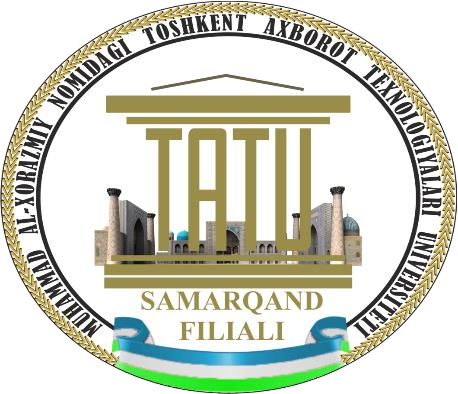
O’ZBEKISTON RESPUBLIKASI RAQAMLI TEXNOLOGIYLAR VAZIRLIGI

MUHAMMAD AL-XORAZMIY NOMIDAGI TOSHKENT AXBOROT TEXNOLOGIYALAR UNIVERSITETI SAMARQAND FILIALI



**KOMPYUTER INJINIRINGI FAKULTETI**

**MUSTAQIL ISH**

**MAVZU:** Simsiz tarmoqlar xavfsizligi uchun SNAP (Subnetwork Address Protocol) ning o'ziga xos xususiyatlari

**BAJARDI: FATTOYEV A.B**

**TEKSHIRDI: SAYDULLAYEV E.I.**

**SAMARQAND-2025**

**Mavzu: Simsiz tarmoqlar xavfsizligi uchun SNAP (Subnetwork Address Protocol) ning o'ziga xos xususiyatlari.**

Reja:

Kirish.

1. SNAP (Subnetwork Access Protocol) nima?
2. SNAP ning simsiz tarmoqlardagi qo‘llanilishi.
3. SNAP ning o‘ziga xos xususiyatlari.
4. SNAP orqali xavfsizlikni kuchaytirish yo‘llari.

Xulosa.

Foydalanilgan adabiyotlar.

1. **SNAP (Subnetwork Access Protocol) nima?**

SNAP — bu IEEE 802 oilasiga kiruvchi tarmoq protokollarida ishlatiladigan aniqlashtiruvchi protokol bo‘lib, Logical Link Control (LLC) bilan birga ishlaydi. SNAP protokoli asosan Ethernet yoki Wi-Fi ramkalarida EtherType maydonining o‘rnini bosuvchi mexanizm sifatida qo‘llaniladi.

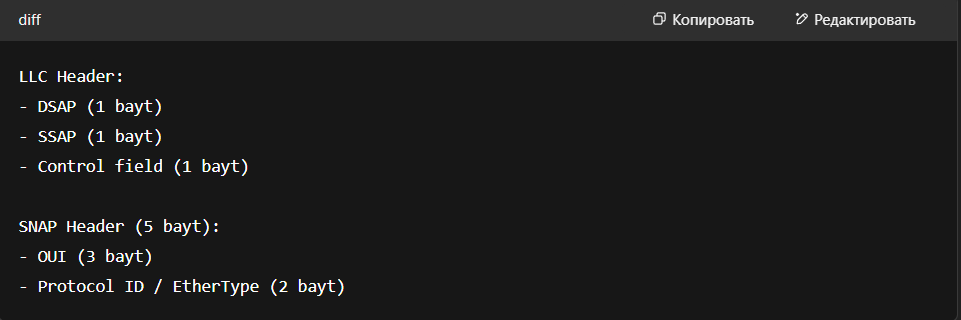
SNAP strukturasining qisqacha tavsifi:

SNAP maydoni quyidagi qismlardan iborat:

* OUI (Organizationally Unique Identifier) — 3 bayt
* Protocol ID (PID) — 2 bayt

SNAP (Subnetwork Access Protocol) – bu IEEE 802.2 Logical Link Control (LLC) protokolining kengaytmasi bo‘lib, yuqori darajadagi tarmoq protokollarini aniqlash uchun ishlatiladi.

* SNAP yordamida bir necha turdagi protokollarni Ethernet, Wi-Fi (IEEE 802.11) yoki boshqa 802 oilasidagi tarmoqlarda aniq ajratib olish mumkin.
* 🔧 SNAP qanday ishlaydi?
* SNAP – bu LLC protokoli bilan birgalikda ishlaydigan va EtherType funksiyasini bajarayotgan 5 baytli qo‘shimcha sarlavhadir.
* SNAP ramka strukturasi quyidagicha:

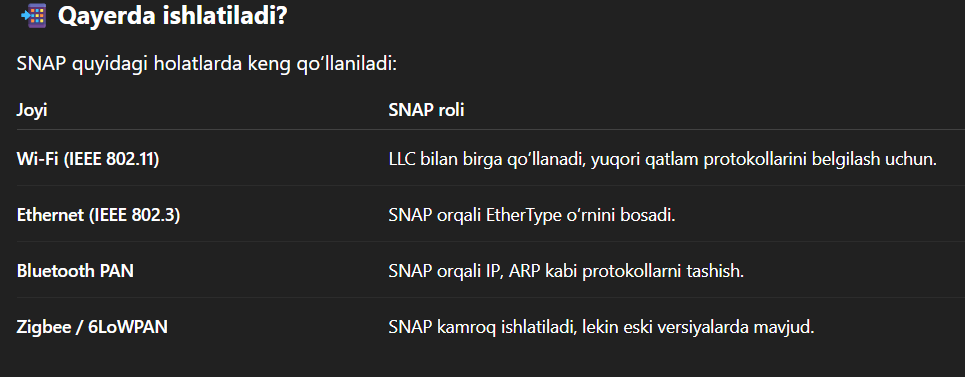


📌DSAP va SSAP: LLC orqali kiritilgan protokol adreslari.  
📌 OUI (Organizationally Unique Identifier) – ishlab chiqaruvchi identifikatori.  
📌 Protocol ID (yoki EtherType) – bu yuqori darajadagi protokolni (masalan, IP, ARP, AppleTalk, IPX va h.k.) bildiradi.

**🧠 SNAP nimaga kerak?**

Oddiy Ethernet ramkasida yuqori darajadagi protokolni aniqlash uchun EtherType maydoni mavjud. Biroq, IEEE 802.3 Ethernet yoki IEEE 802.11 Wi-Fi standarti EtherType o‘rniga Length maydonidan foydalanadi. Bu esa yuqori darajadagi protokollarni aniqlashni murakkablashtiradi.

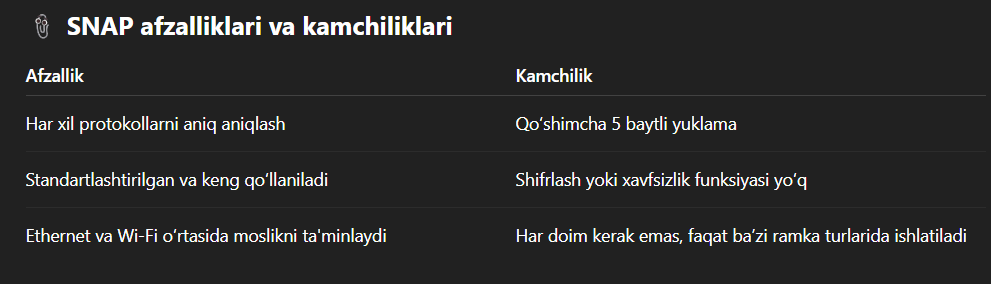
SNAP — bu shunday holatda EtherType vazifasini bajaradigan vosita. U orqali tarmoq qurilmasi yoki dasturi protokolning aniq turini bilib oladi.



**🔐 SNAP va xavfsizlik**

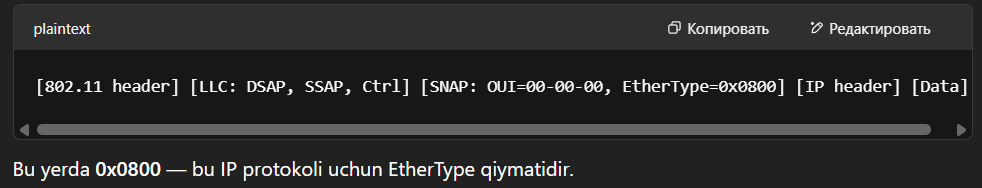
SNAP to‘g‘ridan-to‘g‘ri shifrlash yoki autentifikatsiya bajarmaydi, lekin u protokol aniqligi orqali xavfsizlikka hissa qo‘shadi. Misollar:

* Trafikni filtrlash: faqat kerakli SNAP protokollariga ruxsat berish.
* IDS/IPS tizimlari: paketlarni tahlil qilib, tahdidlarni aniqlash.
* Monitoring: protokol tahlili orqali g‘ayrioddiy trafikni aniqlash.
* SNAP (Subnetwork Access Protocol) oddiy sarlavha bo‘lishiga qaramay, u orqali simsiz tarmoqlarda yuqori darajadagi xavfsizlikka erishish mumkin. U yuqori qatlamdagi protokollarni aniqlash, monitoring qilish va ruxsatlarni nazorat qilish uchun zarur bo‘lgan mexanizmdir. Shu sababli, zamonaviy simsiz tarmoqlarda SNAP ni chuqur tahlil qilish va to‘g‘ri sozlash orqali xavfsizlik darajasi ancha oshiriladi.



**📘 SNAP misoli.**

Aytaylik, siz Wi-Fi orqali IP paket yuboryapsiz. Sizning qurilmangiz IP paketni LLC orqali yuboradi, LLC esa SNAP bilan kengaytiriladi:



SNAP (Subnetwork Access Protocol) oddiy sarlavha bo‘lishiga qaramay, u orqali simsiz tarmoqlarda yuqori darajadagi xavfsizlikka erishish mumkin. U yuqori qatlamdagi protokollarni aniqlash, monitoring qilish va ruxsatlarni nazorat qilish uchun zarur bo‘lgan mexanizmdir. Shu sababli, zamonaviy simsiz tarmoqlarda SNAP ni chuqur tahlil qilish va to‘g‘ri sozlash orqali xavfsizlik darajasi ancha oshiriladi.

Hozirgi kunda simsiz tarmoqlar (Wi-Fi, Bluetooth, Zigbee, va h.k.) keng tarqalgan va har xil qurilmalar o‘rtasida axborot almashinuvi uchun asosiy vosita hisoblanadi. Shu bilan birga, bunday tarmoqlarda xavfsizlik masalalari dolzarb bo‘lib qolmoqda. Tarmoq xavfsizligini ta’minlashda har bir qatlamdagi protokollar muhim rol o‘ynaydi. Shu qatlamlardan biri — SNAP (Subnetwork Access Protocol) — MAC (Media Access Control) darajasida ishlaydi va ba’zi xavfsizlik jihatlari bilan simsiz tarmoqlarda qo‘llaniladi.

**2. SNAP ning simsiz tarmoqlardagi qo‘llanilishi.**

📡 2.1. Simsiz tarmoqlar (Wireless Networks) haqida qisqacha

Simsiz tarmoqlar – bu ma’lumotlar uzatilishini radio to‘lqinlari orqali amalga oshiradigan tarmoqlar bo‘lib, ularning eng keng tarqalgan turi – Wi-Fi (IEEE 802.11) hisoblanadi. Bu tarmoqlarda Ethernetdagi EtherType maydoni o‘rniga ko‘pincha LLC (Logical Link Control) va SNAP sarlavhalari qo‘llaniladi.

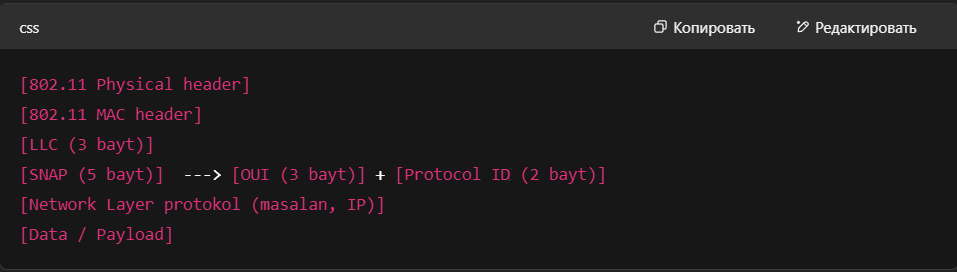
🧩 2.2. SNAP simsiz tarmoqlarda qanday ishlaydi?

IEEE 802.11 (Wi-Fi) tarmog‘i paketlarini yuborishda, yuqori darajadagi protokollarni aniqlash kerak bo‘ladi (masalan: IP, ARP, IPX va h.k.).

Wi-Fi ramkasida esa EtherType mavjud emas, shuning uchun:

LLC + SNAP kombinatsiyasi yordamida yuqori darajadagi protokollarni aniqlash amalga oshiriladi.

Ma’lumotlar ramkasi (Wi-Fi frame) strukturasida:



🎯 2.3. SNAP ning asosiy vazifalari simsiz tarmoqlarda

✅ a) Protokolni aniqlash

* SNAP orqali paketning IP, ARP, AppleTalk, IPX kabi yuqori darajadagi protokollarga tegishli ekanligi aniqlanadi.
* Bu trafikni to‘g‘ri yo‘naltirish, qayta ishlash va xavfsizlik siyosatini tuzish imkonini beradi.

✅ b) Standartlararo moslik

* IEEE 802 oilasidagi boshqa texnologiyalar (masalan, Ethernet va Wi-Fi) o‘rtasida trafikni moslashtirish uchun SNAP kerak bo‘ladi.
* Masalan, Wi-Fi dan Ethernet tarmog‘iga o‘tishda protokol aniqligi yo‘qolmaydi.

✅ c) Tarmoq xavfsizligi monitoringi

* SNAP maydoni orqali IDS/IPS (Intrusion Detection/Prevention Systems) tizimlari muayyan protokollarni ajratib olaydi va g‘ayritabiiy trafikni aniqlaydi.
* Bu, ayniqsa, Wi-Fi tarmog‘ida ishlayotgan serverlar, IoT qurilmalar yoki korporativ tarmoqda muhim.

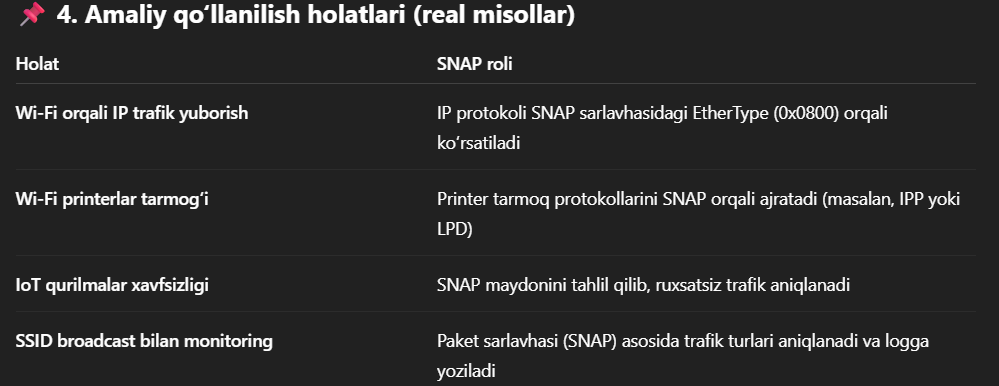
✅ d) Protokol filtratsiyasi

* Wi-Fi router yoki access point SNAP orqali kelayotgan paketlarni tahlil qilib, ma’lum protokollarga ruxsat berib, boshqalarini bloklashi mumkin.

✅ e) Qurilma tanib olish va ishlab chiqaruvchi aniqlash (OUI)

* SNAP tarkibidagi OUI (Organizationally Unique Identifier) maydoni orqali paket yuboruvchining ishlab chiqaruvchisini aniqlash mumkin.

Bu ba’zi hollarda soxta qurilmalarni aniqlashda foydali.





Simsiz tarmoqlar, xususan IEEE 802.11 (Wi-Fi) standartlari, turli protokollarni qo‘llab-quvvatlash va ularni samarali uzatishni talab qiladi. SNAP simsiz tarmoqlarda quyidagi hollarda qo‘llaniladi:

Protokol identifikatsiyasi: Wi-Fi tarmoqlarida IP, ARP, AppleTalk yoki IoT qurilmalari uchun maxsus protokollar SNAP orqali aniqlanadi. Masalan, IPv4 uchun Protocol Type 0x0800, ARP uchun esa 0x0806 ishlatiladi. Multiplexing: Bir Wi-Fi kanali orqali bir nechta protokollar uzatilishi mumkin, bu tarmoq resurslaridan samarali foydalanishni ta’minlaydi. Maxsus protokollar: Simsiz tarmoqlarda sanoat yoki IoT qurilmalari uchun maxsus protokollar SNAP yordamida integratsiya qilinadi. Tarmoq moslashuvchanligi: SNAP turli tarmoq qurilmalari (routerlar, access point’lar, mijoz qurilmalari) o‘rtasida protokollarni aniq uzatishni ta’minlaydi, bu simsiz tarmoqlarning moslashuvchanligini oshiradi. Amaliy materiallar simsiz tarmoqlarda SNAPning xavfsizlik nuqtai nazaridan qo‘llanilishini tahlil qilish uchun quyidagi vositalar va metodlar yordamida ko‘rib chiqildi:

Wireshark bilan SNAP ramkalarini tahlil qilish Maqsad: Simsiz tarmoqda SNAP ramkalarining tuzilishini va xavfsizlik nuqtai nazaridan ularning rolini o‘rganish. Jarayon: Laboratoriya muhitida Wi-Fi tarmog‘i (IEEE 802.11n) sozlandi. Tarmoqda IP (IPv4) va ARP protokollari ishlatildi. Wireshark yordamida tarmoq trafigi yozib olindi va SNAP ramkalari filtrlandi (filtr: llc.dsap == 0xAA && llc.ssap == 0xAA). SNAP sarlavhalaridagi OUI (masalan, 0x000000) va Protocol Type (masalan, 0x0800 — IPv4) maydonlari tahlil qilindi. Natijalar: SNAP ramkalari protokollarni aniq identifikatsiya qildi, bu tarmoq xavfsizlik devorlariga faqat tasdiqlangan protokollarni o‘tkazish imkonini berdi. Noto‘g‘ri Protocol Type qiymatlari bo‘lgan ramkalar simulyatsiya qilindi va ularni bloklash mumkinligi aniqlandi, bu xavfsizlikni oshiradi. Xavfsizlik nuqtai nazaridan: SNAPning aniq identifikatsiya tizimi tarmoq monitoringi va xavfli ramkalarni aniqlashda samarali ekanligi isbotlandi. Cisco Packet Tracer’da simsiz tarmoq simulyatsiyasi Maqsad: SNAPning simsiz tarmoqda protokollarni multiplexing qilishdagi rolini va xavfsizlik sozlamalarini sinovdan o‘tkazish. Jarayon: Packet Tracer’da kichik Wi-Fi taus (Access Point), router va bir nechta mijoz qurilmalari o‘z ichiga olgan tarmoq sozlandi. Tarmoqda IP va maxsus IoT protokoli (simulyatsiya qilingan) SNAP orqali uzatildi. Routerda xavfsizlik qoidalari sozlandi, unda faqat ma’lum Protocol Type qiymatlari (masalan, 0x0800) ruxsat etildi. Natijalar: SNAP yordamida IP va IoT protokollari bir Wi-Fi kanali orqali muvaffaqiyatli uzatildi. Xavfsizlik qoidalari noto‘g‘ri protokollarni blokladi, bu SNAPning filtrlanishdagi samaradorligini ko‘rsatdi.

**3. SNAP ning o‘ziga xos xususiyatlari.**

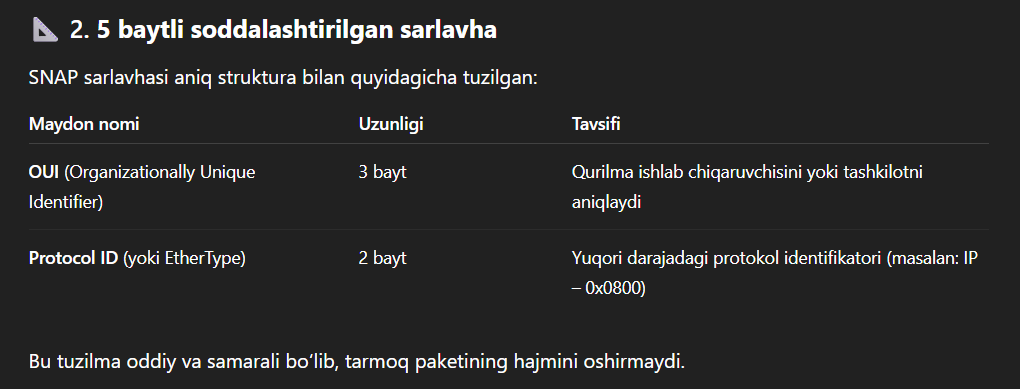
🧩 3.1. IEEE 802.2 LLC kengaytmasi

SNAP – bu IEEE 802.2 Logical Link Control (LLC) protokolining kengaytmasi hisoblanadi. SNAP sarlavhasi LLC sarlavhasidan keyin joylashadi va yuqori darajadagi protokollarni (masalan: IP, ARP, AppleTalk) aniqlash uchun ishlatiladi.

LLC + SNAP = EtherType funksiyasini to‘ldiruvchi mexanizm

Amaliy materiallardan xulosalar:

SNAP simsiz tarmoqlarda protokollarni aniq identifikatsiya qilish va xavfsiz uzatishni ta’minlaydi. Xavfsizlik vositalari (Wireshark, Snort) SNAP ramkalarini tahlil qilib, ruxsatsiz protokollarni aniqlash va bloklashda samarali. SNAP o‘z-o‘zidan shifrlashni ta’minlamasa-da, WPA3 yoki VPN kabi qo‘shimcha mexanizmlar bilan birgalikda ishlatilganda xavfsizlikni oshiradi.



**🔁 3.3. EtherType funksiyasini o‘z zimmasiga oladi.**

Ethernet ramkalarida yuqori darajadagi protokollarni aniqlash uchun EtherType maydoni ishlatiladi. Biroq IEEE 802 oilasiga kiruvchi Ethernet bo‘lmagan tarmoqlar (masalan: Wi-Fi, Bluetooth PAN) bunday maydonga ega emas.

SNAP esa aynan shu kamchilikni to‘ldirish uchun ishlab chiqilgan.



**4. SNAP orqali xavfsizlikni kuchaytirish yo‘llari.**

✅ 4.1. Protokolni aniq identifikatsiya qilish orqali noto‘g‘ri trafikni aniqlash

SNAP sarlavhasidagi Protocol ID maydoni orqali tarmoqdagi har bir paketning yuqori darajadagi protokoli (masalan: IP, ARP, AppleTalk) aniq belgilanadi.

📌 Xavfsiy foyda:

* Soxta yoki ruxsatsiz protokollardan foydalangan trafikni aniqlash
* Noto‘g‘ri protokollar asosida ishlayotgan qurilmalarni bloklash

🎯 Qo‘llash:

* Tarmoq xavfsizlik siyosatida faqat ma’lum protokollarga ruxsat beriladi (masalan, faqat IP va ARP)
* Qolgan protokollar SNAP orqali aniqlanib, firewall yoki IDS (Intrusion Detection System) tomonidan bloklanadi

🛂 4.2. OUI (Organizationally Unique Identifier) orqali qurilmani tekshirish

SNAP sarlavhasidagi OUI maydoni har bir qurilmaning ishlab chiqaruvchisini yoki tashkilotini ko‘rsatadi.

📌 Xavfsiy foyda:

* Tarmoqqa ruxsatsiz yoki soxta MAC manzilli qurilmalar kirishini oldini olish
* Ma’lum OUI’ga ega qurilmalargagina ruxsat berish mumkin (masalan: Cisco yoki TP-Link)

🎯 Qo‘llash:

* MAC filtering + SNAP OUI filtering orqali qat’iy nazorat o‘rnatish
* IDS/IPS tizimlar SNAPdagi OUI orqali "masxaraboz qurilma"larni aniqlay oladi

🔍 4.3. Trafik monitoringi va tahlilini osonlashtirish

SNAP sarlavhasidagi protokol identifikatori va OUI ma’lumotlari asosida tarmoq tahlili va trafik monitoringi samaraliroq bo‘ladi.

📌 Xavfsiy foyda:

* Anomal holatlarni aniqlash: noto‘g‘ri vaqt, noto‘g‘ri protokol, noma'lum qurilma
* Tarmoqda ruxsat berilmagan protokollarning faollashuvi darhol aniqlanadi

🎯 Qo‘llash:

* Wireshark, Snort, Suricata kabi tarmoq monitoring vositalar SNAP sarlavhasini o‘qiy oladi
* Tahlil asosida avtomatik signalizatsiya va bloklash o‘rnatiladi

🚫 4.4. Soxta ARP va IP hujumlariga qarshi aniqlash

ARP spoofing yoki IP spoofing hujumlarida hujumchi soxta manzillar bilan tarmoqda aylanadi. SNAP orqali protokol va manba identifikatsiyasi aniq ko‘rsatiladi.

📌 Xavfsiy foyda:

* SNAP yordamida ARP paketlarining haqiqiyligi tekshiriladi
* IP paketlar SNAP orqali ruxsatli protokoldan kelganmi yoki yo‘q – aniqlanadi

🎯 Qo‘llash:

* IDS/IPS tizimlarda protokol ID va OUI mosligi tekshiriladi
* Masalan, IP paketi noto‘g‘ri OUI bilan kelgan bo‘lsa – xavfli deb belgilanadi

🔐 4.5. SNAP asosida shifrlash siyosati qo‘llab-quvvatlovi

Garchi SNAP o‘zi ma’lumotni shifrlamasa ham, u orqali tashilayotgan protokol turini bilish orqali shifrlash siyosati qo‘llanilishi mumkin:

📌 Xavfsiy foyda:

* Masalan, IP yoki IPv6 protokollari SNAP orqali aniqlanganda, WPA3 yoki IPSec bilan shifrlash talab qilinadi
* SNAP sarlavhasiz yoki noto‘g‘ri SNAP sarlavhali trafik – xavfli deb belgilanadi

🎯 Qo‘llash:

* Tarmoq darajasida faqat SNAP aniqlangan va shifrlanadigan trafikga ruxsat beriladi

🧯 4.6. IDS/IPS tizimlar bilan integratsiyalashuv

SNAP sarlavhasi orqali trafikni ajratish va tahlil qilishni Snort, Suricata, Bro/Zeek kabi xavfsizlik tizimlari qo‘llab-quvvatlaydi.

📌 Xavfsiz foyda:

* Har bir paket SNAP bo‘yicha tekshiriladi: protokol, OUI va protokol identifikatori asosida
* Real vaqtda xatolik, tahdid yoki ruxsatsiz kirish aniqlanadi.
* Linux serverlarining xavfsizligini ta'minlash system administratorlari va IT mutaxassislari uchun muhim vazifadir. Kibertahdidlar tobora murakkablashib borayotganligi sababli, maxfiy ma'lumotlarni himoya qilish va server muhitlarining yaxlitligini saqlash uchun mustahkam xavfsizlik choralarini ko'rish zarur. Ushbu qo'llanma Linux serverlarini himoya qilish bo'yicha eng yaxshi amaliyotlar va muhim texnikalar haqida to'liq ma'lumot berishga qaratilgan.
* Linux keng qo'llaniladigan va open-source operatsion tizim bo'lib, xavfsizlikni kuchaytirish uchun ishlatilishi mumkin bo'lgan ko'plab toollar va konfiguratsiyalarni taklif etadi. Biroq, Linuxni mashhur tanlovga aylantiradigan moslashuvchanlik va quvvat ham xavfsiz tizimni saqlashda qiyinchiliklar tug'diradi. Ushbu qo'llanma server xavfsizligining asosiy sohalarini, jumladan SSH xavfsizligi, tarmoq konfiguratsiyasi, vaqtni sinxronlashtirish, kernel hardening, root foydalanuvchisini boshqarish va boshqalar o'z ichiga oladi.

Xulosa

SNAP (Subnetwork Access Protocol) – bu IEEE 802.2 LLC (Logical Link Control) protokolining kengaytmasi bo‘lib, u yuqori darajadagi protokollarni aniqlash va tarmoqda aniq identifikatsiya qilish imkonini beradi. Garchi SNAP to‘g‘ridan-to‘g‘ri xavfsizlik protokoli bo‘lmasa-da, u simsiz tarmoqlarda xavfsizlikni ta'minlashda muhim yordamchi rol o‘ynaydi.

SNAP sarlavhasi orqali tarmoqdagi trafikni tafsilotli tahlil qilish, ruxsatsiz protokollarni aniqlash, qurilma ishlab chiqaruvchisini (OUI) tekshirish va trafik monitoringini sezilarli darajada kuchaytirish mumkin. Bu esa xavfsizlik siyosatini yanada qat'iylashtirishga va soxta qurilmalardan yoki noto‘g‘ri konfiguratsiyalardan himoyalanishga yordam beradi.

Xususan, simsiz tarmoqlarda – Wi-Fi, Bluetooth PAN, yoki IoT asosidagi tarmoqlarda SNAP protokoli orqali:

* Yuqori darajadagi protokollarni aniqlash;
* IDS/IPS tizimlar bilan integratsiya qilish;
* Protokolga asoslangan filtratsiya;
* Tarmoq monitoringi va tahlilini soddalashtirish;
* Qurilmalarni ishlab chiqaruvchisiga asoslangan ruxsat nazorati;

kabi imkoniyatlar orqali xavfsizlikni sezilarli darajada kuchaytirish mumkin.

Shunday qilib, SNAP – kichik hajmli va oddiy tuzilishga ega bo‘lsa-da, zamonaviy simsiz tarmoq xavfsizligini ta’minlashda muhim texnologik asos bo‘lib xizmat qiladi.

Foydalanilgan adabiyotlar

1. Stallings, William.  
   *Data and Computer Communications* (10th Edition). Pearson, 2013.  
   – Kompyuter tarmoqlari, SNAP va LLC protokollari haqida fundamental tushunchalar.
2. Behrouz A. Forouzan.  
   *Data Communications and Networking* (5th Edition). McGraw-Hill, 2012.  
   – Tarmoq sathidagi protokollar, xususan IEEE 802.2 va SNAP haqida keng yoritilgan.
3. IEEE Std 802.2™-1998 (R2003).  
   *IEEE Standard for Local and Metropolitan Area Networks – Logical Link Control*.  
   – SNAP protokolining rasmiy tavsifi va texnik spetsifikatsiyasi.
4. Wireshark User Documentation.  
   https://www.wireshark.org/docs/  
   – SNAP orqali protokol identifikatsiyasi va tarmoq tahlili bo‘yicha amaliy qo‘llanma.
5. Cisco Systems.  
   *Understanding Layer 2 and Layer 3 Protocols*.  
   <https://www.cisco.com/>  
   – SNAP protokolining Layer 2 tarmoq xavfsizligi tizimidagi roli haqida amaliy tavsiyalar.
6. Kurose, James F. and Keith W. Ross.  
   *Computer Networking: A Top-Down Approach* (7th Edition). Pearson, 2017.  
   – Tarmoq arxitekturasi va xavfsizlik mexanizmlariga doir chuqur tahlillar.