МІНІСТРЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
Сумський державний університет
Факультет електроніки та інформаційних технологій
Кафедра електроніки і комп'ютерної техніки

«До захисту допущено»
Завідувач кафедри
_____Анатолій ОПАНАСЮК
(підпис)
___ _____ 2023р.

КВАЛІФІКАЦІЙНА РОБОТА

на здобуття освітнього ступеня бакалавра

зі спеціальності 172 «Телекомунікації та радіотехніка»,
освітньо-професійної програми «Мережеві та інтернет технології»
На тему: Wi-Fi роутер з підтримкою VPN

Здобувача групи ТК-91 Савченко Дмитро Сергійович

Кваліфікаційна робота містить результати власних досліджень. Використання ідей, результатів і текстів інших авторів мають посилання на відповідне джерело.

_____ Дмитро САВЧЕНКО
(підпис)

Керівник, кандидат к.т.н., доцент

_____Ольга БЕРЕЖНА
(підпис)

Суми – 2023

Сумський Державний Університет

Факультет електроніки та інформаційних технологій

Кафедра електроніки і комп'ютерної техніки

Спеціальність 172 Телекомунікації та радіотехніки

ЗАТВЕРДЖУЮ:

Зав. кафедри Опанасюк А. С.

«__» _____ 2023 р.

Завдання

на кваліфікаційну роботу студентові

Савченко Дмитро Сергійович

1. Тема роботи «Wi-Fi роутер з підтримкою VPN»

затверджено наказом по університету від «31»березня 2023 р. №0316-VI

2. Термін здачі студентом завершеної роботи: 09.06.2023

3. Вихідні дані до роботи: Розробити Wi-Fi роутер з підтримкою VPN за протоколом IPSec.

4. Зміст розрахунково-пояснювальної записки (перелік питань, що підлягають розробленню): Вступ. Огляд літератури та постановка задачі проектування. Розробка, обґрунтування алгоритму функціонування схеми пристрою, що проектується. Розробка та розрахунок принципових електричних схем, вузлів та блоків. Висновки.

5. Перелік графічного матеріалу (з точним зазначенням обов'язкових креслень): 1. Блок-схема алгоритма функціонування. 2. Схема електрична структурна. 3. Схема електрична принципова.

КАЛЕНДАРНИЙ ПЛАН

№ п/п	Назва етапів кваліфікаційної роботи	Термін виконання	Примітка
1	*Огляд літератури та постановка задачі проектування*	16.03.2023	
2	*Розроблення алгоритму роботи та структурної схеми пристрою*	29.03.2023	
3	*Розроблення схеми електричної принципової пристрою*	14.04.2023	
4	*Оформлення пояснювальної записки до кваліфікаційної роботи*	12.05.2023	

Здобувач вищої освіти _____ Керівник _____

(підпис) (підпис)

АНОТАЦІЯ

Записка: 65 стор., 16 рис., 2 додатки, 11 джерел.

Обґрунтування актуальності теми роботи – Тема кваліфікаційної роботи є актуальною, оскільки присвячена розв'язанню створенню Wi-Fi роутера з підримкою VPN за протоколом IPSec, шляхом розробки відповідних методів, моделей та інформаційних технологій.

Об'єкт дослідження — Wi-Fi роутер з підтримкою VPN**.**

Мета роботи — розробити обладнання та програмне забезпечення для Wi-Fi роутера з підтримкою VPN.

Методи дослідження —техногія створення такого пристрою, технологія представлення цього пристрою

Результати — розроблено Wi-Fi роутера з підримкою VPN за протоколом IPSec. Створений продукт, має всі потрібно функції, для використання. Розроблено програмне забезпечення для цього роутера.

ЗМІСТ

ВСТУП

У сучасному цифровому світі, який все більше залежить від безперервного доступу до Інтернету, безпека та приватність стають надзвичайно важливими. Із зростанням кількості підключених пристроїв у домашніх та корпоративних мережах, необхідність забезпечення захисту від зловмисників і збереження конфіденційності стає невідкладною.

Одним з інструментів, що допомагає у забезпеченні безпеки та приватності в Інтернеті, є використання віртуальних приватних мереж (Virtual Private Networks, VPN). VPN-сервіси шифрують і захищають передачу даних між пристроями та мережами, що дозволяє зберігати конфіденційну інформацію в безпеці від несанкціонованого доступу.

У контексті домашньої мережі, Wi-Fi роутери з підтримкою VPN стають все більш популярними серед користувачів, які бажають захистити свою приватність і забезпечити безпечне з'єднання для всіх підключених пристроїв. Ці роутери надають зручну можливість налаштування VPN-з'єднання безпосередньо на рівні мережі, що означає, що всі пристрої, підключені до даного роутера, автоматично користуються захищеним VPN-тунелем.

Мета роботи полягає у дослідженні Wi-Fi роутера з підтримкою VPN. Дослідження включатиме аналіз основних функцій, характеристик і можливостей роутера, а також порівняння їх ефективності, швидкості та захищеності.

На основі отриманих результатів дослідження буде розроблений прототип Wi-Fi роутера з підтримкою VPN, який відповідатиме вимогам безпеки та приватності, а також забезпечуватиме зручність використання та широкі можливості налаштування для користувачів.

1 ОГЛЯД ЛІТЕРАТУРИ ТА ПОСТАНОВКА ЗАДАЧІ ПРОЕКТУВАННЯ

1.1 Постановка задачі

Виходячи із завдання необхідно розробити Wi-Fi роутер з підтримкою VPN, який виконуватиме наступні функції:

- підтримка бездротової мережі;
- маршрутизація трафіку;
- підтримка VPN-протоколів;
- шифрування даних;
- управління налаштуваннями;
- захист від загроз;
- моніторинг трафіку;

При цьому потрібно реалізувати наступні схеми:

- алгоритму;
- електричну структурну;
- електричну принципову.

1.2 Огляд літератури

1.2.1. Віртуальна локальна мережа VLAN

VLAN (Virtual Local Area Network – віртуальна локальна мережа). Віртуальною локальною мережею називається логічна група пристроїв, що мають можливість взаємодіяти між собою безпосередньо на канальному рівні, хоча фізично при цьому вони можуть бути підключені до різних мережних комутаторів. І навпаки, трафік пристроїв, що знаходяться у різних VLAN'ах, повністю ізольований від інших вузлів мережі на канальному рівні, навіть якщо вони підключені до одного комутатора. Це означає, що передача кадрів між різними віртуальними мережами на підставі MAC-адреси неможлива, незалежно від типу адреси – унікальної, групової або широкомовної.

VLAN'и мають такі переваги:

- гнучкість впровадження – VLAN є ефективним способом групування мережевих користувачів у віртуальні робочі групи, незважаючи на їхнє фізичне розміщення в мережі;
- застосування VLAN забезпечує можливість контролю широкомовних повідомлень, що збільшує смугу пропускання доступну для користувача;
- застосування VLAN дозволяє підвищити безпеку мережі, визначивши за допомогою фільтрів, налаштованих на комутаторі або маршрутизаторі політику взаємодії користувачів з різних віртуальних мереж;

1.2.2. Віртуальні приватні мережі (VPN)

Інтернет все частіше використовується як засіб комунікації між комп'ютерами, оскільки він пропонує ефективний та недорогий зв'язок. Однак Інтернет є мережею загального користування і для того, щоб забезпечувати безпечну комунікацію через нього, необхідний якийсь механізм, що задовольняє як мінімум наступним завданням:

- конфіденційність інформації;
- цілісність даних;
- доступність інформації;

Цим вимогам задовольняє механізм, названий VPN (Virtual Private Network – віртуальна приватна мережа) – узагальнена назва технологій, що дозволяють забезпечити одне або декілька мережевих з'єднань (логічну мережу) поверх іншої мережі (наприклад, Інтернет) з використанням засобів криптографії (шифрування, автентифікації, інфраструктури) відкритих ключів, засобів для захисту від повторів і змін повідомлень, що передаються по логічній мережі).

Створення VPN не вимагає додаткових інвестицій і дозволяє відмовитись від використання виділених ліній. Залежно від застосовуваних протоколів та призначення, VPN може забезпечувати з'єднання трьох видів: хост-хост, хост-мережа та мережа-мережа.

Для наочності представимо наступний приклад: підприємство має кілька територіально віддалених філій та "мобільних" співробітників, які працюють вдома або в роз'їзді. Необхідно об'єднати всіх працівників підприємства на єдину мережу. Найпростіший спосіб – це поставити модеми в кожній філії та організовувати зв'язок у міру потреби. Таке рішення, однак, не завжди зручне і вигідне – часом потрібний постійний зв'язок та велика пропускна спроможність. Для цього доведеться або прокладати виділену лінію між філіями або орендувати їх. І те, й інше досить дорого. І тут як альтернатива при побудові єдиної захищеної мережі можна застосовувати VPN-підключення всіх філій фірми через Інтернет та налаштування VPN-засобів на хостах мережі.

VPN використовує такі засоби, як шифрування даних для забезпечення цілісності та конфіденційності, автентифікація та авторизація для перевірки прав користувача та дозволу доступу до віртуальної приватної мережі.

З'єднання VPN завжди складається з каналу типу точка-точка, також відомого під назвою тунель. Тунель створюється в незахищеній мережі, якою найчастіше виступає Інтернет.

Тунелювання (tunneling) чи інкапсуляція (encapsulation) – це спосіб передачі корисної інформації через проміжну мережу. Такою інформацією можуть бути кадри (або пакети) іншого протоколу. При інкапсуляції кадр не передається у тому вигляді, в якому він був згенерований хостом-відправником, а забезпечується додатковим заголовком, що містить інформацію про маршрут,

що дозволяє інкапсульованим пакетам проходити через проміжну мережу (Інтернет). На кінці тунелю кадри деінкапсулюються та передаються одержувачу. Як правило, тунель створюється двома прикордонними пристроями, розміщеними в точках входу до публічної мережі. Однією з явних переваг тунелювання є те, що дана технологія дозволяє зашифрувати вихідний пакет цілком, включаючи заголовок, в якому можуть знаходитися дані, що містять інформацію, яку зловмисники використовують для злому мережі (наприклад, IP-адреси, кількість підмереж і т.д.) .

Хоча тунель VPN встановлюється між двома точками, кожен вузол може встановлювати додаткові тунелі з іншими вузлами. Для прикладу, коли трьом віддаленим станціям необхідно зв'язатися з тим самим офісом, буде створено три окремі VPN-тунелі до цього офісу. Для всіх тунелів вузол на боці офісу може бути одним і тим самим. Це можливо завдяки тому, що вузол може шифрувати та розшифровувати дані від імені всієї мережі.

Усередині приватної мережі самого шифрування немає. Причина в тому, що ця частина мережі вважається безпечною та перебуває під безпосереднім контролем у протилежність до Інтернету. Це справедливо і при з'єднанні офісів за допомогою VPN-шлюзів. Таким чином, гарантується шифрування лише тієї інформації, яка передається небезпечним каналом між офісами.

Існує безліч різних рішень для побудови приватних віртуальних мереж. Найбільш відомі та широко використовувані протоколи – це:

- PPTP (Point-to-Point Tunneling Protocol) – цей протокол став досить популярним завдяки його включенню до операційних систем фірми Microsoft.
- L2TP (Layer-2 Tunneling Protocol) – поєднує протокол L2F (Layer 2 Forwarding) і протокол PPTP. Як правило, використовується в парі з IPSec.
- IPSec (Internet Protocol Security) – офіційний Інтернет-стандарт, розроблений спільнотою IETF (Internet Engineering Task Force).

Для організації VPN на основі PPTP не потрібні великі витрати та складні налаштування: достатньо встановити в центральному офісі сервер PPTP (рішення PPTP існують як для Windows, так і для Linux платформ), а на клієнтських комп'ютерах виконати необхідні налаштування. Якщо ж потрібно об'єднати кілька філій, то замість налаштування PPTP на всіх станціях клієнтів краще скористатися Інтернет-маршрутизатором або міжмережевим екраном з підтримкою PPTP: налаштування здійснюються тільки на прикордонному маршрутизаторі (міжмережевому екрані), підключеному до Інтернету, для користувачів все абсолютно прозоро. Прикладом таких пристроїв можуть бути багатофункціональні Інтернет-маршрутизатори серії DIR/DSR та міжмережні екрани серії DFL.

1.2.3. GRE, L2TP, IPsec

Generic Routing Encapsulation (GRE) – протокол інкапсуляції мережевих пакетів, що забезпечує тунелювання трафіку через мережі без шифрування. Приклади використання GRE:

- передача трафіку (у тому числі широкомовного) через обладнання, яке не підтримує певного протоколу;
- тунелювання IPv6-трафіку через мережу IPv4;
- передача даних через громадські мережі для реалізації захищеного VPN-з'єднання.

Протокол L2TP з'явився об'єднання протоколів PPTP і L2F. Головне достоїнство протоколу L2TP у цьому, що дозволяє створювати тунель у мережах IP, а й у мережах ATM, X.25 і Frame relay. L2TP застосовує як транспорт протокол UDP і використовує однаковий формат повідомлень як для управління тунелем, так і для пересилання даних.

Як і у випадку з PPTP, L2TP починає складання пакета передачі тунель з того, що до поля інформаційних даних PPP додається спочатку заголовок PPP, потім заголовок L2TP. Отриманий у такий спосіб пакет інкапсулюється UDP. Залежно від обраного типу політики безпеки IPSec, L2TP може шифрувати UDP-повідомлення та додавати до них заголовок та закінчення Encapsulating Security Payload (ESP), а також закінчення IPSec Authentication (див. розділ "L2TP over IPSec"). Потім проводиться інкапсуляція в IP. Додається IP-заголовок, що містить адреси відправника та одержувача. На завершення L2TP виконує другу PPP-інкапсуляцію для підготовки даних до передачі.

Комп'ютер-отримувач приймає дані, обробляє заголовок та закінчення PPP, прибирає заголовок IP. За допомогою IPSec Authentication проводиться автентифікація інформаційного поля IP, а ESP-заголовок IPSec допомагає розшифрувати пакет.

Далі комп'ютер обробляє заголовок UDP та використовує заголовок L2TP для ідентифікації тунелю. Пакет PPP тепер містить лише корисні дані, які обробляються або надсилаються вказаному одержувачу.

IPsec (скорочення від IP Security) – набір протоколів для забезпечення захисту даних, що передаються за міжмережевим протоколом IP, дозволяє здійснювати підтвердження автентичності та/або шифрування IP-пакетів. IPsec також включає протоколи для захищеного обміну ключами в мережі Інтернет.

Безпека IPSec досягається рахунок додаткових протоколів, додають до IP-пакету власні заголовки – інкапсуляції. Т.к. IPSec – стандарт Інтернет, то для нього існують документи RFC:

- RFC 2401 (Security Architecture for the Internet Protocol) – архітектура захисту протоколу IP.

- RFC 2402 (IP Authentication header) – автентифікаційний заголовок IP.
- RFC 2403 (The Use of HMAC-MD5-96 within ESP and AH) — використання алгоритму хешування MD-5 для створення аутентифікаційного заголовка.
- RFC 2404 (The Use of HMAC-SHA-1-96 with ESP and AH) – використання алгоритму хешування SHA-1 для створення аутентифікаційного заголовка.
- RFC 2405 (ESP DES-CBC Cipher Algorithm With Explicit IV) – використання алгоритму шифрування DES.
- RFC 2406 (IP Encapsulating Security Payload (ESP)) – шифрування даних.
- RFC 2407 (Internet IP Security Domain of Interpretation for ISAKMP) – область застосування протоколу керування ключами.
- RFC 2408 (Internet Security Association and Key Management Protocol (ISAKMP)) – керування ключами та автентифікаторами захищених з'єднань.
- RFC 2409 (IKE) – обмін ключами.
- RFC 2410 – нульовий алгоритм шифрування та його використання.
- RFC 2411 (IP Security Document Roadmap) – подальший розвиток стандарту.
- RFC 2412 (The OAKLEY Key Determination Protocol) – перевірка автентичності ключа.

IPsec є невід'ємною частиною Інтернет-протоколу IPv6 та необов'язковим розширенням версії Інтернет-протоколу IPv4.

Механізм IPSec вирішує такі завдання:

- аутентифікацію користувачів або комп'ютерів під час ініціалізації захищеного каналу;
- шифрування та автентифікацію даних, що передаються між кінцевими точками захищеного каналу;
- автоматичне постачання кінцевих точок каналу секретними ключами, необхідними роботи протоколів аутентифікації і шифрування даних.

Протокол AH (Authentication Header) – протокол ідентифікації заголовка. Забезпечує цілісність шляхом перевірки того, що жоден біт в частині пакета, що захищається, не був змінений під час передачі. Але використання AH може викликати проблеми, наприклад, при проходженні пакета через пристрій NAT. NAT змінює IP-адресу пакета, щоб дозволити доступ до Інтернету із закритої локальної адреси. Т.к. пакет у такому разі зміниться, то контрольна сума AH стане невірною (для усунення цієї проблеми розроблено протокол NAT-Traversal (NAT-T), що забезпечує передачу ESP через UDP і порт UDP 4500, який використовує в своїй роботі). Також слід зазначити, що AH розроблявся лише задля забезпечення цілісності. Він не гарантує конфіденційності шляхом шифрування вмісту пакета.

Протокол ESP (Encapsulation Security Payload) забезпечує не тільки цілісність і аутентифікацію даних, що передаються, але ще й шифрування даних, а також захист від помилкового відтворення пакетів.

Протокол ESP – інкапсулюючий протокол безпеки, який забезпечує цілісність і конфіденційність. У режимі транспорту ESP-заголовок знаходиться між вихідним заголовком IP і заголовком TCP або UDP. У режимі тунелю ESP-заголовок розміщується між новим IP-заголовком та повністю зашифрованим вихідним IP-пакетом.

Обидва протоколи - AH і ESP - додають власні заголовки IP, кожен з них має свій номер (ID) протоколу, за яким можна визначити, що слідує за IP-заголовком. Кожен протокол, згідно з IANA (Internet Assigned Numbers Authority – організація, відповідальна за адресний простір мережі Інтернет), має власний номер (ID). Наприклад, для TCP цей номер дорівнює 6, а для UDP – 17. Тому дуже важливо при роботі через міжмережевий екран налаштувати фільтри таким чином, щоб пропускати пакети з ID AH та/або ESP протоколу.

Щоб вказати, що у заголовку IP присутня AH, встановлюється ID протоколу 51, а ESP – номер 50.

Протокол IKE (Internet Key Exchange) – стандартний протокол IPsec, який використовується для забезпечення безпеки взаємодії у віртуальних приватних мережах. Призначення IKE – захищене узгодження та доставка ідентифікованого матеріалу для асоціації безпеки (SA).

SA – це термін IPSec для позначення з'єднання. Встановлений SA (захищений канал, званий "безпечною асоціацією" або "асоціацією безпеки" - Security Association, SA) включає секретний ключ і набір криптографічних алгоритмів.

Протокол IKE виконує три основні завдання:

- забезпечує засоби аутентифікації між двома кінцевими точками VPN;
- встановлює нові зв'язки IPSec (створює пару SA);
- керує існуючими зв'язками.

IKE використовує порт UDP з номером 500. При використанні функції NAT Traversal, як згадувалося раніше, протокол IKE використовує порт UDP з номером 4500.

Обмін даними в IKE відбувається у 2 фази. У першій фазі встановлюється асоціація SA IKE. При цьому виконується аутентифікація кінцевих точок каналу та вибираються параметри захисту даних, такі як алгоритм шифрування, сесійний ключ та ін.

У другій фазі SA IKE використовується узгодження протоколу (зазвичай IPSec).

При настроєному VPN-тунелі для кожного протоколу, що використовується, створюється одна пара SA. SA створюються парами, т.к. кожна SA – це односпрямоване з'єднання, а дані необхідно передавати у двох напрямках. Отримані пари SA зберігаються кожному вузлі.

Так як кожен вузол здатний встановлювати кілька тунелів з іншими вузлами, кожен SA має унікальний номер, що дозволяє визначити, до якого сайту він відноситься. Цей номер називається SPI (Security Parameter Index) або індекс параметра безпеки.

SA зберігаються у базі даних (БД) SAD (Security Association Database).

Гнучкість IPSec полягає в тому, що для кожного завдання пропонується кілька способів її вирішення, і методи, вибрані для одного завдання, зазвичай не залежать від методів реалізації інших завдань.

Наприклад, IPSec визначається, що пакети аутентифікуються або за допомогою односторонньої функції MD5, або за допомогою односторонньої функції SHA-1, а шифрування здійснюється з використанням алгоритму DES. Виробники продуктів, у яких працює IPSec, можуть додавати інші алгоритми автентифікації та шифрування. Наприклад, деякі продукти підтримують такі алгоритми шифрування, як 3DES, Blowfish, Cast, RC5 та ін.

Протоколи захисту потоку, що передається (AH і ESP) можуть працювати у двох режимах – у транспортному режимі та в режимі тунелювання. Працюючи у транспортному режимі IPsec працює лише з інформацією транспортного рівня, тобто. шифрується лише поле даних пакета, що містить протоколи TCP/UDP (заголовок IP-пакету не змінюється (не шифрується)). Транспортний режим зазвичай використовується для встановлення з'єднання між хостами.

У режимі тунелювання шифрується весь IP-пакет, включаючи заголовок мережного рівня. Щоб його можна було передати по мережі, він поміщається в інший IP-пакет. Фактично, це захищений IP-тунель. Тунельний режим може використовуватися для підключення віддалених комп'ютерів до приватної віртуальної мережі (схема підключення "хост-мережа") або для організації безпечної передачі даних через відкриті канали зв'язку (наприклад, Інтернет) між шлюзами для об'єднання різних частин віртуальної приватної мережі (схема підключення "мережа") -мережа").

Режими IPsec не є взаємовиключними. На тому самому вузлі деякі SA можуть використовувати транспортний режим, інші – тунельний.

На фазі автентифікації обчислюється контрольна сума пакета ICV (Integrity Check Value). При цьому передбачається, що обидва вузли знають секретний ключ, який дозволяє одержувачу обчислити ICV і порівняти з результатом, надісланим відправником. Якщо порівняння ICV пройшло успішно, вважається, що відправник пакета автентифікований.

У режимі транспорту AH при виконанні розрахунку контрольну суму ICV включаються такі компоненти:

- весь IP-пакет, за винятком деяких полів у заголовку IP, які можуть бути змінені під час передачі. Ці поля, значення яких для розрахунку ICV дорівнюють 0, можуть бути частиною служби (Type of Service, TOS), прапорами, зміщенням фрагмента, часом життя (TTL), а також заголовком контрольної суми;
- усі поля в AH;
- корисні дані пакетів IP.

У тунельному режимі вихідний пакет міститься у новий IP-пакет, і передачі даних виконується виходячи з заголовка нового IP-пакета.

1.2.4. Використання сертифікатів

У разі встановлення VPN-тунелю міжмережевий екран повинен знати, кому він повинен довіряти. При використанні попередньо розподілених ключів все просто. Міжмережевий екран довіряє всім, хто має такий самий ключ. У разі використання сертифікатів міжмережевий екран повинен довіряти всім, чий сертифікат підписаний CA. Перш ніж сертифікат буде прийнято, виконуються такі дії для перевірки автентичності сертифіката.

Кроки створення IPSec-тунелю з використанням сертифікатів аналогічні створенню тунелю з ключами, тільки замість об'єкта з ключами створюється об'єкт із сертифікатами.

1.2.5. Додаткові параметри

Група ключів DH IKE (IKE DH Group). DH – Diffie-Hellman – криптографічний протокол, який дозволяє двом сторонам, які спілкуються через небезпечну мережу (наприклад, Інтернет), згенерувати спільний секретний ключ, який згодом використовуватиметься для шифрування даних між цими сторонами. Криптостійкість алгоритму визначається розміром ключа: 1 (768 bit), 2 (1024 bit) або 5 (1536 bit). Розмір ключа DH групи 1 дорівнює 768 біт. Розмір ключа DH групи 2 дорівнює 1024 біт. Розмір ключа DH групи 5 дорівнює 1536 біт. Чим вище група, тим більше криптоскоїм стає алгоритм, і тим більше ресурсів процесора він споживає.

PFS (Perfect Forward Secrecy – досконала пряма секретність) – додаткове шифрування під час обміну ключами у другій фазі. Якщо функцію PFS увімкнено, для кожного узгодження на другій фазі буде виконуватися новий обмін за протоколом Diffie-Hellman, забезпечуючи нові дані для ключів. Внаслідок чого система має більшу стійкість щодо криптографічних атак. Якщо один ключ буде зламаний, інший ключ не зможе бути отриманий під час використання тієї ж інформації. При цьому збільшується завантаження процесора та знижується загальна продуктивність системи.

На додаток до протоколів та шифрів, VPN також використовують процеси, відомі як рукостискання та хеш-автентифікації, для додаткового захисту та аутентифікації вашого з'єднання.

Рукостискання відноситься до початкового з'єднання між двома комп'ютерами. Це вітання, в якому обидві сторони аутентифікують одна одну та встановлюють правила спілкування.

Під час VPN-квитування VPN-клієнт (тобто ваш пристрій) встановлює початкове з'єднання з VPN-сервером.

Потім це з'єднання використовується для безпечного обміну ключем шифрування між клієнтом та сервером. Цей ключ використовується для шифрування та дешифрування даних на обох кінцях VPN-тунелю протягом сеансу перегляду.

1. Клієнт запитує безпечний сеанс

2. Сертифікат автентифікації та відкритий ключ надіслані назад

3. Клієнт створює симетричний ключ, зашифрований відкритим ключем

4. Зашифрований симетричний ключ надсилається на сервер

5. Симетричний ключ, розшифрований приватним ключем

6. Сесія зашифрована симетричним ключем

При обміні даними VPN зазвичай використовується алгоритм RSA (Rivest-Shamir-Adleman). Хоча процес встановлення зв'язку працює добре і генерує безпечне шифрування, кожен згенерований сеанс можна розшифрувати за допомогою закритого ключа, який використовується при встановленні зв'язку RSA. У цьому сенсі це схоже на головний ключ.

Якщо головний ключ будь-коли буде скомпрометований, його можна буде використовувати для розшифровки кожного захищеного сеансу на цьому VPN-сервері, минулого чи сьогодення. Зловмисник може зламати VPN-сервер та отримати доступ до всіх даних, що проходять через VPN-тунель.

Щоб уникнути цього, потрібно використовувати VPN-сервіси, налаштовані з повною таємністю.

1.2.6. Ідеальна пряма таємність

Досконала пряма секретність - це функція протоколу, яка використовує або алгоритм обміну ключами Діффі-Хеллмана (DH), або алгоритм обміну ключами Діффі-Хеллмана з еліптичною кривою (ECDH) для генерації тимчасових сеансових ключів. Ідеальна пряма секретність гарантує, що ключ шифрування ніколи не буде передано по з'єднанню.

Натомість і VPN-сервер, і VPN-клієнт самостійно генерують ключ, використовуючи алгоритм DH або ECDH. Це математично складний процес, але

досконала пряма секретність істотно усуває загрозу, що виходить від одного закритого ключа, який у разі злому відкриває доступ до всіх захищених сеансів, які коли-небудь розміщені на сервері. Натомість ключі є тимчасовими. Це означає, що вони можуть розкривати лише один конкретний сеанс і нічого більше. Три VPN-протоколи, які ми завжди рекомендуємо нашим читачам – OpenVPN, WireGuard та IKEv2 – усі підтримують ідеальну пряму секретність.

1.2.7. Аутентифікація з хешу

Алгоритми безпечного хешування (SHA) використовуються для перевірки справжності цілісності даних і з'єднань клієнт-сервер. Вони гарантують, що інформація не була змінена під час передачі між джерелом та одержувачем.

SHA працюють шляхом редагування вихідних даних із використанням так званої хеш-функції. Вихідне повідомлення виконується за допомогою алгоритму, і результатом є рядок символів фіксованої довжини, який зовсім не схожий на оригінал. Це відомо як "хеш-значення".

Це одностороння функція – ви не можете запустити процес видалення хешу, щоб визначити вихідне повідомлення за значенням хешу. Хешування корисне, тому що зміна всього символу вхідних вихідних даних повністю змінить значення хеша, яке виводиться з хеш-функції.

VPN-клієнт оброблятиме дані, отримані з сервера, у поєднанні з секретним ключем, за допомогою хеш-функції, узгодженої під час встановлення зв'язку VPN. Якщо хеш-значення, генероване клієнтом, відрізняється від хеш-значення в повідомленні, дані будуть видалені, оскільки повідомлення було підроблено.

Аутентифікація по хешу SHA запобігає атакам "людина посередині", оскільки здатна виявити будь-яке втручання в дійсний сертифікат. Без цього хакер може видати себе за законний VPN-сервер та обманом змусити вас підключитися до небезпечного, де ваша активність може відстежуватися.

Для забезпечення максимальної безпеки ми рекомендуємо використовувати послуги VPN, що використовують SHA-2 або вище. SHA-1 має доведені недоліки, які можуть поставити під загрозу безпеку.

2 РОЗРОБЛЕННЯ АЛГОРИТМУ РОБОТИ ТА СТРУКТУРНОЇ СХЕМИ ПРИСТРОЮ

2.1 Розробка алгоритму функціонування

Алгоритм роботи Wi-Fi роутера з підтримкою VPN, полягає у наступному (рис. 2.1):

Крок 1: Ініціалізуємо роутер.

Крок 2: Перевіряємо чи ініціалізований роутер, якщо так тоді починаємо, якщо ні – до кроку 1.

Крок 3: Робимо підключення до постачальника інтернет-послуг.

Крок 4: Очікування підключення користувача.

Крок 5: Перевіряємо чи підключений користувач, якщо ні повертаємо на попередній крок.

Крок 6: Перевіряємо, чи запитано включити VPN-функцію, якщо так йдемо до наступного кроку, якщо ні, переходимо до кроку 23, перевіряємо чи вимкнуто VPN, якщо ні очікуємо подальших дій користувача, якщо так завершуємо роботу.

Крок 7: Виконуємо аутентифікацію VPN-сервісу.

Крок 8: Отримуємо дані авторизації від користувача.

Крок 9: Обираємо сервер VPN для підключення.

Крок 10: Перевіряємо з'єднання з сервером VPN, якщо ні робимо повторний запит, крок 11, при негативній відповіді, переходимо до попереднього кроку, якщо позитивний переходимо до наступного кроку.

Крок 12: Виконуємо авторизацію на сервері VPN.

Крок 13: Встановлюємо VPN-тунель між роутером та сервером VPN.

Крок 14: Налаштовуємо шифрування трафіку через VPN-тунель.

Крок 15: Перенаправляємо вхідний трафік через VPN-тунель.

Крок 16: Перенаправляємо вихідний трафік через VPN-тунель.

Крок 17: Налаштовуємо маршрутизацію для зашифрованого трафіку.

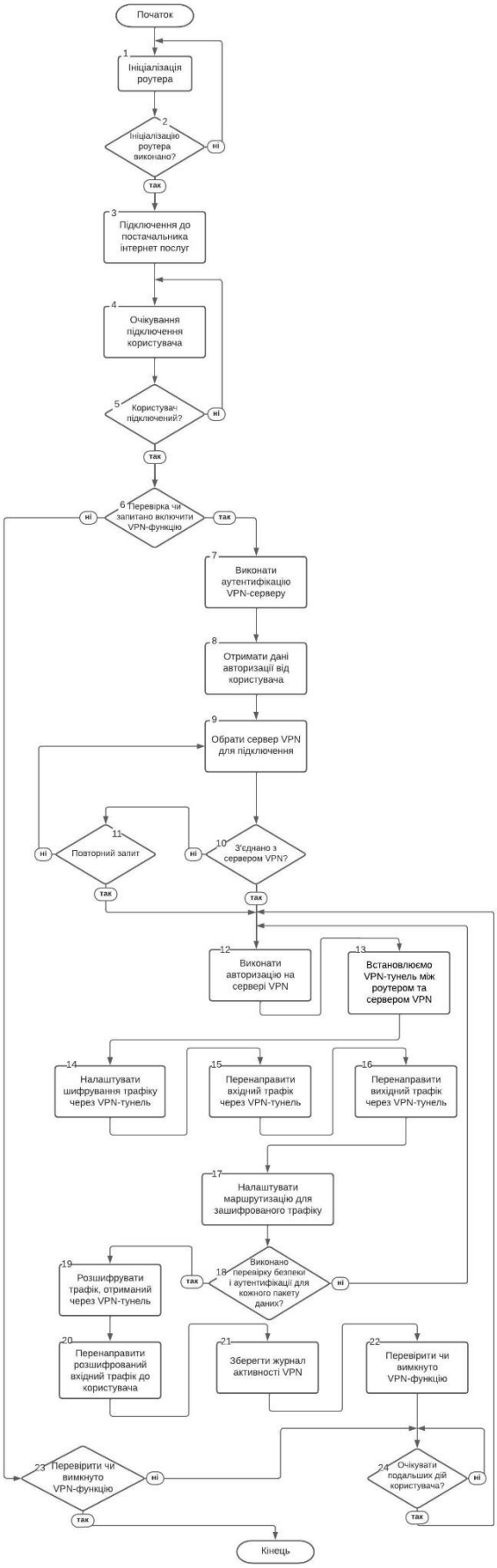


Рисунок 2.1 – Алгоритм функціонування пристрою

Крок 18: Виконуємо перевірку безпеки і аутентифікації для кожного пакету даних, якщо виявлено помилку переходимо до кроку 10, та ще раз встановлюємо з’єднання з VPN сервером, якщо все добре, переходимо до наступного кроку.

Крок 19: Розшифровуємо трафік, отриманий через VPN-тунель.

Крок 20: Перенаправляємо розшифрований вхідний трафік до користувача.

Крок 21: Зберігаємо журнал активності VPN.

Крок 22: Перевіряємо, чи вимкнуто VPN-функцію.

Крок 24: Очікуємо подальших дій користувача, якщо вони є переходимо до кроку 10, та перевіряємо з’єднання VPN серверу, якщо так залишаємось на цьому кроці.

2.2 Обґрунтування структурної схеми

Основне завдання роутера з підтримкою VPN полягає у забезпеченні безпеки, конфіденційності та приватності даних, які передаються через мережу. Він створює захищений тунель між віддаленими мережами або пристроями, що дозволяє передавати дані через незахищені мережі, такі як Інтернет, з використанням шифрування та аутентифікації. VPN-роутер забезпечує конфіденційність даних, захист від несанкціонованого доступу та забезпечує безпеку мережевого зв'язку між різними місцями.

Щоб виконати цю функціональність, мають виконатись наступні дії (рисунок 2.2):

- Отримання та передача даних через мережу. Приймач-передач приймає вхідні пакети даних з зовнішньої мережі та передає їх для подальшої обробки.
- При отриманні пакета, який використовує VPN-протокол, блок аналізу сертифікату та відкритого ключа перевіряє сертифікат та відкритий ключ, які використовуються для аутентифікації та забезпечення безпеки VPN-з'єднання. Це допомагає підтвердити, що з'єднання встановлено з правильним сервером VPN і є безпечним.
- Після аутентифікації блок декапсуляції розбирає отримані пакети VPN і вилучає з них корисну інформацію, включаючи оригінальний IP-заголовок та дані.

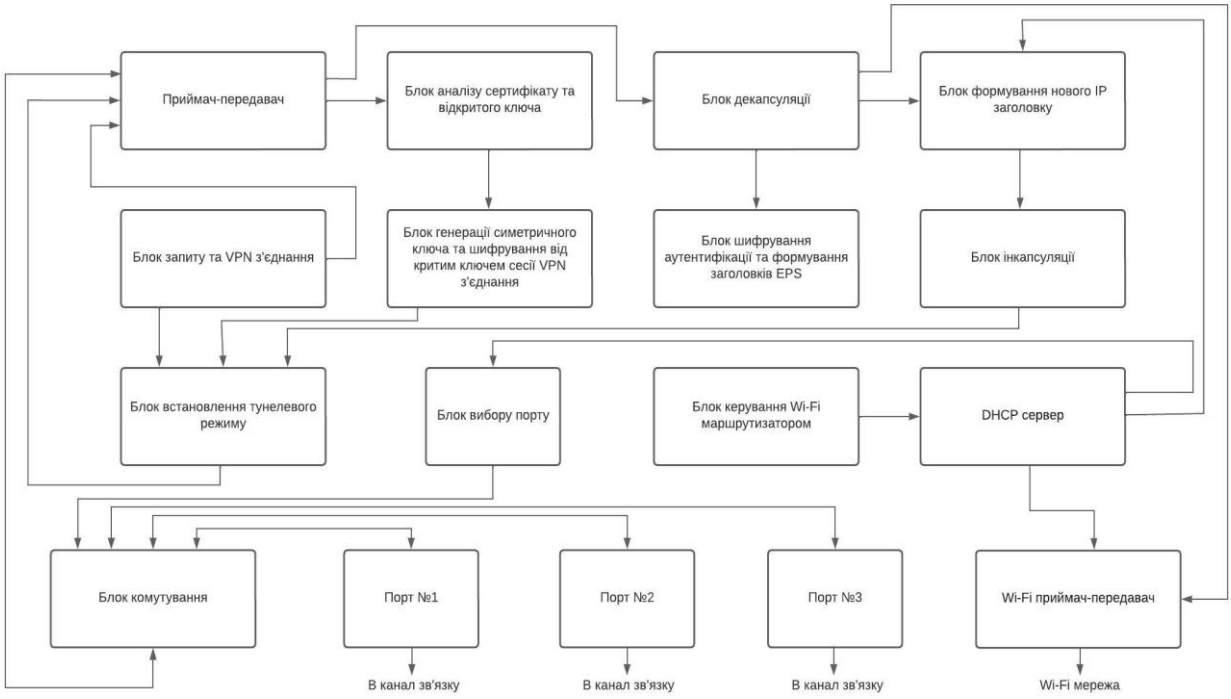


Рисунок 2.2 – Структурна схема пристрою

- Після декапсуляції блок формування нового IP-заголовку створює новий IP-заголовок для даних, що пройшли через VPN. Це дозволяє адресувати пакети для подальшої передачі відповідним чином відповідно до мережевої топології.
- Блок інкапсуляції включає корисну інформацію, що пройшла обробку, у новий пакет з використанням VPN-протоколу. Інкапсуляція включає в себе додавання додаткових заголовків та інформації, необхідних для правильної маршрутизації та обробки пакетів на інших вузлах VPN-мережі.
- Блок шифрування аутентифікації та формування заголовків EPS в свою чергу шифруває корисну інформаці. та додає заголовки для аутентифікації і безпеки VPN-трафіку. Шифрування забезпечує конфіденційність даних, тоді як заголовки дозволяють ідентифікувати та перевіряти цілісність та автентичність пакетів.
- Генерує симетричний ключ для шифрування та розшифрування даних в рамках VPN-з'єднання. Ключ шифрується за допомогою відкритого ключа сесії, який був встановлений під час обміну ключами при налагодженні VPN-з'єднання.
- Потім блок запиту VPN-з'єднання робити ініціювання запиту на встановлення VPN-з'єднання та обмін необхідними даними з сервером VPN для підключення. Він обробляє необхідну протокольну інформацію та налаштовує параметри з'єднання.
- Після успішного запиту та отримання відповіді від сервера VPN, блок встановлення тунелевого режиму встановлює тунелевий режим, який

забезпечує безпеку та приватність даних, що передаються через VPN. Тунель створює захищену "трубку" для передачі даних, яка ізолює їх від зовнішнього середовища.

- Блок вибору порту визначає, які порти будуть використовуватись для вхідного та вихідного трафіку VPN. Він налаштовує маршрутизацію трафіку через відповідні порти, що дозволяє забезпечити правильну передачу даних між зовнішньою мережею та VPN-тунелем.
- Блок керування Wi-Fi маршрутизатором відповідає за керування Wi-Fi-функціональністю роутера, включаючи налаштування безпеки та інших параметрів Wi-Fi-мережі. Він дозволяє налаштовувати режими безпеки, шифрування, доступ до мережі та інші параметри для забезпечення безпеки та зручності використання бездротового з'єднання.
- DHCP-сервер забезпечує автоматичну настройку IP-адрес та інших мережевих параметрів для підключених пристроїв. DHCP-сервер виступає в ролі централізованого джерела настройки мережевих параметрів, спрощуючи процес підключення нових пристроїв до мережі.
- Виконується комутація даних між різними портами та мережами. Він керує передачею даних між пристроями, підключеними до роутера, та дозволяє їм взаємодіяти та обмінюватись інформацією.
- Порт №1, 2, 3, підключають фізичні пристрої до роутера, такі як комп'ютери, телефони, принтери. Кожен порт забезпечує фізичне підключення до мережі та передачу даних між підключеними пристроями.
- Wi-Fi-приймач отримує та передає безпровідний сигналу Wi-Fi. Він приймає бездротовий сигнал від пристроїв, які підключені до Wi-Fi-мережі, та передає їх до роутера для подальшої обробки та передачі даних через мережу.

Встановлення та підтримка VPN-тунелю виконується у два етапи. На першому етапі (фазі) два вузли домовляються про метод ідентифікації, алгоритм шифрування, хеш-алгоритм і групу Diffie-Hellman. Вони також ідентифікують одне одного. Все це може пройти в результаті обміну трьома нешифрованими повідомленнями (так званий агресивний режим, Aggressive mode) або шістьма повідомленнями з обміном зашифрованою інформацією про ідентифікацію (стандартний режим, Main mode).

У режимі Main Mode забезпечується можливість узгодження всіх параметрів конфігурації пристроїв відправника та одержувача, у той час як у режимі Aggressive Mode такої можливості немає, і деякі параметри (група Diffie-Hellman, алгоритми шифрування та аутентифікації, PFS) повинні бути заздалегідь однаково налаштовані на кожному пристрої. Однак, в цьому режимі менше і кількість обмінів, і кількість пакетів, що пересилаються при цьому, в результаті чого потрібно менше часу для встановлення сеансу IPSec.

На другому етапі генеруються дані ключів, вузли домовляються про політику, що використовується. Цей режим, також званий швидким режимом

(Quick mode), відрізняється від першої фази тим, що може встановити лише після першого етапу, коли всі пакети другої фази шифруються. Правильне завершення другої фази призводить до появи Phase 2 SA або IPSec SA і на цьому встановлення тунелю вважається завершеним.

Спочатку на вузол прибуває пакет з адресою призначення в іншій мережі, і вузол ініціює першу фазу з вузлом, який відповідає за іншу мережу. Допустимо, тунель між вузлами був успішно встановлений і чекає на пакети. Однак вузлам необхідно переідентифікувати один одного і порівняти політику за певний період часу. Цей період називається час життя Phase One або IKE SA lifetime.

Вузли також повинні змінити ключ для шифрування даних через час, який називається часом життя Phase Two або IPSec SA lifetime.

Phase Two lifetime коротше, ніж першої фази, т.к. ключ необхідно міняти частіше. Потрібно встановити однакові параметри часу життя для обох вузлів. Якщо цього не виконати, то можливий варіант, коли спочатку тунель буде встановлено успішно, але після першого неузгодженого проміжку часу життя зв'язок перерветься. Проблеми можуть виникнути і в тому випадку, коли час життя першої фази менший за аналогічний параметр другої фази. Якщо налаштований раніше тунель припиняє роботу, то перше, що потребує перевірки – це час життя на обох вузлах.

Ще слід зазначити, що при зміні політики на одному з вузлів зміни набудуть чинності лише за наступного наступу першої фази. Щоб зміни набули чинності негайно, треба забрати SA для цього тунелю з бази даних SAD. Це спричинить перегляд угоди між вузлами з новими налаштуваннями політики безпеки.

Іноді при настроюванні IPSec-тунелю між обладнанням різних виробників виникають труднощі, пов'язані з узгодженням параметрів при встановленні першої фази. Слід звернути увагу на такий параметр, як Local ID – унікальний ідентифікатор кінцевої точки тунелю (відправника та одержувача). Особливо це важливо при створенні кількох тунелів та використанні протоколу NAT Traversal.

3 РОЗРОБЛЕННЯ СХЕМИ ЕЛЕКТРИЧНОЇ ПРИНЦИПОВОЇ ПРИСТРОЮ

3.1 Вибір елементарної бази

Зважаючи на умови побудови пристрою необхідно обрати елементну базу та розробити схему електричну принципову Wi-Fi роутера з підтримкою VPN:

- Флеш-пам'ять
- SDRAM
- Хост-порт USB
- Роз’єм Ethernet
- Зовнішнє джерело живлення
- Програмно-керований перемикач скидання
- Світлодіод
- Антена Wi-Fi
- UART

Wi-Fi роутер з підтримкою VPN, повинен забезпечувати функції відповідних блоків у структурній схемі, а саме:

- Налаштування програмного забезпечення
- Збирання та підтримку передових пакетів
- Підключення до мобільної мережі через USB-модем
- Ethernet-порт, який дозволяє підключати комп'ютери або інші пристрої
- Управління через веб-інтерфейс
- підтримувати функцію прохідний тунель для встановлення безпечного з'єднання між двома віддаленими мережами або пристроями через Інтернет.

Щоб побудувати роутер, слід вибрати мікросхему, на якій буде реалізовано блоки пристрою. Аналізуючи вищезазначені умови та функціонал приладу підібрано таку мікросхему - чіпсета Qualcomm Atheros AR9331, яка включає в себе:

- Процесор Atheros AR7040 400 МГц MISP24kc, інтегрований 802.11n 150 Мбіт/с з вихідною потужністю 20 дБм (100 мВт), який виконує функції обробки даних і керування в рамках чіпсету Qualcomm Atheros AR9331, містить 256 контактів, на яких розташовані входи/виходи, живлення, земля та інші сигнали.
- SDRAM Zentel A3S56D40FTP DDR 256 Мб - оперативна пам'ять (SDRAM) ємністю 256 Мб, яка використовується для зберігання тимчасових даних під час роботи пристрою, у SDRAM використовується типове графічне обозначення для оперативної пам'яті.

- Транзистор 8550M PNP, цей транзистор використовується для здійснення електричного комутації або підсилення сигналів в пристрої.
- SPI флеш-пам’ять S25FL032P 32Mbit, це флеш-пам'ять, яка використовується для зберігання програмного забезпечення і даних, що можуть бути доступні пристрою через протокол SPI.
- Трансформатор Ethernet H1601CG, це трансформатор використовується для забезпечення гальванічної розсічуваності і передачі сигналів Ethernet між різними частинами пристрою.
- Подвійний сигнальний діод Taitron MMBD7000 - подвійний діод використовується для регулювання напруги і перетворення сигналів в пристрої.
- Перемикач живлення з обмеженим струмом TPS204x_205xB - цей перемикач використовується для керування живленням і обмеження струму в пристрої.

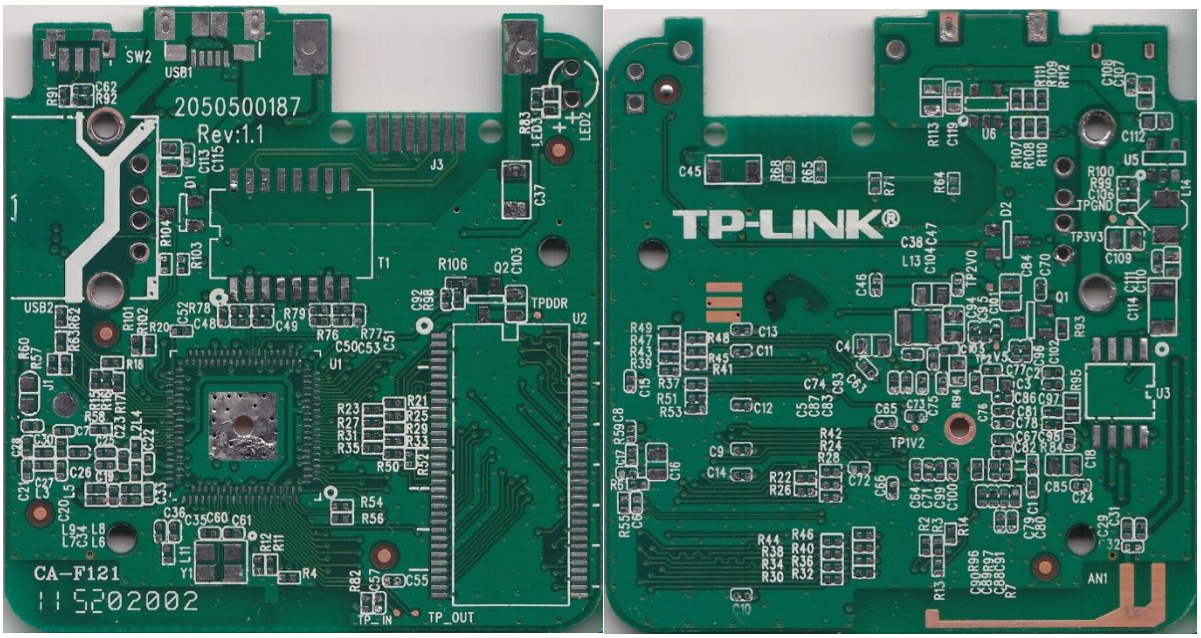


Рисунок 3.1 - Верхня та нижня частина порожньої друкованої плати

Qualcomm Atheros AR9331 оптимально відповідає умовам та функціональним можливостям. Перевагами даного мікроконтролера серед інших аналізованих мікроконтролерів є:

- невеликий розмір;
- низька ціна;
- наявність низхідного USB порту.

3.2 Розрахунок та синтез основних електронних вузлів та блоків пристрою

3.2.1 Мікросхема – чіпсета Qualcomm Atheros AR9331

Atheros AR9331 — це високоінтегрована та економічно ефективна система на чіпі (SoC) IEEE 802.11n 1x1 2,4 ГГц для точки доступу для бездротової локальної мережі (WLAN) і платформ маршрутизатора.

В одному чіпі AR9331 містить процесор MIPS 24K, комутатор Fast Ethernet з п’ятьма портами IEEE 802.3 з MAC/PHY, один USB 2.0 MAC/PHY і інтерфейс зовнішньої пам’яті для послідовного Flash, SDRAM, DDR1 або DDR2, I2S/SPDIF -Вихідний аудіоінтерфейс, інтерфейс SLIC VOIP/PCM, UART і GPIO, які можна використовувати для керування світлодіодами або інших конфігурацій інтерфейсу загального призначення.

AR9331 об’єднує два Gbit MAC плюс п’ятипортовий комутатор Fast Ethernet із двигуном Quality of Service (QoS) із чотирма класами трафіку.

AR9331 інтегрує 802.11n 1x1 MAC/BB/ радіо з внутрішнім PA та LNA. Він підтримує операції 802.11n до 72 Мбіт/с для 20 МГц і 150 Мбіт/с для каналу 40 МГц відповідно, а також швидкість передачі даних IEEE 802.11b/g. Додаткові функції включають вбудовану одноразову програмовану (OTP) пам'ять

Особливості:

- Повна точка доступу IEEE 802.11n 1x1 або маршрутизатор в одному чіпі
- Процесор MIPS 24K, що працює на частоті до 400 МГц
- Зовнішній 16-розрядний інтерфейс пам'яті DDR1, DDR2 або SDRAM
- Підтримка SPI NOR Flash-пам'яті
- Не потрібна зовнішня EEPROM
- 4 Порти LAN і 1 порт WAN Швидкий комутатор IEEE 802.3 Ethernet з автоматичним кросовером, автоматичною полярністю та автоматичним узгодженням у PHY
- Чотири класи QoS на порт
- Повністю інтегрований радіочастотний інтерфейс, включаючи PA та LNA
- Додатковий зовнішній LNA/PA
- Рознесеність комутованих антен
- Високошвидкісний UART для підтримки консолі
- Аудіоінтерфейс I 2 S/SPDIF-out
- SLIC для VOIP/PCM
- Підтримка режиму хост/пристрій USB 2.0
- Підтримка GPIO/LED
- Підтримується налагодження процесора на основі JTAG
- 25 МГц або опорний тактовий вхід 40 МГц

- Розширене управління живленням із динамічним перемиканням годинника для режимів наднизького енергоспоживання
- 148-контактний дворядний пакет LPCC 12 мм x 12 мм

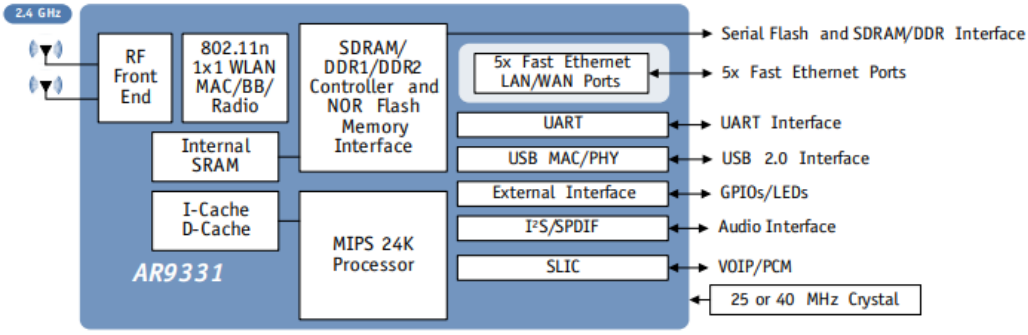


Рис 3.2.2 Блок-схема системи

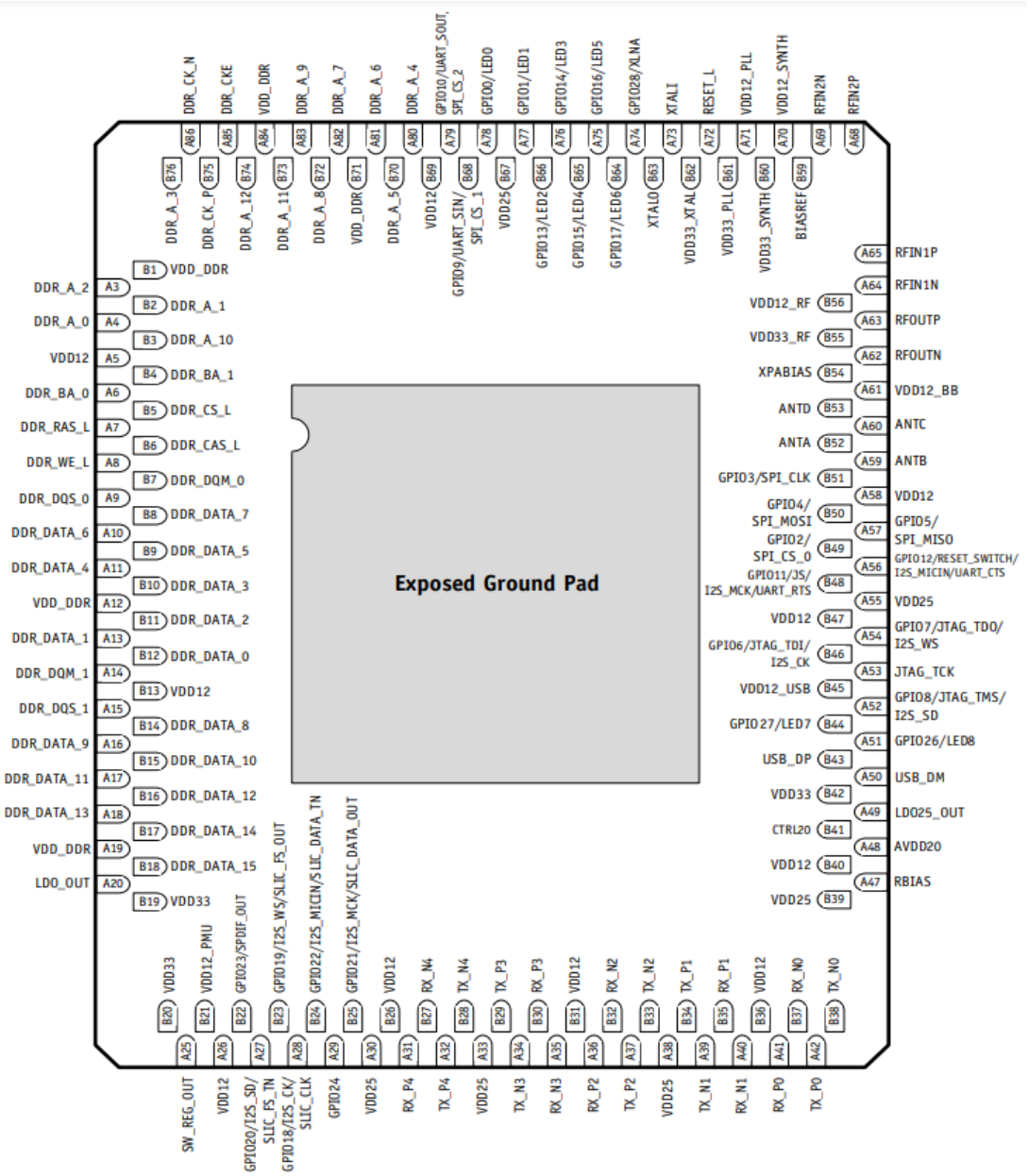


Рис 3.2.3. Дворядна схема розводки LPCC-148 (прозорий вид зверху)

Таблиця 3.2.2 Призначення портів

№ сигналу	Назва сигналу	Тип	Опис
Загальні			
A72	RESET_L	Цифровий вхідний сигнал	Зовнішнє живлення при скиданні
A73	XTALI	Цифровий вхідний сигнал	Кристал 40 МГц або 25 МГц
B63	XTALO	Цифровий вихідний сигнал	
Радіочастоти			
A65	RFIN1P	Аналоговий вхідний сигнал	Перші диференціальні радіочастотні входи
A64	RFIN1N	Аналоговий вхідний сигнал	
A68	RFIN2P	Аналоговий вхідний сигнал	Другі диференціальні радіочастотні входи
A69	RFIN2N	Аналоговий вхідний сигнал	
A63	RFOUTP	Аналоговий вихідний сигнал	Диференціальні радіочастотні виходи
A62	RFOUTN	Аналоговий вихідний сигнал	
Аналоговий інтерфейс			
B59	BIASREF	Аналоговий вхідний сигнал	Напруга зміщення для внутрішніх ПА
B54	XPABIAS	Аналоговий вихідний сигнал	Зміщення для додаткового зовнішнього підсилювача потужності
Управління зовнішнім вимикачем			
B52	ANTA	Цифровий вихідний сигнал	Управління зовнішнім радіочастотним вимикачем
A59	ANTB	Цифровий вихідний сигнал	
A60	ANTC	Цифровий вихідний сигнал	
B53	ANTD	Цифровий вихідний сигнал	
Інтерфейс зовнішньої пам’яті			
A4	DDR_A_O	Цифровий вихідний сигнал	12-бітна зовнішня пам'ять адресна шина
B2	DDR_A_1	Цифровий вихідний сигнал	
A3	DDR_A_2	Цифровий вихідний сигнал	
B76	DDR_A_3	Цифровий вихідний сигнал	
A80	DDR_A_4	Цифровий вихідний сигнал	
B70	DDR_A_5	Цифровий вихідний сигнал	
A81	DDR_A_6	Цифровий вихідний сигнал	
A82	DDR_A_7	Цифровий вихідний сигнал	

B72	DDR_A_8	Цифровий вихідний сигнал	
A83	DDR_A_9	Цифровий вихідний сигнал	
B3	DDR_A_10	Цифровий вихідний сигнал	
B73	DDR_A_11	Цифровий вихідний сигнал	
B74	DDR_A_12	Цифровий вихідний сигнал	
A6	DDR_BA_0	Цифровий вихідний сигнал	2-бітна банківська адреса, щоб вказати, до якого банківського чіпа здійснюється доступ
B4	DDR_BA_1	Цифровий вихідний сигнал	
A85	DDR_CKE	Цифровий вихідний сигнал	Вимикає годинник зовнішньої пам'яті при високому сигналі
B75	DDR_CK_P	Цифровий вихідний сигнал	CK_P і CK_N - це диференціальні тактові входи. Синхронізація всіх адресних і керуючих сигналів пов'язана з перетином позитивного краю CK_P і негативного краю CK_N.
A86	DDR_CK_N	Цифровий вихідний сигнал	
B5	DDR_CS_L	Цифровий вихідний сигнал	Сигнал вибору мікросхеми зовнішньої пам'яті, активний низький
B6	DDR_CAS_L	Цифровий вихідний сигнал	Коли цей сигнал стверджується, він вказує, що адреса є адресою стовпця. Активний, коли сигнал низький.
A7	DDR_RAS_L	Цифровий вихідний сигнал	Коли цей сигнал стверджується, він вказує, що адреса є адресою рядка. Активний, коли сигнал низький.
B12	DDR_DATA_0	Цифровий двонаправлений сигнал	16-бітна шина даних зовнішньої пам'яті
A13	DDR_DATA_1	Цифровий двонаправлений сигнал	
B11	DDR_DATA_2	Цифровий двонаправлений сигнал	
B10	DDR_DATA_3	Цифровий двонаправлений сигнал	
A11	DDR_DATA_4	Цифровий двонаправлений сигнал	
B9	DDR_DATA_5	Цифровий двонаправлений сигнал	

A10	DDR_DATA_6	Цифровий двонаправлений сигнал	
B8	DDR_DATA_7	Цифровий двонаправлений сигнал	
B14	DDR_DATA_8	Цифровий двонаправлений сигнал	
A16	DDR_DATA_9	Цифровий двонаправлений сигнал	
B15	DDR_DATA_10	Цифровий двонаправлений сигнал	
A17	DDR_DATA_11	Цифровий двонаправлений сигнал	
B16	DDR_DATA_12	Цифровий двонаправлений сигнал	
A18	DDR_DATA_13	Цифровий двонаправлений сигнал	
B17	DDR_DATA_14	Цифровий двонаправлений сигнал	
B18	DDR_DATA_15	Цифровий двонаправлений сигнал	
B7	DDR_DQM_0	Цифровий вихідний сигнал	Маска даних DDR для даних з низькими байтами
A14	DDR_DQM_1	Цифровий вихідний сигнал	Маска даних DDR для високих байтів даних
A9	DDR_DQS_0	Цифровий двонаправлений сигнал	Стробоскоп даних DDR для даних з низькими байтами
A15	DDR_DQS_1	Цифровий двонаправлений сигнал	Стробоскоп даних DDR для високих байтів даних
A8	DDR_WE_L	Цифровий вихідний сигнал	Коли цей сигнал стверджується, він вказує на те, що наступна транзакція є записом. Активний, коли сигнал низький.
Комутатор Ethernet			
A42	TX_P0	Аналоговий вихідний сигнал	Передавальна пара порту Ethernet 0
B38	TX_N0	Аналоговий вихідний сигнал	
A41	RX_P0	Аналоговий вхідний сигнал	Порт Ethernet 0 отримує пару
B37	RX_N0	Аналоговий вхідний сигнал	
B34	TX_P1	Аналоговий вихідний сигнал	Передавальна пара порту Ethernet 1
A39	TX_N1	Аналоговий вихідний сигнал	
B35	RX_P1	Аналоговий вхідний сигнал	

A40	RX_N1	Аналоговий вхідний сигнал	Порт Ethernet 1 отримує пару
A37	TX_P2	Аналоговий вихідний сигнал	Передавальна пара порту Ethernet 2
B33	TX_N2	Аналоговий вихідний сигнал	
A36	RX_P2	Аналоговий вхідний сигнал	Порт Ethernet 2 отримує пару
B32	RX_N2	Аналоговий вхідний сигнал	
B29	TX_P3	Аналоговий вихідний сигнал	Передавальна пара порту Ethernet 3
A34	TX_N3	Аналоговий вихідний сигнал	
B30	RX_P3	Аналоговий вхідний сигнал	Порт Ethernet 3 отримує пару
A35	RX_N3	Аналоговий вхідний сигнал	
A32	TX_P4	Аналоговий вихідний сигнал	Передавальна пара порту Ethernet 4
B28	TX_N4	Аналоговий вихідний сигнал	
A31	RX_P4	Аналоговий вхідний сигнал	Порт Ethernet 4 отримує пару
B27	RX_N4	Аналоговий вхідний сигнал	
Інтерфейс введення/виведення загального призначення (GPIO)			
A78	GPIO0	Цифровий двонаправлений сигнал	Мультиплексований контакт GPIO
A77	GPIO1	Цифровий двонаправлений сигнал	
B49	GPIO2	Цифровий двонаправлений сигнал	
B51	GPIO3	Цифровий двонаправлений сигнал	
B50	GPIO4	Цифровий двонаправлений сигнал	
A57	GPIO5	Цифровий двонаправлений сигнал	
B46	GPIO6	Цифровий двонаправлений сигнал	
A54	GPIO7	Цифровий двонаправлений сигнал	
A52	GPIO8	Цифровий двонаправлений сигнал	
B68	GPIO9	Цифровий двонаправлений сигнал	
A79	GPIO10	Цифровий двонаправлений сигнал	
B48	GPIO11	Цифровий двонаправлений сигнал	

A56	GPIO12	Цифровий двонаправлений сигнал	
B66	GPIO13	Цифровий двонаправлений сигнал	
A76	GPIO14	Цифровий двонаправлений сигнал	
B65	GPIO15	Цифровий двонаправлений сигнал	
A75	GPIO16	Цифровий двонаправлений сигнал	
B64	GPIO17	Цифровий двонаправлений сигнал	
A28	GPIO18	Цифровий двонаправлений сигнал	
B23	GPIO19	Цифровий двонаправлений сигнал	
A27	GPIO20	Цифровий двонаправлений сигнал	
B25	GPIO21	Цифровий двонаправлений сигнал	
B24	GPIO22	Цифровий двонаправлений сигнал	
B22	GPIO23	Цифровий двонаправлений сигнал	
A29	GPIO24	Цифровий двонаправлений сигнал	
A51	GPIO26	Цифровий двонаправлений сигнал	
B44	GPIO27	Цифровий двонаправлений сигнал	
A74	GPIO28	Цифровий двонаправлений сигнал	
Спільна група випробувань (JTAG)			
A53	JTAG_TCK	Цифровий вхідний сигнал	Тестове тактування
B46	JTAG_TDI	Цифровий вхідний сигнал	Вхід тестових даних
A54	JTAG_TDO	Цифровий вихідний сигнал	Вихід тестових даних
A52	JTAG_TMS	Цифровий вхідний сигнал	Вибір режиму тестування
Світлодіод (LED)			
A78	LED0	Відкритий сток	WLAN LED1
A77	LED1	Відкритий сток	WLAN LED2

B66	LED2	Відкритий сток	Комутатор Ethernet LED1
A76	LED3	Відкритий сток	Комутатор Ethernet LED2
B65	LED4	Відкритий сток	Комутатор Ethernet LED3
A75	LED5	Відкритий сток	Комутатор Ethernet LED4
B64	LED6	Відкритий сток	Комутатор Ethernet LED5
B44	LED7	Відкритий сток	LED
A51	LED8	Відкритий сток	LED
Звук Inter-IC/формат цифрового інтерфейсу Sony/Philips (I2S/SPDIF)			
A28, B46	I2S_CK	Цифровий вихідний сигнал	Стереогодинник
B25, B48	I2S_MCK	Цифровий вихідний сигнал	Майстер-годинник
A56, B24	I2S_MICIN	Цифровий вхідний сигнал	Введення даних
A27, A52	I2S_SD	Цифровий двонаправлений сигнал	Введення/виведення послідовних даних
A54, B23	I2S_WS	Цифровий вихідний сигнал	Вибір стерео у програмі Word 0 Лівій 1 Правий
B22	SPDIF_OUT	Цифровий вихідний сигнал	Вихід динаміка
Послідовний інтерфейс			
B51	SPI_CLK	Цифровий вихідний сигнал	Послідовний тактовий сигнал SPI
B49	SPI_CS_0	Цифровий вихідний сигнал	Вибір чіпа SPI
B68	SPI_CS_1	Цифровий вихідний сигнал	
A79	SPI_CS_2	Цифровий вихідний сигнал	
A57	SPI_MISO	Цифровий вихідний сигнал	Передача даних від AR9331 до зовнішнього пристрою. Після скидання SPI_MOSI (GPIO_4) вводиться і SPI_MISO (GPIO_5) виводиться, щоб він міг безпосередньо взаємодіяти з пристроєм SPI, таким як послідовний спалах. Якщо послідовний спалах не використовується, ці контакти можуть використовуватися як контакти GPIO.
B50	SPI_MOSI	Вхідні сигнали зі слабким внутрішнім розтягуванням, щоб запобігти плаваючим	Передача даних від зовнішнього пристрою до пристрою AR9331. Після скидання SPI_MOSI

		сигналам, якщо вони залишаються відкритими	(GPIO_4) вводиться і SPI_MISO (GPIO_5) виводиться, щоб він міг безпосередньо взаємодіяти з пристроєм SPI, таким як послідовний спалах. Якщо послідовний спалах не використовується, ці контакти можуть використовуватися як контакти GPIO.
Таблиця опису ліцензування програмного забезпечення (SLIC)			
A28	SLIC_CLK	Цифровий вихідний сигнал	Послідовний тактовий сигнал
B23	SLIC_FS_OUT	Цифровий вихідний сигнал	Синхронізація кадрів зовні
A27	SLIC_FS_IN	Цифровий вхідний сигнал	Синхронізація кадрів всередині
B25	SLIC_DATA_OUT	Цифровий вихідний сигнал	Дані, передані з AR9331 до SLIC
B24	SLIC_DATA_IN	Цифровий вхідний сигнал	Дані, передані з SLIC до AR9331
Універсальний асинхронний приймач/передавач (UART)			
A56	UART_CTS	Цифровий вхідний сигнал	Чистий UART для відправки сигналу
B48	UART_RTS	Цифровий вихідний сигнал	Готовий UART для відправки сигналу (опціональний контакт інтерфейсу UART)
B68	UART_SIN	Цифровий вхідний сигнал	Вхід серійних даних
A79	UART_SOUT	Цифровий вихідний сигнал	Вихід серійних даних
USB			
A50	USB_DM	Аналоговий вхідний сигнал/ Аналоговий вихідний сигнал	Сигнал USB D-, переносить дані USB до та з USB 2.0 PHY
B43	USB_DP	Аналоговий вхідний сигнал/ Аналоговий вихідний сигнал	Сигнал USB D+, переносить дані USB до та з USB 2.0 PHY
Живлення (Power)			
A48	AVDD20		Регульоване джерело живлення 2,0; підключається до зовнішнього колектора PNP.
B41	CTRL20		Зовнішнє управління PNP. Підключається до бази зовнішнього PNP, колектора

			до AVDD20 і випромінювача до VDD33.
A20	LDO_OUT		Зовнішнє джерело живлення. Цей контакт може бути налаштований на вихід від 1,8 В до 3,0 В, а також живити DDRIO та зовнішню пам'ять.
A49	LDO25_OUT		2.62 V вихідна потужність для цифрового вводу-виводу.
A47	RBIAS		Підключіться до 2,43 K□ ±1% резистора до землі
A25	SW_REG_OUT		1.2 V Вихід регулятора комутації
A5, B13, A26, B26, B31, B36, B40, B47, A58, B69	VDD12		1.2 V блок живлення для цифрового Ethernet-комутатора
A61	VDD12_BB		Аналоговий блок живлення 1,2 В
A71	VDD12_PLL		
B21	VDD12_PMU		
B56	VDD12_RF		
A70	VDD12_SYNTH		
B45	VDD12_USB		
A30, A33, A38, B39, A55, B67	VDD25		Живлення цифрового комутатора Ethernet
B19, B20, B42	VDD33		3.3 V Живлення
B61	VDD33_PLL		Аналоговий блок живлення 3,3 В
B55	VDD33_RF		
B60	VDD33_SYNTH		
B62	VDD33_XTAL		
B1, A12, A19, B71, A84	VDD_DDR		Блок живлення зовнішньої пам'яті
Поверхня			
-	GND		Відкрита наземна подушка
Інше			

B48	JS	Цифровий двонаправлений сигнал	Мультиплексована функція для Jumpstart
A56	RESET_SWITCH	Цифровий двонаправлений сигнал	Для зовнішнього кнопкового перемикача; скидає мікропрограму до конфігурації за замовчуванням при натисканні

Функціональний опис, внутрішня структура мікроконтролера AR9331. Рисунок 3.2.4 демонструє функціональну блок-схему AR9331.

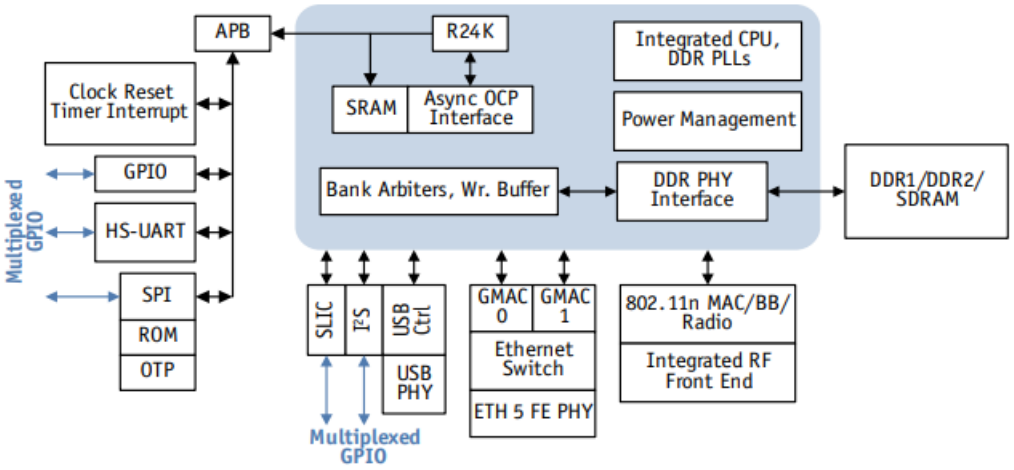


Рисунок 3.2.4. Функціональна структурна схема AR9331

Таблиця 3.2.3 підсумовує функціональні блоки, які включають AR9331.

Таблиця 3.2.3 Описи функціональних блоків

Блок	Опис
CPU	Цей процесор MIPS 24 K може працювати до 400 МГц. Він включає 4-сторонній набір асоціативного кешу інструкцій, 4-позиційний набір асоціативних кешів даних, одноциклове множення-накопичення, а також набори інструкцій MIPS32 і MIPS16. Також підтримуються неблокуючі зчитування кешу.
Контролер пам'яті	AR9331 має два інтерфейси зовнішньої пам'яті. Вони складаються з 16-бітного інтерфейсу пам'яті DDR1 / DDR2 або SDRAM, що підтримує швидкість до 400 Мбіт / контакт, і спалаху типу SPI NOR. AR9331 також містить внутрішню оперативну пам'ять.
Швидкий комутатор Ethernet	AR9331 підтримує чотири порти локальної мережі та один порт WAN з інтегрованим PHY. Підтримується світлодіодна індикація для кожного порту. Чотири порти локальної мережі підключаються до центрального процесора через інтерфейс GMII, і в кожному порту локальної мережі підтримуються чотири пріоритети черги Tx. Порт WAN можна налаштувати для підключення до центрального процесора за допомогою спеціального інтерфейсу MII. Інтерфейс MII може підтримувати до

	чотирьох пріоритетних черг, з простим пріоритетом або зваженим круговим механізмом арбітражу. Підтримуються функції комутатора, такі як QoS і VLAN.
GPIO	28 мультиплексованих контактів GPIO можна використовувати як UART, флеш-інтерфейс SPI, JTAG та аудіоінтерфейс I2S / SPDIF-вихід
I^2S/SPDIF	I^2S/SPDIF вихідний аудіоінтерфейс, що підтримує тактову дискретизацію до 48 кГц і послідовну частоту дискретизації понад 512 *. Він також підтримує плавне перемикання потоку аудіовиходу з I^2S на SPDIF. Також підтримується мікрофон I2S. Може генерувати послідовний годинник для різних частот дискретизації.
SLIC	Інтерфейс SLIC з підтримкою: - Як головний, так і підлеглий режими - Налаштовувана кількість активних слотів - Режими внутрішньої або зовнішньої синхронізації кадрів - Підтримка різної ширини синхронізації кадрів; ширина півбітової тактової частоти, ширина годинника в один біт тощо. - Режими передачі даних із затримкою/без затримки - Як внутрішній, так і зовнішній бітовий годинник; Внутрішня тактова частота програмується - Програми VOIP - Як Rx, так і Tx на різних слотах (настроювані слоти)
SPI	SPI інтерфейс, який можна використовувати для послідовного Flash
USB	Інтерфейс універсальної послідовної шини 2.0 підтримує режим хост/пристрій
Wireless MAC/BB/Radio	Інтегрований 2.4 ГГц 802.11n 1x1 MAC/базовий діапазон/радіо та радіочастотний інтерфейс

Конфігурації

Таблиця 3.2.4 підсумовує параметри конфігурації, що використовуються AR9331. Після скидання процесор виводить адресу 0xBFC00000, яка зіставлена з адресним простором флеш-пам'яті або внутрішнім кодом ПЗУ, використовуючи зовнішній регістр витягування вгору / вниз, щоб вибрати, чи буде AR9331 завантажуватися з Flash або внутрішнього ПЗУ. Процесор AR9331 підтримує тактову частоту до 400 МГц.

Таблиця 3.2.4. Основні параметри конфігурації процесора

Параметр	Опис
Розмір кеша	AR9331 реалізує 4-сторонній набір асоціативного кешу інструкцій і чотиристоронній набір асоціативного кешу даних. Він підтримує одноциклове множення-накопичення, набори інструкцій MIPS32 і MIPS16 і неблокуюче кешоване зчитування.
Endian	AR9331 реалізує велику ендіанську адресацію.
Адресація блоків	AR9331 реалізує послідовне впорядкування.

Адресна карта

Адресний простір AR9331 розділений на три регіони. Перший регіон відображає в пам'яті DDR. Друга регіональна карта – до реєстрів APB, а третя – до реєстрів AHB. На рисунку 3.5 зображено розподіл адресного простору.

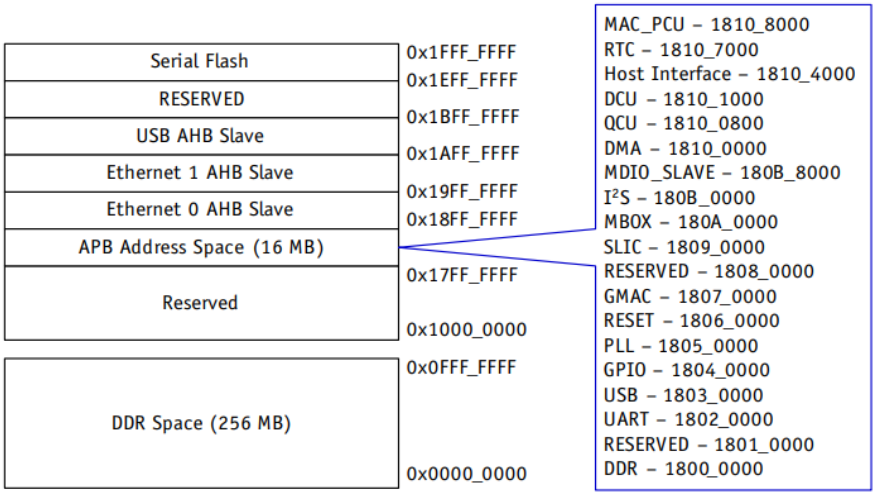


Рисунок 3.2.5 Виділення адресного простору

AHB Master Bus

Деякі головні пристрої AHB підключаються до внутрішнього головного інтерфейсу DDR AHB, наприклад USB, GE0, GE1 WLAN, MAC тощо. AHB кожен з модулів головної шини містить DMA для переміщення даних, наприклад дескрипторів, підготовлених центральним процесором, між головними модулями AHB і зовнішньою пам’яттю.

Міст APB

Одне 16-мегабайтне вікно адресного простору AHB присвячено картографу пристрою APB. Простір APB містить адресні простори реєстрів більшості інтерфейсів, включаючи послідовний флеш, GPIO та UART. Цей простір також забезпечує доступ до сторожового таймера та чотирьох таймерів загального призначення.

Контролер пам'яті DDR

AR9331 підтримує 16-розрядний інтерфейс пам'яті DDR до 64 Мбайт пам'яті в одному пристрої. Він підтримує один виділений інтерфейс «точка-точка» для ЦП тощо виділені інтерфейси точка-точка для ЦП, USB, Ethernet. Транзакції запису буферизуються на кожному інтерфейсі. Він реалізує окремий арбітраж для кожного банку, що забезпечує ефективне конвеєрне планування RAS/CAS/попереднього нарахування.

Блок DDR має п'ять підлеглих інтерфейсів AHB для: GE0, GE1, USB, WLAN і CPU. Зовнішній DDR живиться від AR9331 за допомогою зовнішнього силового транзистора. Таблиця 3.2.5 показує конфігурації DDR.

Таблиця 3.2.5 Конфігурації DDR

Вид девайсу	Кількість пристроїв	Тип пристрою
64 Mbits (4 M x 16)	1	DDR1
128 Mbits (8 M x 16)	1	DDR1
256 Mbits (16 M x 16)	1	DDR1
512 Mbits (32 M x 16)	1	DDR1
256 Mbits (16 M x 16)	1	DDR2
512 Mbits (32 M x 16)	1	DDR2

У таблиці 3.2.6 наведено відповідність внутрішнього адреси процесора, адреси інтерфейсу DDR і адреси фізичної пам'яті.

Таблиця 3.2.6. Зіставлення адрес

Біт адреси CPU	Адреса інтерфейсу DDR	Відповідна 16-бітна адреса пам'яті DDR
0	DDR_A_0, Unused (x16 DRAM)	
1	DDR_A_1	CAS0
2	DDR_A_2	CAS1
3	DDR_A_3	CAS2
4	DDR_A_4	CAS3
5	DDR_A_5	CAS4
6	DDR_A_6	CAS5
7	DDR_A_7	CAS6
8	DDR_A_8	CAS7
9	DDR_A_9	CAS8
10	DDR_A_0	RAS0
11	DDR_BA_0	BA0
12	DDR_BA_1	BA1
13	DDR_A_1	RAS1
14	DDR_A_2	RAS2
15	DDR_A_3	RAS3
16	DDR_A_4	RAS4
17	DDR_A_5	RAS5

18	DDR_A_6	RAS6
19	DDR_A_7	RAS7
20	DDR_A_8	RAS8
21	DDR_A_9	RAS9
22	DDR_A_10	RAS10
23	DDR_A_11	RAS11
24	DDR_A_12	RAS12
25	DDR_A_11	CAS9
26	DDR_A_12	CAS11

UART

AR9331 містить один еквівалентний порт UART 16550 для налагодження/консолі. Виводи UART мультиплексуються з виводами GPIO, тому «Функція вводу-виводу загального призначення (GPIO_FUNCTION_1)» на сторінці 67 вказує, які біти регістрів керують виводами GPIO, які використовуються для функцій UART.

GE0 і GE1

AR9331 об'єднує дві ГБ MAC-карт Ethernet, підключені до комутатора Ethernet. GE0 і GE1 підтримують 2 K, передають FIFO і 2 K отримують FIFO. Порт WAN - це інтерфейс MII, який підключається безпосередньо до PHY всередині комутатора Ethernet. Інший порт підключається до комутатора Ethernet за допомогою інтерфейсу GMII. Через комутатор Ethernet цей порт підключається до чотирьох портів LAN. WAN Ethernet PHY (PHY0) AR9331 може підключатися безпосередньо до комутатора як інший порт, або може бути безпосередньо до центрального процесора через інтерфейс MII.

Інтерфейси PHY (PHY0, PHY1, PHY2, PHY3 і PHY4) можуть підключатися до комутатора в режимі моста. У цьому випадку GE0 повинен бути скинутий. Всі п'ять портів LAN комутуються разом і підключаються до центрального процесора через інтерфейс GMII (MAC0), який управляється бітом ETH_CFG регістра SW_ONLY_MODE. Якщо GE0 підключається окремо до PHY, то MAC5 слід скинути.

Інтерфейс GMII і MII MAC до комутатора Ethernet підтримує чотири черги Tx, кожна з яких має свій власний ланцюжок дескрипторів. Пріоритет DMA_TX_Q0 вище, ніж DMA_TX_Q1 і так далі. Регістри конфігурації DMA є окремими для кожної черги. Підтримуються два арбітражні механізми: один є простим пріоритетом, а інший - зваженим круговим арбітражем.

Аналогічно і для решти черг. У разі кругового арбітражу в довгостроковій перспективі кількість пакетів, що відправляються в чергу, гарантовано буде в

співвідношенні запрограмованих ваг. Вага НУЛЯ заборонена. Слід зазначити, що ваги вказані на пакетній основі, а не на кількості байтів, переданих у цій черзі. Крім того, 19-бітний лічильник вільного ходу (працює на AHB_CLK) оновлюється в полі дескриптора, як показано нижче як на дескрипторі передачі, так і на прийомі. Це оновлення виконується як частина оновлення дескриптора, яке ядро MAC DMA вже робить після завершення передачі або прийому. Програмне забезпечення може відстежувати затримку на основі пакета за допомогою цього дескриптора Мітка часу та регістра безкоштовного таймера.

Інтерфейс MDC/MDIO

Інтерфейс MDC/MDIO, який є внутрішнім для AR9331, дозволяє користувачам отримувати доступ до внутрішніх регістрів Ethernet MAC/PHY. Внутрішні комутаторні регістри мають ширину 32 біта, але доступ MDIO має ширину лише 16 біт, тому для доступу до всіх 32 біт внутрішніх регістрів потрібно два цикли доступу. Адресний інтервал більше, ніж 10 біт, підтримуваних MDIO, тому верхні біти адреси повинні бути записані у внутрішні регістри, подібно до методу доступу до режиму сторінки.

Контролер комутатора Ethernet

На рисунку 3.6 представлена структурна схема Ethernet Switch.

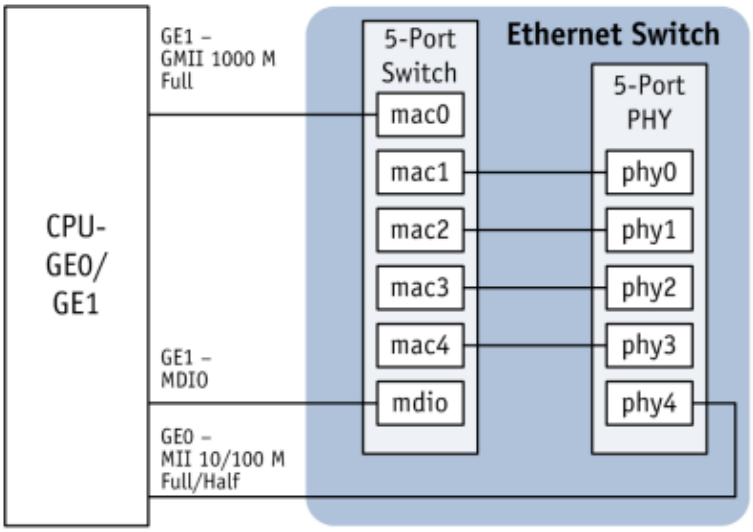


Рис. 3.2.6. Структурна схема комутатора Ethernet

Контролер Ethernet Switch виконує більшість комутаційних функцій AR9331. Контролер містить п'ять портів швидкого Ethernet зі швидкістю 10/100 Мбіт/с, кожен з яких містить чотири рівні якості обслуговування, 802.1Q VLAN, VLAN на основі портів і лічильники статистики RMON. AR9331 об'єднує п'ять двошвидкісних приймачів-передавачів Ethernet (PHY) 10/100 і один однопортовий 10/100/1000 контролерів доступу до медіа (MAC), а також тканину спільного перемикача пам'яті з нульовою швидкістю дроту, що не блокує.

Таблиця пошуку адрес запису розміром 1 КБ використовує два записи на сегмент, щоб уникнути хеш-зіткнень і підтримувати продуктивність пересилання пакетів. Таблиця введення адреси надає доступ для читання/запису з послідовного інтерфейсу та інтерфейсу процесора, де кожен запис може бути налаштований як статичний запис. 1024 MAC-адреси підтримуються підтримкою автоматичного навчання, старіння та статичної адреси. Комутатор Ethernet також підтримує основні функції комутатора, включаючи дзеркальне відображення портів, підтримку трансляції штормів, управління потоком у повнодуплексному режимі та протитиск у напівдуплексі, автоматичне узгодження 802.3, блокування портів, лічильники MIB, обмеження швидкості входу та вихідної швидкості, а також автоматичний зв'язок швидкості та дуплексу між фізичними та MAC-адресами. У таблиці 3.2.7 зведені функції комутатора Ethernet AR9331.

Таблиця 3.2.7. Комутатор Ethernet

Блок	Опис
Контролери доступу до медіа (MAC)	AR9331 об'єднує шість незалежних швидких MAC-карт Ethernet, які виконують всі функції специфікацій IEEE 802.3 та IEEE 802.3u, включаючи форматування кадрів, зачистку кадрів, перевірку CRC, CSMA/CD, обробку зіткнень та контроль потоку зворотного тиску тощо. Кожна MAC-картка підтримує роботу 10 Мбіт/с або 100 Мбіт/с у повнодуплексному або напівдуплексному режимі.
Повнодуплексний контроль потоку	Пристрій AR9331 підтримує повнодуплексне регулювання потоку IEEE 802.3x, повнодуплексне регулювання потоку в примусовому режимі та напівдуплексний протитиск. Якщо партнер по каналу підтримує автоматичне узгодження, повнодуплексне керування потоком 802.3x автоматично веде переговори між віддаленим вузлом і AR9331. Якщо ввімкнено повнодуплексне керування потоком, коли вільний буферний простір майже порожній, AR9331 надсилає сумісну з IEEE 802.3x ПАУЗУ, щоб зупинити віддалений пристрій від надсилання більшої кількості кадрів.
Напівдуплексний контроль потоку	Напівдуплексний контроль потоку регулює віддалену станцію, щоб уникнути падіння пакетів під час перевантаження мережі. Функція зворотного тиску підтримується для напівдуплексних операцій. Коли вільний буферний простір майже порожній, пристрій AR9331 передає малюнок застрягання на порту і змушує до зіткнення. Якщо режим напівдуплексного управління потоком не встановлений, вхідний пакет відпадає, якщо немає буферного простору.
Міжпакетний розрив (IPG)	IPG - це час простою між будь-яким і послідовним пакетами з одного порту. Типовий IPG становить 9,6 мкс для 10 Мбіт/с Ethernet і 960 мкс для 100 Мбіт/с для швидкого Ethernet 100 Мбіт/с.
Блокування портів	AR9331 підтримує блокування портів. Якщо один порт встановлений для блокування порту, можуть бути відправлені тільки отримані кадри з адресою джерела unicast, знайдені в таблиці ARL і не мають порушення члена. Інші заблоковані кадри скидаються або перенаправляються на порт процесора регістром управління, LOCK_DROP_EN.
Запобігання переадресації кадрів	AR7240 може бути налаштований таким чином, щоб запобігти пересиланню одноадресних або багатоадресних кадрів, які містять невідому адресу призначення. Це може бути зроблено на основі кожного порту, так що кадри

	з невідомими адресами виходять тільки в порт, де підключений сервер або маршрутизатор. Широкомовні кадри, переадресовані на порт процесора, також можна запобігти.
Незаконні кадри	AR7240 відкидає всі незаконні кадри, такі як помилка CRC, великі пакети (довжина більше максимальної довжини) і виконані пакети (довжина менше 64 байт).

VLAN для портів локальної мережі

Комутатор підтримує 16 VLAN IEEE 802.1Q і функціональність VLAN на основі портів для всіх кадрів, включаючи кадри управління, коли 802.1Q включено на вхідному порту.

Кадри без тегів відповідають VLAN на основі порту, навіть якщо вхідний порт має ввімкнений режим 802.1Q. Дивіться таблицю 3.2.8

Таблиця 3.2.8. Комутатор Ethernet VLAN

VLAN	Опис
На базі порту	Кожен вхідний порт містить регістр, що обмежує вихідні (або вихідні) порти, на які він може надсилати кадри. Цей регістр VLAN на основі порту має поле PORT_VID_MEM, яке містить параметр на основі порту. Якщо біт PORT_VID_MEM встановлений рівним одиниці, порту дозволяється відправляти кадри в порт 0, біт в порт 2 і так далі. Під час скидання PORT_VID_MEM кожного порту встановлюється на значення всіх 1, за винятком власного біта кожного порту, який очищається до нуля. Зверніть увагу, що порт процесора - це порт 0.
IEEE 802.1QVLANs	AR9331 підтримує максимум 16 записів у таблиці VLAN. Пристрій підтримує діапазон ідентифікаторів VLAN 4096 від 0 до 4095. AR9331 підтримує лише спільне навчання VLAN (SVL). Це означає, що рішення про переадресацію базуються на MAC-адресі призначення кадру, яка повинна бути унікальною серед усіх VLAN.

Додавання тегів та видалення тегів вихідних кадрів підтримується за допомогою 802.1Q VLAN або статично за допомогою VLAN на основі портів. Рамки можуть виходити з вимикача трьома способами:

- Передавати без змін
  Кадри без тегів виходять з порту без тегів, тоді як кадри з тегами залишають теговані.
- Передавати без тегів
  Кадри без тегів залишають порт незмінним, тоді як кадри з тегами залишають без тегів.
- Передати з тегами
  Кадри з тегами залишають порт незмінним, тоді як тег IEEE додається до кадрів без тегів перед виходом.

Коли тег додається до кадру без тегів, кадр вставляється безпосередньо після вихідної адреси кадру та містить чотири байти.

- Перший байт завжди 0x81.
- Другий байт завжди 0x00.
- Біти PRI вказують на пріоритет кадру, визначений параметром пріоритету вихідного порту.
- Біт CFI завжди встановлюється на 0.

Біти VID вказують на VID, призначений кадру, як визначено у вихідному порту за замовчуванням VID.

Кадр із тегами, що залишає порт з тегами, може мати змінені біти VID. Якщо VID вхідного кадру був 0x000, замість цього кадру призначається VID порту входу за замовчуванням. Подвійне маркування - це метод ізоляції одного IEEE 802.1Q VLAN від іншого IEEE 802.1Q.

VLAN ієрархічним способом, сумісним з комутаторами, готовими до IEEE 802.1Q, якщо ці комутатори підтримують максимальний розмір кадру 1526 байт або більше. Таким чином, додатковий або подвійний тег розміщується перед нормальним тегом кадру, тим самим збільшуючи розмір кадру на чотири байти.

Подвійне маркування можна вибрати на основі порту за портом. Як правило, для будь-якого порту, у якому ввімкнено подвійне додавання тегів, також увімкнено подвійне додавання тегів. Порти з увімкненим подвійним тегуванням вхідного копіювання очікують, що всі вхідні кадри міститимуть додатковий тег, який необхідно видалити з кадру перед виконанням політики проникнення порту у кадр. У цьому режимі політика входу видаляє перший тег IEEE 802.3ac, який з'являється після адреси джерела в кожному кадрі. Якщо кадр без тегів не змінено, перемикач ігнорує всі дані з вилучених тегів.

Якість обслуговування (QoS) для портів локальної мережі

AR9331 розпізнає QoS-інформацію вхідних кадрів і відображає різні рівні вихідного пріоритету. AR9331 визначає пріоритет кадрів на основі DA, TOS/TC, VLAN та порту. Кожен з них має біт включення, який можна застосувати. Якщо вибрано більше одного типу пріоритету, можна визначити порядок, у якому слід застосовувати пріоритет кадру. Пріоритетні біти включення та вибір порядку біти встановлюються базою порту на 0x110 для порту 0, 0x210 для порту 1 тощо.

Таблиця 3.2.9. Пріоритетні біти включення та їх опис

Пріоритет кадрів	Опис
DA	Встановіть DA_PRI_EN біт в 1 і додайте адресу до набору таблиць ARL priority_over_en 1. Біти пріоритету ARL можна використовувати як пріоритет DA.

ToS/TC	Встановіть IP_PRI_EN біт в 1 і встановіть регістр відображення пріоритетів IP.
VLAN	Встановіть для VLAN_PRI_EN (біт) значення 1 і встановіть регістр відображення пріоритету TAG.
Повноваження порту за замовчуванням	Встановіть PORT_PRI_EN на 1, а базовий регістр портів ING_PORT_PRIORITY.

Після прибуття пакети направляються в одну з чотирьох доступних пріоритетних черг на основі:

- Біти пріоритету в полі заголовка
- Адреса призначення кадру (якщо в таблиці ARL з визначеним пріоритетом біт пріоритету включений)
- Кадр VID (якщо в таблиці VLAN і перевизначення пріоритету включено)
- Тег 802.3, що містить інформацію про пріоритет 802.1p (якщо ввімкнено на порту)
- Пріоритет порту за замовчуванням, як визначено в регістрі

Кожне з правил класифікації пріоритетів дозволяє, щоб дизайнери могли використовувати будь-яку комбінацію;

Пріоритет може бути вимкнений або замовлення може бути обраний окремо для кожного порту. Перевантаженість потоку пакетів протягом тривалого періоду часу змушує фрейми опускатися без контролю потоку. Потоки з вищим пріоритетом отримують більший відсоток відкритих буферів, і цей відсоток визначається режимом планування. Такі функції, як протитиск і контроль паузи кадрів, реалізовані для підтримки нульових втрат пакетів під час заторів. AR9331 гарантує, що всі неперевантажені потоки перетинають перемикач без погіршення, незалежно від ситуацій перевантаження в інших місцях комутатора.

QoS для AR9331 може слідувати одній з трьох схем пріоритету, або фіксована, зважена справедлива, або змішана схема режиму. У схемі з фіксованим пріоритетом всі вихідні пакети залишають комутатор, починаючи з черги з найвищим пріоритетом. Після того, як ця черга була очищена, наступна черга з найвищим пріоритетом починає розгін пакетів, поки вона не буде спорожнена і так далі. Цей метод гарантує, що всі пакети з високим пріоритетом будуть відправлені з комутатора якомога швидше.

Для зваженої справедливої схеми пакети виходять з чіпа порядку 8, 4, 2, 1 пакетів для чотирьох пріоритетів черги AR9331. (вісім пакетів виходять з черги з найвищим пріоритетом, потім чотири з другої за величиною черги і так далі). Цей метод дозволяє найвищому пріоритету отримати свої пакети першими, а інші черги, що залишилися, не повністю голодують від виходу.

Змішана схема режиму змішує як зважену справедливу, так і фіксовану схеми. Черга з найвищим пріоритетом спочатку розганяє свої пакети, поки черга не буде очищена, а решта черг будуть слідувати зваженій вихідній схемі 4, 2, 1, як згадувалося раніше. Це гарантує, що черга з найвищим пріоритетом вийде зі своїх пакетів якомога швидше, тоді як решта черг рівномірно розкидають свої пакети без голодування черги.

Обмеження ставки

AR9331 підтримує обмеження вхідної та вихідної швидкості на основі портів. Всі кадри можуть бути обмежені, але кадри керування та відомі багатоадресні кадри є єдиними типами, які можуть бути обрані користувачем. Лімітна швидкість входу може бути встановлена від нуля до 1 Гбіт/с з кроком 32 Кбіт/с. Базовий регістр портів використовується для визначення обмежених байтів для підрахунку. Типовим параметром обмеження швидкості є включення байтів кадру від початку преамбули до кінця RCS з додатковим мінімальним IFG.

Трансляцію контролю штормів

AR9331 підтримує трансляцію контролю штормів. Деякі конструкції перемикачів можуть вимагати обмеження швидкості прийому кадрів. Типи кадрів, що підлягають обмеженню, можна вибрати окремо для кожного порту. Бажана максимальна ставка повинна бути обрана користувачем, а потім запрограмована.

Одинадцять різних частот кадрів від 1k (20K) до 210K в секунду. Блок лічильників статистики підтримує набір із сорока лічильників MIB на порт. Ці лічильники забезпечують набір статистики Ethernet для кадрів, прийнятих при попаданні і переданих на вихід. Інтерфейс регістра дозволяє центральному процесору захоплювати, читати або очищати значення лічильника.

Лічильники підтримують:

- RMON MIB
- Ethernet-подібний MIB
- MIB II
- Міст MIB
- RFC2819

Інтерфейс процесора підтримує:

- Автоматична трансляція лічильників MIB після напівзаповнення
- Автоматична трансляція лічильників MIB після тайм-ауту
- Автоматична передача лічильників MIB за запитом
- Очищення всіх лічильників MIB

Лічильники MIB в комутаторі призначені для локальної мережі та порту процесора. Для глобальної мережі лічильники MIB знаходяться в GE1.

Робота перемикача

Дві таблиці, вбудовані в AR9331, допомагають розподіляти вхідні пакети, таблиця ARL і таблиця VLAN. Адресна база даних зберігається у вбудованій SRAM і може зберігати до 1024 адресних записів. Час старіння за замовчуванням для цієї таблиці становить 300 секунд. Одну адресу можна шукати в таблиці, і вона може бути використана для отримання наступного читання з усієї таблиці. Записи в таблиці можуть завантажуватися і очищатися. Всі записи можуть бути очищені, і це можна розділити на очищення лише нестатичних записів, усіх записів на порт або всіх нестатичних записів на порт.

Таблиця VLAN підтримує один пошук, і вона може бути використана для отримання наступного читання з усієї таблиці. Записи можуть бути завантажені або очищені, а записи можуть бути очищені, як в цілому, так і для кожного порту.

Дзеркальне відображення порту

Вхідні, вихідні та адресні пакети призначення можуть бути дзеркально відображені AR9331. Для дзеркального відображення пакетів DA дзеркальний біт включення повинен бути встановлений в таблиці ARL. Щоб віддзеркалити порт, просто встановіть номер дзеркального порту.

Дзеркальне відображення портів є лише серед портів локальної мережі, а не для глобальної мережі.

Портовий контроль

Таблиця 3.2.10 показує стани портів, підтримувані AR9331.

Таблиця 3.2.10. Портові контролі

Стан	Опис
Вимкнуто	Рамкам заборонено входити або залишати вимкнений порт. Навчання не відбувається на відключених портах.
Блокування	Тільки кадри MGMP допускаються до входу в заблокований порт. Всі інші типи кадрів відкидаються. Навчання вимкнено на заблокованих портах.
Слухач	Тільки кадри управління можуть входити або виходити з порту прослуховування. Всі інші типи кадрів відкидаються. Навчання відключено на портах прослуховування.
Навчання	Тільки фрейми управління можуть входити або виходити з навчального порту. Всі інші типи кадрів відкидаються, але навчання відбувається на всіх хороших кадрах, включаючи некеровані кадри.
Пересилання	Нормальна робота. Всі кадри можуть входити або виходити з порту пересилання. Навчання відбувається на всіх хороших кадрах.

3.2.2 SDRAM Zentel A3S56D40FTP DDR 256 Мб

A3S56D40FTP — це 4 банки x 4 194 304 слова x. 16-бітна синхронна DRAM з подвійною швидкістю передачі даних з інтерфейсом SSTL_2. Усі сигнали управління та адреси посилаються на передній фронт CLK. Вхідні дані реєструються на обох краях стробоскопа даних і вихідні дані та строб даних посилаються на обидва краю CLK. A3S56D30/40FTP досягає дуже високої тактової частоти до 250 МГц.

Особливості SDRAM Zentel A3S56D40FTP:

- Vdd=VddQ=2,5 В+0,2 В (-4, -5E, -5)
- Архітектура подвійної швидкості передачі даних; дві передачі даних за такт
- Двонаправлений стробоскоп даних (DQS) передається/приймається разом з даними
- Диференціальний вхід тактового сигналу (CLK і /CLK)
- DLL вирівнює переходи DQ і DQS з краями переходів CLK DQS
- Команди, введені на кожному позитивному фронті CLK
- Дані та маска даних, пов’язані з обома краями DQS
- 4 банківські операції, які контролюються BA0, BA1 (адреса банку)
- /CAS latency - 2.0 / 2.5 / 3.0 / 4.0 (програмований)
  Довжина серії - 2 / 4 / 8 (програмована)

  Тип серійної зйомки - послідовний / чергуваний (програмований)
- Автоматична попередня зарядка / Попередня зарядка за весь банк, керована A10
- Підтримка одночасної автоматичної попередньої зарядки
- 8192 циклів оновлення / 64 мс (одночасне оновлення 4 банків)
- Автоматичне оновлення та самооновлення
- Адреса рядка A0-12 / Адреса стовпця A0-9(x8) /A0-8(x16)
- Інтерфейс SSTL_2
- Пакет 400-mil, 66-контактних пакетів Thin Small Outline Package (TSOP II) з кроком свинцю 0,65 мм

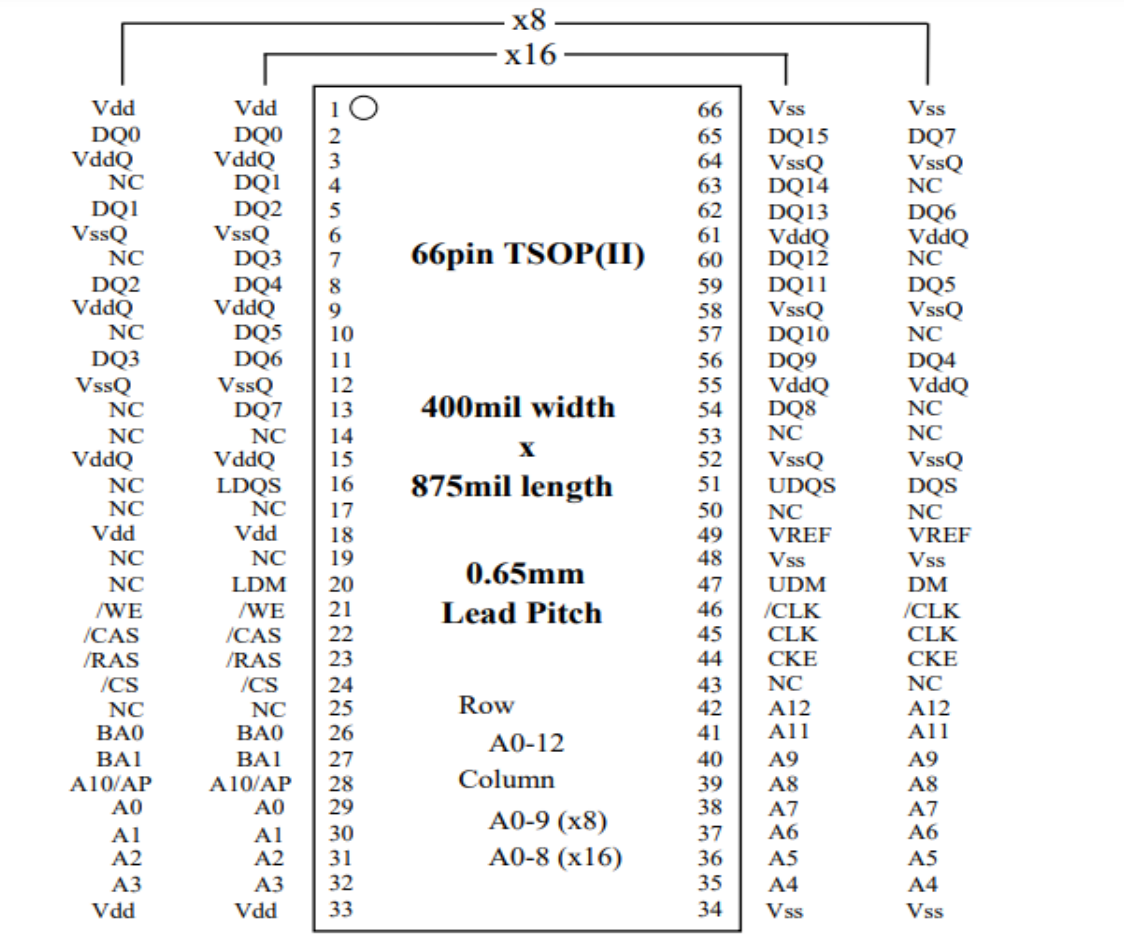
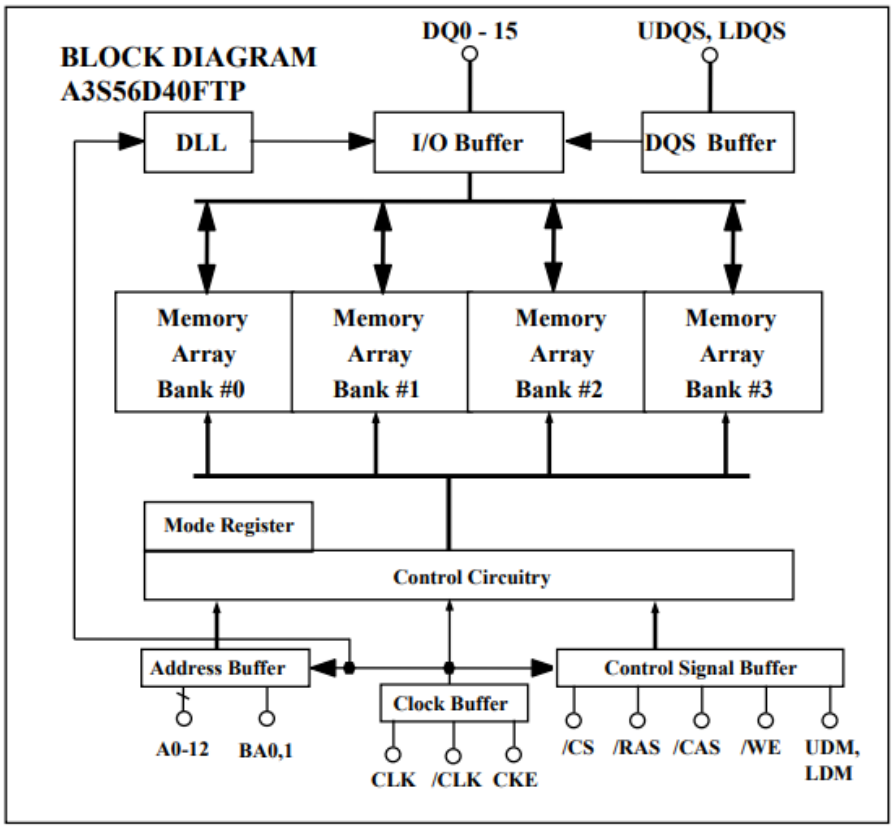


Рис. 3.2.7. Призначення контактів (вид зверху) 66-контактний TSOP

Таблиця 3.2.11. Функції контактів 66-контактного TSOP

Назва	Тип	Опис
CLK, /CLK	Введення	Тактовий сигнал: CLK і /CLK є диференціальними входами синхронізації. Усі вхідні сигнали адреси та керування дискретизуються на перетині позитивного фронту CLK і негативного фронту /CLK. Вихідні (прочитані) дані посилаються на перетини CLK та /CLK (обидва напрямки перетину).
CKE	Введення	Увімкнути тактовий сигнал: CKE керує вимкненням живлення та самооновленням. Прийняття CKE LOW забезпечує відключення живлення Precharge або Self Refresh (усі банки

		неактивні), або Active Power Down (активний рядок у будь-якому банку). Встановлення рівня CKE HIGH забезпечує вихід із вимкнення живлення або вихід із самооновлення. Після запуску Self Refresh CKE стає асинхронним введенням. Вимкнення живлення та самооновлення зберігаються, поки CKE НИЗЬКИЙ
/CS	Введення	Вибір мікросхеми: коли /CS має значення HIGH, будь-яка команда означає відсутність операції.
/RAS, /CAS, /WE	Введення	Комбінація /RAS, /CAS, /WE визначає основні команди.
A0-12	Введення	A0-12 визначає адресу рядка/стовпця разом із BA0,1. Адреса рядка визначається A0-12. Адреса стовпця визначається A0-9(x8) і A0-8(x16). A10 також використовується для позначення варіанту попередньої зарядки. Коли A10 є ВИСОКИМ за командою читання/запису, виконується автоматична попередня зарядка. Коли A10 є ВИСОКИМ за командою Precharge, усі банки попередньо заряджаються
BA0,1	Введення	Адреса банку: BA0,1 визначає один із чотирьох банків, до яких застосовується команда. BA0,1 має бути встановлено за допомогою команд Active, Precharge, Read, Write.
DQ0-7 (x8), DQ0-15 (x16),	Введення-виведення	Введення/виведення даних: шина даних.
DQS (x8), UDQS, LDQS (x16)	Введення-виведення	Data Strobe: вихід з даними для читання, введення з даними для запису. Вирівняно по краях з даними для читання, з центром у даних для запису. Використовується для запису даних запису. Для x16 LDQS відповідає даним на DQ0-DQ7; UDQS відповідають даним на DQ8-DQ15.
DM (x8), UDM, LDM (x16)	Введення	Маска вхідних даних: DM — це сигнал маски введення для запису даних. Вхідні дані маскуються, коли DM отримує ВИСОКУ вибірку разом із цими вхідними даними під час доступу для запису. DM відбирається на обох краях DQS. Хоча контакти DM є лише вхідними, навантаження DM відповідає навантаженню DQ і DQS. Для x16 LDM відповідає даним на DQ0-DQ7; UDM відповідає даним на DQ8-DQ15.
Vdd, Vss	Джерело живлення	Джерело живлення для масиву пам'яті та периферійних схем.
VddQ, VssQ	Джерело живлення	VddQ і VssQ подаються в буфери DQ, DQS
VREF	Введення	Опорна напруга SSTL_2.



Type Designation Code

This rule is applied to only Synchronous DRAM family.

A 3 S 56 D 4 0 F TP –G4

- Speed Grade — G: Green part; 5: 200MHz @CL=3.0, 166MHz @CL=2.5, and 133MHz @CL=2.0; 5E: 200MHz @CL=3.0/2.5, and 133MHz @CL=2.0; 4: 250MHz @CL=3.0/4.0, 200MHz @CL2.5, and 133MHz @CL=2.0
- Package Type TP: TSOP(II)
- Process Generation
- Function Reserved for Future Use
- Organization 2^n 4: x16
- **DDR Synchronous DRAM**
- Density 56: 256M bits
- Interface S:SSTL_2
- Memory Style (DRAM)
- Zentel DRAM

Рисунок 3.2.8. Блок-схема A3S56D40FTP

A3S56D30/40FTP забезпечує базові функції: активність, читання/запис, попереднє заряджання та автоматичне/самооновлення, налаштування режиму реєстрації, завершення пакету. Кожна команда визначається керуючими сигналами /RAS, /CAS і /WE на передньому фронті CLK. На додаток до 3 сигналів, /CS, CKE і A10 використовуються як вибір мікросхеми, опція оновлення та опція попередньої зарядки відповідно. Щоб дізнатися детальніше визначення команд, перегляньте таблицю істинності команд.

3.2.3 SPI Flash S25FL032P 32Mbit

Вибір одного чіпа SPI призначений для зовнішнього флеш-пам’яті для завантаження чіпа. Два настроювані чіпи доступні для біт-бенгу за допомогою GPIO, які налаштовують зовнішні компоненти. Як підлеглий пристрій AHB, контролер SPI підтримує лише текстові транзакції. Оскільки послідовний флеш-пам’ять підтримує функцію кешованого читання (але не кешованого запису), ЦП повинен виконувати некешований запис, але читання можна прискорити виконанням кешованого читання. За замовчуванням біт REMAP_DISABLE дорівнює нулю які доступні ише 4 Мбайт. Якщо встановити цей біт на 1, можна отримати доступ до 16 Мбайт флеш-пам’яті.

S25FL032P — це пристрій флеш-пам’яті на 3,0 В (2,7–3,6 В) з одним джерелом живлення. Пристрій складається із 64 однотипних секторів по 64 КБ з двома (верхніми або нижніми) секторами по 64 КБ, далі розділеними на тридцять два підсистеми по 4 КБ секторах.

Пристрій приймає дані, записані на SI, і виводить дані на SO. Пристрої є призначений для програмування в системі зі стандартним системним джерелом живлення 3,0 В VCC.

Пристрій S25FL032P додає такі високопродуктивні функції за допомогою 5 нових інструкцій:

- Подвійний вихід для зчитування з використанням контактів SI та SO як вихідних контактів із тактовою частотою до 80 МГц
- Чотири вихідні зчитування з використанням контактів SI, SO, W#/ACC і HOLD# як вихідних контактів із тактовою частотою до 80 МГц
- Високоефективне зчитування подвійного вводу/виводу з використанням контактів SI і SO як вхідних і вихідних контактів із тактовою частотою до 80 МГц
- Високопродуктивне зчитування Quad I/O за допомогою контактів SI, SO, W#/ACC і HOLD# як вхідних і вихідних контактів на тактовій частоті до 80 МГц
- Програмування чотирьох сторінок з використанням контактів SI, SO, W#/ACC і HOLD# як вхідних контактів для програмування даних на тактовій швидкості до 80 МГц

Кожному пристрою потрібен лише джерело живлення 3,0 В (від 2,7 В до 3,6 В) для функцій читання та запису. Внутрішньо генеровані та регульовані напруги надаються для роботи програми. Цей пристрій вимагає високого подача напруги на висновок W#/ACC, щоб увімкнути режим прискореного програмування.

Пристрій S25FL032P також пропонує одноразову програмовану область (OTP) до 128 біт (16 байт) для постійна безпечна ідентифікація та додаткові 490

байт простору OTP для іншого використання. Ця область OTP може програмувати або читати за допомогою інструкцій OTPP або OTPR.

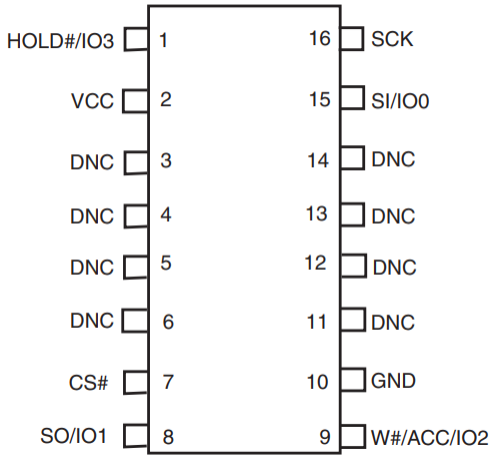


Рисунок 3.2.9. Схема підключення 16-контактного пластикового малого корпусу (SO)

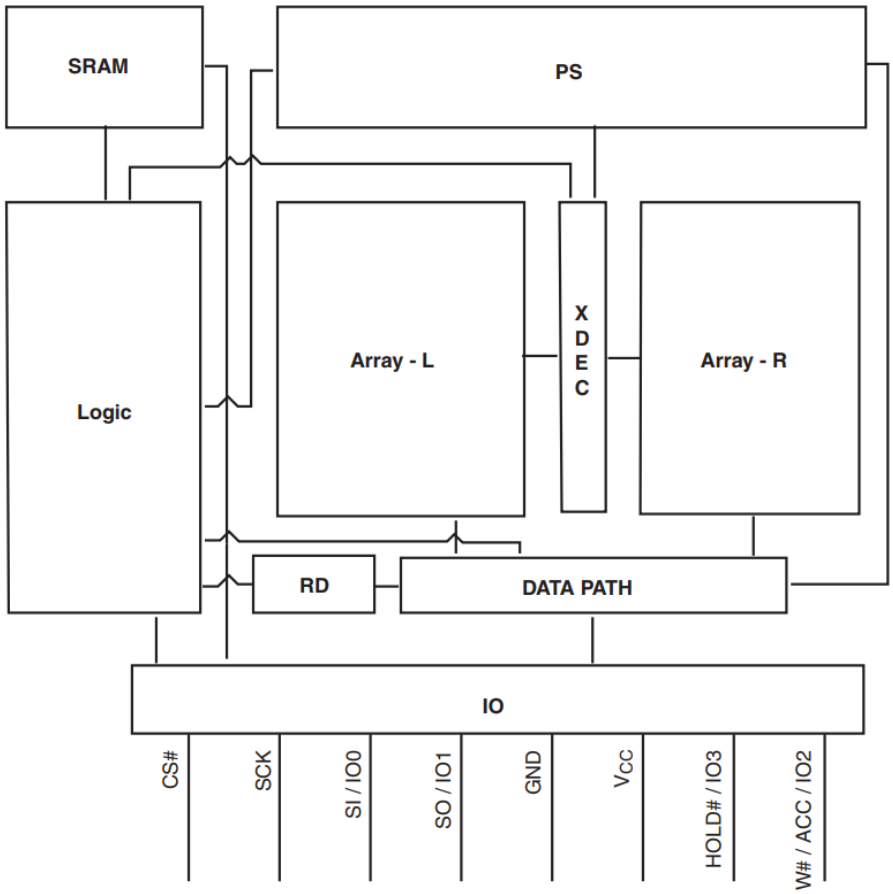
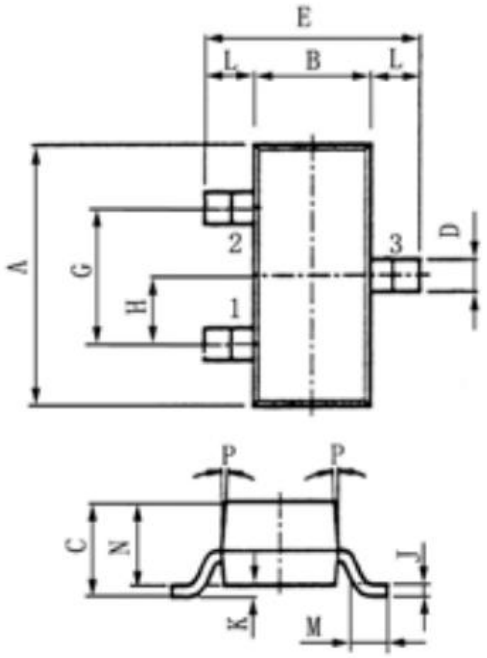


Рисунок 3.2.10. Блок-схема SPI Flash S25FL032P

3.2.4 Транзистор 8550M PNP

Призначення: застосування підсилювача потужності.



单位 :mm

A	2.90±0.20
B	1.30+0.20/−0.15
C	1.30MAX
D	0.40+0.15/−0.05
E	2.40+0.30/−0.20
G	1.90±0.2
H	0.95±0.1
J	0.10+0.10/−0.05
K	0.00~0.10
L	0.55±0.1
M	0.20MIN
N	1.00+0.20/−0.10
P	7°

Рисунок 3.2.11. Блок-схема 8550M PNP транзистора

Таблиця 3.2.12. Абсолютний максимум показників (Ta=25 ℃)

Назва	Показник	Одиниця
V_{CBO}	-40	V
V_{CEO}	-25	V
V_{EBO}	-6.0	V
I_C	-800	mA
I_B	-200	mA
P_C	450	mW
T_j	150	℃
T_{stg}	-65~150	℃

Таблиця 3.2.13. Електричні характеристики (Ta=25 ℃)

Назва	Тестовий стан	Показник			Одиниця
		min	Тип	max	
V_{CBO}	I_C=-0.1mA I_E=0	-40			V

V_{CEO}	I_C=-2.1mA I_B=0	-25			V
V_{EBO}	I_E=-0.1mA I_C=0	-6.0			V
I_{CBO}	V_{CB}=-35V I_E=0			-0.1	μA
I_{EBO}	V_{EB}=-6.0V I_C=0			-0.1	μA
$h_{FE(1)}$	V_{CE}=-1.0V I_C=-100mA	85		300	
$h_{FE(2)}$	V_{CE}=-1.0V I_C=-500mA	40			
$h_{FE(3)}$	V_{CE}=-1.0V I_C=-5.0mA	45			
$V_{CE(sat)}$	I_C=-500mA I_B=-50mA		-0.28	-0.6	V
$V_{BE(sat)}$	I_C=-500mA I_B=-50mA		-0.98	-1.2	V
V_{BE}	V_{CE}=-1.0V I_C=-10mA		-0.66	-1.0	V
f_T	V_{CE}=-10V I_C=-50mA	100	200		MHz
C_{ob}	V_{CE}=-10V I_E=0 f=1.0MHz		15		pF

3.2.5 Трансформатор Ethernet H1601CG

Особливості цього трансорматора:

- Розроблено відповідно до первинних вимог IEEE802.3 і ANSIX3.263
- Індуктивність 350uH min. зі зміщенням постійного струму 8 mA
- Діапазон робочих температур від 0°C до +70°C
- Діапазон температур зберігання від -25°C до +125°C

Таблиця 3.2.13. Специфікація трансорматора Ethernet H1601CG

Електрична специфікація H1601CG						
OCL(uH min) @ 100KHx/0.2V	Коефіцієнт обертів		Cross talk (dB min)			HI-POT (Vrms)
з 8mA DC Bias	TX	RX	30MHz	60MHz	100MHz	
350	1CT:1CT	1CT:1CT	-40	-35	-30	1500

Внесені втрати (dB max)	Зворотні втрати (dB min)	DCMR (dB min)

1-100MHz	1-30MHz	40MHz	50MHz	60-80MHz	100MHz	30MHz 60MHz 100MHz
-1.0	-18	-14.4	-13.1	-12	-10	-40 -35 -30

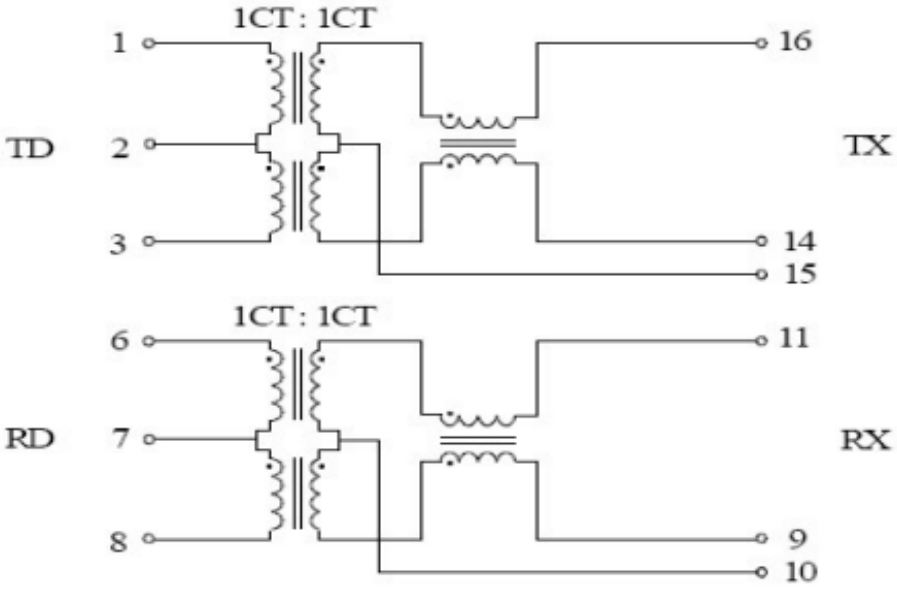


Рис 3.2.12. Схема трансформатора Ethernet H1601CG

3.2.6 Перемикач живлення з обмеженим струмом TPS204x_205xB

Особливості:

- 70-мОм High-Side MOSFET
- Безперервний струм 500 мА
- Перегрівання та коротке замикання
- Точне обмеження струму
- (0,75 А хв., 1,25 А макс.)
- Робочий діапазон: від 2,7 В до 5,5 В
- Типовий час наростання 0,6 мс
- Блокування зниженої напруги
- Звіт про несправності (ОС)
- Відсутність збоїв ОС під час увімкнення
- Максимальний струм живлення в режимі очікування:
- 1 мкА (одинарний, подвійний) або 2 мкА (потрійний, чотириразовий)
- Діапазон температур навколишнього середовища: від -40°C до 85°C
- Визнано UL, номер файлу E169910

– Додаткове визнання UL для TPS204

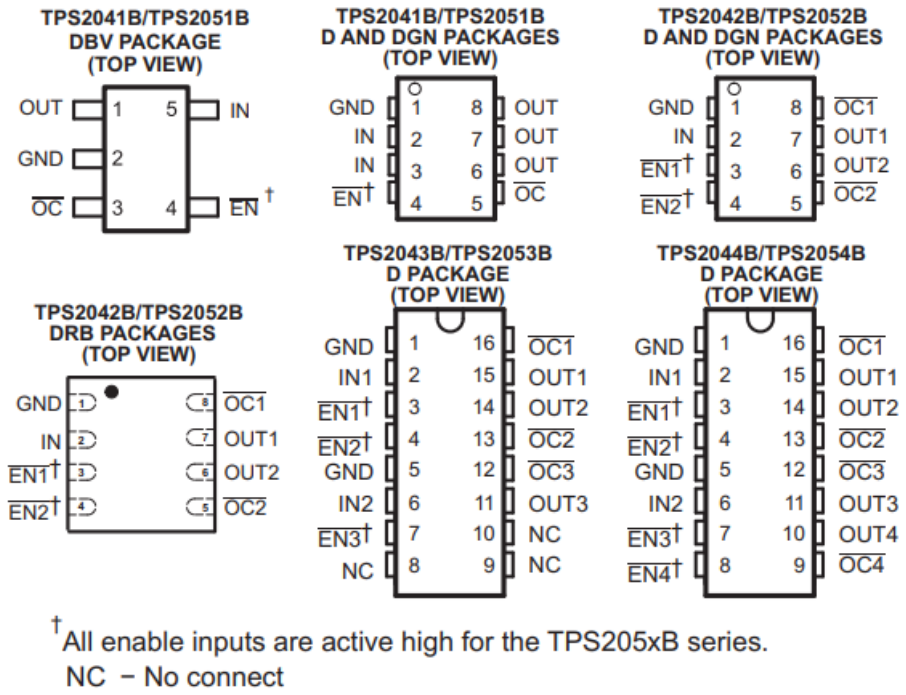


Рисунок 3.2.13. Схема портів перемикача живлення з обмеженим струмом TPS204x_205xB

Перемикачі розподілу живлення TPS204xB/TPS205xB призначені для застосувань, де ймовірно виникнуть високі ємнісні навантаження та короткі замикання. Ці пристрої містять 70-мОм N-канальні MOSFET перемикачі живлення для систем розподілу електроенергії, які потребують кількох перемикачів живлення в одному корпусі. Кожен перемикач керується логічним входом дозволу. Привід затвора забезпечується внутрішнім зарядним насосом, призначеним для контролю часу наростання та спаду перемикача живлення, щоб мінімізувати стрибки струму під час перемикання. Зарядний насос не потребує зовнішніх компонентів і дозволяє працювати від джерел живлення до 2,7 В.

Коли вихідне навантаження перевищує поріг обмеження струму або існує коротке замикання, пристрій обмежує вихідний струм до безпечного рівня, перемикаючись у режим постійного струму, підтягуючи логічний вихід надструму (OCx) до низького рівня. Коли безперервні сильні перевантаження та короткі замикання збільшують розсіювання потужності в комутаторі, спричиняючи підвищення температури переходу, схема теплового захисту вимикає комутатор, щоб запобігти пошкодженню. Відновлення після термічної вимикається автоматично, коли пристрій достатньо охолоне. Внутрішня схема гарантує, що перемикач залишається вимкненим, доки не буде присутня належна вхідна напруга. Цей перемикач розподілу живлення призначений для встановлення обмеження струму на рівні 1 А.

Таблиця 3.2.14. Інформація приладу

T_A	Робота	Рекомендований максимальний струм навантаження	Типове обмеження струму короткого замикання при 25C	Вид перемикачів	Комплекс приладів			
					MSOP	SOIC	SOT-23	SON
-40C до 85C	Низька активність	0.5A	1A	1	TPS2041BDGN	TPS2041BD	TPS2041BDBV	
	Висока активність			1	TPS2051BDGN	TPS2051BD	TPS2051BDBV	
	Низька активність			2	TPS2042BDGN	TPS2042BD		TPS2042BDRB
	Висока активність			2	TPS2052BDGN	TPS2052BD		TPS2042BDRB
	Низька активність			3	-	TPS2043BD		
	Висока активність			3	-	TPS2053BD		
	Низька активність			4	-	TPS2044BD		
	Висока активність			4	-	TPS2054BD		

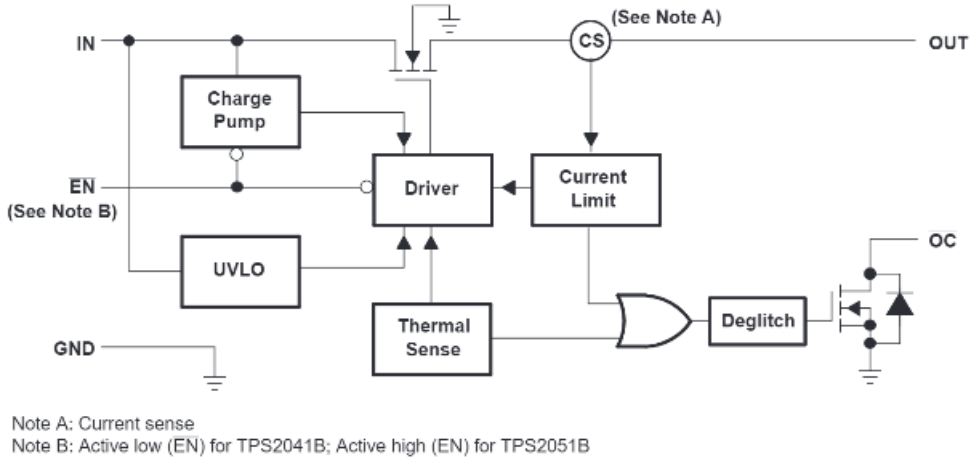


Рис. 3.2.14. Функціональна схема TPS2041B і TPS2051B

3.2.7 Вибір типу оперативної пам’яті SDRAM

Вибираючи опертивну память для роутера необхідно врахувати наступні параметри:

- Ємність
- Тип памяті
- Швидкодія
- Енергоефективність

Зважаючи на вимоги, в приладі будемо використовувати Zentel A3S56D30/40FTP він забезпечує базові функції: активність, читання/запис, попереднє заряджання та автоматичне/самооновлення, налаштування режиму реєстрації, завершення пакету, має тип пам’яті DDR та ємність 256 Мб, що ідеально підходить нам.

3.2.8 Вибір типу SPI Flash

Вибираючи опертивну память для роутера необхідно врахувати наступні параметри:

- Ємність
- Тип пам’яті
- Швидкодія
- Енергоефективність
- Температурний діапазон

Зважаючи на вимоги, в приладі будемо використовувати флеш-пам’ять S25FL032P на 3,0 В з одним джерелом живлення, ємністю 32Mbit, також він пропонує одноразову програмовану область до 128 біт для постійної безпечної ідентифікації та додаткові 490 байт простору OTP для іншого використання.

3.2.9 Вибір типу транзистора

Вибираючи транзистор для роутера необхідно врахувати наступні параметри:

- Тип транзистора
- Напруга розпилювання
- Максимальний струм
- Потужність розсіювання
- Коефіцієнт посилення
- Температурний діапазон

Зважаючи на вимоги, в приладі будемо використовувати транзистор 8550M PNP, він має гарний показник максимально допустимої напруги до 25V та максимально допустимого струму, та достатню потужність для розсіювання тепла.

3.2.10 Вибір типу трансформатора Ethernet

Вибираючи транзистор для роутера необхідно врахувати наступні параметри:

- Вихідна потужність
- Вхідна та вихідна напруга
- Індуктивність
- Ефективність
- Розмір та монтаж

Зважаючи на вимоги, в приладі будемо використовувати трансформатор Ethernet H1601CG, він має індуктивність 350uH min. зі зміщенням постійного струму 8 mA, та гарні показниеи вихідної потужності.

3.2.11 Вибір типу перемикача живлення

Обираючи перемикач живлення для роутера необхідно врахувати наступні параметри:

- Напруга і струм
- Механічна цінність
- Надійність
- Зручність в експлуатації

Зважаючи на вимоги, в приладі будемо використовувати перемикач живлення з обмеженим струмом TPS2041_2051B, він дозволяє працювати від джерел живлення до 2,7 В, має безперервний струм 500 мА, автоматичне блокування зниженої напруги.

ВИСНОВОК

В кваліфікаційній роботі бакалавра було проведено дослідження та аналіз джерел літератури у відповідності з поставленим завданням було розроблено Wi-Fi роутер з функцією VPN. До складу центрального блоку пристрою входять:

- чіпсета Qualcomm Atheros AR9331, яка включає в себе:
- процесор Atheros AR7040 400 МГц MISP24kc
- SDRAM Zentel A3S56D40FTP DDR 256 Мб
- Транзистор 8550M PNP
- SPI флеш-пам’ять S25FL032P 32MbitТрансформатор Ethernet H1601CG
- Подвійний сигнальний діод Taitron
- Перемикач живлення з обмеженим струмом TPS2041_2051B.

Виконуючи розробку пристрою було складено алгоритм роботи, створено схему електричну структурну та схему електричну принципову.

При створені схеми електричної структурної було проведено аналіз та опис функцій, які виконує кожен окремий блок схеми. На основі перерахованих та описаних функцій було запропоновано технічне рішення по вибору елементної бази пристрою.

СПИСОК ЛІТЕРАТУРИ

1. Reverse-Engineering work on the TL-WR703N 150M 802.11n Wi-Fi Router. URL: http://squonk42.github.io/TL-WR703N/ (дата звернення: 23.04.2023).
2. TP-Link TL-WR703N https://oldwiki.archive.openwrt.org/toh/tp-link/tl-wr703n (дата звернення: 27.04.2023).
3. Qualcomm Atheros AR7xxx, AR9xxx and QCA9xxx boards https://oldwiki.archive.openwrt.org/doc/hardware/soc/soc.qualcomm.ar71xx#ar9331 (дата звернення: 29.04.2023).
4. AR9331 Data Sheet https://www.openhacks.com/uploadsproductos/ar9331_datasheet.pdf (дата звернення: 02.04.2023).
5. TP-Link WR703N Teardown http://www.kean.com.au/oshw/WR703N/teardown/ (дата звернення: 10.05.2023).
6. 10/100Base Single Port Transformer H1601CG Data Sheet http://www.kean.com.au/oshw/WR703N/teardown/H1601CG%20Ethernet%20Transformer.pdf (дата звернення: 14.05.2023).
7. Current-Limited, Power-Distribution Switches Data Sheet http://www.kean.com.au/oshw/WR703N/teardown/TPS204x_205xB%20current%20limited%20power%20switch.pdf (дата звернення: 19.05.2023).
8. Transistor 8550-S8550M_3CG8550M Data Sheet http://www.kean.com.au/oshw/WR703N/teardown/S8550M%20PNP%20Transistor.pdf (дата звернення: 21.05.2023).
9. Flash S25FL032P Data Sheet http://www.kean.com.au/oshw/WR703N/teardown/S25FL032P%2032Mbit%20SPI%20Flash.pdf (дата звернення: 23.05.2023).
10. 256Mb DDR SDRAM Specification Data Sheet http://www.kean.com.au/oshw/WR703N/teardown/Zentel%20A3S56D40FTP%20DDR%20256Mb%20SDRAM.pdf (дата звернення: 23.05.2023).

Бирин О.О., Савченко Д.С. Захист інформації на базі методу книжкового гамування в інфокомунікативних системах: матеріали міжнар. наук-практ. конф., м.Суми, 24-28 квітня 2023 р. Суми, 2023

ДОДАТОК А

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
СУМСЬКИЙ ДЕРЖАВНИЙ УНІВЕРСИТЕТ

ФІЗИКА, ЕЛЕКТРОНІКА, ЕЛЕКТРОТЕХНІКА

ФЕЕ :: 2023

МАТЕРІАЛИ
та програма

МІЖНАРОДНОЇ НАУКОВОЇ КОНФЕРЕНЦІЇ
молодих вчених

(Суми, 24–28 квітня 2023 року)

Суми
Сумський державний університет
2023

11.

Захист інформації на базі методу книжкового гамування в інфокомунікаційних системах

Борисенко О.А., *професор*; Бережна О.В., *доцент*;
Горішняк А.О., *аспірант*; Бирин О.О., *студент гр. ТК-91*;
Савченко Д.С., *студент гр. ТК-91*
Сумський державний університет, м. Суми, Україна

Впровадження сучасних інфокомунікаційних систем вимагає посилення вимог до безпеки інформації, що надає особливої актуальності пошуку високопродуктивних алгоритмів захисту інформації, що передається, з необхідною криптографічною стійкістю.

Аналіз методів захисту інформації показав, що при використанні асиметричних шифрів відсутня необхідність пересилання секретних ключів, але реалізація таких алгоритмів потребує виконання складних обчислень і, відповідно, вимагає більше часу для шифрування в порівнянні з симетричними шифрами. Тому доцільно розглянути можливість використання алгоритмів симетричного шифрування, які характеризуються швидким шифруванням з високою криптостійкістю.

За результатами дослідження пропонується використання методу гамування вхідних повідомлень, який забезпечує найбільшу криптостійкість за умови використання гами довжиною не менше ніж довжина вхідного повідомлення. Різновидом такого методу шифрування є метод книжкового гамування, який дозволяє використовувати в якості гами сторінки шифрувального блокноту. Принцип шифрування полягає у заміні символів вхідного повідомлення і символів гами цифровими еквівалентами, які потім підсумовуються за модулем N, де N – кількість символів у алфавіті, що застосовується. Неможливість проведення частотного аналізу зашифрованого таким методом повідомлення значно підвищує стійкість даного шифру до несанкціонованого розшифрування. Складність передачі гами шифру отримувачу зашифрованих повідомлень пропонується подолати шляхом формування множини шифрувальних блокнотів (можливо із застосуванням відкритих джерел) і алгоритму вибору сторінок блокноту для здійснення операцій шифрування/розшифрування.

Запропонований метод книжкового гамування є більш ефективним при апаратній реалізації, що дозволить в інфокомунікаційних системах забезпечити швидке шифрування з високим рівнем криптостійкості.

ДОДАТОК Б

```
$ cat <<EOF > ft2232h-scan.cfg
interface ftdi
ftdi_vid_pid 0x0403 0x6010
ftdi_layout_init 0x0018 0x05fb
adapter_khz 100
shutdown
EOF

interface ftdi
ftdi_vid_pid 0x0403 0x6010
ftdi_layout_init 0x0018 0x05fb
adapter_khz 600

jtag newtap auto0 tap -expected-id 0x00000001 -irlen 5
target create auto0.tap mips_m4k -endian big -chain-position auto0.tap

init
halt

# pll initialization
mww 0xb8050008 0x00018004
mww 0xb8050004 0x00000352
mww 0xb8050000 0x40818000
mww 0xb8050010 0x001003e8
mww 0xb8050000 0x00818000
mww 0xb8050008 0x00008000
sleep 1

# Setup DDR1 config and flash mapping
mww 0xb8000000 0x7fbc8cd0
```

```
mww 0xb8000004 0x9dd0e6a8


mww 0xb8000010 0x8
mww 0xb8000008 0x133
mww 0xb8000010 0x1
mww 0xb800000c 0x2
mww 0xb8000010 0x2
mww 0xb8000010 0x8
mww 0xb8000008 0x33
mww 0xb8000010 0x1
mww 0xb8000014 0x4186
mww 0xb800001c 0x8
mww 0xb8000020 0x9
mww 0xb8000018 0xff

# UART
mww 0xb8020004 0x4388
mww 0xb8020008 0xc2000

# GPIO
mww 0xb8040028 0x48002

load_image barebox-2015.01.0/barebox.bin 0xa0100000 bin
resume 0xa0100000
shutdown
```