ДЕРЖАВНИЙ УНІВЕРСИТЕТ ТЕЛЕКОМУНІКАЦІЙ
НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ ЗАХИСТУ ІНФОРМАЦІЇ

КАФЕДРА ІНФОРМАЦІЙНОЇ ТА КІБЕРНЕТИЧНОЇ БЕЗПЕКИ

Пояснювальна записка

до бакалаврської роботи

на тему:

«ДОСЛІДЖЕННЯ ШЛЯХІВ ТА РОЗРОБКА РЕКОМЕНДАЦІЙ ЩОДО ЗАХИСТУ БЕЗПРОВОДОВОЇ МЕРЕЖІ ІЗ ВИКОРИСТАННЯ CISCO IDENTITY SERVICES ENGINE»

Виконав: студент 4 курсу, групи БСД-41
спеціальності 125 Кібербезпека
освітньо-професійної програми «Інформаційна та кібернетична безпека»
(шифр і назва спеціальності)
Івахненко К.В.
(прізвище та ініціали)
Керівник Довженко Н.М.
(прізвище та ініціали)
Рецензент
(прізвище та ініціали)
Нормоконтролер Чумак Н.С.
(прізвище та ініціали)

КИЇВ – 2023

ВСТУП

Актуальність дослідження. Мобільні гаджети проникли не тільки в наше життя, а й у роботу. Хто не читає корпоративної пошти зі свого смартфона? Вимоги бізнесу та сучасного світу покладають на підрозділи IT досить складне завдання забезпечити доступ користувачам до корпоративних ресурсів з будь-якого пристрою.

Багато хто хоче мати можливість використовувати персональні пристрої для роботи (BYOD). Це ж так просто “бути на зв'язку” та “в роботі”, коли крім свого планшета більше нічого немає. Віддалений доступ через VPN давно став нормою для більшості організацій. IT-підрозділи змушені синхронізувати політики доступу та налаштування на пристроях дротової, бездротової мережі та мережі віддаленого доступу.

Користувач повинен отримати однаковий рівень мережевих сервісів, щоб ефективно виконувати свою роботу як мобільного співробітника. Вимоги бізнесу до мобільності користувачів визначають прив'язку політики не до місця підключення, а до користувача – це ускладнює налаштування мережі та супровід.

Питання підтримки також множаться на кількість можливих варіантів доступу до мережі. Найчастіше навіть для базової оцінки поточних проблем у мережі знадобиться впровадження засобів автоматизації. Для скорочення часу на підтримку користувачів, було б зручно мати можливість бачити ім'я користувача у всіх логах та вікнах моніторингу. Це виключить необхідність знайти як і чим підключений користувач до мережі.

Мета роботи – розробити рекомендації щодо застосування методів та засобів захисту безпроводової мережі за допомогою Cisco Identity Services Engine.

Об’єкт дослідження – безпроводова мережа.

Предмет дослідження – методи та засоби захисту безпроводової мережі. *Практичне значення одержаних результатів.* Рекомендації щодо захисту

безпроводової мережі за допомогою Cisco Identity Services Engine можуть бути використані у сфері забезпечення ефективності використання та зберегти свої дані.

Апробація результатів. Основні наукові результати роботи доповідалися та обговорювалися на одній конференції.

1) Науково-практична конференція «Цифрова трансформація кібербезпеки», Навчально-наукового інституту захисту інформації, 27 квітня 2023 р.

1 АНАЛІЗ СУЧАСНИХ БЕЗПРОВОДОВИХ МЕРЕЖ

1.1 Визначення безпроводових мереж і технологій

Залежно від області, безпроводові мережі можна розділити на чотири групи застосування та діапазон сигналу: безпроводові персональні мережі (WPAN), безпроводові локальні мережі (WLAN), безпроводові міські мережі (WMAN) і безпроводові глобальні мережі (WWAN). Рис. 1.1 ілюструє ці чотири категорії [1].

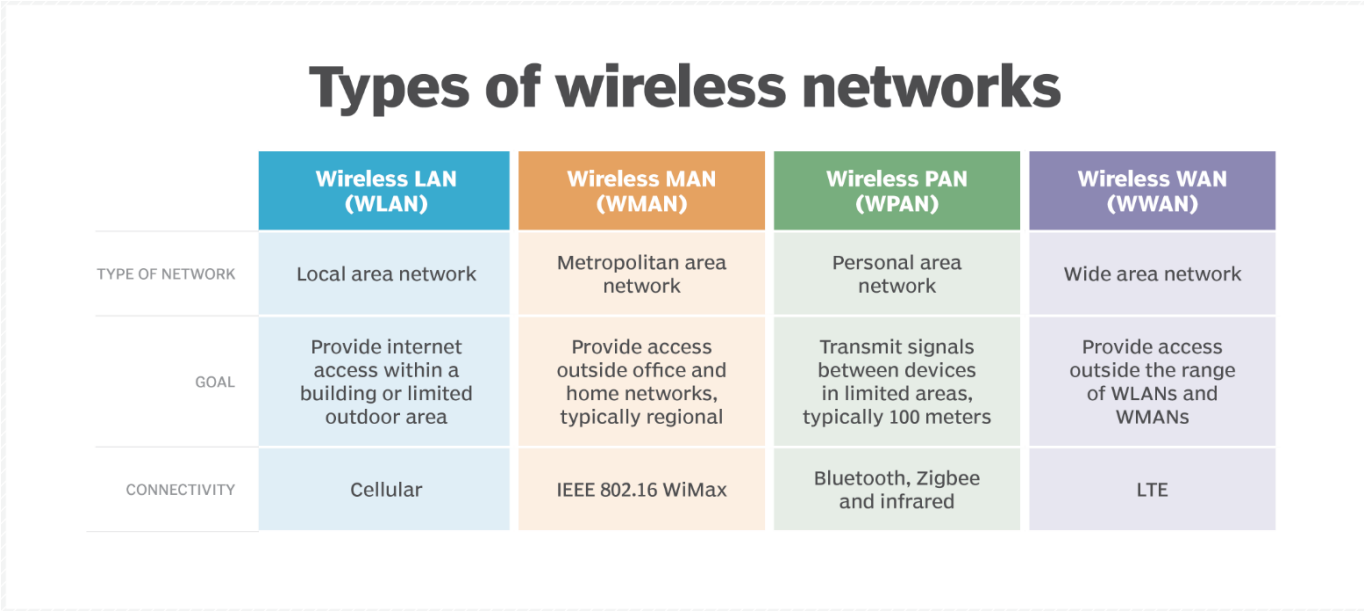

Рис. 1.1. Класифікація безпроводових мереж

Крім того, безпроводові мережі також можна розділити на два широких сегменти: малого радіусу дії та далекого радіусу дії. Безпроводовий зв'язок малого радіусу дії відноситься до обмежених мереж на обмежену територію. Це стосується локальних мереж (LAN), наприклад корпоративних будівель, шкільних кампусів, виробничих підприємств або будинків, а також особисті локальні мережі (PAN), де портативні комп'ютери знаходяться в безпосередній близькості один від одного, де інша потреба в спілкуванні. Ці мережі зазвичай працюють без ліцензії спектр,

зарезервований для промислового, наукового та медичного (ISM) використання [7]. Доступні частоти відрізняються від країни до країни. Найпоширенішими діапазонами є на частотах 2,4 ГГц і 5 ГГц, які доступні в більшості країн світу. Наявність цих частот дозволяє користувачам працювати в безпроводових мережах без отримання ліцензії, причому безкоштовно. Оскільки ліцензія не потрібна для використання, вона сприяє розширенню таких мереж. В мережах дальнього радіусу зв’язку зазвичай надають компанії, які продають безпроводове підключення як послугу. Ці мережі охоплюють великі території, такі як столична область (WMAN), штат або провінція, або ціла країна. Мета мережі дальнього радіусу дії — це забезпечення безпровідного покриття в усьому світі. Найбільш поширеним є мережа дальнього радіусу дії — безпроводова глобальна мережа (WWAN). Коли справді потрібне глобальне покриття, супутникові мережі також доступні [4].

Безпроводові персональні мережі (WPAN). Безпроводові персональні мережі базуються на стандарті IEEE 802.15. Вони дозволяють зв'язок на дуже короткій відстані, близько 10 метрів. На відміну від інших безпроводових мереж, з’єднання через WPAN передбачає невелику кількість або відсутність інфраструктури або пряме підключення до світу за межами зв’язку. Це дозволяє впроваджувати невеликі, енергоефективні, недорогі рішення для широкого діапазону таких пристроїв як смартфон і КПК.

Ці мережі характеризуються низьким споживанням енергії та низькою швидкістю передачі даних. Такі різного роду мережі ретранслюють такі технології, як Bluetooth, IrDA, ZigBee або UWB [2].

З точки зору застосування, Bluetooth призначений для безпроводової миші, клавіатури та гарнітури hands-free, IrDA призначений для з’єднання «точка-точка» між двома пристроями для простої передачі даних і синхронізації файлів, ZigBee розроблено для надійних безпроводових мереж моніторингу та керування, а також UWB орієнтований на мультимедійні канали з високою пропускною здатністю.

• **Bluetooth.** Bluetooth відповідає стандарту IEEE 802.15.1. Спочатку був Bluetooth призначений для низького енергоспоживання, малого радіусу дії та всеспрямованого (вказують на багатоточковий) зв'язка і дешеві пристрої, які будуть використовуватися як заміна кабелю, з’єднання пристроїв через спеціальне з’єднання радіохвиль. Сучасні розробники розробляють компоненти та системи з підтримкою Bluetooth для низки додаткових програм [9]. Ця технологія працює для трьох різних класів пристроїв: Клас 1, клас 2 і клас 3, де радіус дії становить приблизно 100 метрів, 10 метрів і 1 метр відповідно. Використовуючи діапазон 2,4 ГГц, два пристрої в зоні покриття один з одним може спільно використовувати до 720 Кбіт/с ємності або швидкості передачі. Найбільший зазвичай використовується клас 2. Мережа Bluetooth також називається пікомережею та складається з 8 активних мереж пристроїв у відносинах головний-підлеглий. Перший пристрій Bluetooth у пікомережі головний, а всі інші пристрої є підлеглими, які спілкуються з головним. А пікомережа зазвичай має радіус дії 10 метрів, хоча діапазон може досягати 100 метрів, які можна досягти за ідеальних обставин. Для забезпечення безпеки, кожне посилання закодовано та захищене від прослуховування та перешкод. Можна підключити дві пікомережі і утворити скаттернет. Пристрій Bluetooth може брати участь у кількох пікомережах водночас, таким чином допускаючи можливість того, що інформація може надходити за межі зони покриття однієї пікомережі. Пристрій у розсіяній мережі може бути підлеглим до декількох пікомереж, але майстер лише в одній із них [8].

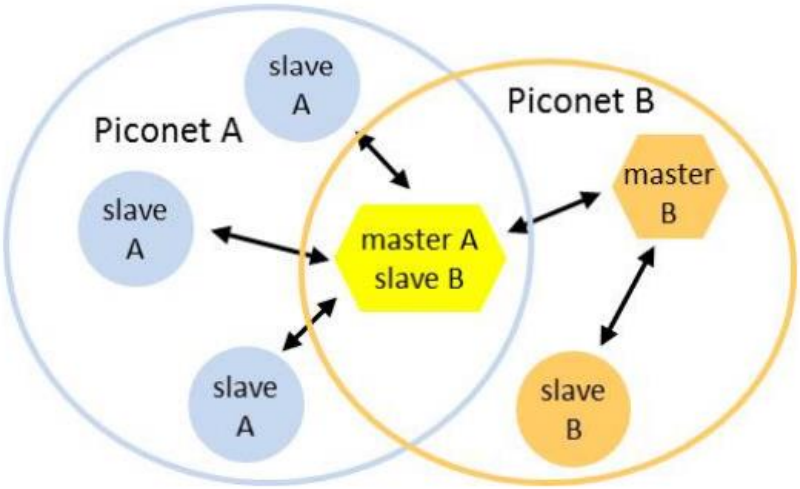

Рис. 1.2. Головний у пікомережі А є підлеглим піконетом Б у скаттернеті Bluetooth з двома пікомережами

- **IrDA.** Асоціація інфрачервоних даних (IrDA) визначає повний набір інфрачервоних стандартів зв'язку. IrDA відноситься до цього набору стандартів і звик забезпечувати безпроводове підключення до пристроїв, для яких зазвичай використовуються кабелі підключення. IrDA малопотужний, недорогий, односпрямований (точка-точка), вузький кутовий (< 30º) конус, спеціальний стандарт передачі даних, призначений для роботи на відстані до 1 метра та на швидкості від 9600 біт/с до 4 Мбіт/с (зараз), 16 Мбіт/с (в стадії розробки). Деякі з пристроїв, які використовують IrDA, це ноутбуки, КПК, принтери та камери.

• **ZigBee.** ZigBee базується на стандарті IEEE 802.15.4 і був розроблений як відкритий глобальний стандарт для задоволення унікальних потреб простого впровадження, високої надійності, недорогі, малопотужні та низькошвидкісні мережі безпроводових пристроїв. ZigBee працює через неліцензовані діапазони, включаючи максимум 2,4 ГГц, 900 МГц і 868 МГц швидкість передачі 250 Кбіт/с, достатня для задоволення потреб датчиків і автоматизації безпроводових. ZigBee також служить для створення великих безпроводових мереж, які не потребують великої кількості даних, а також пропускної здатності. У мережі ZigBee можуть брати участь два різні типи пристроїв: повнофункціональні пристрої (FFD) і пристрої зі зниженою функціональністю (RFD) [7]. FFD можуть працювати в три режими, які служать координатором WPAN, координатором або пристроєм. RFD тільки призначений для надзвичайно простих застосувань, таких як вимикач світла. ZigBee підтримує три різні топології: зірку, сітку та дерево кластерів, які показано на рисунку 1.3. У топології «зірка» зв’язок встановлюється між пристроями та єдиний центральний контролер, який називається координатором WPAN. У сітчастій топології будь-який пристрій може спілкуватися з будь-яким іншим пристроєм, якщо вони знаходяться в зоні дії

один одного. Мережа кластерного дерева є окремим випадком сітчастої мережі, в якій більшість пристрої є FFD, а RFD може підключатися до мережі дерева кластерів як листовий вузол на кінці гілки. Будь-який з FFD може виконувати роль маршрутизатора і забезпечувати служби синхронізації з іншими пристроями та маршрутизаторами. Є лише один із цих маршрутизаторів координатор WPAN [2].

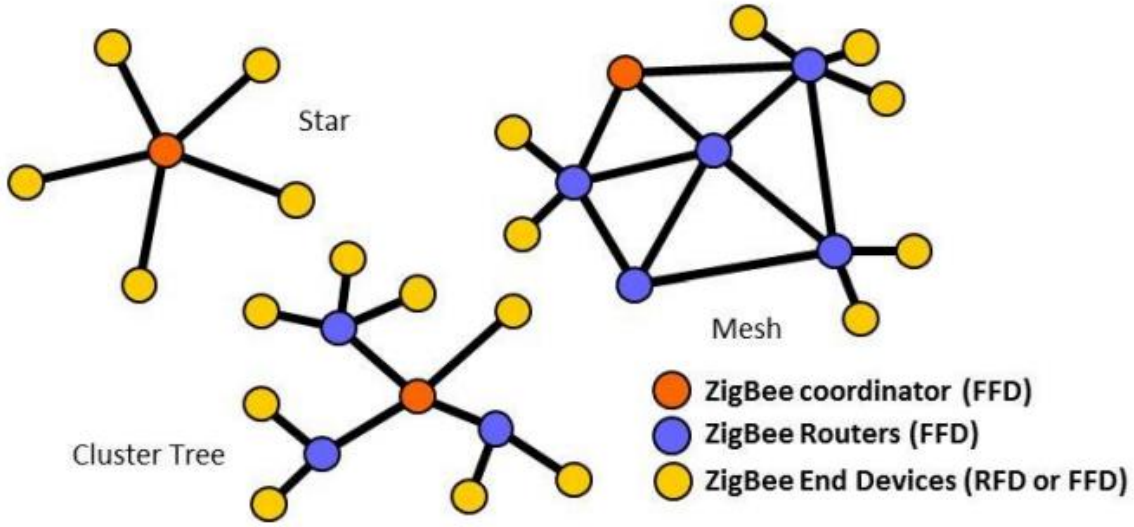

Рис. 1.3. Схема структури мережі ZigBee

• **UWB.** На основі стандарту IEEE 802.15.3 технологія Ultra Wide Band (UWB) нещодавно привернув велику увагу як високошвидкісний безпровідний зв'язок малого радіусу дії для приміщень комунікацій. UWB служить зовсім іншим цілям, ніж інші технології згадані в цьому розділі. UWB забезпечує переміщення великих файлів із високою швидкістю передачі даних швидкості на короткі відстані. Таким чином, UWB забезпечує передачу даних від 110 Мбіт/с до 480 Мбіт/с на відстані до кількох метрів, що може задовольнити більшість мультимедійних даних таких програм, як доставка аудіо та відео в домашній мережі, а також може виконувати роль безпроводового кабелю, який замінює високошвидкісну послідовну шину, таку як USB 2.0 і IEEE 1394. В Америці частоти для UWB були виділені в діапазоні 3,1 ГГц до діапазону 10,6 ГГц. Проте в Європі частоти включають дві частини: від 3,4 ГГц до

4,8 ГГц і від 6 ГГц до 8,5 ГГц. UWB - передачі передають інформацію, генеруючи радіоенергію на певному рівні часових інтервалів та займають велику смугу пропускання (рис. 1.4), і таким чином уможливлюючи позиціонування імпульсу або часову модуляцію. Інформація також може бути модульована на UWB сигналів (імпульсів) шляхом кодування полярності імпульсу, його амплітуди та/або за допомогою ортогональні імпульси. Імпульси UWB можуть надсилатися спорадично з відносно низькою частотою імпульсів для підтримки часової або позиційної модуляції, але також може надсилатися зі швидкістю до інверсної ширини смуги імпульсу UWB [2].

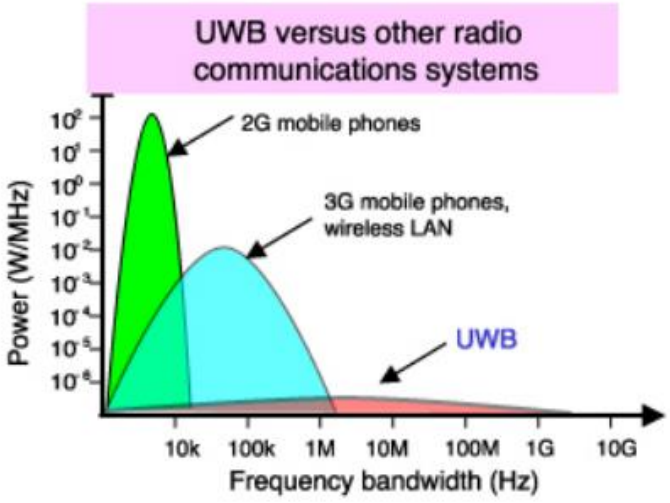

Рис.1.4. Використання потужності та смуги частот UWB

Безпроводова локальна мережа (WLAN). Безпроводові локальні мережі (WLAN) призначені для забезпечення безпроводового доступу в зонах із типовим радіусом дії до 100 метрів і використовуються переважно вдома, у школі, комп'ютерній лабораторії або офісне середовище (рис. 1.5). Це дає користувачам здатність пересуватися в межах місцевої зони покриття та залишатися на зв'язку в мережі. Мережі WLAN базуються на стандартах IEEE 802.11, які продаються під торговою маркою Wi-Fi. Через конкуренцію інші стандарти, такі як HiperLAN, ніколи не отримували широке комерційне впровадження. IEEE 802.11 було простіше в реалізації і швидше вийшов на ринок [1].

IEEE 802.11 — це сімейство різних стандартів для безпроводових локальних мереж.

IEEE 802.11b був першим прийнятим стандартом, який підтримував до 11 Мбіт/с у неліцензованому діапазоні спектру 2,4 ГГц. Потім був розроблений стандарт IEEE 802.11g як наступник IEEE 802.11b з більшою пропускною здатністю. Доступ IEEE 802.11g до точки, підтримуватиме клієнтів 802.11b і 802.11g. Так само ноутбук з IEEE карткою 802.11g матиме доступ до існуючих точок доступу 802.11b, а також до нових точок доступу 802.11g. Це тому, що використовуватимуться безпроводові локальні мережі на основі 802.11g, де той самий діапазон 2,4 ГГц, який використовує 802.11b. Максимальна швидкість передачі для IEEE швидкості безпроводового з'єднання 802.11g становить 54 Мбіт/с, але вона автоматично відключатиметься від 54 Мбіт/с коли радіосигнал слабкий або якщо виявлено перешкоди [7].

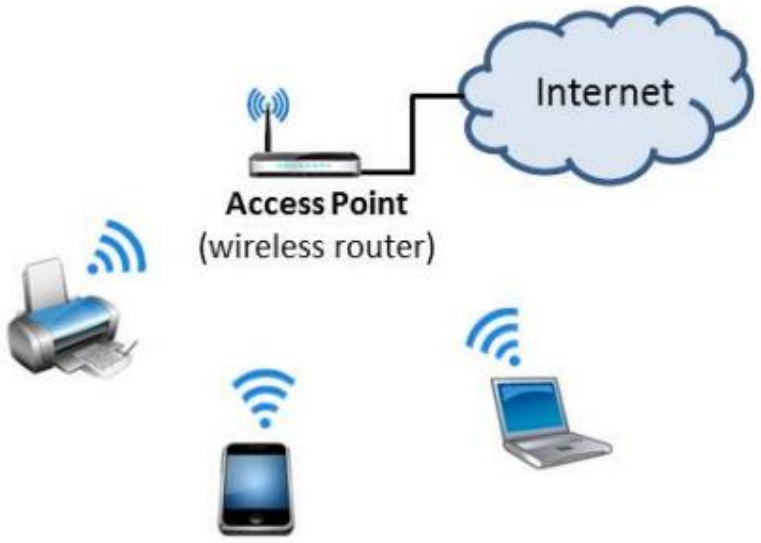

Рис.1.5. Діаграма домашньої WLAN

Безпроводова міська мережа (WMAN). Безпроводові міські мережі (WMAN) є третьою групою безпроводових мереж у мережі. WMAN базуються на стандарті IEEE 802.16, який часто називають WiMAX (Всесвітня сумісність для мікрохвильового доступу). WiMAX – це комунікаційна технологія, яка підтримує

багатоточкову архітектуру, спрямовану на надання високошвидкісної безпроводової передачі даних через міські мережі [12]. Це дає змогу з’єднувати менші безпроводові локальні мережі за допомогою WiMAX, створюючи велику WMAN. Таким чином, мережа між містами може бути досягнута без необхідності дорогої прокладки кабелів.

WiMAX схожий на Wi-Fi, але забезпечує покриття на більшій відстані. Поки Wi-Fi призначений для забезпечення покриття відносно невеликих територій, наприклад, в офісах або гарячих точках, WiMAX працює на двох частотних діапазонах, суміші ліцензованих і неліцензований діапазон, від 2 ГГц до 11 ГГц і від 10 ГГц до 66 ГГц, і може передавати близько 70 Мбіт/с на відстань 50 км тисячам користувачів через одну базову станцію, як показано на рисунку 1.6. Оскільки він може працювати на двох частотах смуги WiMAX, то може працювати як у зоні прямої видимості, так і поза межами прямої видимості. На частоті від 2 до 11 ГГц діапазон частот, він працює поза зоною прямої видимості, коли комп’ютер знаходиться всередині будівлі зв'язується з вежею/антеною поза будівлею. Коротка частота передачі нелегко порушити через фізичні перешкоди. Вища частота передачі використовується для обслуговування прямої видимості. Це дає змогу використовувати вежі/антени і спілкуватися один з одним на більшій відстані [7].

Рис.1.6. Схема мережі WiMaX

Безпроводова глобальна мережа (WWAN). Безпроводові глобальні мережі простягаються понад 50 кілометрів і зазвичай використовують ліцензовані частоти. Ці типи мереж можна підтримувати на великих територіях, таких як міста чи країни, за допомогою кількох супутникових систем або антен за допомогою постачальника послуг Інтернету. В основному доступні дві технології: Цифрова стільникова телефонія та супутники.

• **Мережі стільникового зв'язку.** У системі стільникового зв'язку зона покриття розділена на стільники. Стільниковий передавач, при центральній комірки, призначений для обслуговування окремої комірки. Всі передавачі є підключені до базової станції, а останні – до мобільного зв’язку комутатора, який з'єднує стільникову та проводову телефонну мережу [13]. Система намагається ефективно використовувати доступні канали за допомогою низької потужності передавачів, щоб дозволити повторне використання частоти на набагато менших відстанях.

Різні покоління клітин були розроблені з початку 1980-х років. Перше покоління, 1G, був аналоговим і розробленим виключно для голосових дзвінків і майже не враховує послуги передачі даних, зі швидкістю до 2,4 кбіт/с. Друге покоління, 2G, базувалося на цифрових технологіях та мережевій інфраструктурі (GSM), із можливістю текстових повідомлень і швидкістю передачі даних до 64 Кбіт/с. 2,5G покоління було між другим і третім. Іноді його називають 2G + GPRS, це розширена версія 2G, зі швидкістю до 144 Кбіт/с. Покоління 3G було представлено в 2000 році зі швидкістю передачі даних до 2 Мбіт/с. Швидкість 3.5G – це вдосконалена версія 3G, яка використовує HSDPA для прискорення передачі даних до 14 Мбіт/с. Нарешті, четверте покоління, 4G, здатне забезпечити до 1 Гбіт/с швидкості і будь-який вид обслуговування у будь-який час відповідно до вимог користувача, будь-де [7].

• **Супутник.** Безпроводовий зв'язок також можна розвивати через супутник. Завдяки своїй високій швидкості на висоті, супутникові передачі можуть охоплювати

широку територію над поверхнею землі. Це може бути дуже корисним для користувачів, які знаходяться у віддалених районах або на островах, де підводні кабелі не працюють. У цих випадках потрібні супутникові телефони.

Кожен супутник оснащений різними транспондерами, що складаються з трансивера та антени. Вхідний сигнал посилюється, а потім ретранслюється на іншій частоті [4].

Рис.1.7. Супутникові та стільникові мережі.

1.2 Архітектура мережі

Терміни та термінологія. У цьому підрозділі наведено визначення різних термінів, які використовуються в безпроводовій мережі архітектури. Однак не всі записи загальної архітектури існують у всіх технологіях та точні функції можуть відрізнятися.

Логічна архітектура 802.11 містить кілька основних компонентів: станція (STA), безпроводова точка доступу (AP), незалежний базовий набір послуг (IBSS), базовий набір послуг (BSS), система розподілу (DS) і розширений набір послуг (ESS). Деякі з компонентів логічної архітектури 802.11 відображаються безпосередньо на апаратних

пристроях, такі як STA та безпроводові точки доступу. Безпроводовий STA містить карту адаптера, ПК картку або вбудований пристрій для забезпечення безпроводового підключення. Безпроводова точка доступу функціонує як міст між безпроводовими STA та існуючою магістралью мережі для доступу до мережі [8].

Станцією (STA) може бути ПК, ноутбук, КПК, телефон або будь-який інший пристрій здатність втручатися в безпроводове середовище.

Точка доступу (AP), яку іноді називають базовою станцією (BS) — це пристрій, який дозволяє безпроводовим пристроям підключення до проводової мережі за допомогою Wi-Fi або відповідних стандартів.

Базовий набір послуг (BSS) складається з точки доступу та всіх пов’язаних з нею точок доступу ДПА. AP діє як головний для керування STA у цьому BSS. Найпростіший BSS складається з одного AP і одного STA [10].

Розширений набір послуг (ESS) — це набір однієї або кількох взаємопов’язаних базових послуг набору (BSS), які відображаються як єдиний BSS на рівні керування логічним з’єднанням, де у будь-який час, станція, пов’язана з однією з цих BSS.

Коли всі станції в BSS є мобільними станціями і немає з’єднання для проводової мережі BSS, вона називається незалежною BSS (IBSS). IBSS є спеціальна мережа, яка не містить точок доступу, що означає, що вони не можуть підключитися до неї у будь-який інший базовий набір послуг.

Система розподілу (DS) — це механізм, за допомогою якого точки доступу обмінюються кадрами один з одним і проводовими мережами, якщо такі є. DS не обов'язково є мережею, і стандарт IEEE 802.11 не визначає жодної конкретної технології для DS [9]. Майже в усіх комерційних продуктах проводовий Ethernet використовується як магістральна мережа технології.

Рис.1.8. Незалежні та інфраструктурні базові набори послуг (BSS)

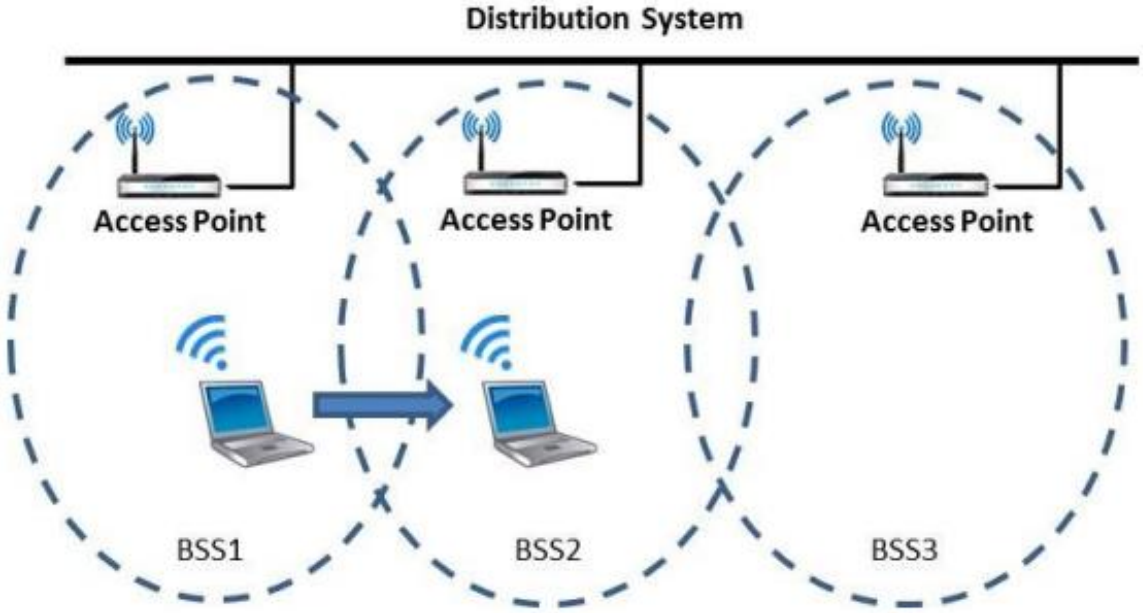

Рис. 1.9. Підтримка мобільності з розширеним набором послуг (ESS)

Архітектури. У безпроводових мережах є два режими налаштування безпроводової архітектури, ad hoc та інфраструктури. У спеціальному режимі, пристрої передають безпосередньо однорангові пристрої, а в інфраструктурному режимі, пристрої спілкуються через точку доступу, яка служить мостом до інших мереж.

Режим ad hoc. У режимі ad hoc усі пристрої в безпроводовій мережі підключаються безпосередньо для спілкування один з одним у режимі однорангового

зв’язку (точка-точка). Мережа не має структури або фіксованих точок. Для цього не потрібна точка доступу та зв'язок між пристроями.

Режим ad hoc найбільше підходить для невеликої групи пристроїв і всі ці пристрої повинні бути фізично присутні в безпосередній близькості один від одного. При виконанні мережа страждає, коли кількість пристроїв зростає. Відключення випадкових пристроїв може часто виникати, а також режим ad hoc може бути важкою роботою для мережі адміністратора для керування мережею [7]. Спеціальний режим має ще одне обмеження: мережі в режимі ad hoc не можуть з'єднуватися з проводовою локальною мережею, а також не можуть отримати доступ до інтернету без встановлення спеціальних шлюзів.

Однак режим ad hoc чудово працює в невеликому середовищі та забезпечує найпростіший режим і найменш дорогий спосіб налаштувати безпроводову мережу.

Режим інфраструктури. Інша архітектура безпроводової мережі — це режим інфраструктури. Всі прилади є підключеними до безпроводової мережі за допомогою точки доступу (AP). Безпроводова точка доступу - це зазвичай маршрутизатори або комутатори, які перетворюють радіохвильові дані в проводові Ethernet, діючи як міст між проводовою локальною мережею та безпроводовими користувачами.

Підключення кількох точок доступу через проводову магістраль Ethernet, може ще більше розширитися покриття безпроводової мережі, як мобільний пристрій виходить із зони дії однієї точки доступу і переходить в зону дії іншої. Як результат, безпроводові клієнти можуть вільно переміщатися з одного домену точки доступу в інший і залишати безперебійним підключення до мережі.

Інфраструктурний режим забезпечує покращену безпеку, зручність керування та набагато більше масштабованості та стабільності. Однак інфраструктурний режим несе доплату витрати на розгортання точок доступу, таких як маршрутизатори або комутатори.

Розширений ідентифікатор набору послуг (ESSID). Розширена ідентифікація набору послуг (ESSID) є одним із двох типів набору послуг ідентифікації (SSID). У

тимчасовій безпроводовій мережі без точок доступу, де використовується базова ідентифікація набору послуг (BSSID). В безпроводовій інфраструктурі мережі, яка включає точку доступу, використовується ESSID, але все одно може використовуватися посилання як SSID.

Ідентифікатор набору послуг (SSID) — це буквено-цифровий ключ із 32 символами (максимум) для визначення назви безпроводової локальної мережі.

Деякі постачальники називають SSID назвою мережі. Для безпроводових пристроїв у мережі, щоб спілкуватися один з одним, усі пристрої повинні бути налаштовані за допомогою того самого SSID.

Стандарт IEEE 802.11. IEEE 802.11 — це набір засобів керування доступом до середовища (MAC) і фізичного рівня (PHY). специфікації для впровадження безпроводових локальних мереж у версіях 2.4, 5 і 60 діапазону частот ГГц.

Вони створені та підтримуються робочою групою IEEE 802.11 [10]. Основна версія стандарту була випущена в 1997 році і мала наступні зміни. Стандарт і поправки є основою для безпроводових мережевих продуктів за допомогою бренду Wi-Fi.

Протокол 802.11. Комітет стандартів IEEE 802 визначає два окремі рівні — логічний зв’язок керування (LLC) і керування доступом до середовища (MAC) для канального рівня OSI еталонної моделі. Безпроводовий стандарт IEEE 802.11 визначає характеристики для фізичного рівня і рівня керування доступом до медіа (MAC), який здійснює зв’язок до рівня LLC, як показано на рисунку 1.10.

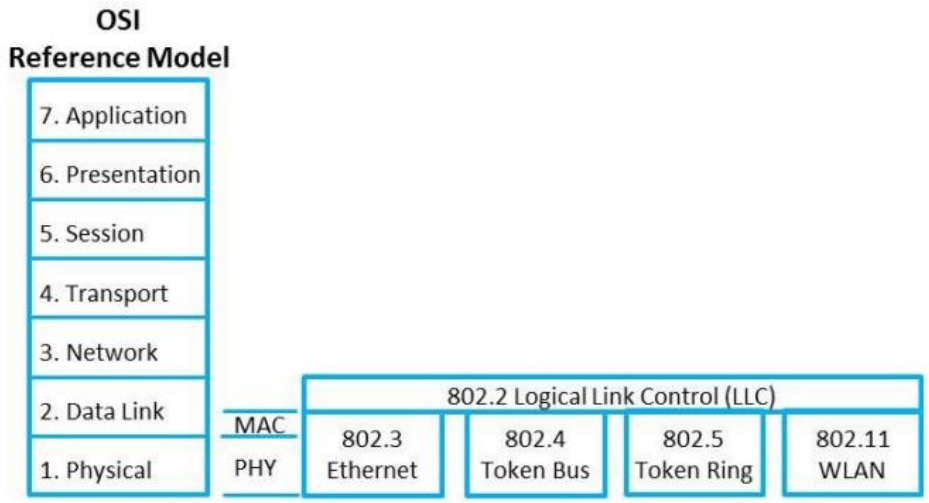

Рис. 1.10. Класифікація стандарту IEEE 802.11 з еталонною моделлю OSI

Усі компоненти архітектури 802.11 належать або до медіа-доступу підрівня управління (MAC) канального рівня або фізичного рівня (PHY) [2].

802.11 MAC Frame. Стандарт IEEE 802.11 MAC Frame, як показано на рисунку 1.11, складається з MAC заголовок, тіло кадру та послідовність перевірки кадру (FCS). Формат кадру MAC містить набір із дев'яти полів, які з'являються у фіксованому порядку в усіх кадрах.

Поле керування кадром. Поле керування кадром (рис. 1.11) містить керуючу інформацію, яка використовується для визначення типу кадру MAC 802.11 і надання інформації, необхідної для наступного поля, щоб зрозуміти, як обробляти кадр MAC.

Нижче наведено опис кожного підполя/поля керування кадрами:

• Protocol Version надає поточну версію використовуваного протоколу 802.11. Одержувачі STA використовують це значення для визначення версії протоколу отриманого кадру, який підтримується.

• Type and Subtype визначають функцію кадру. Є три поля різних типів фрейму: контроль, дані та керування. Є кілька полів підтипу для кожного типу кадру. Кожен підтип визначає специфіку функцій для виконання пов'язаного типу кадру [8].

• To DS and From DS вказує, чи йде кадр або виходить з нього DS (розподілена система) і використовується лише у кадрах типу даних STA пов'язаного з AP.

• More Fragments вказує, чи є більше фрагментів кадру, даних або тип управління, якого слід дотримуватися.

• Retry вказує, чи є кадр для даних або керування типів, який ретранслюється.

• Power Management вказує, чи перебуває STA, що надсилає, в активному режимі або у режимі енергозбереження.

• More Data вказує STA в режимі енергозбереження, що точка доступу має наіслати більше кадрів [5]. Він також використовується для точок доступу для позначення додаткової широкомовної/багатоадресної передачі кадрів для слідкування.

• WEP вказує, чи використовується шифрування та автентифікація в рамках. Його можна встановити для всіх кадрів даних і кадрів керування, які мають підтип встановлених на автентифікацію.

• Order вказує на те, що всі отримані кадри даних мають бути оброблені по порядку.

Тривалість/Поле ID. Це поле використовується для всіх кадрів типу керування, крім підтипу Power Save (PS), опитування, щоб вказати тривалість, що залишилася, необхідну для отримання наступного кадру способу передавання. Якщо підтипом є PS Poll, поле містить асоціацію ідентифікатора (AID) передавального STA.

Адресні поля. Залежно від типу фрейму, чотири поля адреси міститимуть комбінацію таких типів адрес:

• Ідентифікатор BSS (BSSID) унікально ідентифікує кожну BSS. Коли кадр від STA в інфраструктурі BSS, BSSID — це MAC-адреса точки доступу. Коли кадр походить від STA в IBSS, BSSID є випадковим згенерованим локально адміністрованим MAC-адресом STA, який ініціювала IBSS [6].

• Адреса призначення (DA) вказує MAC-адресу кінцевого пункту призначення для отримання рами.

• Адреса джерела (SA) вказує на MAC-адресу вихідного джерела, яке спочатку створено і передано кадру.

• Адреса отримувача (RA) вказує на MAC-адресу наступного безпосереднього STA на безпроводовому носії для отримання кадру.

• Адреса передавача (TA) вказує на MAC-адресу STA, який передав кадр на безпроводове середовище [10].

Контроль послідовності. Поле керування послідовністю містить два підполя: поле «Номер фрагмента» та поле «Порядковий номер», як показано на рис. 1.11.

Опис кожного підполя/поля керування послідовністю виглядає наступним чином:

• Порядковий номер вказує на порядковий номер кожного кадру. В послідовності, номер однаковий для кожного кадру, надісланого для фрагментованого кадру; інакше, число збільшується на одиницю до досягнення 4095, після чого починається з нуля знову.

• Номер фрагмента вказує номер кожного кадру, надісланого фрагментованою рамкою. Початкове значення встановлюється на 0, а потім збільшується на одиницю для кожного наступного кадру, надісланого із фрагментованого кадру.

Тіло фрейму. Тіло фрейму містить дані або інформацію, включену до будь-якого керування типом або кадри типу даних.

Послідовність перевірки кадрів. STA, що передає, використовує перевірку циклічної надлишковості (CRC) для всіх полів заголовок MAC і поле тіла кадру для генерації значення FCS [7]. Отримаючи потім, STA використовує те саме обчислення CRC для визначення власного значення FCS поля, щоб перевірити, чи виникли помилки у кадрі під час способу передавання.

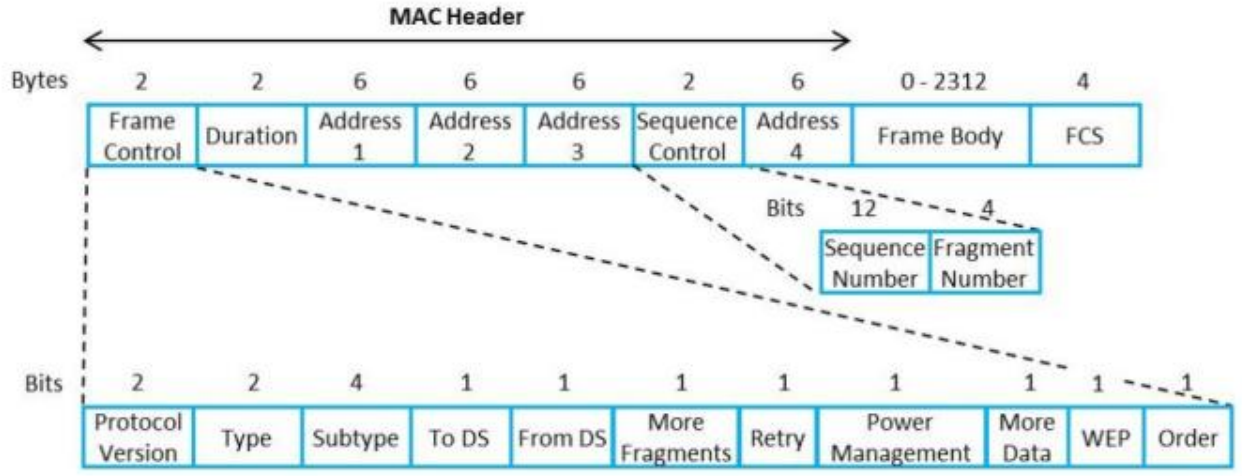

Рис. 1.11. Поля керування кадрами та керування послідовністю у форматі кадру MAC 802.11

Підрівень 802.11 PHY. На фізичному (PHY) підрівні IEEE 802.11 визначає ряд кодувань і схеми передачі безпроводового зв'язку, найпоширенішими з яких є спектр розширення частоти (FHSS), розширення прямої послідовності спектру (DSSS) і ортогональне частотне мультиплексування (OFDM) схеми передачі. На рисунку 1.12 показано 802.11, 802.11b, 802.11a, 802.11g, Стандарти 802.11n і 802.11ac, які існують на підрівні PHY. Ці стандарти описані в наступних розділах [2].

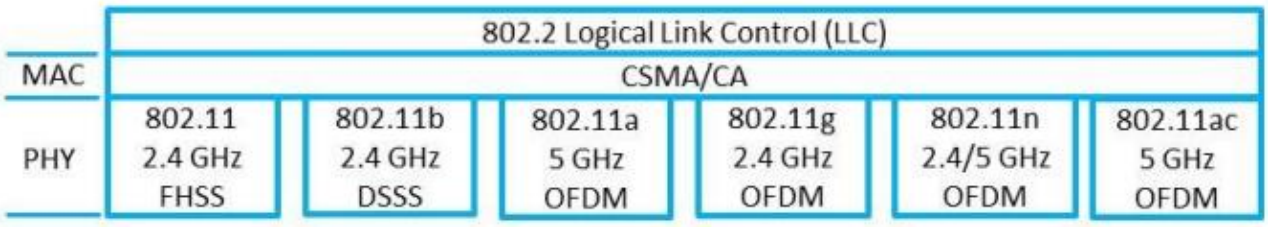

Рис. 1.12. Схема стандартів IEEE 802.11 показані у відповідних розділах

IEEE 802.11. Швидкість передачі даних для оригінального стандарту IEEE 802.11 становить 2 Мбіт/с із використанням FHSS схеми передачі та смуги частот ISM, яка працює в частоті діапазон від 2,4 до 2,5 ГГц. Однак, за не ідеальних умов, низька швидкість передачі даних використовується зі швидкістю 1 Мбіт/с.

802.11b. Основним удосконаленням IEEE 802.11 завдяки IEEE 802.11b є стандартизація фізичного рівня для підтримки вищих бітрейтів. IEEE 802.11b підтримує дві додаткові швидкості, 5,5 Мбіт/с і 11 Мбіт/с, використовуючи діапазон частот 2,4 ГГц. DSSS схема передачі використовується для забезпечення вищої швидкості передачі даних. Бітрейт 11 Мбіт/с досяжна в ідеальних умовах. Чим менше ідеальних умов, тим повільніше використовуються швидкості 5,5 Мбіт/с, 2 Мбіт/с і 1 Мбіт/с.

Важливо відзначити, що 802.11b використовує ту саму смугу частот, яку використовує мікрохвильові печі, безпроводові телефони, радіоняні, безпроводові відеокамери, пристрої Bluetooth тощо.

802.11a. IEEE 802.11a працює зі швидкістю передачі даних до 54 Мбіт/с і використовує частоту 5 ГГц у діапазоні частот. Замість DSSS, 802.11a використовує OFDM, що дозволяє передавати дані підчастотами паралельно і забезпечує більшу стійкість до перешкод більшої пропускної здатності. Ця високошвидкісна технологія забезпечує безпроводовий зв'язок локальної мережі для кращої роботи програм, для відео та конференцій.

Оскільки вони не працюють на тих самих частотах, що й інші пристрої (наприклад, безпроводові телефони, які працюють у діапазоні частот 2,4 ГГц), OFDM та IEEE 802.11a забезпечують як вищу швидкість передачі даних, так і чистіший сигнал. Бітрейт становить швидкість 54 Мбіт/с, яка досяжна в ідеальних умовах. У не ідеальних умовах, повільніші швидкості використовують 48 Мбіт/с, 36 Мбіт/с, 24 Мбіт/с, 18 Мбіт/с, 12 Мбіт/с і 6 Мбіт/с.

802.11g. IEEE 802.11g працює на швидкості до 54 Мбіт/с, але використовує частоту 2,4 ГГц для діапазону частот і OFDM. 802.11g також зворотно сумісний з 802.11b і може працювати на бітрейті 802.11b і використовувати DSSS. Безпроводова мережа 802.11g, адаптери можуть підключатися до безпроводової точки доступу 802.11b і безпроводової мережі 802.11b, де адаптери можуть підключатися до безпроводової точки доступу 802.11g. Таким чином, 802.11g забезпечує шлях міграції

для мереж 802.11b до стандартної технології, сумісної з частотою з вищим бітрейтом. Існуючі адаптери безпроводової мережі 802.11b не можуть бути оновлено до 802.11g шляхом оновлення мікропрограми адаптера, їх необхідно замінити. На відміну від переходу з 802.11b на 802.11a (у якому всі мережеві адаптери в і безпроводові клієнти, і безпроводові точки доступу повинні бути замінені одночасно), перехід із 802.11b на 802.11g можна здійснювати поступово.

Як і 802.11a, 802.11g використовує 54 Мбіт/с в ідеальних умовах і меншу швидкість 48 Мбіт/с, 36 Мбіт/с, 24 Мбіт/с, 18 Мбіт/с, 12 Мбіт/с і 6 Мбіт/с менше, ніж ідеальні умови.

802.11n. Стандарт IEEE 802.11n спрямований на покращення відстані (до 250 м) і мережі пропускної здатності, порівняно з двома попередніми стандартами, 802.11a та 802.11g, зі значним збільшенням максимальної швидкості необроблених даних з 54 Мбіт/с до 600 Мбіт/с в ідеалі умов, додавши технологію з декількома входами та декількома вихідними каналами 40 МГц, більшої смуги пропускання. Ця технологія, яка називається MIMO, використовує декілька безпроводових сигналів і антен, на передавач і приймач. Його можна використовувати в діапазоні частот 2,4 ГГц або 5 ГГц.

802.11ac. Стандарт 802.11ac, оновлення 802.11n, забезпечує аналогічний діапазон, але збільшує пропускну здатність. Він працює в діапазоні 5 ГГц і включає формування променя, широкі діапазони частот і кілька антен для передачі теоретичних даних зі швидкістю до 1,3 Гбіт/с, більш ніж подвоєна пікова швидкість 600 Мбіт/с з 802.11n [9].

1.3 Безпека безпроводових мереж

Безпроводові мережі зазвичай не такі безпечні, як проводові. Проводові мережі, на самому базовому рівні надсилають дані між двома точками, A і B, які є підключені мережевим кабелем. Однак, безпроводові мережі передають дані в кожному напрямку

до кожного пристрою, який прослуховує, в межах обмеженого діапазону. Проводову мережу можна захистити на її краях, наприклад, обмеживши фізичний доступ і встановлення брандмауерів. Безпроводова мережа з такими ж заходами все ще вразлива для прослуховування. Тому безпроводові мережі вимагають більше цілеспрямованих зусиль для підтримки безпеки.

Безпечний зв'язок. Безпеку зв’язку часто описують у термінах трьох елементів: Автентифікація, конфіденційність і цілісність.

Автентифікація гарантує, що вузли є тими, ким вони себе видають. Автентифікація зазвичай базується на демонстрації знання загального секрету, наприклад ім’я користувача та пароль. У більш складних системах володіння, спільний секрет можна продемонструвати шляхом підтвердження володіння маркером, який є більшим та важко вкрасти, або підробити, як-от сертифікат або смарт-картка.

Конфіденційність гарантує, що перехоплювачі не зможуть прочитати мережевий трафік.

Конфіденційність зазвичай захищається шифруванням вмісту повідомлення. Шифрування застосовує відомий оборотний метод перетворення (званим шифром або алгоритмом шифрування) до вихідного вмісту повідомлення (званого відкритим текстом), їх кодування або маскування для створення зашифрованого тексту. Тільки ті, хто вміють, можуть повернути процес (розшифрувати повідомлення), тим самим відновити вихідний текст. Найбільш поширеними формами шифрування є математичні перетворення, які використовують змінну, яка називається ключем, як частина їх маніпуляцій. Призначений отримувач повинен знати як правильний метод, так і значення використовуваного ключа, щоб мати можливість розшифрувати повідомлення. Для комерційних схем шифрування, метод буде загальновідомим. Захист секретності ключа стає вирішальним.

Цілісність гарантує доставку повідомлень без змін. У контексті безпеки комунікацій це стосується здатності переконатися що отримане повідомлення не було

жодним чином змінено та є ідентичним повідомлення, яке було надіслано. Одним із прикладів є байти послідовності перевірки кадрів (FCS), перевірки цілісності, але вони не вважаються безпечними. Звичайні байти FCS не обчислюються над текстовим повідомленням і захищені шифруванням. Натомість вони обчислюються над зашифрованим текстом за допомогою відомого методу та надсилаються у відкритому вигляді (не зашифровано). Байти FCS допомагають ідентифікувати випадково отримані пакети, які пошкоджено під час транспортування.

Поняття цілісності іноді розширюють, включаючи перевірку джерела повідомлення, де збігається із зазначеним джерелом. Мітки часу та послідовність повідомлень числа можуть захистити від «атак повторів», але, знову ж таки, вони не враховуються безпечними, якщо вони не захищені шифруванням.

Безпека завжди відносна. Для кожного захисту є (або скоро буде) успішна атака. Для кожної атаки є (або скоро буде) успішний захист. Справді лише час і зусилля. Чим краще захист, тим більше час і зусилля, необхідні для порушення.

Правильний захист – це той, який є збалансованим і відповідає очікуваному діапазону нападу. Баланс важливий у двох сенсах. По-перше, найслабша ланка має бути безпечною достатньо. По-друге, пасивні елементи автентифікації, шифрування та цілісності, де перевірка повинна бути підкріплена активними елементами, такими як моніторинг і переслідування спроби порушень, дотримання дисципліни безпеки тощо. Правильний захист це той, у якому зловмисники потребують трохи більше часу та зусиль ніж вони готові інвестувати. Заходи безпеки накладають витрати та обмеження захисникам. Як і будь-яке інше бізнес-рішення, ці компроміси необхідно прийняти з відкритими очима.

Конфіденційність і шифрування. Досягається конфіденційність (запобігання несанкціонованому доступу до вмісту повідомлення) шляхом захисту вмісту даних за допомогою шифрування. Шифрування є необов’язковим у WLAN, але без нього будь-який аналогічний пристрій, сумісний із стандартами, у межах досяжності може читати весь мережевий трафік.

Існують три основні покоління підходів до безпеки для WLAN. Оскільки наприкінці 1990-х років алгоритми безпеки Wi-Fi зазнали багатьох оновлень, повне знецінення старих алгоритмів і значний перегляд новіших алгоритмів, у хронологічному порядку має таке представлення:

• WEP (Wired Equivalent Privacy)

• WPA (захищений доступ Wi-Fi)

• WPA2 (захищений доступ Wi-Fi, версія 2)

WEP. WEP було ратифіковано як стандарт безпеки Wi-Fi у вересні 1999 року. Перші версії WEP не були особливо надійними, навіть на той час, коли вони були випущені, оскільки обмеження США на експорт різних криптографічних технологій призвели до обмеження виробниками своїх пристроїв лише 64-бітним шифруванням. Коли обмеження були зняті, її було збільшено до 128-біт. Незважаючи на введення 256-бітове шифрування WEP, 128-бітне залишається одним із найпоширеніших реалізацій.

Незважаючи на зміни в алгоритмі та збільшений розмір ключа, з часом численні недоліки безпеки були виявлені в стандарті WEP і, як обчислювальна потужність зростали, експлуатувати їх ставало легше й легше. Ще в 2001 році з'явилися експерименти з підтвердженням концепції, а в 2005 році ФБР оприлюднило демонстрацію (з метою підвищення обізнаності про слабкі місця WEP), де вони зламали паролі WEP за лічені хвилини за допомогою безкоштовного доступного програмного забезпечення.

Незважаючи на різні вдосконалення, обхідні шляхи та інші спроби підкріпити систему WEP залишається дуже вразливою, а системи, які покладаються на WEP, повинні бути такими оновленими або, якщо оновлення безпеки не є варіантом заміни. Альянс Wi-Fi офіційно припинив роботу WEP у 2004 році .

WPA. Щоб усунути вразливості в WEP, торгова група Wi-Fi Alliance створила WPA на початку 2003 р. Найбільш поширеною конфігурацією WPA є WPA-PSK (PreShared Key). Ключі, які використовуються WPA, є 256-бітними, що значно

перевищує 64-бітні ключі. бітові та 128-бітні ключі, що використовуються в системі WEP.

Деякі зі значних змін, реалізованих за допомогою WPA, містять повідомлення перевірки цілісності (щоб визначити, чи зловмисник перехопив або змінив передані пакети між точкою доступу та клієнтом) і протокол цілісності тимчасового ключа (TKIP). TKIP використовує систему ключів для кожного пакету, яка була значно безпечнішою, ніж фіксований ключ, який використовується в системі WEP. Пізніше TKIP був замінений просунутим стандартом шифрування (AES).

Незважаючи на те, що WPA значно покращив WEP, привид WEP переслідуваний WPA. TKIP, основний компонент WPA, був розроблений для легкого згортання через оновлення мікропрограми на існуючі пристрої з підтримкою WEP. Таким чином, це повинно було переробляти певні елементи, що використовуються в системі WEP, які, зрештою, також були експлуатовані.

WPA, як і його попередник WEP, був продемонстрований через перевірку концепції та використовував публічні демонстрації, щоб бути вразливим до вторгнення. Цікаво, що процес, за допомогою якого зазвичай порушується WPA, не є прямою атакою на WPA алгоритм (хоча такі атаки були успішно продемонстровані), але за допомогою атаки на додаткову систему, яка була розгорнута з WPA, Wi-Fi Protected Settings (WPS), призначене для легкого підключення пристроїв до сучасних точок доступу.

WPA2. З 2006 року WPA офіційно замінено WPA2. Один з найбільш значними змінами між WPA і WPA2 стало обов'язкове використання AES алгоритмів і впровадження CCMP (Режим шифрування лічильника з блокуванням Chaining Message Authentication Code Protocol) як заміна TKIP (все ще збережено в WPA2 як резервну систему та для взаємодії з WPA).

Наразі основною вразливістю системи безпеки WPA2 невідома (і вимагає, щоб зловмисник уже мав доступ до захищеної мережі Wi-Fi мережі, щоб отримати доступ до певних ключів, а потім увічнити атаку на інші пристрої в мережі).

Таким чином, наслідки безпеки відомих вразливостей WPA2 майже повністю обмежені мережами корпоративного рівня та майже не заслуговують практичного розгляду щодо безпеки домашньої мережі.

На жаль, та сама вразливість, яка є найбільшою дірою в броні WPA, вектор атаки через Wi-Fi Protected Setup (WPS), залишається в сучасних WPA2 - здатні точки доступу. Хоча проникнення в захищену мережу WPA/WPA2 із використанням цієї вразливості, вимагає від 2 до 14 годин тривалих зусиль сучасного комп'ютера, що все ще є законною проблемою безпеки, і WPS має бути вимкнено (і, якщо можливо, прошивку точки доступу слід перепрошити на дистрибутив, який навіть не підтримує WPS, тому вектор атаки повністю видалено) [9].

Нижче наведено базовий список упорядкованих поточних методів безпеки Wi-Fi від найкращого до гіршого:

1. WPA2 + AES
2. WPA + AES
3. WPA + TKIP/AES (TKIP існує як резервний метод)
4. WPA+ TKIP
5. WEP
6. Відкрита мережа (без безпеки взагалі)

В ідеалі Wi-Fi Protected Setup (WPS) буде вимкнено, а рівень безпеки встановлено WPA2 + AES. Усе інше в списку є не ідеальним кроком нижче [2].

1.4 Переваги та недоліки

Безпроводові мережі мають низку ключових переваг перед проводовими мережами, наприклад мобільність, економічність і адаптивність, але є й деякі недоліки, наприклад безпека. Нижче наведено основні переваги та недоліки безпроводової мережі проти проводової мережі.

У наведеному нижче списку підсумовано деякі переваги безпроводових мереж:

Підвищена ефективність. Покращений обмін даними забезпечує швидшу передачу інформації всередині підприємствами, а також між партнерами та клієнтами. Наприклад, продавці можуть дистанційно перевіряйте рівень запасів і ціни під час телефонних розмов.

Краще покриття та мобільність. Проводи прив’язують вас до одного місця. Перехід на безпроводовий зв’язок означає, що було досягнуто свободу змінити своє місцезнаходження, не втрачаючи з’єднання, без необхідності додаткового кабелю або адаптера для доступу до офісних мереж.

Гнучкість. Офісні безпроводові працівники можуть об’єднуватися в мережу, не сидячи за спеціальним місцем комп’ютера та можуть продовжувати продуктивну роботу, перебуваючи поза офісом. Це може призвести до нових стилів роботи, таких як робота вдома або прямий доступ до корпоративних даних під час перебування на сайтах клієнтів.

Економія коштів. Безпроводові мережі можуть бути легшими та дешевшими для встановлення, особливо в будівлях, які є пам’ятками архітектури або де орендодавець не дозволить установку кабелів. Відсутність проводів і кабелі знижують вартість. Це досягається поєднанням факторів відносно до низької вартості безпроводових маршрутизаторів, відсутність необхідності риття траншей, буріння та подачі проводу всередині стін або інші методи, які можуть знадобитися для фізичного з'єднання. Крім того, не потрібно обслуговування проводів.

Адаптивність. Швидка та проста інтеграція пристроїв у мережу та висока гнучкість зміни установки. Нові можливості/додатки, безпроводова мережа може дозволити вам пропонувати нові продукти або послуги. Наприклад, багато залів очікування вильоту в аеропорту, вокзали, готелі, кафе та інші ресторани встановили послуги безпроводової мережі в гарячих точках для забезпечення мобільного зв’язку користувачам для підключення свого обладнання до домашнього офісу під час подорожі.

Існують також певні недоліки, пов'язані з використанням безпроводових мереж.

Безпека. Тому безпроводова передача більш вразлива для атак неавторизованих користувачів, де особливу увагу слід приділити безпеці.

Проблеми з установкою. Можна відчути перешкоди, якщо інші в тій самій будівлі також використовують безпроводовий зв’язок технології або за наявності інших джерел радіосигналів. Це може призвести до поганого зв’язку, або у крайніх випадках, втрата безпроводового зв’язку взагалі.

Покриття. У деяких будівлях отримати рівномірне покриття може бути важко, що призводить до появи чорних плям, де немає сигналу. Наприклад, в конструкціях, побудованих із застосуванням сталевої арматури матеріалів, вам може бути важко підібрати використовувані радіочастоти.

Швидкості передачі. Безпроводова передача може бути повільнішою та менш ефективною, ніж проводова мережа. У більших безпроводових мережах, саме магістральна, як правило, проводова та безпроводова [9].

1.5 Додатки

Безпроводовий зв'язок у вбудованих системах продовжує зростати. Forrester Research, компанія, яка зосереджується на бізнес-наслідках зміни технологій, повідомляє, що за кілька коротких років використовувалося до 95% пристроїв для доступу до Інтернету, а також є пристрої, відмінні від ПК, які використовують вбудовану систему.

Існує багато додатків для вбудованих пристроїв з інтерфейсом Wi-Fi:

• Застосування для промислових процесів та керування, де є також дорогі або незручні проводові з’єднання, на прикладі візьмемо машини, що постійно рухаються.

• Екстрені програми, які вимагають негайного та тимчасового налаштування, наприклад ситуації на полі бою чи стихійні лиха.

• Мобільні програми, такі як відстеження активів.

• Камери спостереження (можливо, ви не хочете, щоб їх було легко помітити, але кабелі важко приховати).

• Вертикальні ринки, такі як медицина, освіта та виробництво.

• Зв'язок з іншими пристроями Wi-Fi, такими як ноутбук або КПК.

• Додатки від машини до машини (M2M).

Посилаючись на останній пункт, до нього відноситься термін «машина до машини» (M2M), технології яких дозволяють безпроводовим і проводовим системам спілкуватися з іншими пристроями одного типу. Іншою характеристикою зв’язку M2M є те, що цей взаємозв’язок дозволяє перш за все автоматизований зв'язок між віддаленими машинами та одним, або більше рівнів програм централізованого керування. Він забезпечує роботу в режимі реального часу, а також моніторинг і контроль без необхідності втручання людини.

За даними ABI Research, технологічної дослідницької та консультативної корпорації, більше понад 30 мільярдів пристроїв будуть безпроводово підключені до інтернету речей (Інтернет усього) до 2020 року [9].

У безпроводовому просторі M2M існує два основних класи взаємозв’язків: короткий асортимент і широка площа. Переважаюча широкомасштабна технологія застосовується вбудованою системою стільникових модулів для підключення віддалених пристроїв до інтернету або серверів додатків. Стільниковий модуль містить багато тих самих функцій, які ви знайдете в стільниковому зв’язку телефону, включаючи передачу голосу та даних, і ідеально підходить для вбудованих програм.

Програми M2M можна знайти в багатьох галузях, зокрема: автоматичне зчитування лічильників (AMR), торговельні автомати, торговельні (POS) термінали, транспорт і логістика (управління автопарком), охорона здоров'я, технології безпеки та багато інших програм [10].

Висновки до першого розділу

Проаналізовано безпроводові мережі та безпроводові технології. Були представлені схеми таких безпроводових технологій як Bluetooth, IrDA, ZigBee або UWB з споживанням енергії та низькою швидкістю передачі даних.

Досліджено архітектуру мережі з різними видами 802.11, приладами мобільності, режимами ad hoc, інфраструктури тощо.

Наведено складові безпеки безпроводових мереж, щодо конфіденційності та цілісності. Досліджено історію розвитку безпроводової локальної мережі WiFi.

Представлено переваги та недоліки до безпроводових технологій та мереж, які допоможуть зробити правильний вибір та уникнути їх у тій чи іншій ситуації під час використання.

2 ДОСЛІДЖЕННЯ ПРОДУКТУ CISCO IDENTITY SERVICES ENGINE В ЕФЕКТИВНОСТІ ЗАХИСТУ ДО БЕЗПРОВОДОВИХ МЕРЕЖ

2.1 Визначення продукту Cisco Identity Services Engine

Cisco ISE (Identity Services Engine) — це платформа для політик ідентифікації та контролю доступу, що дозволяє компаніям/організаціям забезпечити відповідність, оптимізувати свої послуги операцій і підвищення безпеки їх інфраструктури. ISE дозволяє збирання інформації в реальному часі від користувачів, пристроїв і мереж. Адміністратор мережі може налаштувати ISE для прийняття проактивних рішень шляхом прив'язки ідентичності до елементів мережі, таких як контролери WLAN, шлюзи VPN, комутатори центрів обробки даних або комутатори доступу. ISE поєднує багато різних функцій в одному пристрої, такі як автентифікація, авторизація та облік (AAA). Він також містить додатки керування гостьовим доступом для адміністратора, моніторинг кінцевих пристроїв і багато інших функцій. Cisco ISE доступний у двох різних форматах: як віртуальна машина або пристрій Cisco SNS. Віртуальна машина зрозуміла сама за себе, маючи будь-які базові знання про віртуальні машини. SNS, з іншого боку, є стійковим сервером, попередньо налаштованим як сервер ISE, який продається від Cisco. Адміністратор може отримати сервер і встановити його на свою серверну стійку та використовувати це, наприклад, для запитів авторизації та автентифікації. Інформація про товар і технічні характеристики продукту для захищеного мережевого сервера Cisco можна знайти на їх веб-сайті. Ціну Cisco ISE неможливо знайти на веб-сайті Cisco. Щоб отримати ціну, людина повинна попросити рахунок-фактуру від Cisco, але оцінки для віртуальної машини в тисячах ліцензій та пристрої SNS близько 10 000 євро.

Cisco ISE має три різні розподілені розгортання для мереж різного розміру. Ці архітектури називаються малими, середніми та великими. Малий ISE складається з

двох Cisco ISE вузлів, в яких один із вузлів ISE функціонує як основний і вторинний пристрій, а інший функціонує як резервний. Головний вузол ISE синхронізовує або реплікує весь його вміст до вторинного вузла. Це тримає їх обох в курсі інформації у випадку, якщо основний вузол ISE втрачає живлення або підключення, то вторинний вузол повинен взяти на себе. Також можливе розділене розгортання, коли навантаження AAA розділене між двома вузлами Cisco ISE для оптимізації робочого процесу AAA. Обидва вузли повинні обробляти повне навантаження запитів AAA у випадку з'єднання або втрати живлення у будь-якому з них, де невелика віртуальна машина ISE вимагає 16 ядер.

ISE — це набагато більше, ніж концепція додаткової безпеки та «інтуїтивної» мережі, але ми дійдемо до цього.

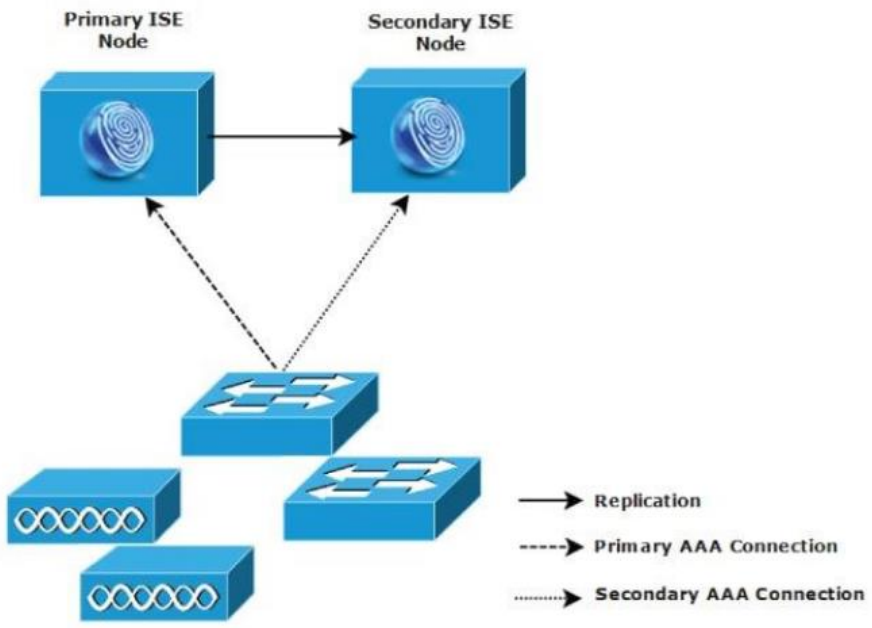

Рис. 2.1 Розгортання малої мережі Identity Services Engine

У розгортанні середнього розміру можна виділити кілька нових вузлів для AAA та продовжувати використовувати старі первинні та вторинні вузли для функцій налаштування та журналювання [2]. У певному сенсі це розділене розгортання, оскільки воно розподіляє навантаження між різними вузлами, але окремий вузол не

обов’язково повинен бути здатний обробляти все робоче навантаження у разі втрати живлення або з’єднання. Потрібна віртуальна машина середнього розміру для розгортання 16 ядер.

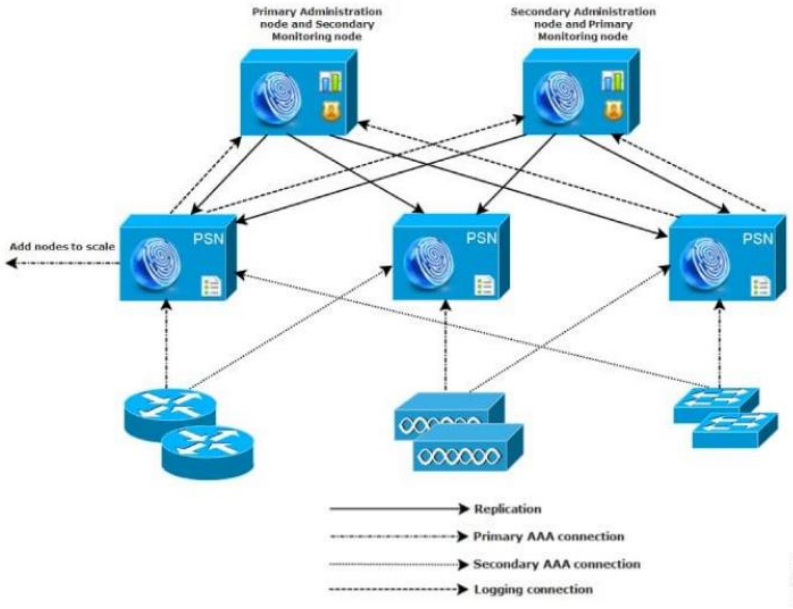

Рис. 2.2 Розгортання середнього розміру віртуальної машини

Розгортання великих мереж не є значно більш особливим, ніж мережі середнього розміру. Потрібен балансувальник навантаження, і він використовує більше вузлів ISE для різних цілей. Великий сервер Cisco ISE вимагає 24 ядер на віртуальній машині. Під час створення Cisco ISE потрібна відповідна ліцензія для сервера. Це може бути маленький, середній або великий.

Простіше кажучи, Cisco ISE дозволяє адміністратору забезпечити високобезпечний доступ до мережі користувачам та іншим пристроям. Це забезпечує легку видимість мережі, тому моніторинг стає більш ефективний. Cisco ISE природно працює з пристроями Cisco, але також підтримує пристрої сторонніх виробників. Деякі пристрої сторонніх виробників підтримують лише проводовий або безпроводовий режим[2].

Функціональні можливості Cisco ISE

- Будучи сервером Radius, Cisco ISE підтримує функції, які підтримують класичні сервери Radius (такі як добре відома Cisco ACS – система контролю доступу). Отже, розгорнувши Cisco ISE, ви можете запустити:
- Механізм 802.1x у мережі Wi-Fi
- Механізм 802.1x у проводовій мережі
- Аутентифікація та налаштування атрибутів для користувачів, підключених через VPN
- MAC Authentication Bypass (MAB), що означає автентифікацію пристрою за допомогою MAC-адрес [13].

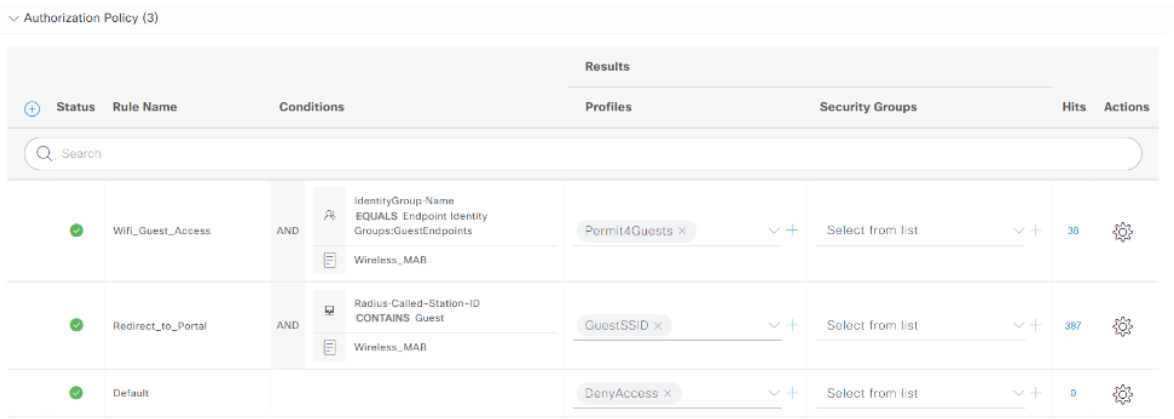

Рис. 2.3. Успіх авторизації користувача через гостьовий акаунт у додатку Cisco ISE

Механізми ISE. Identity Services Engine використовує так звані розширені зв’язки Radius CoA (Change of Authorization), які роблять можливою динамічну взаємодію між вузлом ISE (Policy Service Node) і мережевими пристроями, такими як комутатори, маршрутизатори, мережеві контролери Wi-Fi та брандмауери.

CoA. ISE використовує логічні умови, створені адміністратором, який застосовує певну причинно-наслідкову логіку: ЯКЩО умова, ТО результат . За допомогою комбінацій умов ISE може реагувати на умови, що виникають у мережі, і самостійно спілкуватися з мережевими пристроями, наприклад, надсилаючи їм пакет

CoA з інформацією про встановлення порту на комутаторі в стан вимкнення або перенаправляючи певного користувача із URL Redirect, якщо він не відомий системі.

Далі на прикладі використання такого причинно-наслідкового циклу. Треба взяти пристрій із встановленою MAC-адресою, який намагається підключитися до мережі. По-перше, MAC-адреса перевіряється в базі даних, якщо вона вже зареєстрована. Якщо так, підключення завершено. Якщо такої адреси немає, ISE спускається вниз по драбині правил і перенаправляє користувача на портал реєстрації гостей.

Нижче можна побачити, як це виглядає з точки зору конфігурації.

Рис. 2.4. Пошагові функції для ефективної роботи Cisco ISE

Профілювання. Профілювання або здатність ISE розуміти тип пристрою, браузер, виробника, тип пристрою, як-от телефон чи ноутбук, і ОС, дозволяє реагувати, наприклад, під час передачі пакету з налаштованим запитувачем 802.1x, тобто частиною програмного забезпечення відповідає за підключення клієнтів до захищеної мережі 802.1x для користувача.

За допомогою профілювання Cisco ISE надсилає потрібний пакет на потрібний пристрій, наприклад, інший на MacBook з OSX і інший на пристрій Lenovo з Windows 10 [1].

2.2 Опис базової платформи AAA RADIUS

Не вдаючись у подробиці, будемо використовувати RADIUS як приклад, щоб описати типову архітектуру AAA, таку як ті, що використовуються інтернет-провайдером або провайдером. У цих типах архітектур існує проміжний елемент — сервер доступу до мережі, який працює як клієнт RADIUS. Клієнт несе відповідальність за надсилання інформації користувача на сервери RADIUS і подальші дії відповідно до отриманої відповіді.

Сервери RADIUS отримують запит клієнта та виконують автентифікацію користувача на основі отриманих даних (зазвичай щодо серверів каталогів), повертаючи конфігурацію з необхідною інформацією, щоб клієнт міг отримати доступ до служби автентифікованого користувача. Під час цього процесу автентифікації та авторизації перевіряються дійсність користувача та ресурси, до яких він має авторизований доступ [15]. Ця процедура доповнюється процесом обліку, який реєструє релевантні дані сеансу та який зазвичай використовується для створення реєстрацій встановлення ставок.

Автентифікація та авторизація. Користувач, який запитує доступ, робить запит, надсилаючи свою інформацію користувача та пароль до NAS, який він встановлює на рівні зв’язку точка-точка (PPP). NAS, який діє як клієнт RADIUS, повторно надсилає запит на сервер RADIUS. Цей запит включає інформацію кінцевого користувача разом із його паролем, який зашифровано за допомогою пароля, який надається спільно з сервером (Автентифікатором). Сервер перевіряє автентифікацію за допомогою будь-якого з підтримуваних механізмів: PAP, CHAP, EAP (механізми на основі запиту-відповіді), вхід до Unix, LDAP тощо та отримує відповідну інформацію, пов’язану з клієнтом. Якщо сервер RADIUS авторизується по доступу, він надсилає повідомлення (Access Accept) із серією вкладених параметрів, які характеризують з’єднання, наприклад IP-адресу та пропускну здатність. Якщо доступ відхилено, в автентифікації/авторизації буде

відмовлено, про що користувача буде поінформовано за допомогою повідомлення про відмову в доступі, яке вказує на причини відмови [2].

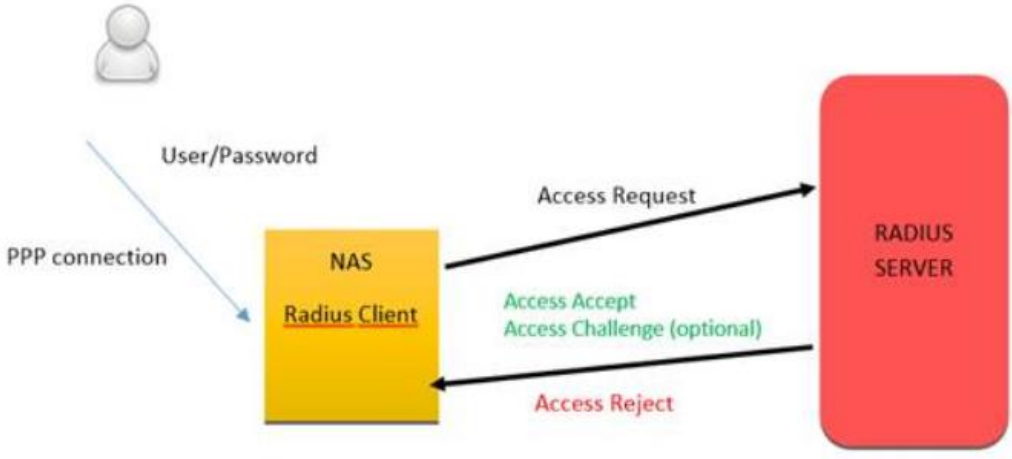

Рис. 2.5. Потік повідомлень у процесі автентифікації/авторизації RADIUS

Найпоширеніші повідомлення RADIUS представлені нижче.

RADIUS має у своєму розпорядженні такі повідомлення для контролю всіх фаз процесу AAA:

Доступ-Запит. Надсилається клієнтом RADIUS для запиту автентифікації та авторизації доступу до мережі.

Доступ-Прийняти. Надсилається сервером RADIUS у відповідь на повідомлення “Access-Request”. Це повідомлення сповіщає клієнта про його автентифікацію та авторизацію, яким він відповідає, надаючи необхідні атрибути.

Доступ-Відмова. Надсилається сервером RADIUS у відповідь на повідомлення “Access-Request”. Це повідомлення інформує клієнта про те, що його запит відхилено, із поясненням причини.

Access-Challenge. Надсилається сервером RADIUS у відповідь на повідомлення “Access-Request”. Це повідомлення надсилається клієнту з викликом, на який клієнт повинен відповісти.

Облік-Запит. Надсилається клієнтом RADIUS, щоб указати інформацію про прийняте з'єднання. Це може бути тип запуску або зупинки, щоб почати або зупинити облік.

Облік-Відповідь. Надсилається сервером RADIUS у відповідь на повідомлення «Accounting-Request». Це повідомлення сповіщає про правильне отримання запиту та запускає процес сесії [2].

2.3 Опис базової платформи AAA TACACS+

TACACS+ — це відкритий стандартний протокол безпеки, який використовується для централізованої перевірки будь-якого користувача, який намагається отримати доступ до маршрутизатора або сервера доступу до мережі. Він був розроблений компанією Cisco для служб автентифікації, авторизації та обліку. TACACS+ означає Terminal Access Controller Access-Control System Plus, але його не слід плутати з TACACS. TACACS був попередником TACACS+, але вони несумісні, і TACACS+ замінив TACACS [2].

ISE підтримує протокол TACACS+ для розширеного контролю та аудиту конфігурацій мережевих пристроїв. Мережний пристрій можна налаштувати для запиту Cisco ISE для автентифікації та авторизації та керування діями адміністратора мережі. Крім того, мережевий пристрій також повідомляє Cisco ISE з інформацією про кожен сеанс і командні операції для процесів обліку та аудиту [14].

Додавання мережевих пристроїв за допомогою TACACS+. Адміністратори ISE можуть додавати мережеві пристрої за допомогою деталей TACACS+ з консолі ISE, включаючи IP-адресу та спільний секрет.

Точний контроль і аудит Перевагою використання Cisco ISE з TACACS+ є його точний контроль. ISE допомагає створювати правила та застосовувати їх до відповідних користувачів. Наприклад, ви можете додати адміністраторів пристрою як внутрішніх користувачів і налаштувати їхні паролі для ввімкнення. Крім того, через

живі журнали та звіти адміністратори ISE також можуть перевіряти, які користувачі використовували які команди.

Служба доступу до адміністрування пристрою. Адміністратор ISE, що розробляє службу доступу до адміністрування пристрою, може створювати політики, які дозволяють результатам TACACS, таким як набори команд і профілі оболонки, бути частиною правила політики авторизації.

Як згадувалося раніше, протокол TACACS+ використовується між сервером Cisco ISE та мережевим пристроєм (клієнт AAA або TACACS+). Майте на увазі, що Cisco ISE може розділяти запити на автентифікацію, авторизацію та облікові записи.

Рис. 2.6. Принцип роботи протоколу TACACS+

1. Коли адміністратор мережевого пристрою (користувач терміналу) намагається ввійти на пристрій (клієнт AAA/TACACS+) через Telnet або SSH, пристрій миттєво запитує Cisco ISE (сервер AAA та TACACS+) через протокол TACACS для перевірки автентифікації.

2. Сервер Cisco ISE, у свою чергу, використовує набори автентифікації політики, щоб або відповісти «прийняти», або «відхилити» мережевому пристрою.

3. Якщо користувачеві надано доступ > мережевий пристрій запитує Cisco ISE за допомогою TACACS+ для авторизації. Сервер ISE перевіряє правила політики авторизації для результатів TACACS+, таких як набори команд і профілі оболонки.

4. Потім користувачеві надається набір команд або профілів оболонки для виконання певних дій на мережевому пристрої.

5. Нарешті, сервер Cisco ISE забезпечує облік, реєструючи дії та надаючи звіти, щоб адміністратор ISE міг проводити детальні перевірки [3].

TrustSec. TrustSec — це програмно - визначена технологія сегментації, розроблена Cisco. Замість використання IP-адреси, він використовує ролі кінцевих точок для керування контролем доступу до мережі. Це можна керувати та налаштовувати за допомогою Cisco ISE. За допомогою мережі TrustSec адміністратор може реалізувати сегментацію мережі без зміни топології. Зазвичай сам адміністратор міг би додати більше або видалити VLAN, але в цьому випадку це не потрібно. З Cisco TrustSec, адміністратор може додати теги групи безпеки (SGT) до кінцевої точки доступу до мережі наприклад, маршрутизатор, комутатор або брандмауер, який зазвичай базується на місці розташування користувача, пристрої або сам користувач. SGT підтримуються лише пристроями Cisco. Проте протокол обміну SGT (SXP) можна використовувати для розповсюдження SGT через мережу для пристроїв які не мають апаратної підтримки Cisco TrustSec [11].

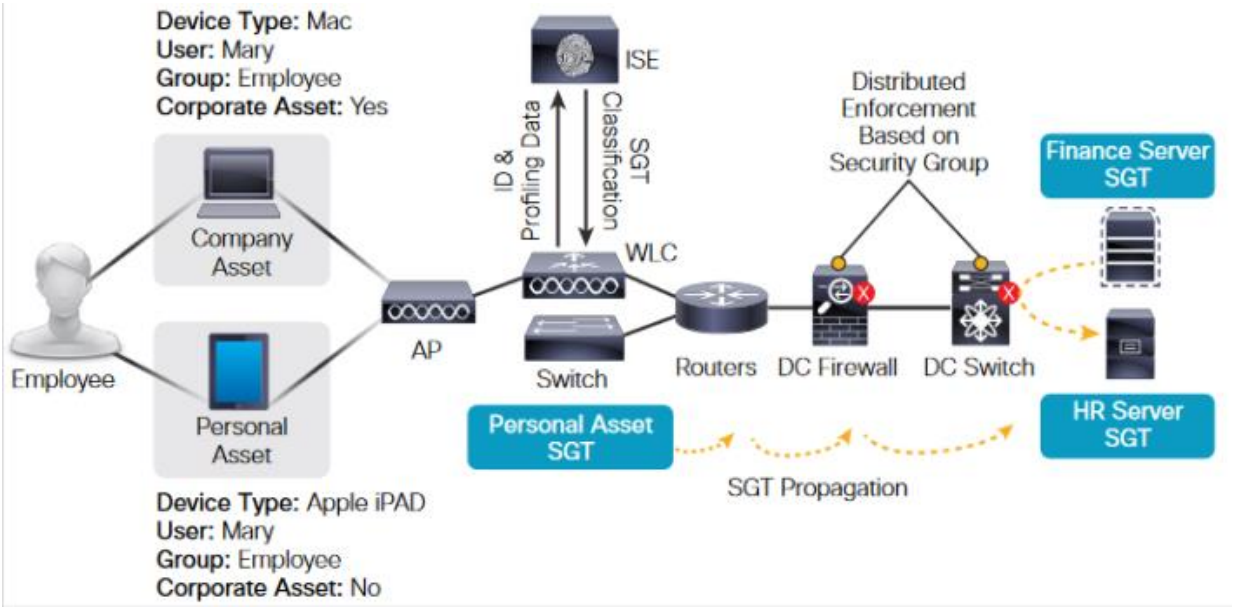

Рис. 2.7. Приклад використання SGT

Як показано на рис. 2.7, особистий актив має SGT, який не дозволяє отримати доступ до корпоративні активи. Cisco TrustSec може допомогти компанії знизити витрати, заощадивши час, зробити BYOD простішим і доступнішим і зробити всю мережу трохи більше динамічний. TrustSec також підтримує гнучку автентифікацію. Що це означає, що він поєднує 802.1X і MAB в один процес автентифікації. Зазвичай їх три режими, у яких розгорнуто TrustSec. Це режим моніторингу, режим низького впливу та закритий режим, який раніше був відомий як режим високого рівня безпеки.

Режим монітора. Режим моніторингу використовує дані журналу для перевірки. Адміністратори можуть використовувати цей режим, щоб переконатися, що всі пристрої проходять правильну автентифікацію, і виявити пристрої у своїй мережі яким там не місце. По суті, це працює як режим аудиту. Щоб забезпечити, аутентифікація проходить гладко, режим моніторингу використовує 802.1X або MAB. Якщо у пристрої є відсутній запитувач 802.1X або неправильно налаштований. Відкритий режим автентифікації в режим моніторингу гарантує, що доступ не буде заборонено, і він збиратиме дані про спробу [2].

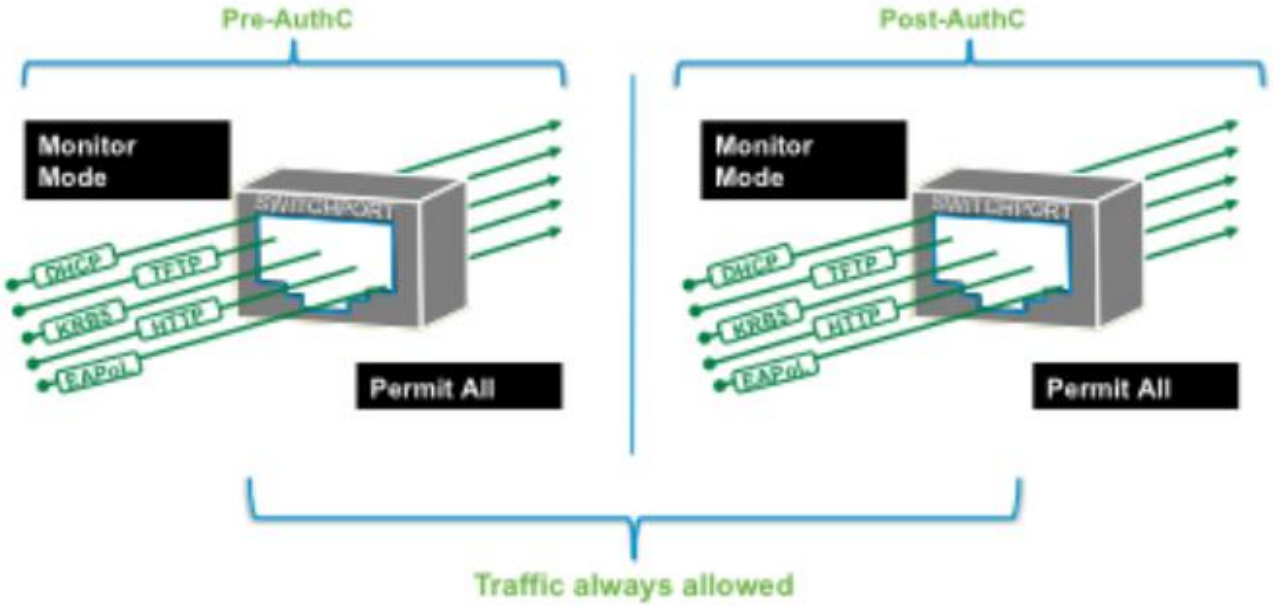

Рис. 2.8. Процес використання режиму моніторингу

На наступному рисунку 2.9 показано потік використання режиму монітора. Спочатку він дізнається MAC а потім перевіряє, чи в нього автентифікований Dot1X [2]. Якщо ні, мине час очікування та використає MAB. Якщо що не вдається, він все одно отримає доступ до мережі. Якщо Dot1X або MAB успішні, вони виграють доступ до мережі.

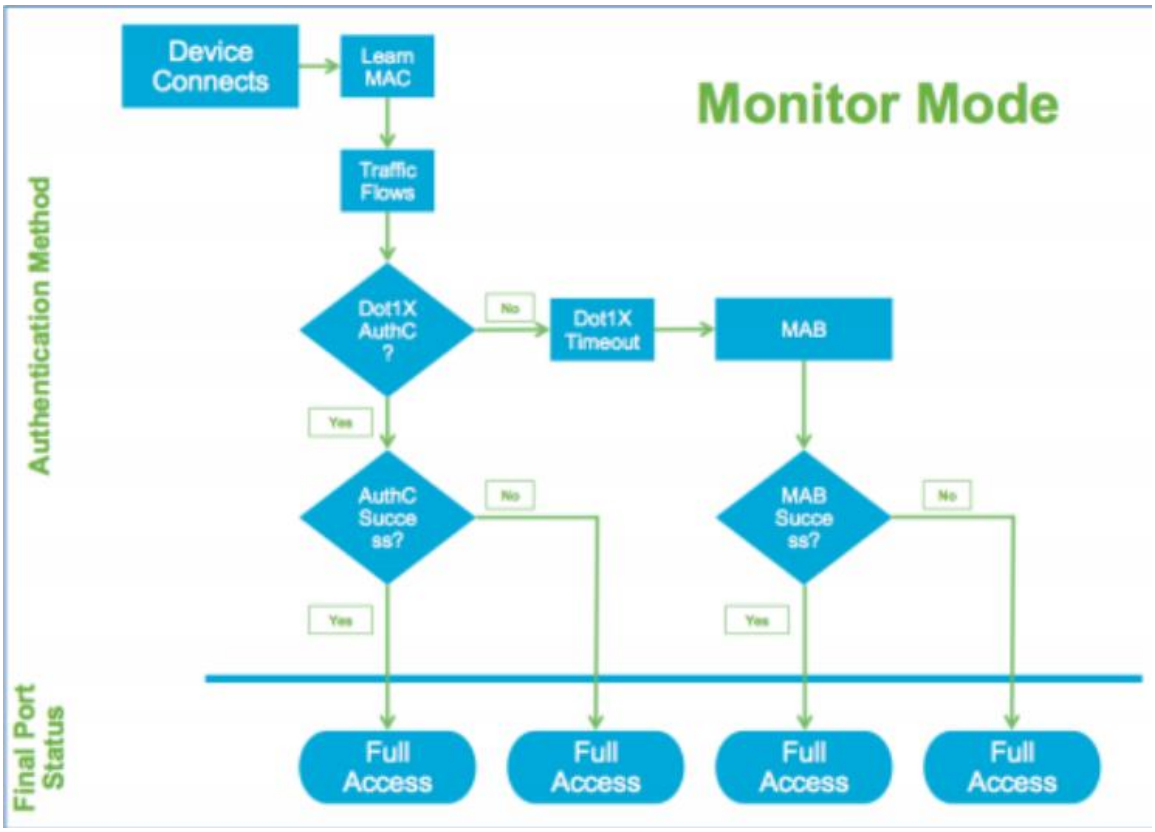

Рис. 2.9. Блок-схема режиму моніторингу з використанням Dot1x і MAB

Режим низького впливу. Режим низького впливу можна використовувати, щоб дозволити підключеним пристроям отримувати IP від DHCP використання DNS або навіть доступ до Інтернету. Однак режим блокує будь-який доступ до внутрішніх мережевих ресурсів. Це досягається шляхом розгортання режиму моніторингу, а потім його застосуванням Access Control List (ACL) до порту комутатора. Цей ACL надає порту обмежений доступ. Після успішної автентифікації користувача йому буде

надано кращий доступ до мережі. Це лише приклади того, чого можна досягти за допомогою режиму низького впливу його призначення.

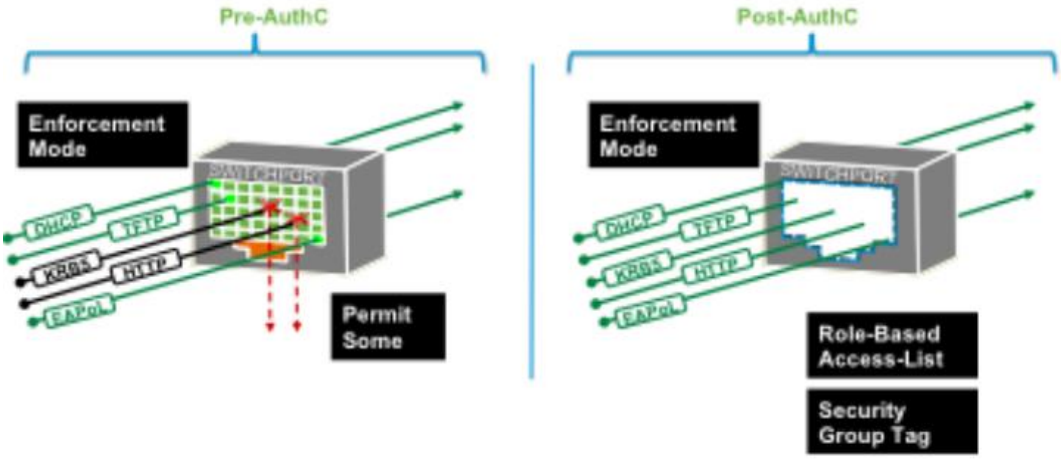

Рис. 2.10. Приклад режиму низького впливу

Процес автентифікації в режимі низького впливу працює подібно до режиму моніторингу, єдиним винятком якого є результат і статус порта комутатора. По суті, це дозволяє адміністратору для підвищення безпеки мережі. Обмежений доступ може бути забезпечений на основі результатів автентифікації та процесу авторизації за допомогою поєднання ACL та (завантажуваних ACL) із портом із підтримкою Cisco TrustSec.

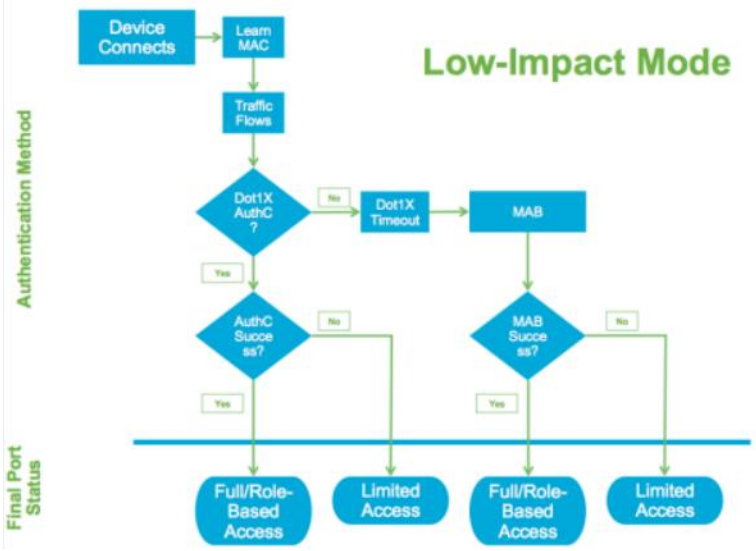

Рис. 2.11. Блок-схема режиму з низьким рівнем впливу

Закритий режим. Так званий режим за замовчуванням 802.1X є закритим режимом, який раніше був відомий як режим високого рівня безпеки. Працює майже так, як було описано раніше в цій дипломній роботі. Закритий режим рекомендується для тих, хто має досвід і готовий мати справу з нюансами, пов'язаними з налаштуванням чогось подібного. Закритий режим відрізняється від режиму моніторингу та режиму низького впливу тим, що автентифікація пройшла успішно, увесь майбутній трафік видалено. Це включає DHCP, DNS і ARP, наприклад.

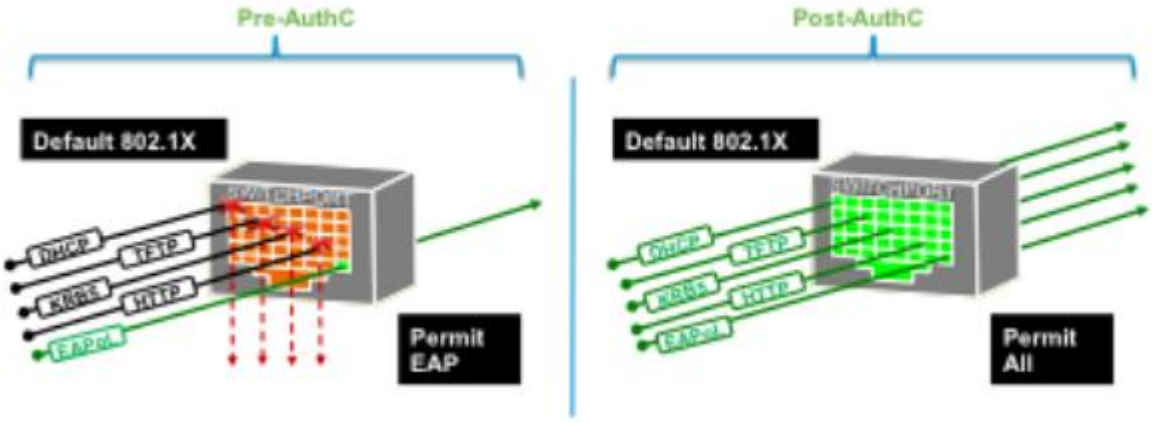

Рис. 2.12. Аутентифікація 802.1X у закритому режимі

Отже, закритий режим є типовим типом під час використання 802.1X для автентифікації та авторизації користувачів мережі. Якщо автентифікація не вдається через 802.1X або MAB, зазвичай він закриває комутатор або просто надає обмежений доступ. Обмежений доступ може означати що він скидає все, крім пакетів, необхідних для автентифікації [8].

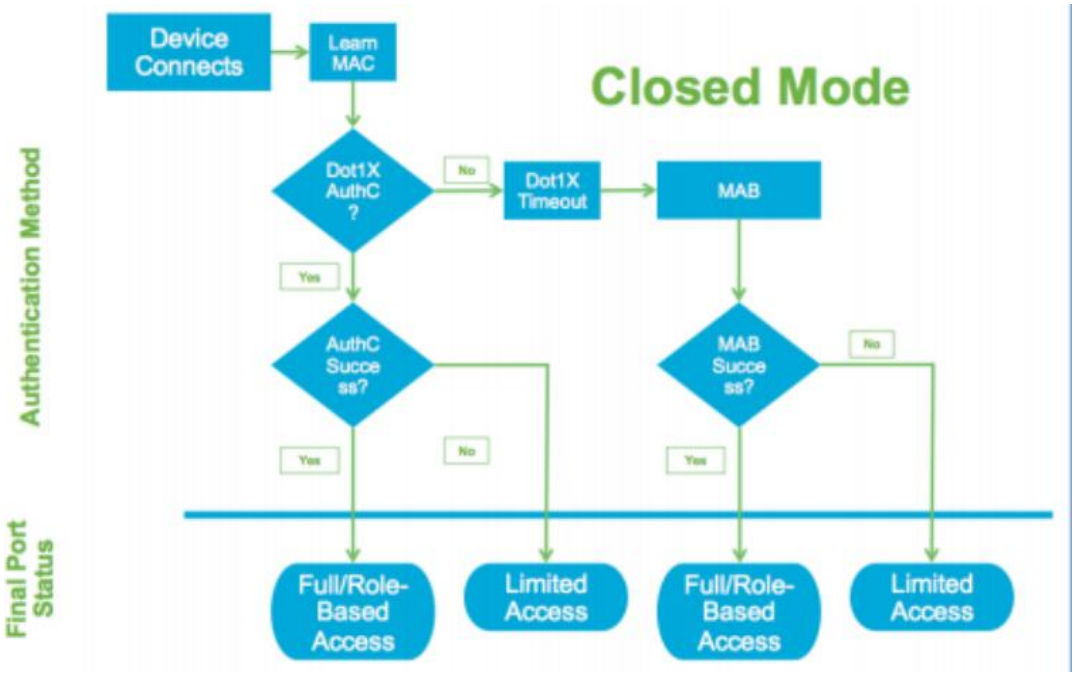

Рис. 2.13. Блок-схема закритого режиму

Висновки до другого розділу

Досліджено такий продукт як Cisco Identity Services Engine, його функціонал, що за що відповідає та який набагато більше, ніж концепція додаткової безпеки та «інтуїтивної» мережі. Проаналізовано три різні розподілені розгортання для мереж різного розміру, які називаються малими, середніми та великими.

Розглянуто базову платформу AAA RADIUS та AAA TACACS+, які в цілому займаються автентифікацією та авторизацією і є функціями Cisco ISE.

Проаналізовано базову платформу AAA TACACS+ та його три різні режими, які мають свої відмінності та власне використання випадків.

Представлено процес діяльності базової платформи AAA RADIUS щодо повідомлень та їх перелік.

3 РЕАЛІЗАЦІЯ МЕТОДІВ ЗАХИСТУ БЕЗПРОВОДОВОЇ МЕРЕЖІ НА ОСНОВІ КОРПОРАТИВНИХ ОРГАНІЗАЦІЙ

3.1 Встановлення та налаштування Cisco ISE-сервера

Ця інсталяція Cisco ISE 2.6 використовуватиме віртуальну машину, точніше VMware. У цьому випадку для Cisco ISE використовується розгортання середнього розміру. В даному випадку так встановлений на ESXi-сервері. У клієнті ESXi почнеться вибір New Virtual Machine розгортання. Вибір спеціальної інсталяції необхідний для встановлення, як це робить ISE та не потрібно багато місця. Рекомендованого обсягу зберігання даних достатньо. Важливо вибрати правильну версію зі спадного списку, тобто Linux і Red Hat Enterprise Linux 7 у цьому випадку. Після цього клієнт запитає кількість віртуальних розеток і кількість ядер. У цьому випадку використовується ISE середнього розміру, якому потрібно 16 ядер. Однак рекомендується вибрати більшу потужність процесора для збільшення стабільності, оскільки 16 ядер є лише мінімальною вимогою. Рекомендовано E1000 Драйвер NIC для забезпечення правильного порядку адаптерів за замовчуванням. Вибір VMXNET3 може спричинити деякі проблеми та, можливо, змусити переналаштувати адаптер ESXi, щоб синхронізувати його з ISE замовленням адаптера. Для цього встановлення необхідний Paravirtual як контролер SCSI. Під час створення віртуального диска рекомендується використовувати великий диск. ISE підтримує обидва тонкі та густе забезпечення. На наступній сторінці відмовостійкість можна зняти, оскільки це не так необхідно. Остання сторінка дозволяє остаточно перевірити конфігурацію. Натиснути кнопку “завершити встановлення”. Тепер систему VMware встановлено [2].

Щоб розпочати початкову конфігурацію, потрібно завантажити щойно встановлений Cisco ISE. Зіставлення CD/DVD із образом ISO продовжить процес і з’явиться екран пропонуючи користувачеві вибрати варіант завантаження. У цьому

випадку (вибрано інсталяцію Cisco ISE (клавіатура/монітор). Після чого ISE почне інсталювати програмне забезпечення що може зайняти деякий час. Після того, як програмне забезпечення було встановлено, користувачеві потрібно буде нажати «налаштування», щоб налаштувати ISE. Тепер ISE попросить користувача надіслати наступні параметри в порядку.

• Ім'я хоста

• IP-адреса для інтерфейсу Ethernet (eth0)

• Маска мережі

• Шлюз

• доменне ім'я DNS

• Додайте інший сервер імен (необов’язково)

• Сервер NTP

• Додайте інший сервер NTP (необов’язково)

• Системний часовий пояс

• Ім'я користувача

• Пароль

Після завершення програми налаштування система автоматично перезавантажиться [5].

Після перезавантаження система запитає у користувача ім’я користувача та пароль з підказкою входу. У разі успіху, ISE має запрацювати. Щоб переконатися в цьому, введіть наступну команду.

show application

Тепер має відображатися, що ISE запущено. Щоб перевірити стан процесів ISE, введіть наступну команду.

Show application status ise

Тепер буде показано запущені процеси. Зараз ISE запущений і працює він доступний через CLI або веб-графічний інтерфейс [2].

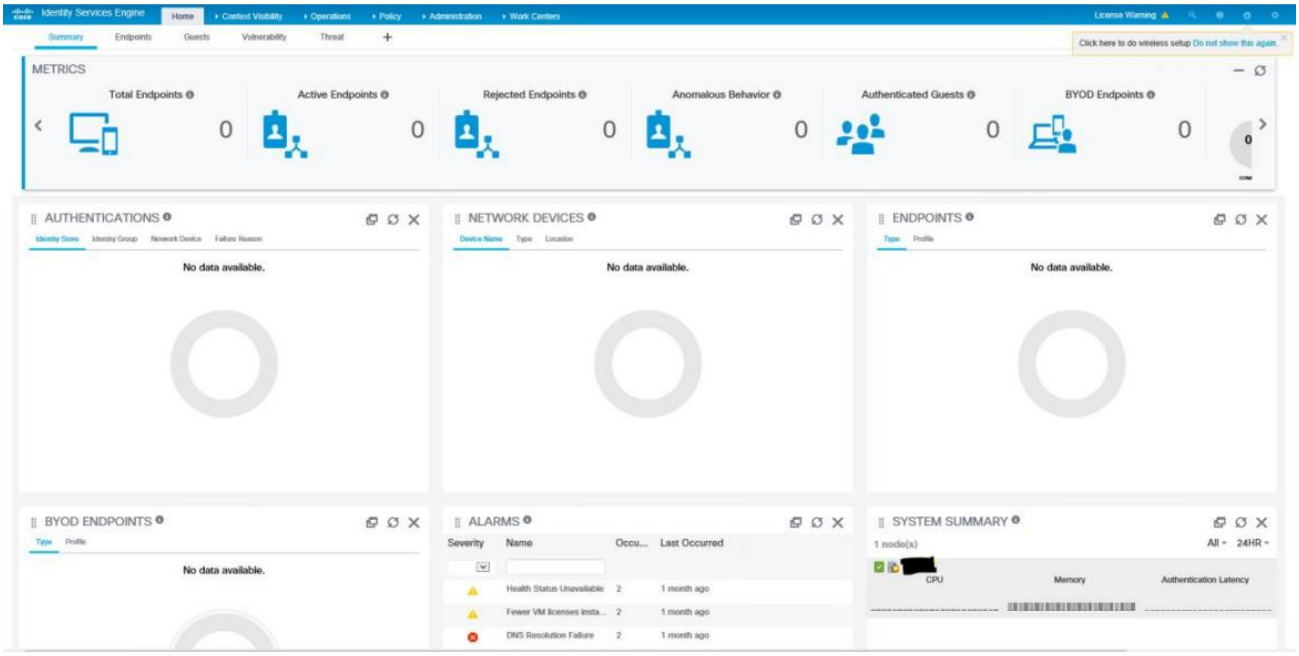

Рис. 3.1. Еталонне зображення веб-інтерфейсу користувача Cisco ISE 2.6

3.2 Розроблення набору політик щодо захисту у безпроводовій мережі

Набори політик були представлені вперше у версії 2.3. Набори політик спрощують керування політиками автентифікації та авторизації. Вони дозволяють адміністратору мережі легко налаштувати та переглянути політики. Коли пристрій намагається підключитися до мережі, він зробить це першим, перевіривши набори політики на відповідність умовам, після чого пристрій авторизується в мережі. Існує два (2) рівні наборів політик, тобто «Батьки» та «Дитина» рівень. На батьківському рівні можна встановити умови для пристроїв. Набори правил батьківського рівня можна переміщувати, просто перетягуючи їх. Для перевірки можна додати поле «Дозволені протоколи», протоколи доступу або послідовності серверів [10].

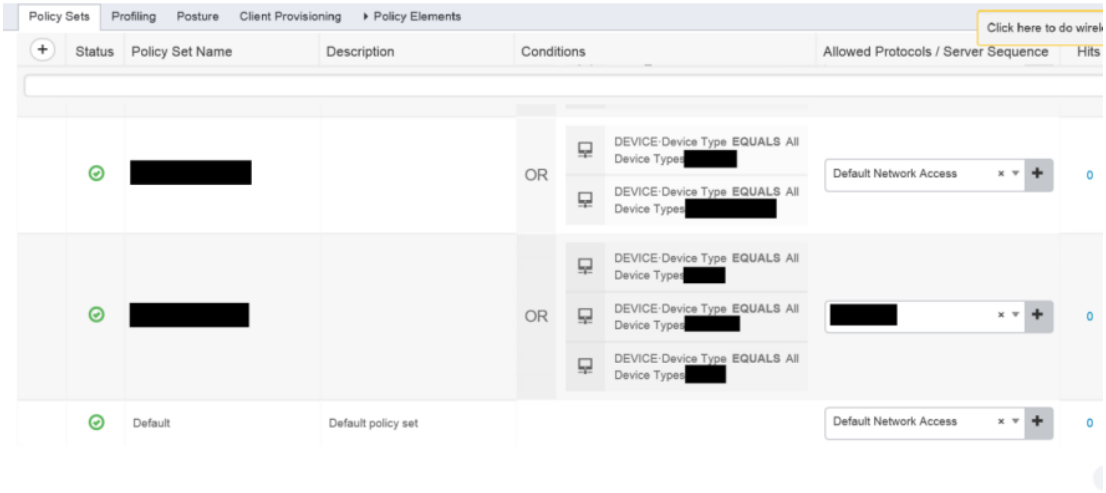

Рис. 3.2. Інтерфейс батьківського рівня наборів політик

У цьому випадку, якщо ноутбук під'єднано до мережі безпроводовим способом, він перейде до політики за замовчуванням набору та авторизується в мережі, встановлені правилами всередині набору політик [3].

На дочірньому рівні можна створювати правила для автентифікації користувача та встановлювати конкретні правила авторизації. Наприклад, якщо користувач перебуває у віддаленому/другорядному офісі, це так можна автоматично налаштувати користувача на певну VLAN або якщо користувач має певну групу Active Directory, користувач налаштований на певну VLAN. Якщо в компанії є гості і є мережа лише для них, можна налаштувати так, щоб користувачі без відповідних сертифікатів на їхньому комп'ютері повинні спочатку отримати доступ до веб-інтерфейсу користувача порталу. Рис. 3.3 нижче показано, як політика авторизації працює з будь-яким користувачем, і спочатку перевіряє, чи пристрої користувача мають сертифікат, потім перевіряють, чи вони безпроводові, а потім, нарешті, чи є частина групи Active Directory під назвою «Laptop8200». Якщо пристрої не збігаються з усі ці, це правило пропустить і перейде до наступного у списку [2].

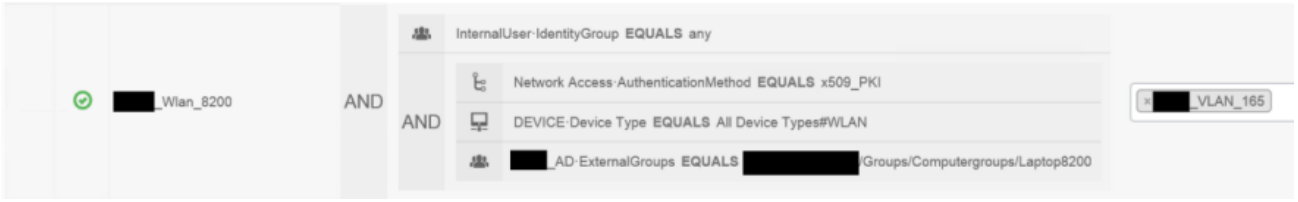

Рис. 3.3. Приклад політики дочірнього рівня

Можливості майже безмежні. Правила політики авторизації встановлюються за допомогою умов студії. Студія умов працює, дозволяючи користувачеві перетягувати різні умови, які повинні мати пристрої. Це дозволяє використання умовного такого твердження, як And, Or і Is not. Якщо Active Directory уже налаштовано, це буде видно в студії умов під час спроби використати AD для чогось. Він автоматично дізнається про існуючі групи, що дозволяє легко налаштувати адміністратора.

Рис. 3.4. Еталонне зображення студії умов

Зрештою, ядро ISE можна знайти в наборах політик, коли мова йде про мережу управління доступом. Наборів політик не існувало раніше у версіях, старших за версію 2.3, але вони все ще мали ті самі налаштування правил автентифікації та авторизації. Крім того, умови Studio також були представлені в цій версії. Це одна з ключових причин версії, яка настійно рекомендується версія 2.3 або новіша [12].

3.3 Налаштування розподіленого середовища Cisco ISE

Cisco ISE підтримує розділене розгортання, розподілене середовище і кластери. Вони всі однакові, але з більш складними назвами. В принципі, що це дозволяє адміністратору налаштувати один сервер ISE, потім скопіювати його та потім згрупувати оригінал і копію разом, щоб використовувати їх як одне ціле. Це корисно, коли сервер має бути доступним постійно. У разі поломки або пошкодження одного з серверів втрати потужності, вторинний вузол візьме на себе роботу. Кластер також можна використовувати для спільного використання робочого навантаження між двома серверами ISE [6].

Кластеризація двох серверів ISE дуже проста. По-перше, дві установки ISE на різних потрібні сервери та IP-адреси. У першому ISE, який є основним вузлом, можна знайти вкладку адміністратора, а всередині є кнопка вибору розгортання. Зліва, є колонка. Далі слід відкрити вкладку «Розгортання», після чого первинну ISE знайдено. Є розділ, де вибирається роль для ISE. Якщо цієї частини немає та ще не торкнувся, слід сказати автономний. Якщо змінити це на основний, це вийде первинний ISE. Тепер потрібен самопідписаний сертифікат від вторинного вузла ISE.

Щоб отримати самопідписаний сертифікат від вторинного вузла ISE, має бути вкладка адміністратора, треба клацнути і потрібно вибрати “Системні сертифікати”. Звідти можна натиснути кнопку експорту і воно знайдено. Тепер на вкладці сертифікатів основного вузла ISE можна відкрити кнопку імпорту і воно буде знайдено. На першій сторінці є вкладка реєстру під вузлами розгортання. Там можна зареєструвати вторинний вузол ISE. Встановити ім’я хоста, ім’я користувача та пароль для нього. Тепер вторинний ISE повинен бути автоматично налаштований як вторинний вузол, а основний вузол — як інший вузол моніторингу. Треба зберегти налаштування та має з’явитися спливаюче вікно, яке повідомляє, що для синхронізації двох вузлів потрібно кілька хвилин. Тепер налаштовано розподілене середовище з розгортанням середньої мережі [2].

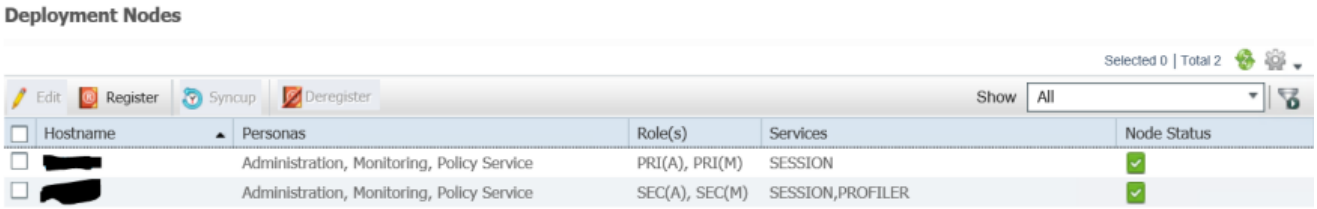

Рис. 3.5. Два вузли ISE, згруповані разом (перша є основною, а друга є вторинною)

Вузол Cisco ISE може мати будь-яку з наступних персон:

- Вузол адміністрування;
- Вузол служби політики;
- Вузол моніторингу;
- Вузол Inline Posture.

Вузол Cisco ISE може надавати різні послуги на основі персони, яку він приймає. Кожен вузол у розгортанні, за винятком вузла Inline Posture, може взяти на себе функції адміністрування, служби політики та моніторингу [15]. У розподіленому розгортанні ви можете мати таку комбінацію вузлів у своїй мережі:

- Первинний і вторинний вузли адміністрування для високої доступності;
- Пара вузлів моніторингу для автоматичного перемикання після відмови;
- Один або більше вузлів Policy Service для перемикання сеансу після відмови;
- Пара Inline Вузли положення для високої доступності.

Час приєднання, також треба визначити, які служби працюватимуть на яких вузлах; в інших слова, визначається, яку особу матиме вузол. Можна об’єднати більше ніж один вузол ISE разом, щоб створити багатовузлове розгортання, відомо зазвичай у полі як куб ISE. Важливо розуміти, що перед будь-яким ISE вузли можуть бути об’єднані разом, вони повинні довіряти адміністративним сертифікатам один одного. Без цієї довіри ви отримаєте повідомлення про помилку і зв’язку про те, що «вузол був недоступний», але першопричиною є відсутність довіри. Подібно до сценарію підключення до безпечного веб-сайту, який не використовує надійний сертифікат, де

буде видно помилку SSL у веб-переглядачі. Це просто так, тільки це базується на захисті транспортного рівня (TLS). Якщо використовуються стандартні самопідписані сертифікати в ISE, то потрібно буде імпортувати публічний сертифікат кожного вузла ISE в адміністрацію кожного вузла, оскільки всі вони є самопідписаними (ненадійні) сертифікати, і кожен вузол ISE повинен довіряти основному вузлу та основний вузол повинен довіряти кожному з інших вузлів. Замість того, щоб мати справу з імпортом відкритих ключів для цих самопідписаних сертифікатів, найкраща практика полягає в тому, щоб завжди використовувати сертифікати, видані з того самого надійного джерела. У цьому випадку лише кореневі сертифікати потрібно додати до списку довірених сертифікатів [16].

Далі треба зробити вузол адміністрування політики основним пристроєм, оскільки всі вузли ISE є автономними за замовчуванням, і треба спочатку підвищити вузол ISE який стане основним вузлом адміністрування політики (PAN), щоб бути основним пристроєм замість автономного.

На рис. 3.6 показано встановлення вузла адміністрування політики основним пристроєм.

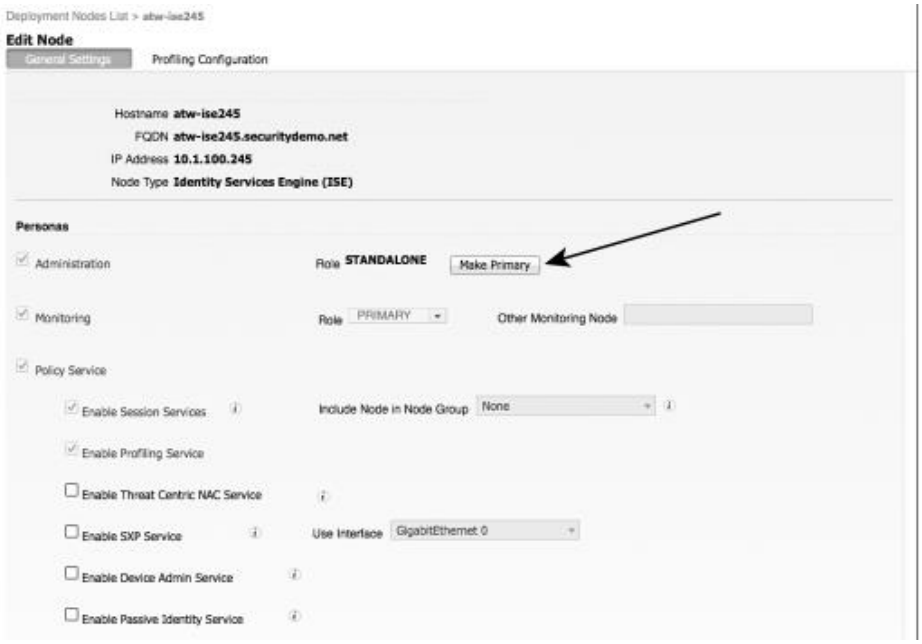

Рис. 3.6. Процес встановлення основного пристроя.

Висновки до третього розділу

Реалізовано методи захисту безпроводової мережі у корпоративній організації, як його правильно встановити та здійснити вход до нього.

Продемонстровано набір політик для використання та захисту мережі, де можна виставити вимоги для автоматичної роботи, виявлення вразливостей, сторонніх користувачів а також хто і як зможе отримати доступ до цього продукту.

Представлено налаштування розподіленого середовища Cisco ISE, який є важливим у захисті.

ВИСНОВКИ

В бакалаврській роботі отримано наступні наукові та науково-практичні результати:

– досліджено поняття безпроводових мереж та безпроводових технологій та їх важливість у використанні населення і організацій з підприємствами. Проведено аналіз безпеки безпроводових мереж, її захист у використанні та протидії вразливостям, а також приведені переваги та недоліки з додатками;

– проаналізовано поняття Cisco Identity Services Engine. Досліджено його у експлуатації, його функції, такі як AAA RADIUS та AAA TACACS+. Визначено хто може отримати доступ до продукту, де саме може це зробити, як може захиститу свою корпоративну організацію на багато років;

– проведено аналіз класифікації сучасних безпроводових мереж, які є у експлуатації. Досліджено їх діяльність малого та далекого радіусу дії з використанням додатків Bluetooth, IrDA, ZigBee та UWB. Приведено архітектуру мережі з її режимом ad hoc та режимом інфраструктури, а також використання стандарту IEEE 802.11 і протоколу 802.11 для правильної роботи мережі;

– реалізовано повний обсяг інсталяції продукту, розроблення для нього набору політик для захисту безпроводової мережі для автоматичного функціонування в майбутньому і налаштування розподіленого середовища Cisco ISE, який є невід’ємною частиною у використанні та наданні послуг;

– розроблено рекомендації щодо захисту безпроводової мережі та автоматизації для більшої ефективності у використанні.