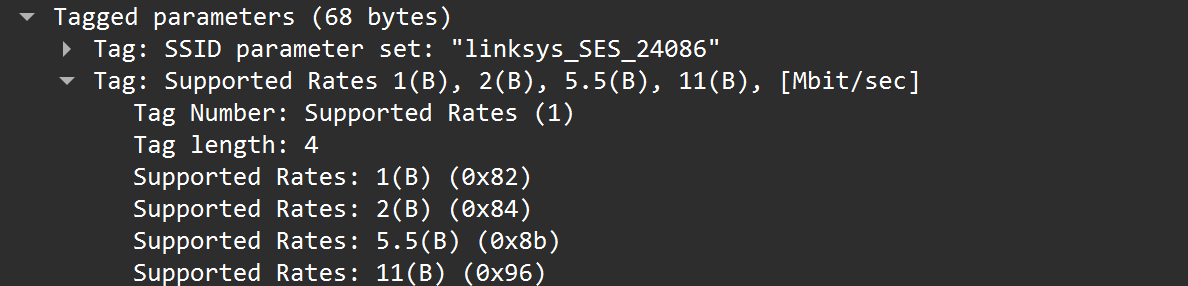


Figure 34 “linksys\_ses\_24086” дэмжих хурд

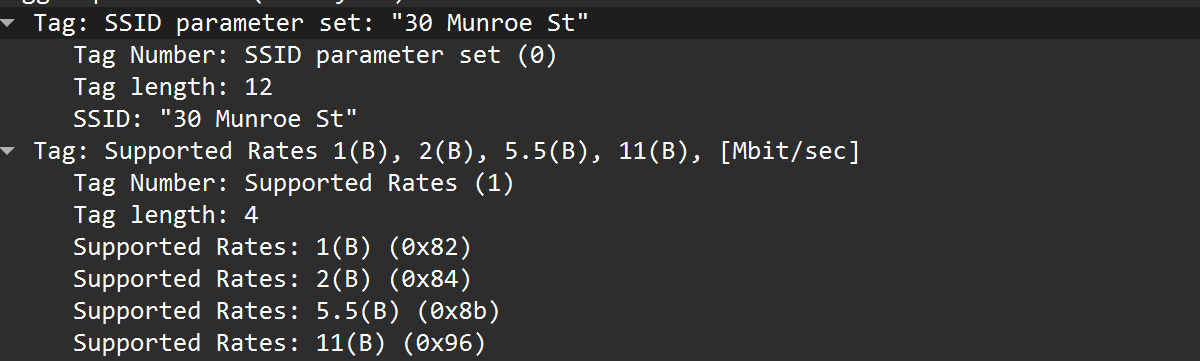


Figure 35"30 Munroe St" дэмжих хурд

* 1. Хост HTTP хүсэлт илгээж байгаа үеийн 802.11 фремийг ажигла. Alice.txt файлыг татан авч байх үед хэдэн МАС хаяг байна вэ? Ямар зориулалттайг тайлбарла.



Figure 36 MAC Address

Reciver address: BSS-ийн хаяг.

Transmitter address: Alice.txt файлыг татах хүсэлтын илгээсэн хостын МАС хаяг.

Destination address: router-ний хүсэлт илгээсэн төхөөрөмжтэй холбогдсон interface-ийн МАС хаяг.

* 1. Хостыг “30 Munroe St” төхөөрөмжөөс салах үед хэдэн төрлийн мессеж дамжуулагдсан бэ? Зураглаж тайлбарла.

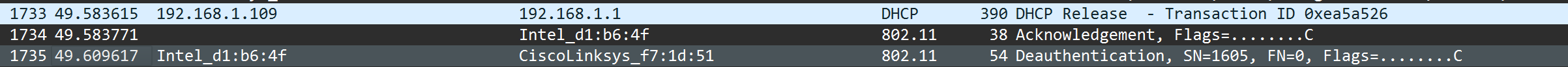


Figure 37 төхөөрөмжөөс салах

49.583615-д хост DHCP Server руу DHCP release мессежийг илгээсэн.

49.609617-д хост нь DEAUTHENTICATION frame-ийг илгээсэн тухайн frame-ийн Frametype нь Management, subframe type нь байж 12 Deauthentication-г илэрхийлнэ.



* 1. “linksys\_ses\_24086”-тай хост холбогдох оролдлого хийхэд хэдэн AUTHENTICATION фрем дамжуулагдсан бэ? Ямар утгатай вэ?

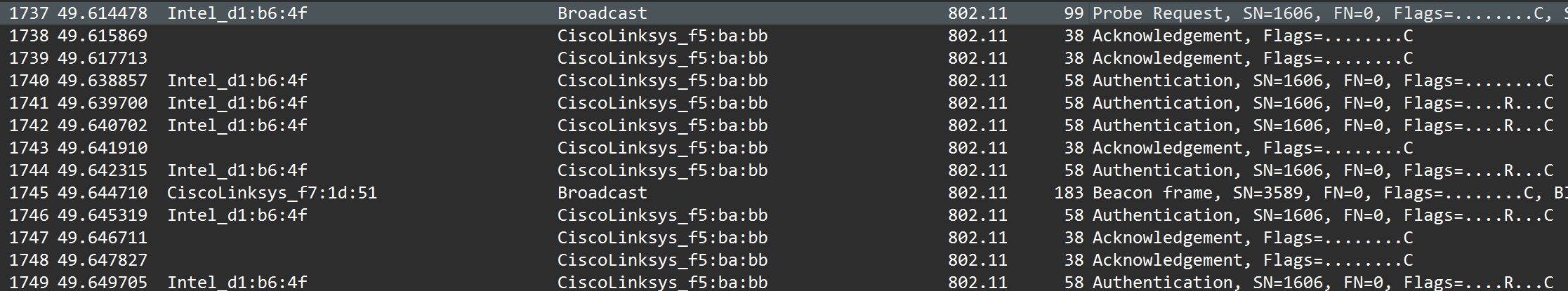


Figure 38 Auyhentication

5 удаа AUTHENTICATION фрем дамжуулагдсан, энэ нь Authentication оролдлого амжилтгүй болсон гэдгийг илтгэнэ.

* 1. Хост хүсэлт илгээхэд “linksys\_ses\_24086”-ээс AUTHENTICATION-ний хариулт ирсэн байна уу?

Ирсэн, AUTHENTICATION -г хүлээн авч АСК мессеж илгээсэн.

* 1. Хоёрдахь удаагаа “linksys\_ses\_24086”-тай холбогдох оролдлого хийхэд өмнөхтэйгээ ижил байсан уу? Яагаад?



Figure 39 Association request

Өөр байна, хоёр дахь удаа холбогдох оролдлого хийхэд AUTHENTICATION хийгээгүй шууд Association request -ийг илгээсэн, гэхдээ АР-ээр олон ACK ирсэн тул холболт амжилтгүйг илэрхийлнэ.

* 1. “30 Munroe St” -тай хост холбогдох үед AUTHENTICATION фрем солилцсон уу? Ямар харулт хүлээн авсан бэ? Жич: “wlan.fc.subtype == 11and wlan.fc.type == 0 and wlan.addr == IntelCor\_d1:b6:4f” түлхүүрээр шүүлтүүрдэж харна уу.

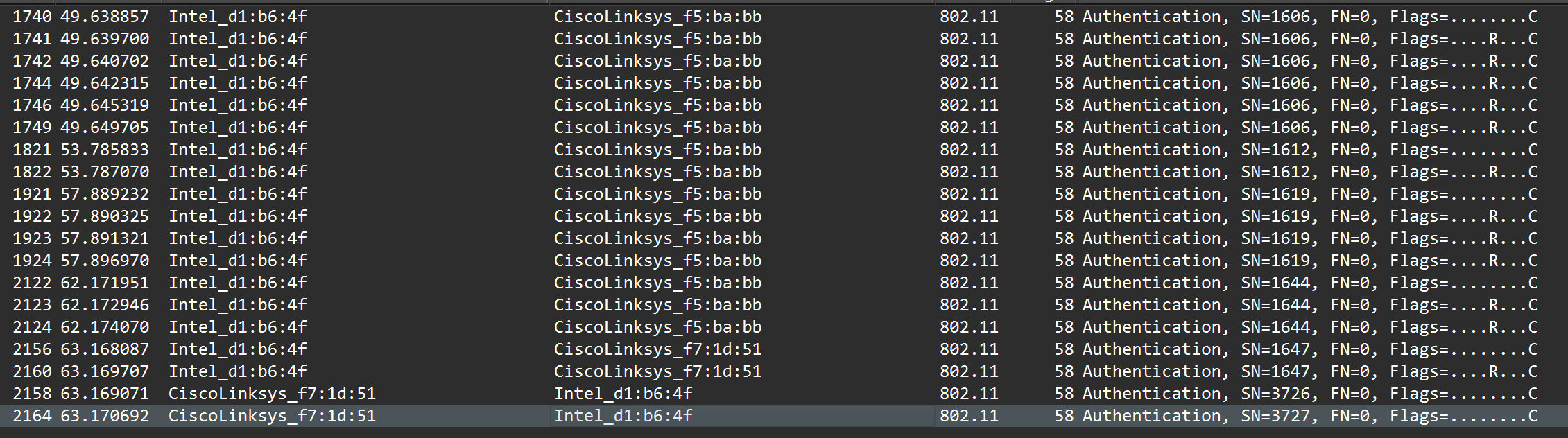


Figure 40 authentication

“30 Munroe St” – оос клент руу ед AUTHENTICATION фрем илгээж хариу өгсөн.

* 1. Probe request, probe response фремүүдэд дэх SSID, илгээгч болон хүлээн авагчийн МАС хаяг нь аль төхөөрөмжийн байна вэ?

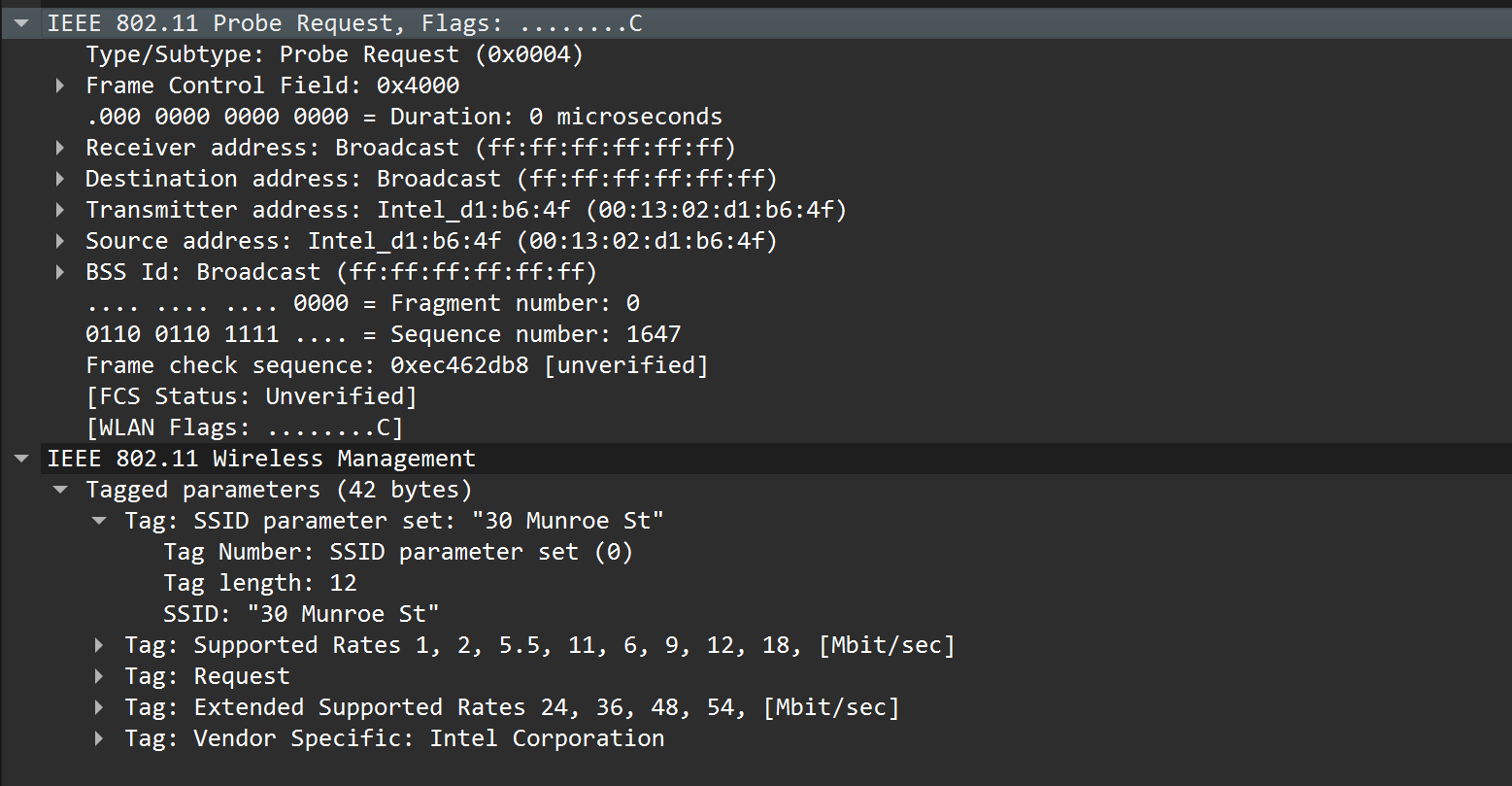


Figure 41 Probe request

SSID: 30 Munroe St

Transmitter address ба Source address : client ийн МАС хаяг

Receiver and Destination address: Broadcast хаяг

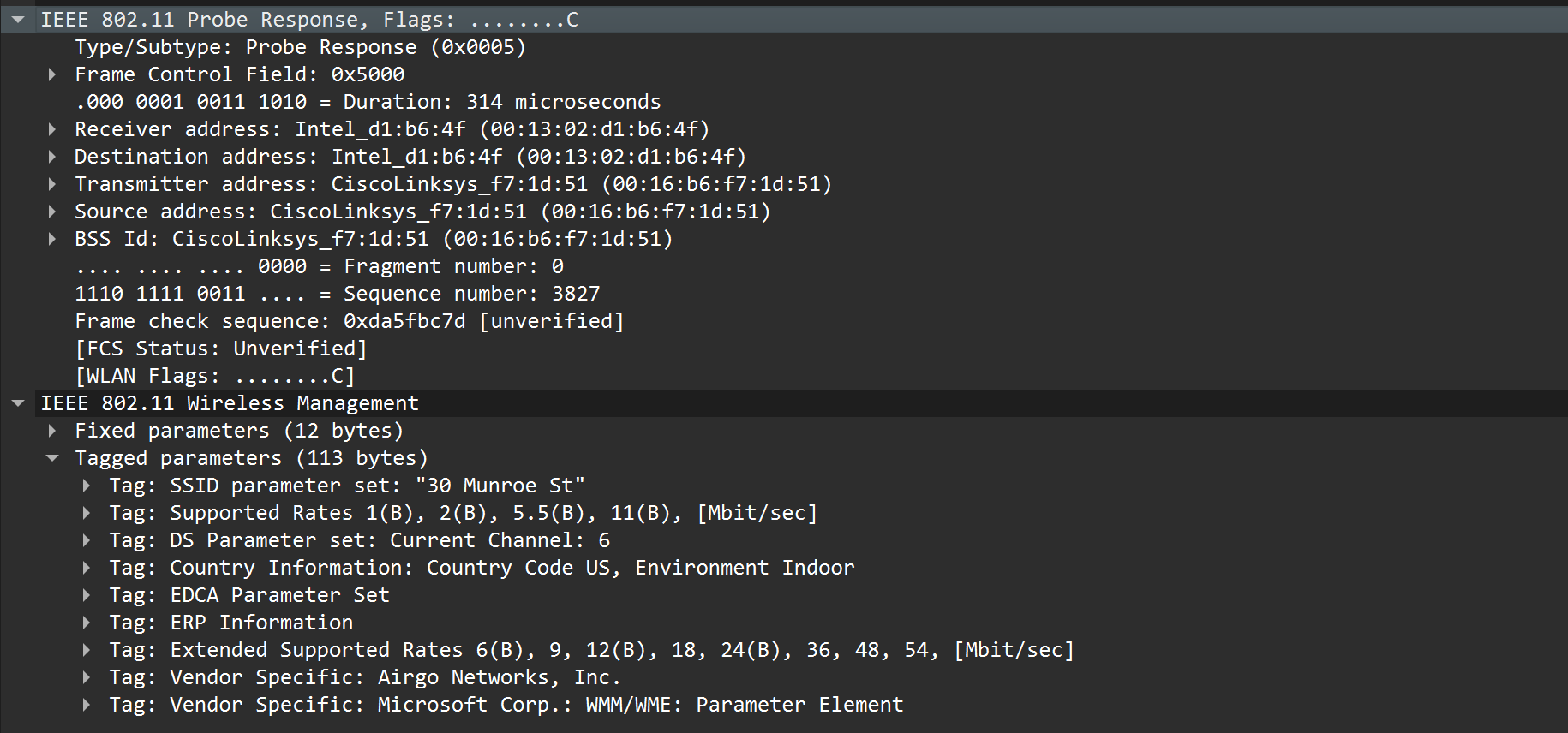


Figure 42 Probe response

SSID: 30 Munroe St

Receiver and Destination address: Клентийн МАС хаяг

Transmitter and Source address: AccessPoint-ийн МАС хаяг

* 1. “linksys\_ses\_24086” ба “30 Munroe St” төхөөрөмжүүд ямар төлөвт ажиллаж байна вэ? Яагаад?





30 Munroe St төхөөрөмж нь assciated төлөвтэй, учир нь Association Request болон Association Response фрэймүүдийн солилцсон.

Харин linksys\_ses\_24086 төхөөрөмж зөвхөн Association Request фрэймүүдийг хүлээж аваад Association Response фрэйм илгээсэнгүй.

* 1. Утасгүй сүлжээний WEP, WPA, WPA2 баталгаажуулалтын аргуудыг харьцуулсан хүснэгт хийж аль нь илүүг тайлбарла.

|  |  |  |  |
| --- | --- | --- | --- |
|  | WEP | WPA | WPA2 |
| Нэвтрүүлсэн он | 1997 | 2003 | 2004 |
| Шифрлэлтийн алгоритм | RC4 (40-bit эсвэл 104-bit) | TKIP (Temporal Key Integrity Protocol) | AES (Advanced Encryption Standard) |
| Нууцлалын түлхүүрийн урт | 64-bit эсвэл 128-bit | 128-bit | 128-bit, 192-bit, эсвэл 256-bit |
| Нэвтрэх түлхүүрийн солилцоо | Гар аргаар тохируулна | Автомат түлхүүр солилцоо | Автомат түлхүүр солилцоо |
| Хэрэглээ | Одоо хэрэглэхгүй болсон | Хуучин төхөөрөмжүүдэд ашиглагддаг | Орчин үеийн ихэнх сүлжээнүүд |
| Баталгаажуулалтын төрөл | Open System, Shared Key | Pre-Shared Key (PSK), 802.1X | Pre-Shared Key (PSK), 802.1X |

**Шалгах асуулт**

1. Утасгүй сүлжээний давуу болон сул талын СВОТ анализ хий.

**Давуу тал:**

* Холболтын төхөөрөмжийн хамрах хүрээнд доторх хөдөлгөөнт байдал
* Холболт үүсгэх, салгах үйлдэл хялбар
* Суурьлуулахад хялбар
* Утастай сүлжээг олон янзаар өргөтгөх боломж олгодог гэх мэт

**Сул тал:**

* Аюулгүй байдал сул
* Нууц үгийн хэрэглэгчидэд түгээх арга зам хэрэгтэй
* Хэрэглэгчидийг хянах боломж хомс
* Халдлагад өртөг магадлал өндөр гэх мэт

**Боломжууд:**

* Wi-Fi стандарт зэрэг утасгүй технологийн дэвшил нь гүйцэтгэл, хурд, аюулгүй байдлыг сайжруулахад хүргэдэг.
* IoT төхөөрөмжүүдийн хэрэглээ нэмэгдэж байгаа нь WLAN-д эдгээр төхөөрөмжийг холбох, удирдахад чухал үүрэг гүйцэтгэх боломжийг бий болгож байна.
* 5G болон захын тооцоолол зэрэг шинээр гарч ирж буй технологиудыг нэгтгэх нь WLAN сүлжээний чадавхи болон гүйцэтгэлийг сайжруулж чадна.
* Утасгүй холболтын эрэлт хэрэгцээ өссөөр байгаа тул WLAN-тай холбоотой бүтээгдэхүүн, үйлчилгээг өргөжүүлэх боломж гарч байна.
* Алсын зайнаас ажиллах нь найдвартай, аюулгүй утасгүй холболтын эрэлтийг нэмэгдүүлж, WLAN үйлчилгээ үзүүлэгчдэд боломж олгож байна.

**Thearts:**

* Кибер аюул заналхийлэл, тэр дундаа хакердах, мэдээлэл зөрчих зэрэг нь WLAN сүлжээний аюулгүй байдалд ихээхэн аюул учруулж байна.
* WLAN зах зээл дэх хүчтэй өрсөлдөөн нь үнийн дайн, бүтээгдэхүүн, үйлчилгээг ялгахад бэрхшээл учруулж болзошгүй.
* Утасгүй сүлжээний хязгаарлагдмал хүртээмж нь хүн ам шигүү суурьшсан газруудад ачаалал үүсгэж, гүйцэтгэлийг бууруулдаг.
* Технологийн хурдацтай дэвшил нь одоо байгаа WLAN дэд бүтцийг хуучирч, байнга шинэчлэх, хөрөнгө оруулалт хийх шаардлагатай болдог.

1. Packet tracer программ дээрээс харахад утастай ба утасгүй сүлжээгээр дамжуулж байгаа фремүүд ялгаатай юу? Мөн пакетууд ялгаатай юу?

Фремүүдийн ялгаатай.

|  |  |  |
| --- | --- | --- |
|  | Утастай сүлжээ(Ethernet Frame) | Утасгүй сүлжээ (IEEE 802.11 Frame) |
| Фреймийн бүтэц | Ethernet фреймийн толгой ба хаяглагдсан бүтэцтэй. | IEEE 802.11 фреймд илүү олон талбарууд (MAC хаяг, SSID гэх мэт). |
| Хаяглалт | Source, Destination MAC хаяг. | Source, Destination, BSSID (Basic Service Set Identifier). |
| Хяналтын талбар | FCS (Frame Check Sequence) ашигладаг. | FCS болон нэмэлт хяналтын талбаруудтай. |
| Баталгаажуулалт ба Холболт | Холболтын баталгаажуулалт шаардлагагүй. | Association, Authentication шаарддаг. |

Утастай болон утасгүй сүлжээнд IP пакетийн бүтэц адилхан байдаг.

1. Утасгүй сүлжээнд ашиглах хэдэн төрлийн төхөөрөмж байдаг вэ?
   * + Wireless Router: Интернетийн холболтыг утасгүй болон утастай төхөөрөмжүүдэд хуваарилдаг, Wi-Fi сүлжээ үүсгэхээс гадна Ethernet порттой байдаг.
     + Access Point: Утасгүй төхөөрөмжүүдийг сүлжээнд холбох зориулалттай. Ихэвчлэн байгууллагын дотоод сүлжээнд ашиглагддаг бөгөөд SSID үүсгэж, дохио дамжуулна.
     + Wireless Network Adapter: Компьютер, зөөврийн төхөөрөмжийг утасгүй сүлжээнд холбох төхөөрөмж.
     + Wireless Controller: Олон тооны Access Point-ийг төвлөрүүлэн удирддаг төхөөрөмж.
     + Wireless Repeater: Утасгүй сүлжээний дохиог хүлээн авч, дахин дамжуулснаар хамрах хүрээг өргөтгөнө.
     + Wireless Bridge: Хоёр тусдаа сүлжээг утасгүйгээр холбох зориулалттай.

**Дүгнэлт**

802.11 стандарт нь утасгүй сүлжээний технологийн хөгжлийг тодорхойлдог бөгөөд хурд, найдвартай байдал, аюулгүй байдал гэсэн гурван гол үзүүлэлт дээр суурилж хөгжсөөр байна. Орчин үеийн сүлжээнүүдэд Wi-Fi 6 (802.11ax) болон WPA3 ашиглах нь үр ашиг, аюулгүй байдлыг хамгийн өндөр түвшинд хүргэх боломжтой.