ТЕХНОЛОГИЧНО УЧИЛИЩЕ ЕЛЕКТРОННИ СИСТЕМИ
към ТЕХНИЧЕСКИ УНИВЕРСИТЕТ - СОФИЯ

ДИПЛОМНА РАБОТА

по професия код 523050 „Техник на компютърни системи“
специалност код 5230502 „Компютърни мрежи“

Тема: Изграждане на корпоративна мрежа чрез трета фаза на DMVPN

Дипломант:
Иоан Николаев Евгениев

Дипломен ръководител:
Виктор Борисов

СОФИЯ

2025

Използвани съкращения

IP - Internet Protocol

EGP - Exterior Gateway Protocol

IGP - Interior Gateway Protocol

BGP - Border Gateway Protocol

RIP - Routing Information Protocol

EIGRP - Enhanced Interior Gateway Routing Protocol

OSPF - Open Shortest Path First

MAC address - Media Access Control address

LAN - Local Area Network

UDP - User Datagram Protocol

TCP - Transmission Control Protocol

NHRP - Next Hop Resolution Protocol

NHS - Next Hop Server

DMVPN - Dynamic Multipoint Virtual Private Network

Увод

Dynamic Multipoint Virtual Private Network (DMVPN) е модерно решение за сигурна и динамична свързаност между отдалечени мрежови обекти. Технологията позволява изграждането на гъвкави и мащабируеми VPN мрежи чрез автоматично създаване на тунели между отдалечените точки, без да е необходимо предварително дефиниране на връзките между тях. Това значително намалява сложността на управлението на мрежата и улеснява разширяването ѝ.

В основата на DMVPN стои използването на протокола Next Hop Resolution Protocol (NHRP), който позволява динамично разпознаване и разрешаване на IP адресите на крайните точки в тунелната мрежа. За изграждането на надеждна и ефективна комуникация в DMVPN е използван протоколът за маршрутизация EIGRP (Enhanced Interior Gateway Routing Protocol), който предлага бързо адаптиране към промените в мрежовата топология и ефективно управление на маршрутите, а за осигуряване на конфиденциалността и автентичността на предаваните данни, DMVPN използва GRE (Generic Routing Encapsulation) тунели, защитени с IPsec (Internet Protocol Security)

Настоящата дипломна работа има за цел да анализира изграждането и функционирането на DMVPN с използване на посочените протоколи. В работата ще бъдат разгледани основните механизми на DMVPN, както и практическото му приложение в съвременните корпоративни мрежи.

Първа глава - Използвани технологии

1.1 Основи на мрежовата архитектура

1.1.1 Мрежови модели: OSI и TCP/IP

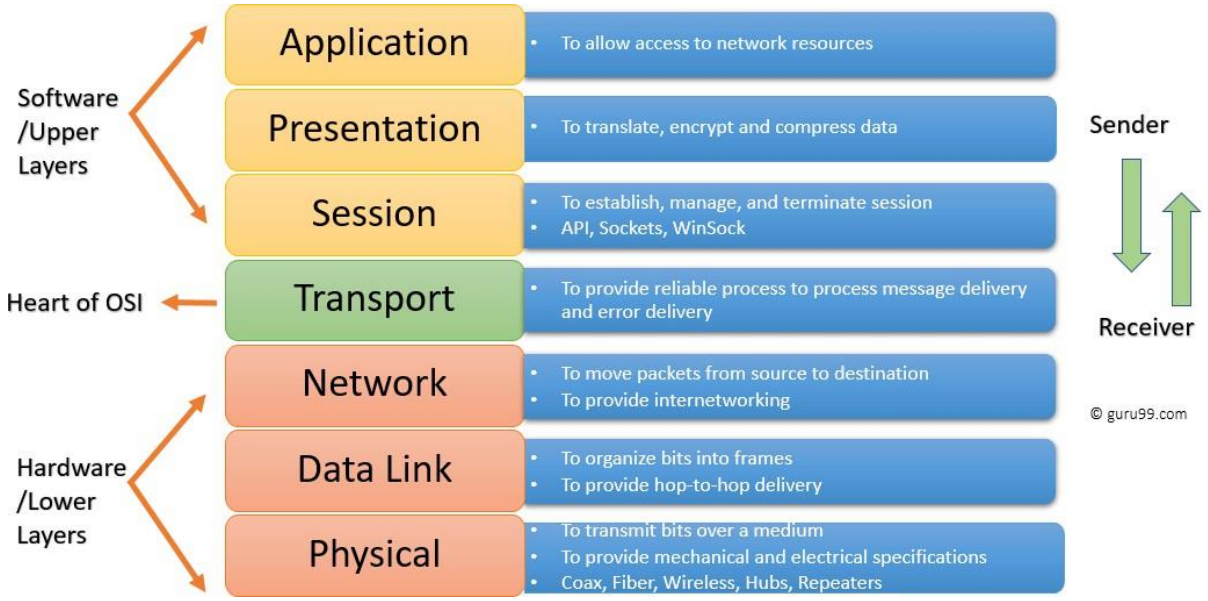
В сферата на компютърните мрежи са разработени различни модели, които определят функциите, необходими за комуникация между устройствата. Тези структури стандартизират и организират сложните процеси, свързани с предаването на данни.

OSI[1] е модел, разработен от International Organization for Standardization (ISO), за да предостави стандартизиран начин за концептуализиране на мрежовата комуникация. Той разделя процеса на мрежова комуникация на седем отделни слоя, като всеки от тях е отговорен за специфични функции. Този модулен подход осигурява гъвкавост, тъй като всеки слой може да използва различни протоколи, за да изпълнява своята роля.

- Слоеве на модела OSI

Моделът OSI притежава 7 слоя(фиг. 1.1.1.1), като е напълно теоретичен и не се използва в реалните мрежи:

1. Физически слой (Physical layer): Отговаря за физическото предаване на данни по носители, като кабели и радиовълни. Примери включват Ethernet (IEEE 802.3) и Wi-Fi (IEEE 802.11).
2. Канален слой (Data Link layer): Осигурява предаване без грешки между съседни мрежови възли. Основни протоколи са Ethernet и Point-to-Point Protocol (PPP).
3. Мрежов слой (Network layer): Отговаря за маршрутизацията и адресирането на данните, така че те да достигнат до предвидената дестинация. Протоколите включват Internet Protocol (IP) и Internet Control Message Protocol (ICMP).
4. Транспортен слой (Transport layer): Гарантира надеждно доставяне на данни, контрол на потока и корекция на грешки. Основни протоколи са Transmission Control Protocol (TCP) и User Datagram Protocol (UDP).
5. Сесиен слой (Session layer): Управлява сесиите или връзките между приложенията. Контролира създаването, поддръжката и прекратяването на сесиите.
6. Представителен слой (Presentation layer): Обработва форматирането, криптирането и компресирането на данните, за да осигури съвместимост между различните системи.
7. Приложен слой (Application layer): Осигурява интерфейс с крайния потребител и приложения като уеб браузъри или клиенти за електронна поща. Протоколите включват HTTP, FTP и SMTP.



фиг 1.1.1.1

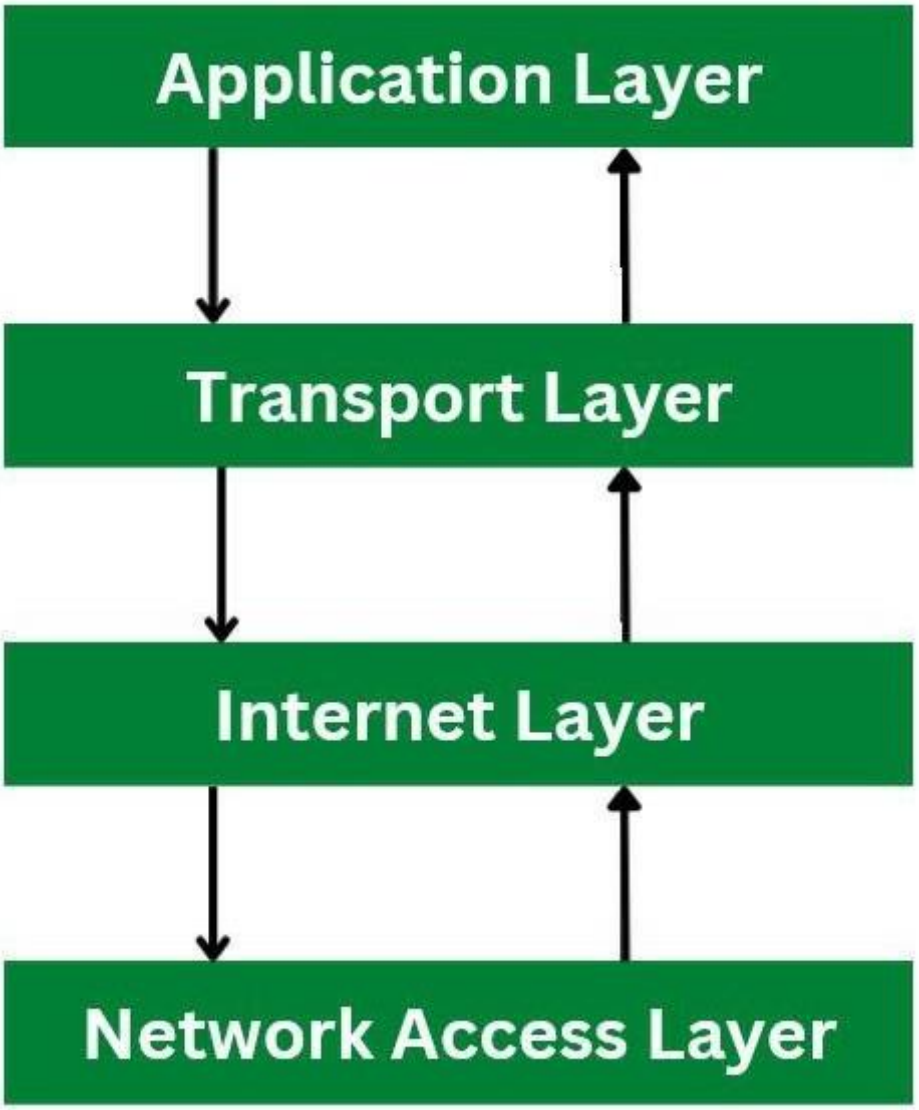
Моделът OSI не се използва директно в съвременните мрежи, но служи като ориентир за разбиране и обсъждане на мрежови процеси. Неговата слоеста структура предоставя ясна рамка за проектиране и отстраняване на неизправности в мрежите. Например, ако данните не могат да бъдат предадени, инженерите могат да изолират проблема, като анализират съответния слой.

Въпреки че е концептуално стабилен, моделът OSI не винаги се прилага директно в реалните мрежи. Практическите нужди на мрежите са довели до приемането на по-опростения TCP/IP модел.

- Слоеве на модела TCP/IP

TCP/IP моделът или Internet Protocol Suite, възниква, първоначално известен като ARPANET. За разлика от OSI, TCP/IP е пряко приложим в реалните мрежи. Моделът TCP/IP се състои от четири или пет слоя, в зависимост от интерпретацията(фиг 1.1.1.2):

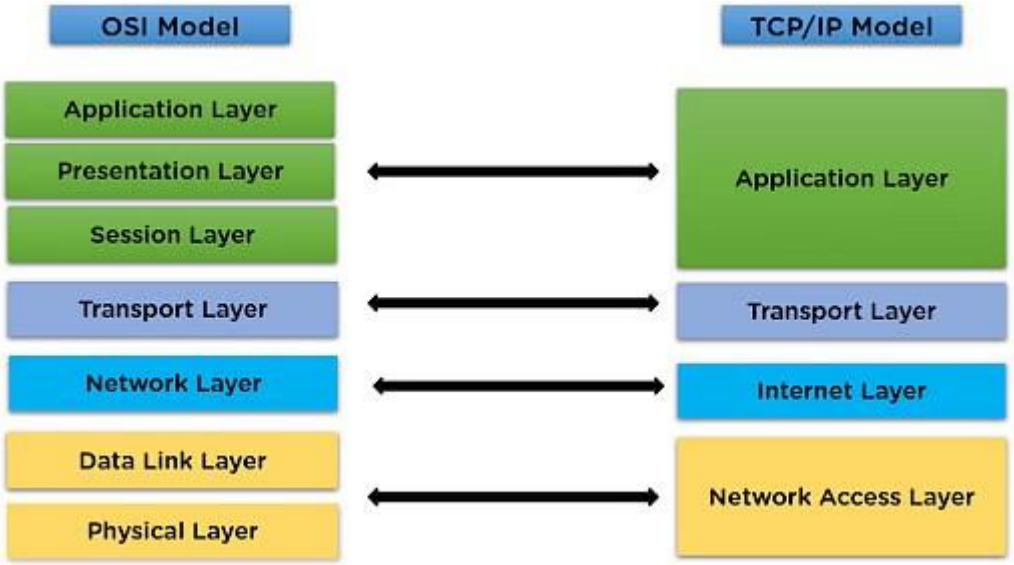
1. Мрежов достъп: Този слой се грижи както за предаването на сурови битове по физическата среда, така и за организиране на данните в кадри и осигуряване на надеждно предаване между възли в същата мрежа. Той управлява достъпа до мрежовия носител, адресирането в локалната мрежа и контрола на грешките.
2. Интернет слой: Съответства на мрежовия слой на OSI. Internet Protocol (IP) работи тук, като обработва адресирането и маршрутизацията.
3. Транспортен слой: Подобен на транспортния слой на OSI, той гарантира доставянето на данни от край до край. TCP осигурява надеждна комуникация, докато UDP акцентира върху скоростта.
4. Приложен слой: Комбинира функциите на приложния, представителния и сесийния слой на OSI. Протоколите включват HTTP, FTP и DNS.



фиг 1.1.1.2

1.1.2 Сравнение между OSI и TCP/IP

За разлика от OSI, TCP/IP е проектиран за реално приложение и може да поддържа огромни мрежи, като глобалния интернет. Неговата независимост от доставчици позволява устройства от различни производители да комуникират безпроблемно. Въпреки широко разпространеното му използване, моделът TCP/IP няма детайлността на OSI. Например, той комбинира няколко слоя на



OSI, като представителния и сесийния, в единен приложен слой (фиг 1.1.2.1).

фиг 1.1.2.1

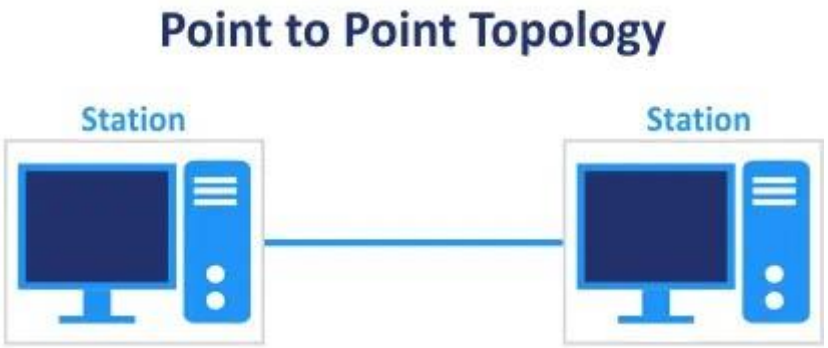
1.2 Мрежови топологии

Мрежовата топология се отнася до начина на подреждане на устройствата и връзките в една мрежа. Тя играе особена роля за определяне на ефективността, разходите, мащабируемостта и надеждността на мрежата. Съществуват различни видове топологии[2], които се използват в зависимост от специфичните нужди и ограничения на системата, включително точка-точка(point-to-point), звезда(star), мрежа (mesh), шинна(bus), пръстеновидна(ring), дървовидна(tree) и хибридна(hybrid) топология. Всяка от тях има свои уникални характеристики, предимства и недостатъци.

1.2.1 Топология point-to-point

Топологията point to point е най-простата форма на мрежа, при която две устройства са свързани директно чрез една

комуникационна връзка(фиг 1.2.1.1). Тази структура е особено ефективна в случаи, когато само две устройства трябва да комуникират, тъй като предаването на данни се извършва без намесата на други устройства. Простотата на тази топология осигурява висока скорост и сигурност на комуникацията с минимално забавяне. Въпреки това, мащабируемостта е ограничена, тъй като добавянето на нови устройства изисква създаване на отделни връзки за всяко ново устройство, което става непрактично за по-големи мрежи. Освен това, повреда на връзката напълно прекъсва комуникацията между устройствата, което прави топологията неподходяща за критични системи, които изискват резервиране. Въпреки ограниченията, топологията point to point се използва широко в ситуации, изискващи директна комуникация, като например свързване на периферни устройства към компютър.

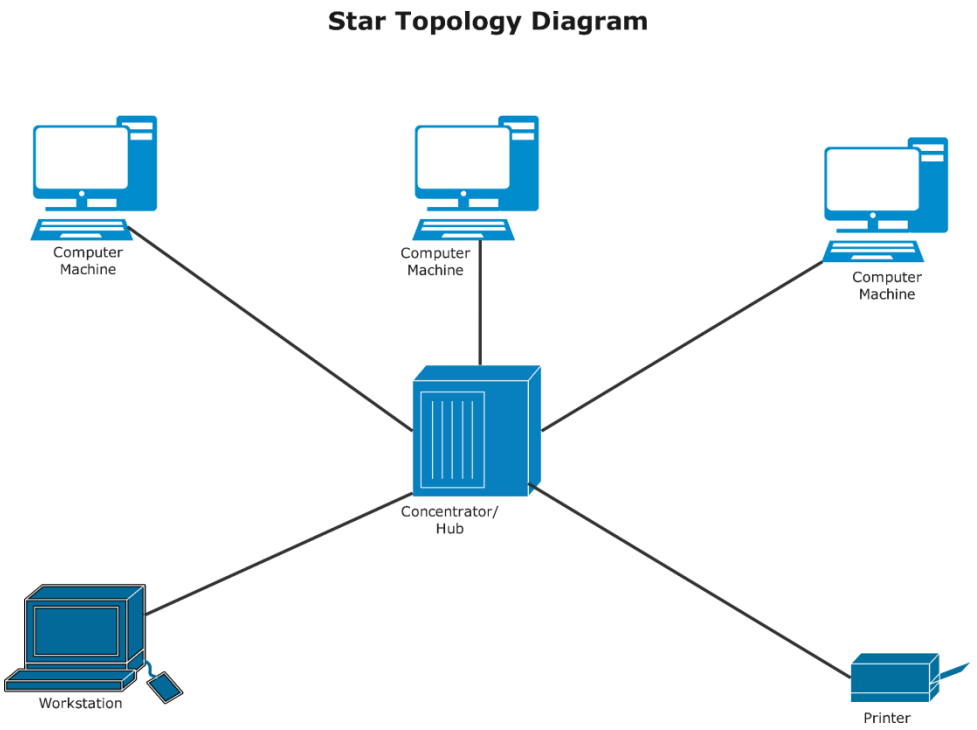


фиг 1.2.1.1

1.2.2 Топология star

Star топологията е една от най-популярните мрежови структури, особено в локалните мрежи (LAN). При тази топология всички устройства са свързани към централен хъб, комутатор или маршрутизатор, който управлява комуникацията между тях (фиг

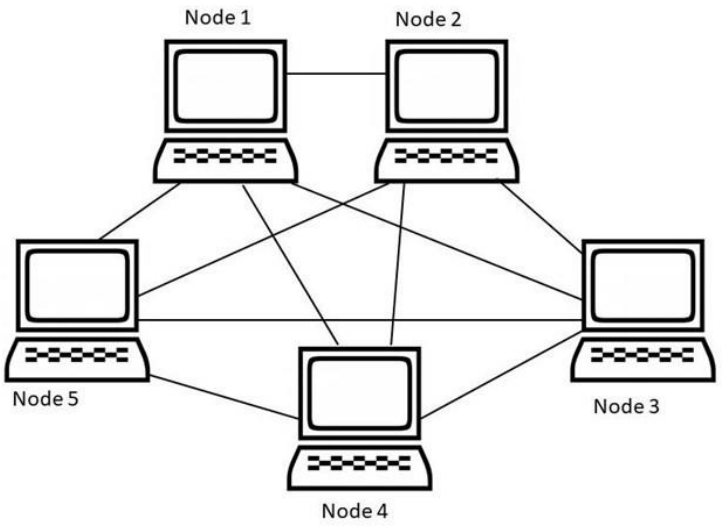
1.2.2.1). Централизираната структура улеснява диагностицирането на проблеми и поддръжката, тъй като неизправностите могат лесно да бъдат локализирани в отделно устройство или в централния хъб. Мащабируемостта също е значително предимство на тази топология – добавянето на нови устройства е лесно и не влияе на функционирането на съществуващите. Въпреки това, зависимостта от централния хъб представлява основен недостатък: ако хъбът се повреди, цялата мрежа спира да функционира. Но тази топология все пак остава предпочитана поради надеждността и лесното управление.



фиг 1.2.2.1

1.2.3 Mesh топология

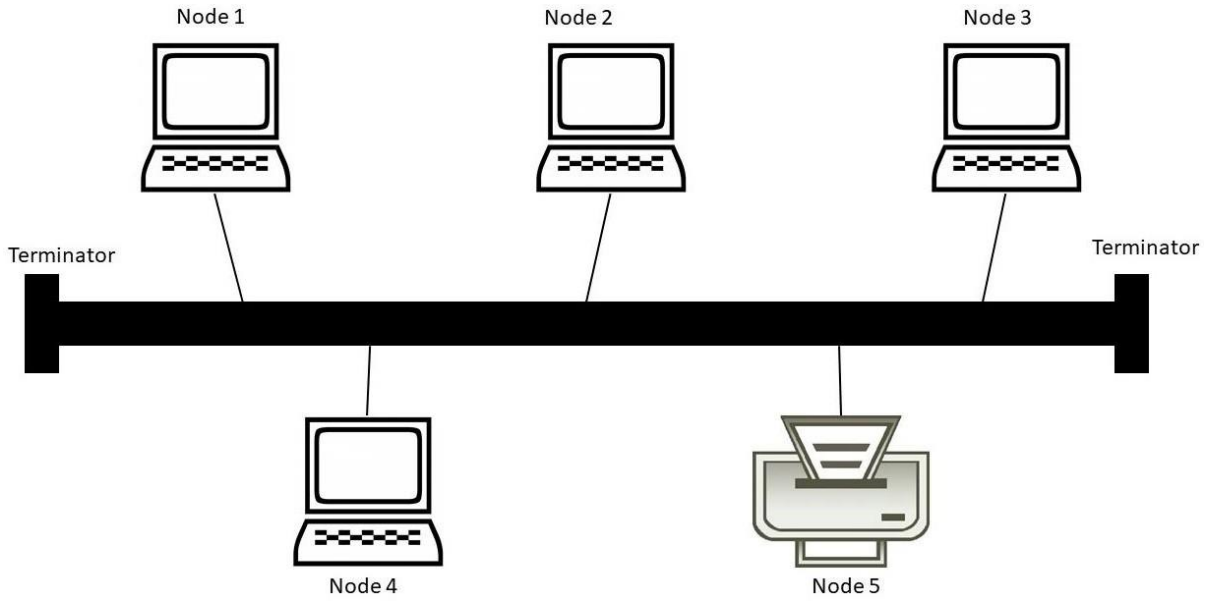
Mesh топологията осигурява високо свързана мрежа, при която всяко устройство е свързано с всички останали, било то директно в пълна мрежа или избирателно в частична мрежа(фиг 1.2.3.1). Тази структура предлага резервираност и надеждност, тъй като данните могат да преминават по множество маршрути. Ако една връзка се повреди, комуникацията може да продължи чрез алтернативни маршрути. Това прави mesh топологията особено подходяща за критични системи и мрежи с голям трафик. Въпреки това, предимствата идват с висока цена. Изграждането на mesh топология изисква значителни ресурси както за хардуер, така и за кабели, което я прави скъпа и сложна за изпълнение. Поддръжката и отстраняването на неизправности също могат да бъдат предизвикателство поради многото връзки. Въпреки тези трудности, mesh топологията често се използва в големи и надеждни мрежи, където надеждността е основен приоритет, като например в телекомуникациите и големите центрове за данни.



фиг 1.2.3.1

1.2.4 Bus топология

Bus топологията е проста и икономична структура, при която всички устройства споделят един общ комуникационен канал, наречен шина(фиг 1.2.4.1). Тази простота улеснява настройката и разширяването, тъй като нови устройства могат да бъдат свързани с минимални усилия. Въпреки това, общият характер на шината представлява значителни ограничения. С увеличаването на броя на устройствата мрежата става податлива на претоварване, което намалява общата ѝ производителност. Освен това, повреда на шината води до пълен срив на мрежата, което подчертава критична точка на отказ. Отстраняването на неизправности също може да отнеме време, тъй като дефектите трудно се локализират.

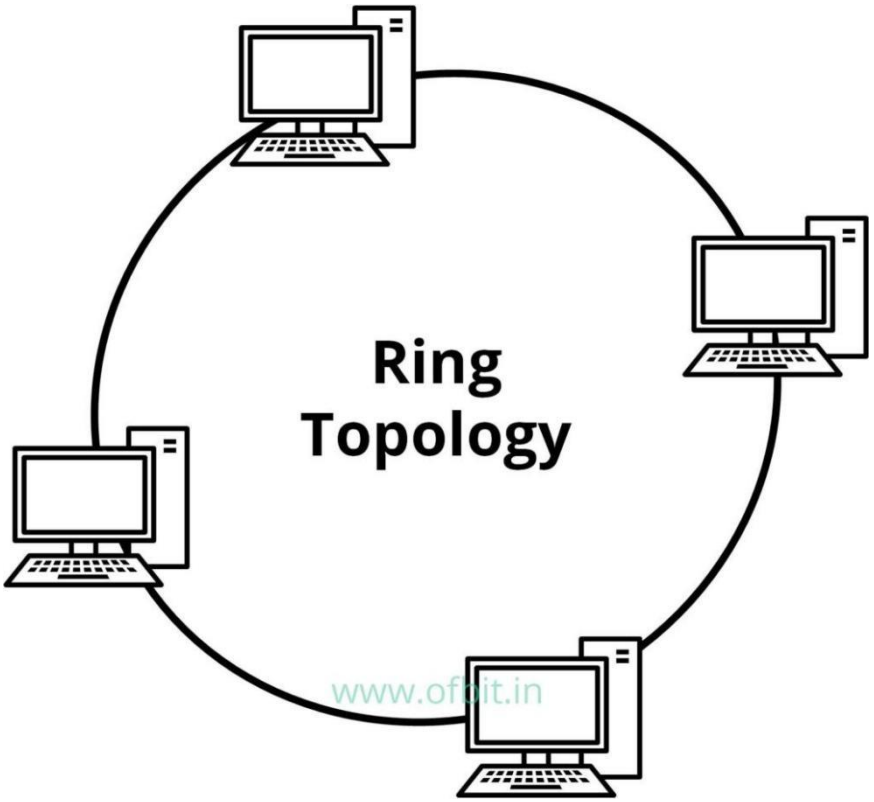


фиг 1.2.4.1

1.2.5 Ring топология

При ring топологията устройствата са свързани в кръг, като всяко устройство е свързано със съседните си(фиг 1.2.5.1). Данните

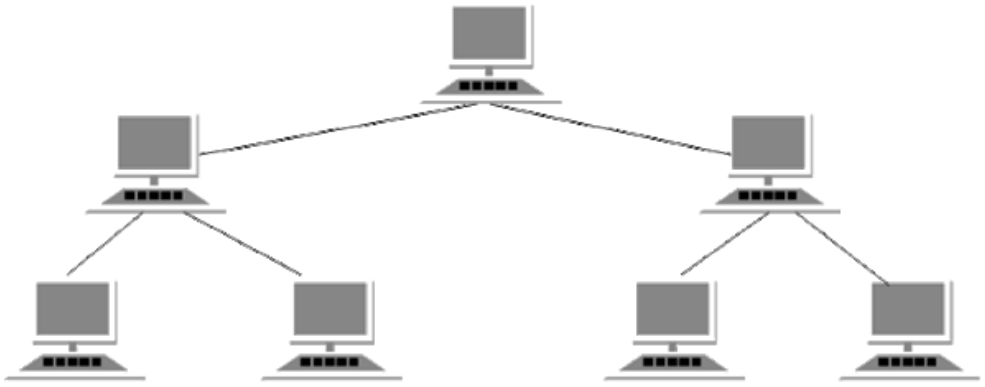
преминават през пръстена в една посока (еднопосочна) или в двете посоки (двупосочна). Този подреден поток на данни минимизира сблъсъците, като осигурява ефективна комуникация. Въпреки това, структурата на пръстена има своите недостатъци. Повреда на което и да е устройство или връзка може да наруши цялата мрежа, което прави устойчивостта на неизправности значително предизвикателство. Освен това, с увеличаването на броя на устройствата, латентността става проблем, тъй като данните трябва да преминат през множество устройства, за да достигнат до дестинацията. Въпреки тези ограничения, ring топологията все още се използва в определени сценарии, където ефективната и предсказуема комуникация е от съществено значение, като например в токен-ринг мрежи.



фиг 1.2.5.1

1.2.6 Дървовидна топология

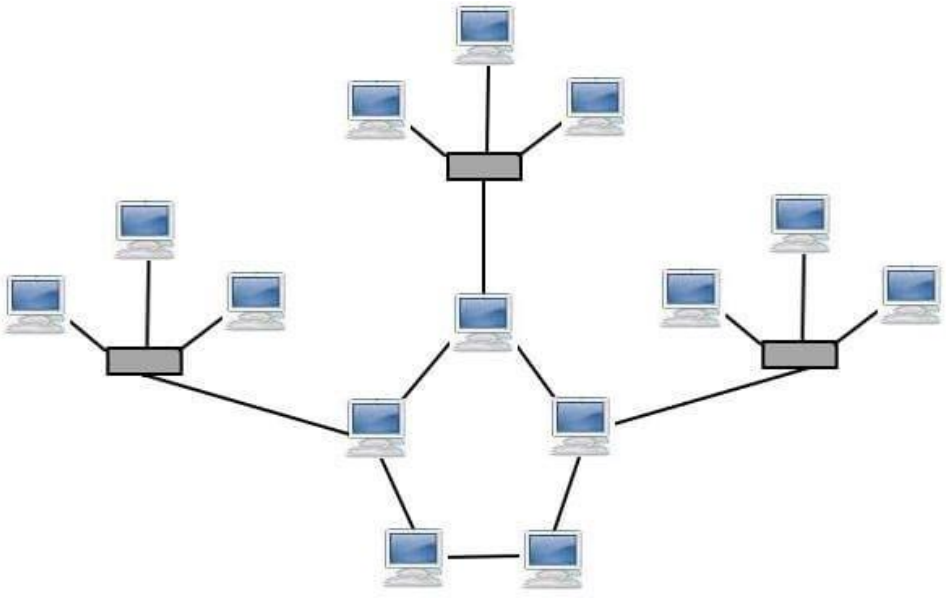
Дървовидната топология комбинира характеристиките на star и bus, създавайки йерархична структура от взаимосвързани устройства(фиг 1.2.6.1). Тази структура позволява изграждането на мащабируеми мрежи, тъй като нови устройства могат да се добавят към йерархията без големи промени. Структурата също така улеснява изолирането на неизправности; проблеми в един клон обикновено не засягат цялата мрежа. Въпреки това, зависимостта от централен гръбнак представлява уязвимост. Ако хъбът се повреди, комуникацията в мрежата се прекъсва. Освен това настройката и поддръжката на дървовидна топология изисква внимателно планиране и може да бъде скъпа поради обширното окабеляване и хардуер. Тази топология често се използва в големи организационни мрежи, където мащабируемостта и изолирането на грешки са приоритети.



фиг 1.2.6.1

1.2.7 Хибридна топология

Хибридната топология е универсален и гъвкав подход, който комбинира две или повече основни топологии, като star, mesh и bus, в една мрежа(фиг 1.2.7.1). Това позволява на мрежовите дизайнери да използват предимствата на различни топологии, като минимизират техните недостатъци. Например, хибридна мрежа може да използва топология star за централните хъбове и mesh топология за критичните устройства, изискващи висока резервираност. Тази гъвкавост прави хибридната топология подходяща за големи и сложни мрежи с разнообразни изисквания. Въпреки това, сложността на дизайна увеличава предизвикателствата при реализацията и поддръжката. Разходите за настройка също могат да бъдат високи поради разнообразието от хардуер и окабеляване. Хибридната топология остава широко използвана в корпоративните мрежи поради адаптивността и мащабируемостта си.

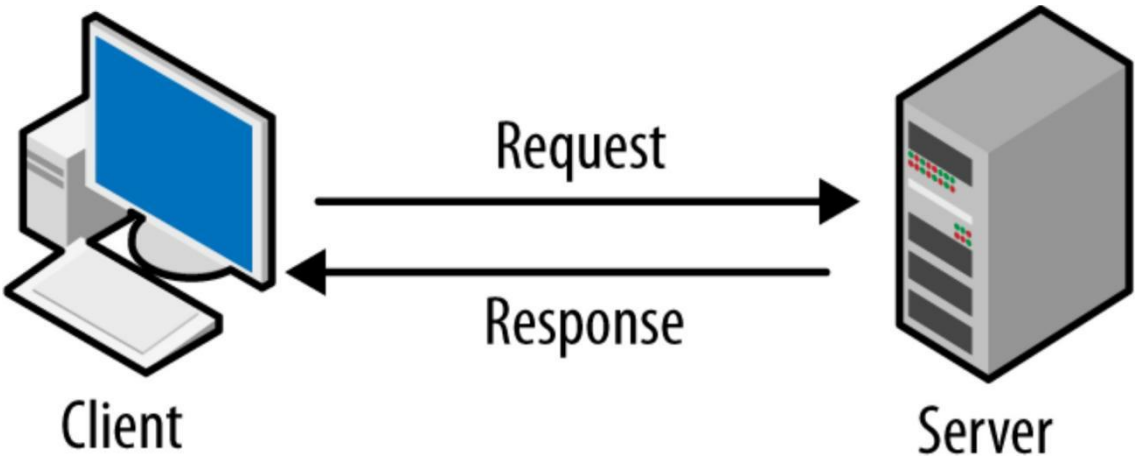


фиг 1.2.7.1

1.3 Мрежови устройства

1.3.1 Клиенти и сървъри

Клиентите и сървърите са основата на мрежовата комуникация, определени от своите роли в споделянето и достъпа до ресурси. Клиентът е устройство, което осъществява достъп до услуги, докато сървърът е устройство, което предоставя тези услуги(фиг 1.3.1.1). Тези роли са гъвкави - едно и също физическо устройство може да бъде клиент в един сценарий и сървър в друг, в зависимост от своята функция в мрежата. Например, сървър може да хоства уеб страница или база данни, а клиентът може да бъде лаптоп или смартфон, който извлича тази информация.



фиг 1.3.1.1

Сървърите често се асоциират с мощни компютри, предназначени да обработват заявки от много клиенти, като например сървър на Netflix, който стриймва филми към хиляди

потребители. Въпреки това, всяко устройство, включително персонални компютри или смартфони, може да действа като сървър, когато споделя ресурси. По същия начин клиентите варират от обикновени устройства като телевизори, които стриймват съдържание, до корпоративни системи, които достъпват вътрешни ресурси като електронни таблици.

Пример за динамичния характер на тези роли може да се види в домашните мрежи. Ако един компютър споделя филмов файл с друг, първият компютър действа като сървър, а вторият като клиент. Тази динамика демонстрира гъвкавостта на архитектурата клиент-сървър както в малки, така и в големи мрежи. Освен това и двата типа устройства често се наричат крайни точки (endpoints) или крайни хостове (end hosts), подчертавайки тяхната роля като източник или дестинация в мрежата.

1.3.2 Комутатори

Комутаторите[3] са основни компоненти на мрежовата инфраструктура, които позволяват комуникация между устройствата в рамките на локална мрежа. За разлика от крайните точки, комутаторите не инициират или прекратяват комуникация, а вместо това действат като посредници, насочващи данните между устройствата. Например, в офисна среда, комутаторите свързват компютри, принтери, камери за видеонаблюдение и сървъри, което позволява ефективно споделяне на ресурси и комуникация.

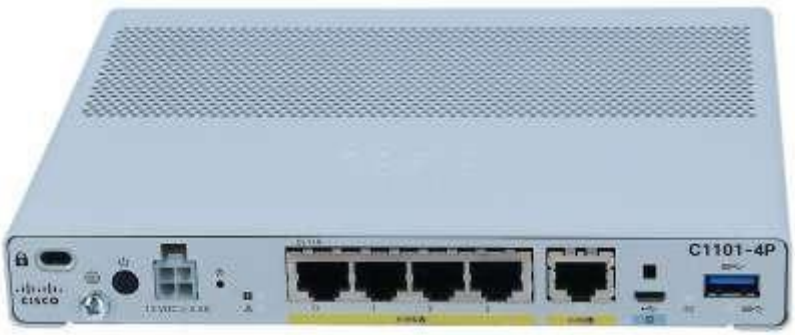
фиг 1.3.2.1

Комутаторите обикновено имат множество портове (или интерфейси), които служат като физически конектори за устройствата. Повечето комутатори разполагат с 24 до 48 порта, за да поддържат множество устройства едновременно(фиг 1.3.2.1). Тези портове се свързват с кабели, създавайки централен хъб за комуникация в рамките на LAN. Въпреки това, комутаторите са ограничени до управление на комуникацията в една мрежа и не могат да се свързват директно с външни мрежи, като например интернет.

Комутаторите използват напреднали технологии, за да осигурят ефективно предаване на данни между свързаните устройства. Въпреки че спецификата на тяхната работа включва сложни мрежови концепции, основната им цел е ясна: да осигурят плавна и надеждна комуникация в рамките на LAN. За да се разшири тази комуникация извън една локална мрежа или към интернет, е необходим друг тип устройство - маршрутизатор.

1.3.3 Маршрутизатори

Маршрутизаторите са предназначени да улеснят комуникацията между локални мрежи и външни мрежи, като например интернет(фиг 1.3.3.1). За разлика от комутаторите, които свързват устройства в рамките на една локална мрежа, маршрутизаторите работят на ръба на LAN-а, гарантирайки, че данните могат да пътуват между отделни мрежи. Например, маршрутизатор може да свърже домашна мрежа с интернет, което позволява на устройства като лаптопи и смартфони да имат достъп до онлайн услуги.

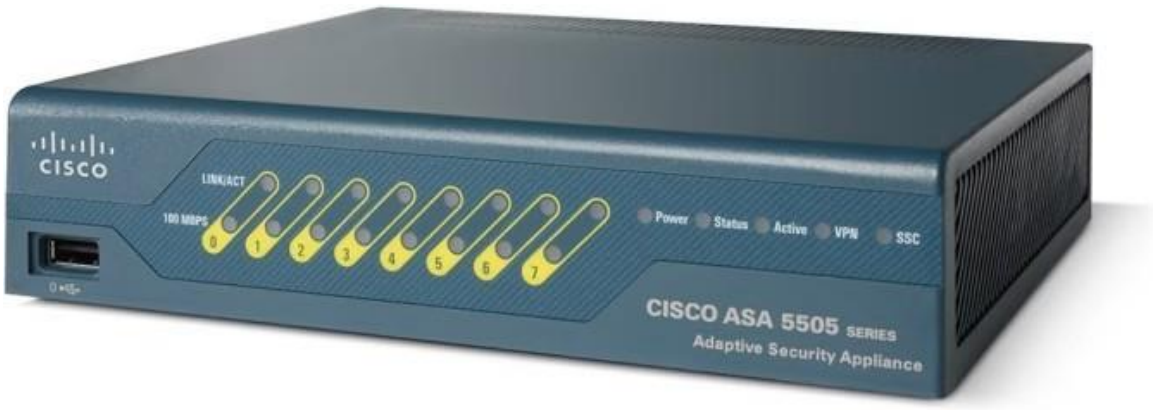


фиг 1.3.3.1

Маршрутизаторите играят критична роля в определянето на най-добрите пътища за предаване на данни между мрежите, което гарантира ефективна и надеждна комуникация. Те използват различни технологии и протоколи за маршрутизиране на пакети с данни, което ги прави незаменими при комуникация в голям мащаб. Докато комутаторите се фокусират върху вътрешната свързаност, маршрутизаторите осигуряват мост между вътрешни и външни мрежи.

1.3.4 Защитни стени

Когато устройствата са свързани към външни мрежи, като интернет, те са изложени на потенциални рискове за сигурността. За да се смекчат тези рискове, мрежите често използват защитни стени (firewalls). Те проверяват целия входящ и изходящ трафик и решават дали да го позволят или блокират въз основа на предварително зададени правила.



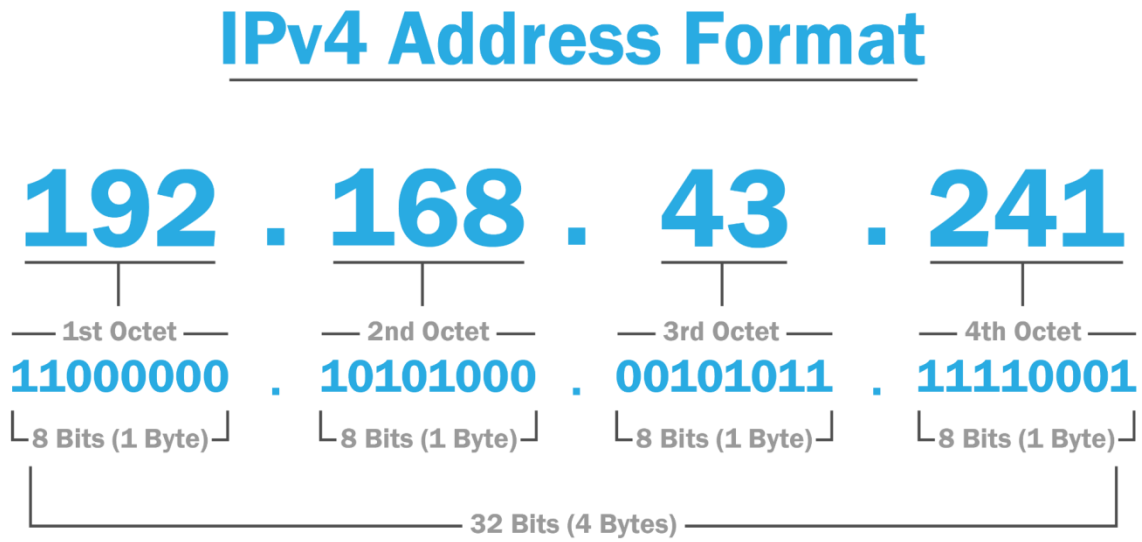
фиг 1.3.4.1

Докато персоналните устройства като компютри използват базирани на софтуер (host-based) защитни стени, по-големите мрежи разчитат на специализирани мрежови защитни стени, които работят в по-голям мащаб(фиг 1.3.4.1). Въпреки че основните устройства за мрежова инфраструктура са маршрутизатори и комутатори, защитните стени предоставят критичен слой защита, като гарантират, че само оторизиран трафик може да влиза и излиза от мрежата.

1.4 IP Адресиране

1.4.1 Основни концепции на IP

IPv4 адресът[4] е основен елемент в мрежовите комуникации, който служи като идентификатор за устройствата в мрежата. IPv4 адресите са съставени от 32 бита, разделени на четири групи по 8 бита, наречени октети. Тези битове се представят в точково десетично(dotted decimal) означение за по-лесно възприемане от хората. Например, двоичният адрес 11000000.10101000.00101011.11110001 се представя в десетичен вид като 192.168.43.241(фиг 1.4.1.1). Тази структура е от съществено значение за разграничаване на устройствата и мрежите в локални и глобални комуникации.

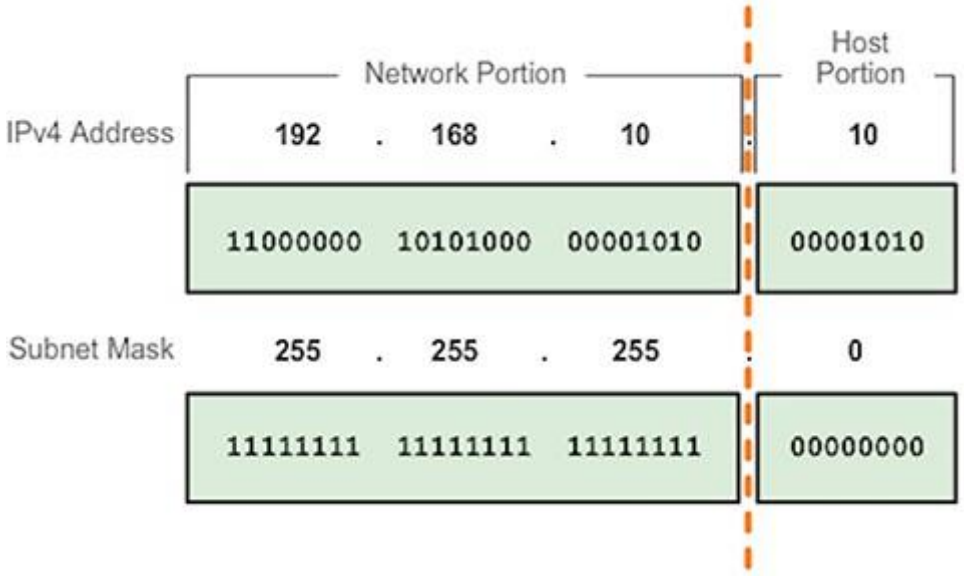


фиг 1.4.1.1

1.4.2 Дължина на префикса: Определяне на мрежовата част

Дължината на префикса, отбелязана като /X, указва броя на битовете, използвани за мрежовата част на IP адреса. В примера 192.168.43.241/24, префиксът /24 означава, че първите 24 бита (192.168.43) принадлежат към мрежовата част, а останалите 8 бита (.241) представляват хостовата част.

Мрежовата част се споделя от всички устройства в една и съща мрежа. Например, всички устройства в локална мрежа с адрес 192.168.10.0/24 ще имат еднакви първи три октета, като например 192.168.10.1 или 192.168.10.10(фиг 1.4.2.1). Въпреки това, всички устройства ще имат уникална хостова част, за да се различават в рамките на тази мрежа.

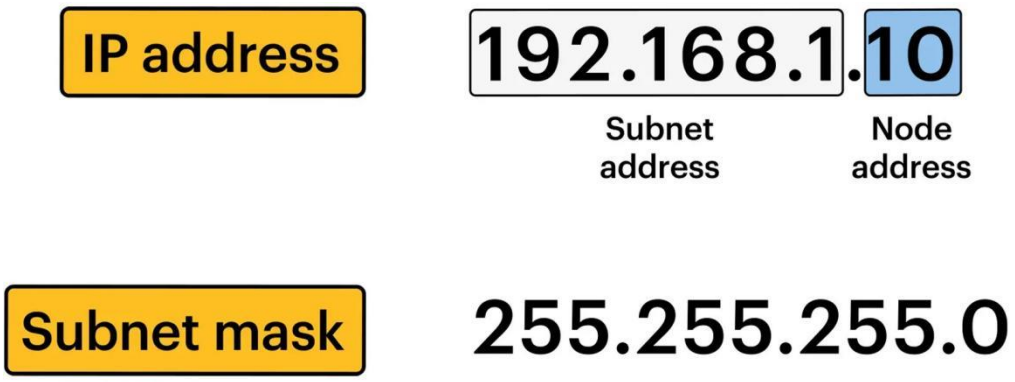


фиг 1.4.2.1

1.4.3 Подмрежови маски

Вместо да се използва нотацията /X, мрежовата и хостовата части могат да бъдат указани чрез подмрежова маска. Подмрежовата маска е 32-битово число, което съответства на IP адреса и указва коя част представлява мрежата и коя част представлява хоста(фиг 1.4.3.1). Битовете в подмрежовата маска, зададени на 1, показват мрежовата част, докато тези, зададени на 0, показват хостовата част. Например:
IP адрес: 172.16.20.21
Подмрежова маска: 255.255.0.0
В двоичен вид подмрежовата маска 255.255.0.0 се превежда като 11111111.11111111.00000000.00000000, което означава, че първите 16 бита от IP адреса (172.16) принадлежат към мрежовата част, а останалите битове (20.21) към хостовата част. Тази подмрежова маска е еквивалентна на дължина на префикс /16.

Подмрежовите маски са особено полезни за разделяне на голяма мрежа на по-малки подмрежи, което може да подобри сигурността и управляемостта. Чрез персонализиране на подмрежовите маски, мрежовите администратори могат ефективно да разпределят IP диапазони и да контролират размера на мрежите.



фиг 1.4.3.1

1.4.4 Цел на подмрежовите маски

Подмрежовите маски са от съществено значение за определяне дали две устройства са в една и съща мрежа. Когато две устройства се опитват да комуникират, техните подмрежови маски се прилагат към IP адресите, за да се идентифицира мрежовата част. Ако мрежовите части съвпадат, устройствата могат да комуникират директно. В противен случай тяхната комуникация трябва да премине през маршрутизатор, за да достигнат едно до друго.

1.5 Маршрутизация

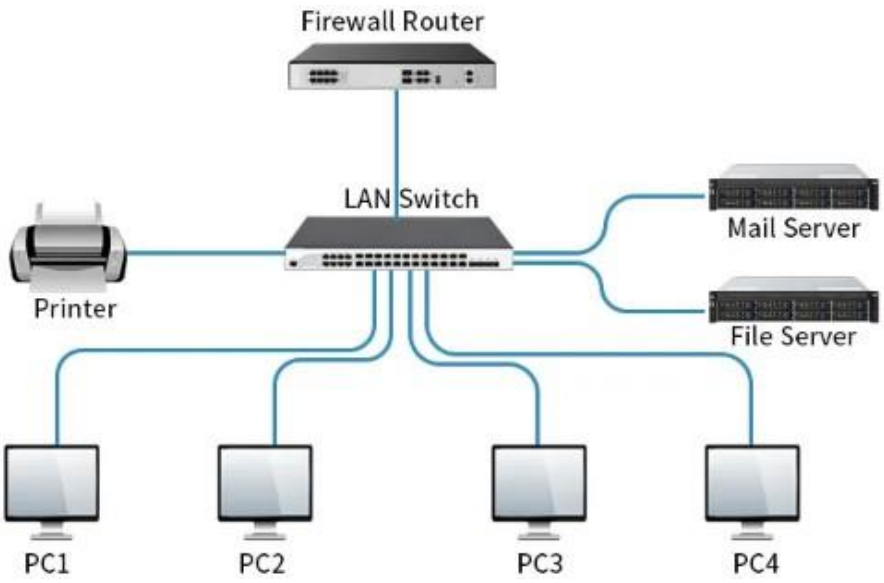
1.5.1 Основи на маршрутизацията и видове маршрути

Маршрутизацията[5] е ключов процес в компютърните мрежи, който определя как пакетите се предават от източника до дестинацията. Различните методи за маршрутизация предоставят на маршрутизаторите гъвкавост при обработката на пакети,

базирайки се на информацията в таблицата за маршрутизация и конфигурацията на мрежата.

- Изпращане на пакети в рамките на една и съща мрежа

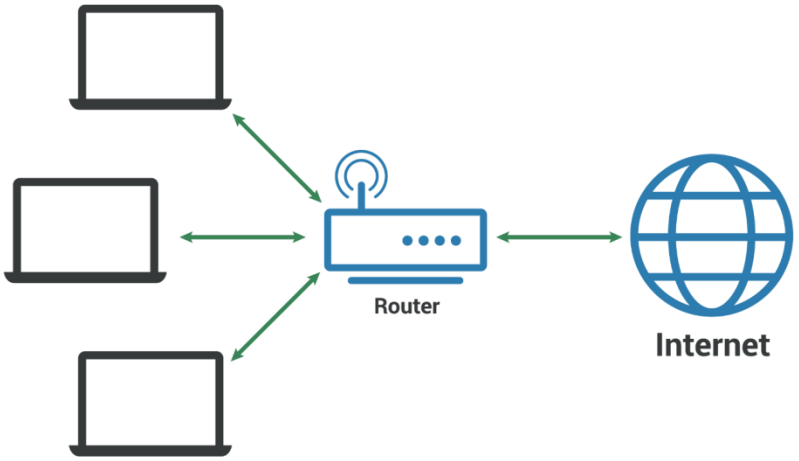
Ако дестинацията на пакета е в същата мрежа като изпращача, не е необходимо използването на маршрутизатор. В този случай пакетът се капсулира в рамка, чийто MAC адрес на дестинацията съвпада с MAC адреса на целевото устройство(фиг 1.5.1.1).



фиг 1.5.1.1

- Изпращане на пакети към различна мрежа

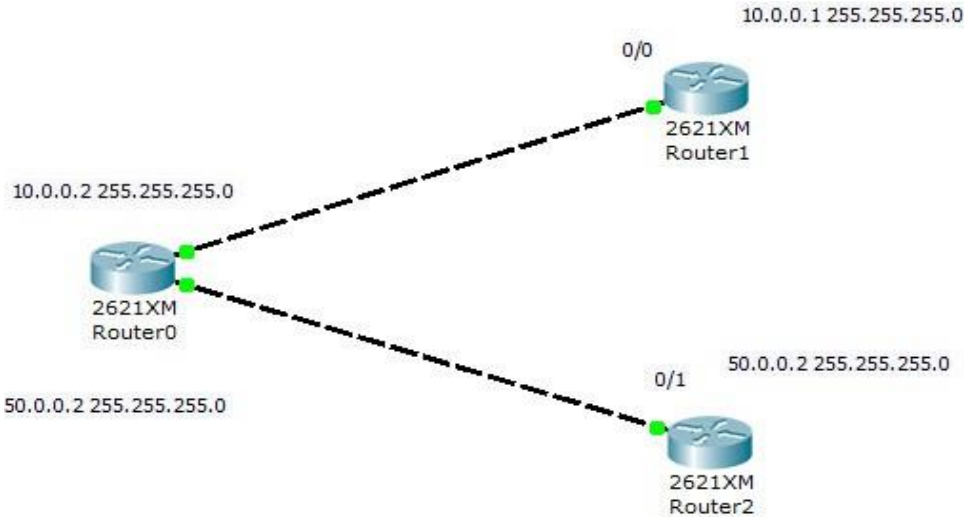
Когато крайното устройство трябва да изпрати пакет към дестинация извън своята локална мрежа, то използва шлюза по подразбиране (default gateway), обикновено маршрутизатор, за да препрати пакета(фиг 1.5.1.2). В този случай устройството енкапсулира пакета в рамка, като задава MAC адреса на дестинацията да съвпада с MAC адреса на интерфейса на маршрутизатора в същата мрежа.



фиг 1.5.1.2

- Свързани маршрути

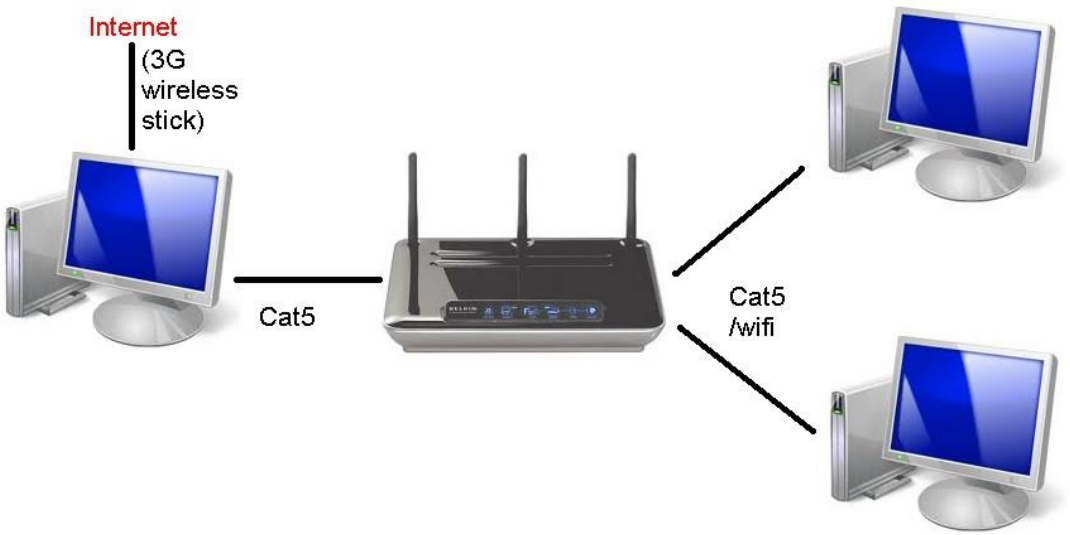
Свързаните маршрути представляват маршрути до мрежите, към които интерфейсът на маршрутизатора е директно свързан (фиг 1.5.1.3). При всяко свързано устройство с IP адрес, което е в up/up състояние, се добавя един свързан маршрут в таблицата за маршрутизация. Свързаните маршрути се използват за лесно и бързо предаване на пакети в локалните мрежи. Те осигуряват основата за комуникация в директно свързани сегменти на мрежата.



фиг 1.5.1.3

- Локални маршрути

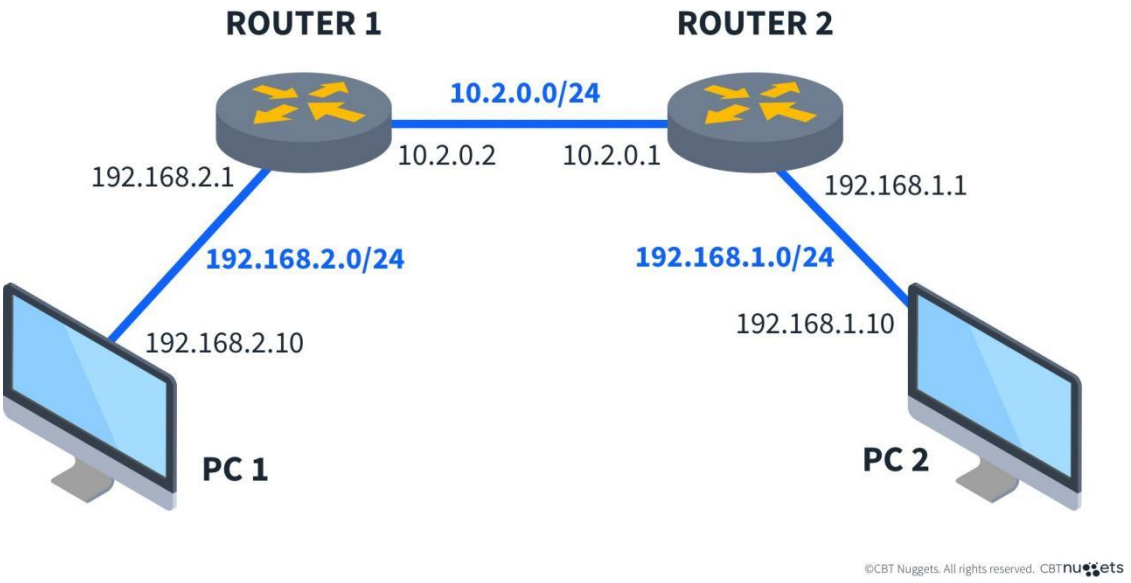
Локалните маршрути, за разлика от свързаните маршрути, посочват точно IP адреса на интерфейса на маршрутизатора. Всеки локален маршрут се добавя автоматично към таблицата за маршрутизация с дължина на префикса /32, независимо от префикса на мрежата, към която е свързан интерфейсът. Локалните маршрути са важни, защото разграничават адреса на маршрутизатора от другите адреси в същата мрежа. Ако няма локален маршрут, маршрутизаторът може погрешно да препраща пакети, предназначени за него самия, към друго устройство в мрежата(фиг 1.5.1.4).



фиг 1.5.1.4

1.5.2 Статична маршрутизация

Статичната маршрутизация се използва, когато маршрути се конфигурират ръчно от администратор. Тази техника е особено полезна за мрежи с предвидима и стабилна структура, където маршрутите рядко се променят(фиг 1.5.2.1).



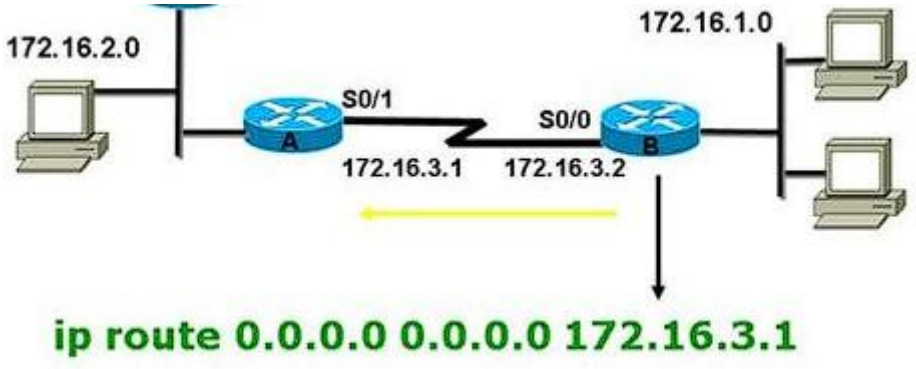
фиг 1.5.2.1

Когато маршрутизатор трябва да препрати пакет към дестинация, която не е в директно свързана мрежа, администраторът може ръчно да добави статичен маршрут.

Основно предимство на статичната маршрутизация е нейната предсказуемост. Въпреки това, тя изисква ръчно обновяване при промяна на мрежовата топология, което я прави по-малко подходяща за големи или динамични мрежи.

- Конфигуриране на маршрут по подразбиране

Маршрутът по подразбиране (default route) е най-общият маршрут, който може да бъде конфигуриран в маршрутизатора. Той използва дестинация 0.0.0.0/0, която съответства на всички IP адреси(фиг 1.5.2.2).



фиг 1.5.2.2

Маршрутите по подразбиране се използват за пренасочване на пакети към дестинации, за които няма по-специфични маршрути в таблицата. Това често се използва за предоставяне на връзка към интернет.

Конфигурирането на маршрут по подразбиране е особено важно за оптимизацията на таблицата за маршрутизация, тъй като премахва необходимостта от съхраняване на подробна информация за всички възможни мрежи в интернет.

1.5.3 Динамична маршрутизация

Динамичното маршрутизиране е процес, който позволява на маршрутизаторите автоматично да споделят информация за мрежата помежду си, което им дава възможност да създават и актуализират своите таблици за маршрутизиране, без да е необходимо ръчно конфигуриране за всеки маршрут. Чрез използването на протоколи за маршрутизиране, маршрутизаторите комуникират и обменят информация за маршрути, която използват, за да определят динамично най-добрите пътища за пренасочване

на пакети в мрежата. Тази възможност значително подобрява ефективността и адаптивността на мрежите, особено в среди, където топологията на мрежата е подложена на чести промени.

- Мащабируемост на динамичната маршрутизация

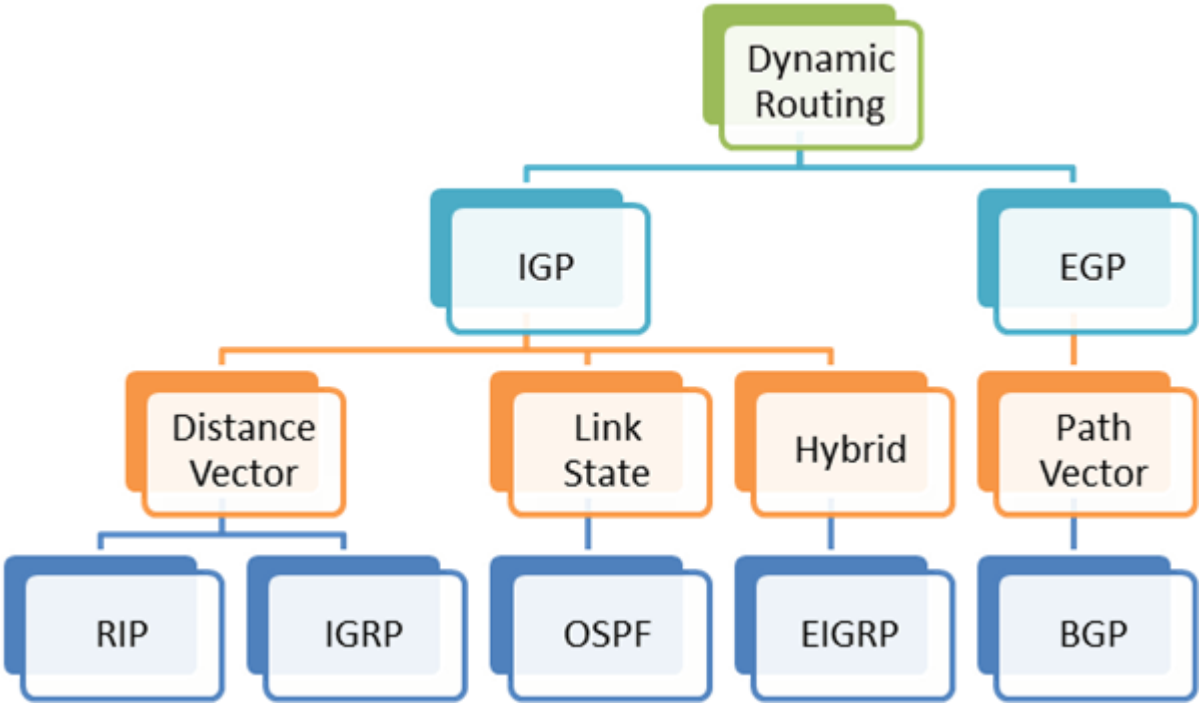
Едно от най-значимите предимства на динамичното маршрутизиране е неговата мащабируемост. Докато статичното маршрутизиране може да бъде достатъчно за малки мрежи, то става все по-неудобно и податливо на грешки с увеличаване на размера и сложността на мрежите. Динамичните протоколи за маршрутизиране са проектирани да се справят с големи и сложни мрежови инфраструктури. Те не само опростяват управлението на обширни мрежи, но и гарантират, че маршрутизаторите могат автоматично да се адаптират към промени, като добавяне на нови подмрежи, повреди на връзки или променливи модели на трафик.

- Видове протоколи за маршрутизиране

Динамичните протоколи за маршрутизиране се делят на два основни типа: протоколи за вътрешна шлюзова маршрутизация (IGP) и протоколи за външна шлюзова маршрутизация (EGP). IGP се използват в рамките на една автономна система (AS), която обикновено представлява мрежата на една организация или предприятие. Тези протоколи гарантират, че маршрутизаторите в една и съща автономна система споделят информация и сътрудничат за изграждането на консистентен изглед на мрежата. Примери за IGP са Routing Information Protocol (RIP), Open Shortest Path First (OSPF) и Enhanced Interior Gateway Routing Protocol (EIGRP). Всеки от тези протоколи има свои характеристики и механизми за определяне на най-добрите пътища въз основа на

фактори като брой скокове(hops), цена на връзката или честотна лента(фиг 1.5.1.3).

EGP, от друга страна, се използват за обмен на информация за маршрути между различни автономни системи. Те са от съществено значение за свързването на различни мрежи, като тези на различни предприятия или интернет доставчици (ISP). Border Gateway Protocol (BGP) е най-широко използваният EGP и служи като гръбнак на интернет маршрутизацията. BGP позволява на маршрутизаторите да споделят информация за достъпни мрежи и да установяват политики за контролиране на трафика между автономните системи. По този начин се осигурява ефективна и надеждна свързаност в глобалния интернет.



фиг 1.5.3.1

- Функции на протоколите за динамична маршрутизация

Работата на динамичните протоколи за маршрутизиране включва периодичен обмен на информация за маршрути между маршрутизаторите. Този процес позволява на маршрутизаторите да научават за нови маршрути, да откриват промени в мрежата и да актуализират съответно своите таблици за маршрутизиране. Повечето протоколи разчитат на специфични алгоритми за изчисляване на най-добрите пътища. Например, OSPF използва алгоритъма на Дейкстра за най-кратък път, докато RIP използва алгоритъма на Белман-Форд. Тези алгоритми отчитат различни метрики, като разстояние, забавяне или стойност, за да определят оптималния маршрут за пренасочване на пакети.

Динамичното маршрутизиране също така подобрява устойчивостта на мрежите. Когато връзка се повреди или стане претоварена, маршрутизаторите, използващи динамични протоколи, могат бързо да идентифицират алтернативни пътища и да пренасочат трафика, за да поддържат свързаността. Тази адаптивност минимизира времето на прекъсване и осигурява ефективно използване на наличните мрежови ресурси. Освен това, тъй като динамичното маршрутизиране автоматично разпространява промените в цялата мрежа, то намалява административното натоварване, свързано с ръчното преконфигуриране на маршрутите в отговор на мрежови модификации.

Въпреки нуждата от повече изчислителни ресурси в сравнение със статичното маршрутизиране предимствата на динамичното маршрутизиране, особено по отношение на мащабируемост,

адаптивност и автоматизация, го правят важен инструмент за съвременните мрежи.

1.6 Протокол за динамично маршрутизиране EIGRP

1.6.1 Основни понятия за EIGRP

Enhanced Interior Gateway Routing Protocol (EIGRP)[6] е хибриден протокол за маршрутизиране с динамично разстояние и състояние на връзката. EIGRP изпраща ъпдейти на маршрута до маршрутизатори в рамките на същата автономна система. Обикновено EIGRP открива съседни маршрутизатори с помощта на мултикаст ъпдейти, но могат да се конфигурират статични съседи, които са извън границата на мултикаст, и тези статични съседи получават едноадресни ъпдейти.

Конвергентната технология на EIGRP се основава на алгоритъм, наречен Diffusing Update Algorithm (DUAL). Алгоритъмът гарантира работа без създаване на цикъл във всеки момент по време на изчисляване на маршрута и позволява на всички устройства, участващи в промяна на топологията, да се синхронизират. Устройства, които не са засегнати от промени в топологията, не участват в повторните изчисления.

1.6.2 Процес на обмен на маршрути (DUAL алгоритъм)

DUAL крайното състояние на машината представлява процеса на вземане на решения за изчисляване на маршрути. Проследяват се всички маршрути, рекламирани от всички съседи. Използва се информация за разстоянията (наричана метрика), за да се изберат ефективни и безциклови маршрути.

Маршрутите, добавяни в таблицата с маршрути, се избират въз основа на допустими наследници. Наследник е съседно устройство (използвано за препращане на пакети), което осигурява път с най-ниска цена до дестинацията и гарантирано не е част от цикъл в маршрута.

При промяна в топологията се проверява за наличие на допустими наследници. Ако такива съществуват, те се използват, за да се избегне ненужно преизчисляване.

Когато няма допустими наследници, но съществуват съседи, рекламиращи дестинацията, се налага преизчисляване за определяне на нов наследник. Времето, необходимо за преизчисляване на маршрута, влияе върху времето за конвергенция.

1.6.3 EIGRP Метрични тегла

EIGRP използва метрични тегла, известни като K-стойности, при изчисляване на маршрути и метрики(фиг 1.6.3.1). Стойностите

по подразбиране за EIGRP метриките са внимателно подбрани, за да осигурят оптимална производителност в повечето мрежи.

K Value	Component	Description	Default Cisco Device value
K1	Bandwidth	Lowest bandwidth of route	1
K2	Load	Worst load on route based on packet rate	0
K3	Delay	Cumulative interface delay of route	1
K4	Reliability	Worst reliability of route based on keep alive	0
K5	MTU	Smallest MTU in path	0

фиг 1.6.3.1

1.6.4 EIGRP Метрични разходи

Освен K-стойности, EIGRP използва и характеристиките на връзката, за да изчисли комбинирана метрична стойност. За да се избегне нестабилност в мрежата при промяна на характеристиките на връзката, могат да се настроят някои от стойностите, използвани при изчислението.

Изчислението включва пет K-стойности (като множители) и пет векторни атрибута(фиг 1.6.4.1). По подразбиране три от K-стойностите са 0, което значително опростява формулата:

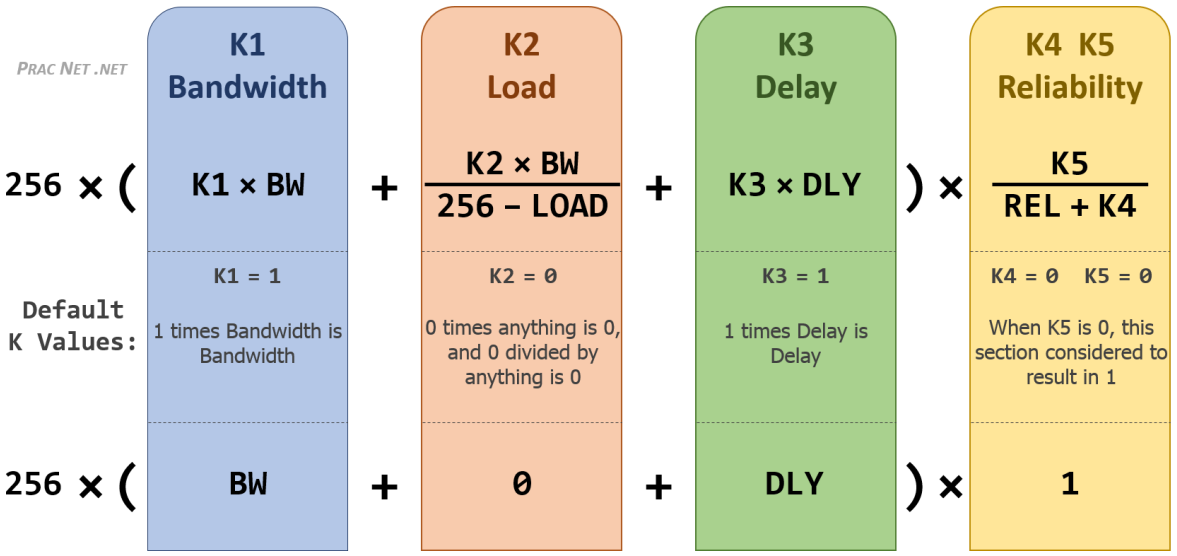
- метрична стойност = 256 * (пропускателна способност + закъснение)

Могат да се променят стойностите за пропускателна способност и закъснение за маршрути, които се преразпределят към или от процеса на EIGRP. Конкретно, тези стойности могат да се зададат чрез командата default-metric (за задаване на стойности по подразбиране за всички видове преразпределени маршрути) или чрез командата redistribute metric (за задаване на стойности за конкретен тип маршрут).

Пропускателна способност (Bandwidth): Представлява минималната пропускателна способност на маршрута, в килобита за секунда, като диапазонът е от 1 до 4 294 967 295 Kbps. Във формулата пропускателната способност се мащабира и обръща чрез следната формула:

- (10^7 / минимална пропускателна способност в килобита за секунда)
- Закъснение (Delay): Представлява закъснението на маршрута, измерено в десети от микросекунда.

Останалите характеристики, които не се използват от защитни устройства, включват надеждността на връзката, ефективното натоварване на маршрута и минималното MTU (maximum transmission unit) на маршрута. Въпреки че тези стойности не се използват, те трябва да се конфигурират, ако се правят промени чрез споменатите команди.



фиг 1.6.4.1

1.7 Мрежова сигурност

1.7.1 Основни концепции за сигурност

- Какво означава една мрежа да бъде сигурна

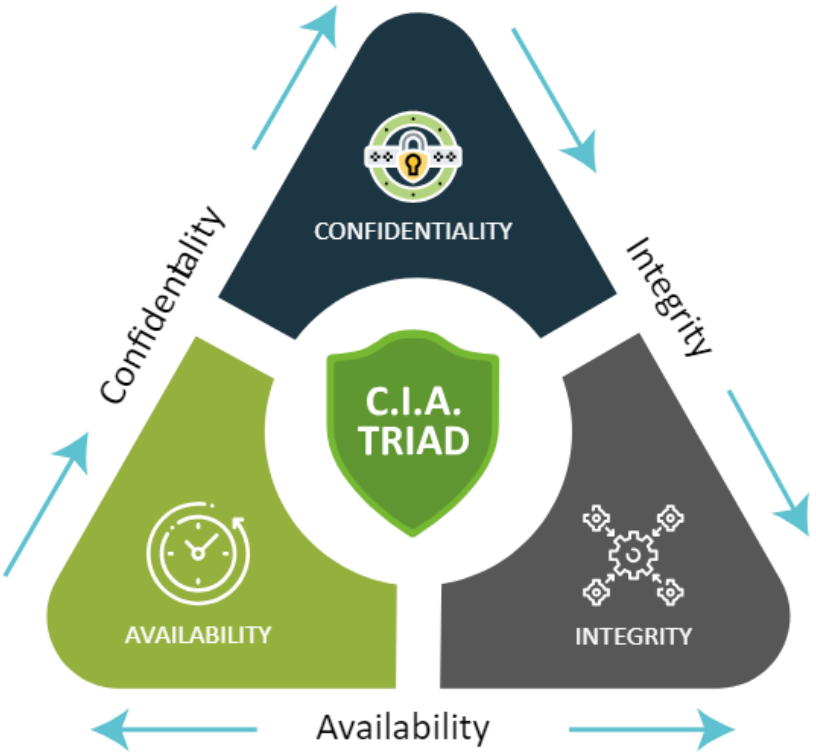
Концепцията за мрежова сигурност се основава на защитата на мрежата и свързаните с нея устройства от неоторизиран достъп, злоупотреба и злонамерени действия. Сигурността гарантира, че системите и данните остават защитени, като същевременно са достъпни и надеждни за оторизирани потребители.

- Триадата на сигурността (CIA)

Триадата на сигурността (CIA) е основна рамка, която определя целите на информационната сигурност. Тя се състои от конфиденциалност(confidentiality), интегритет(integrity) и наличност(availability). Конфиденциалността гарантира, че системите и данните са достъпни само за оторизирани лица. Защитата на конфиденциалността включва използването на

механизми като контрол на достъпа, криптиране и други мерки за предотвратяване на неоторизиран достъп. Интегритетът осигурява, че системите и данните са надеждни. Данните не трябва да бъдат променяни по време на съхранение или предаване, освен от оторизирани потребители. Механизми като контроли на суми(checksum), хеширане(hesh) и сигурни протоколи за предаване поддържат интегритета на данните. Наличността осигурява, че системите и данните са достъпни за оторизирани потребители, когато това е необходимо. Наличността се поддържа чрез механизми за резервиране, автоматично превключване и защита срещу прекъсвания като атаки от тип "отказ на услуга" (DoS).

Триадата на сигурността представлява трите основни елемента на сигурността. При ефективно прилагане тези принципи гарантират защитата на системите чрез предотвратяване на неоторизиран достъп, неоторизирани промени и недостъпност. Както е показано на фигура 1.7.1.1, тези елементи се свързват взаимно, за да образуват триадата. При възникване на проблеми със сигурността анализирайте как конкретни атаки влияят на конфиденциалността, интегритета или наличността на системата и как мерките за сигурност отговарят на тези предизвикателства.



фиг 1.7.1.1

- Уязвимости, експлойти и заплахи

Нито една система не е напълно сигурна – всяка система има слабости, които могат да бъдат експлоатирани. Тези слабости формират основата на заплахите за мрежовата сигурност. Уязвимостта е потенциална слабост в система или данни, която може да компрометира тяхната сигурност. Например, некоректна конфигурация на софтуер може да представлява уязвимост. Експлойтът е инструмент, техника или действие, което използва уязвимост, за да причини вреда. Например, използването на зловреден софтуер за експлоатация на слаба парола е експлойт. Заплахата е реалната възможност уязвимостта да бъде експлоатирана. Заплахата е актьор или събитие, което цели да навреди на системата, като използва уязвимости.

Нека кажем, че нашата система е една къща. Прозорецът представлява уязвимост, камъкът, който може да счупи прозореца, е експлойт, а натрапникът, който планира да хвърли камъка, е заплаха. Мерките за сигурност – като поставянето на метални решетки на прозорците – намаляват заплахите, като адресират уязвимостите. В контекста на мрежовата сигурност, например, злонамерен актьор, който експлоатира уязвимости в протокола DHCP, представлява заплаха. Техники за смекчаване като DHCP Snooping спомагат за защитата на тези уязвимости.

- Чести заплахи

Съвременните мрежи са изправени пред широк спектър от заплахи, които могат да компрометират тяхната конфиденциалност, интегритет и наличност. Атаките от тип "отказ на услуга" (DoS) нарушават работата на целевата система, правейки я недостъпна за легитимните потребители, и основно компрометират наличността. Един често срещан вид DoS атака е SYN flood. В този случай нападателят залива целевия сървър със SYN съобщения за иницииране на TCP връзки. Целта отговаря със SYN-ACK съобщения, като резервира ресурси за всяка връзка. Нападателят никога не завършва ръкостискането, оставяйки таблицата за връзки на целевата система запълнена с незавършени връзки. Това води до невъзможност легитимните потребители да се свържат със сървъра. Когато атаката се извършва от ботнет (мрежа от заразени устройства), тя се класифицира като разпределена атака от тип "отказ на услуга" (DDoS).

Атаките със spoofing включват фалшифициране на идентичността на устройство, често чрез използване на фалшиви IP

или MAC адреси. Примери включват SYN flood атаки с фалшиви IP адреси за прикриване на самоличността на нападателя и DHCP изтощение, при което фалшиви MAC адреси изчерпват IP адресите на DHCP сървъра, отказвайки достъп на легитимните устройства. При такава атака нападателят изпраща фалшиви заявки до трети сървъри (рефлектори), принуждавайки ги да изпращат отговори към целта, претоварвайки я. Ако отговорите са непропорционално големи спрямо заявките, атаката се класифицира като усилена атака.

Атаките "човек в средата" (MITM) възникват, когато нападателят прихваща комуникация между две страни, получавайки достъп до чувствителни данни или променяйки съобщенията. Например, ARP отравянето пренасочва мрежовия трафик към нападателя чрез изпращане на фалшиви ARP отговори. Разузнавателните атаки събират информация за целевата система, често като подготовка за други атаки. Разузнаването може да включва публично достъпни данни (разузнаване от открити източници) или инструменти като WHOIS за получаване на контактни данни за собствениците на домейни.

- Зловреден софтуер

Зловреднният софтуер(malware) включва вредни програми, които заразяват устройства и извършват злонамерени дейности. Обичайни видове зловреден софтуер включват вируси(virus), които се прикрепят към легитимни програми и се разпространяват при изпълнение; червеи(worms), които се разпространяват без човешка намеса чрез експлоатиране на мрежови уязвимости; троянски коне(trojan), които се представят за легитимен софтуер, за да

измамят потребителите да ги изпълнят; бекдори(backdoor), които предоставят неоторизиран достъп до заразени устройства; и рансъмуер(ransomware), който криптира файлове и изисква плащане за тяхното декриптиране. Много видове зловреден софтуер разчитат на човешки действия, като отваряне на злонамерени прикачени файлове към имейли.

- Атаки, свързани с пароли

Паролите остават критичен компонент на автентикацията, но са уязвими към различни атаки. Познаването използва лична информация (например рождени дни), получена чрез разузнаване. Атаките с речници(dictionary) използват автоматизирани инструменти за тестване на често срещани пароли, докато “brute force” атаките тестват всяка възможна комбинация от пароли. Техники за намаляване на риска включват използването на силни, сложни пароли и активирането на допълнителни нива на защита, като двуфакторна автентикация (2FA).

1.7.2 Интернет VPN

В мрежовата среда терминът "WAN" (широкообхватна мрежа) се отнася до мрежа, обхващаща голяма географска площ, обикновено използвана за свързване на отдалечени обекти като клонове или центрове за данни. Въпреки че интернетът отговаря на широкото определение за WAN, публичната му същност контрастира с частния характер на повечето WAN мрежи. Интернетът обаче може да служи като среда за сигурна комуникация между отдалечени обекти, когато се комбинира с виртуални частни мрежи (VPNs)[7].

- Преглед и функционалност на VPN

Виртуалната частна мрежа (VPN) е технология, която създава защитена връзка чрез обществени мрежи, като интернет, или частни мрежи, например корпоративен интранет. Основната цел на VPN е да гарантира поверителност, сигурност и анонимност чрез криптиране на данните и скриване на IP адреса на потребителя. Той използва протоколи за тунелиране, за да създаде сигурна връзка между устройства. Данните се прехвърлят през криптиран тунел, който защитава информацията от неупълномощен достъп. Тази технология често се използва за осигуряване на дистанционен достъп, защита на личните данни и заобикаляне на географски ограничения.

- Предимства на VPN мрежите

VPN технологиите предоставят множество предимства, които ги правят изключително полезни както за корпоративни, така и за лични потребители. Основното предимство е подобрената сигурност. Тя предпазва потребителите от хакери и други злоумишлени действия.

Дистанционният достъп е друго предимство, което позволява на служители да работят безопасно, независимо къде се намират. Освен това, VPN мрежите осигуряват поверителност и анонимност, като маскират IP адреса на потребителя и предпазват неговата онлайн активност.изкл

Друго съществено предимство е възможността за заобикаляне на ограничения, като например достъп до съдържание, което е блокирано в определени региони.

- Протоколи за VPN

Различните VPN мрежи използват разнообразни протоколи, всеки от които предлага специфични предимства и е подходящ за различни приложения. Един от най-разпространените протоколи е IPsec (Internet Protocol Security). Той предоставя сигурно криптиране и автентикация, което го прави отличен избор за защита на комуникацията както в корпоративни, така и в лични среди.

Друг популярен протокол е OpenVPN, който се отличава с отворения си код. Тази характеристика го прави не само гъвкав и сигурен, но и широко използван, тъй като предлага оптимален баланс между производителност и защита.

L2TP (Layer 2 Tunneling Protocol) често се комбинира с IPsec, за да осигури по-високо ниво на сигурност. Тази комбинация е предпочитана за среди, които изискват криптиране и надеждна защита на данните.

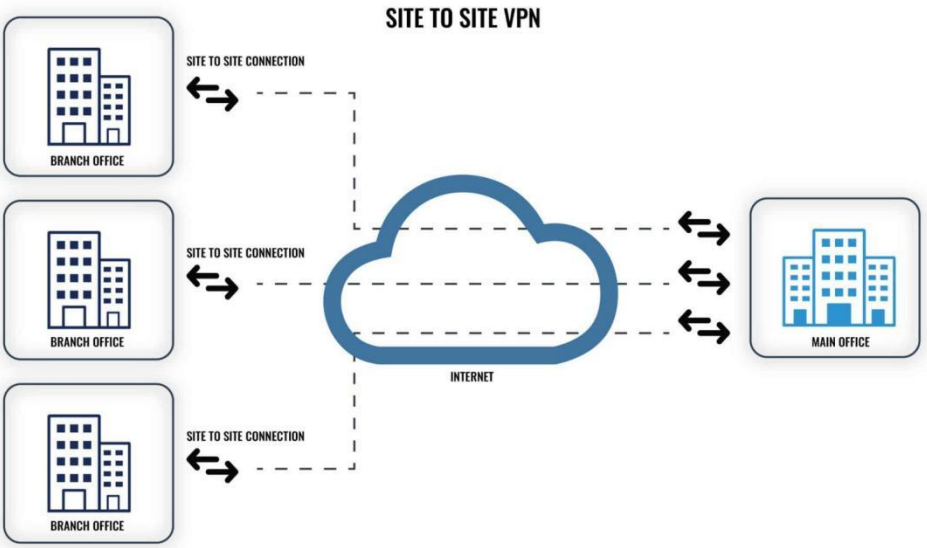
Всеки от тези протоколи е създаден с определена цел, като предоставя различни нива на сигурност, бързина и надеждност, за да отговори на нуждите на потребителите и организациите.

1.7.3 Видове VPN

- Сайт-към-сайт VPN (Site-to-Site)

Site-to-site VPN създава постоянен, сигурен тунел между две устройства (обикновено маршрутизатори), за да свърже две отдалечени локации през публична мрежа като интернет(фиг 1.7.3.1). Най-често използваният протокол за site-to-site VPN е IPsec.

Концепцията за тунелиране включва капсулиране на пакет от данни в друг пакет, добавяйки слоеве на сигурност по време на предаването. Процесът включва криптиране на пакет от маршрутизатор, за да се скрият съдържанието и предназначението му. Този криптиран пакет след това се капсулира в друг пакет, насочен към отдалечения маршрутизатор. При пристигане на пакета, маршрутизаторът го декриптира и го предава сигурно на крайния получател.

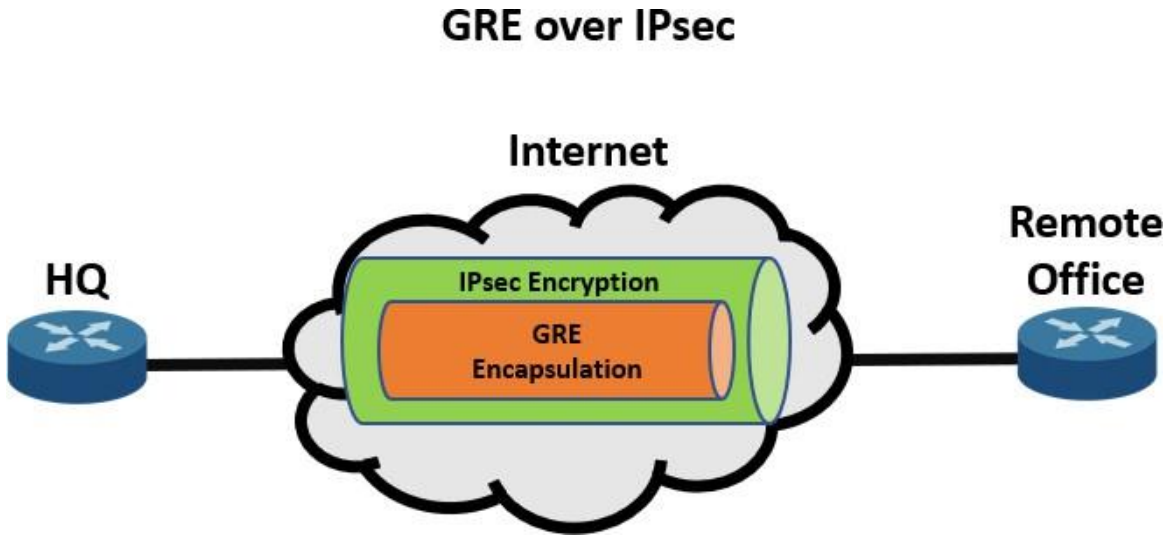


фиг 1.7.3.1

Този метод гарантира, че само двата края на тунела - двата маршрутизатора - могат да декриптират и достъпват данните, запазвайки конфиденциалността и целостта.

- GRE over IPsec

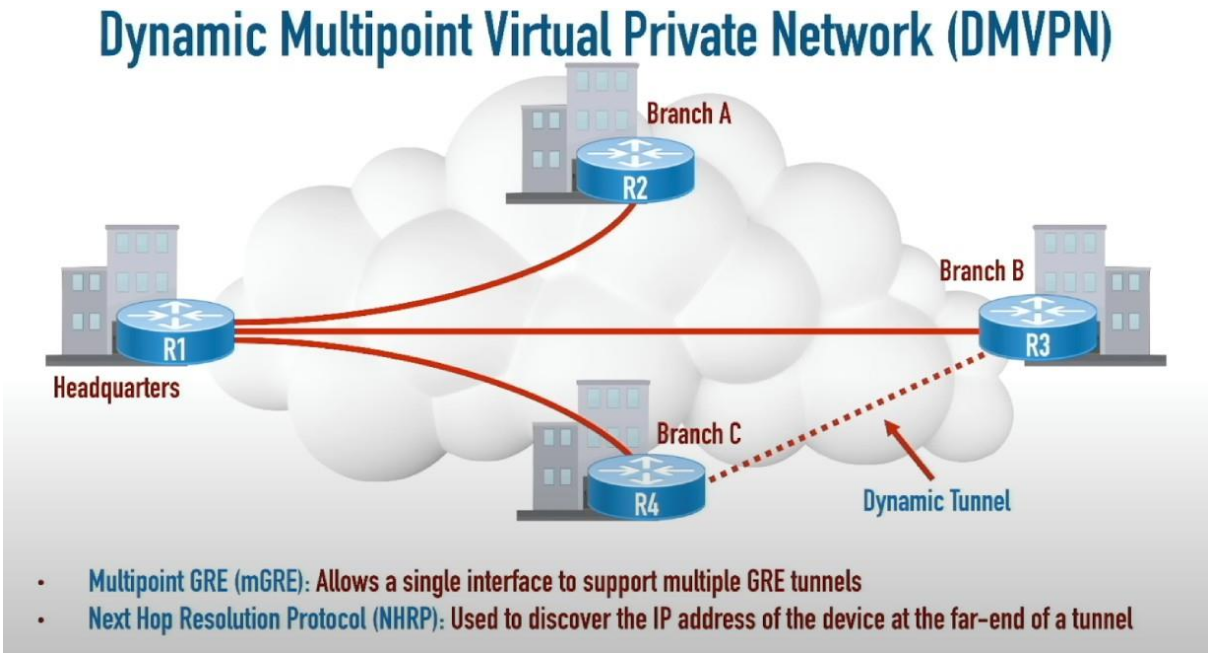
Въпреки че IPsec предлага надеждно криптиране, то поддържа само unicast трафик, което ограничава използването му с протоколи, които разчитат на broadcast или multicast трафик, като OSPF. За преодоляване на това ограничение често се използва Generic Routing Encapsulation (GRE) в комбинация с IPsec. GRE поддържа multicast и broadcast трафик, но сам по себе си не криптира данните. Комбинирането на GRE с IPsec предоставя както гъвкавостта на GRE, така и сигурността на IPsec, позволявайки multicast съобщения да преминават през сигурния тунел(фиг 1.7.3.2). Пакетът първо се капсулира с GRE хедър и нов IP хедър. Полученият GRE пакет след това се криптира и капсулира с IPsec хедър преди предаването. Този многослоен подход осигурява сигурна и гъвкава комуникация през интернет.



фиг 1.7.3.2

- Dynamic Multipoint VPN (DMVPN)

Основно предизвикателство при традиционните IPsec конфигурации е мащабируемостта. Настройването на индивидуални VPN тунели за всяка нова локация в мрежата може да стане трудоемко и податливо на грешки. Dynamic Multipoint VPN (DMVPN), решава този проблем, като опростява създаването на пълна мрежа от тунели(фиг 1.7.3.3).



фиг 1.7.3.3

С DMVPN е необходимо да се конфигурира само топология тип "хъб и споук" (hub and spoke). Маршрутизаторът-хъб разпространява информация за мрежата, което позволява на spoke маршрутизаторите да създават директно тунели помежду си динамично. Въпреки че DMVPN може да използва некриптирани GRE тунели по подразбиране, IPsec се прилага за сигурна комуникация.

- Основни предимства и ограничения

Интернет VPN-ите предлагат големи предимства като икономичност, елиминирайки нуждата от специализирани линии, и мащабируемост чрез решения като DMVPN, които улесняват разширяването на мрежата. Те също предоставят гъвкавост чрез осигуряване на сигурни, при поискване връзки за индивидуални потребители и подобрена сигурност чрез протоколи като IPsec и TLS, които гарантират целостта и конфиденциалността на данните.

Въпреки това, интернет VPN-ите също крият предизвикателства, като сложността на конфигурацията и управлението, особено в големи мрежи. Тяхното представяне зависи в голяма степен от качеството и капацитета на основната интернет връзка. Освен това, без надеждни мерки за сигурност, VPN-ите могат да бъдат уязвими на атаки като отказ на услуга (DoS).

1.7.4 Протокол за сигурност IPsec

IPsec[8] е набор от протоколи, предназначени за осигуряване на сигурна комуникация. Той осигурява конфиденциалност, цялостност и удостоверяване на данните, като шифрова и удостоверява IP пакетите. Работейки на мрежовия слой, IPsec позволява сигурна комуникация между различни мрежови устройства и е широко използван за изграждане на VPN-и и защитени отдалечени връзки.

Един от минусите на IPsec е неговата неспособност да поддържа broadcast и multicast трафик. Това е особено важно в

контекста на динамичните маршрутизиращи протоколи като EIGRP и OSPF, които използват multicast за размяна на маршрутизираща информация. Когато тези протоколи работят върху IPsec, те не могат ефективно да комуникират, което ограничава функционалността им.

За да се преодолее този недостатък, IPsec често се комбинира с GRE. Чрез внедряване на GRE over IPsec мрежите могат да комбинират предимствата на двата протокола. В тази конфигурация първо се капсулира IP пакет с GRE хедър и нов IP хедър, което позволява поддръжка на multicast и broadcast трафик. След това този GRE-капсулиран пакет се шифрова и капсулира отново с IPsec заглавка и допълнителен IP хедър, което осигурява поверителност и цялостност на данните. В резултат на това се генерират общо три IP хедъра: оригиналният хедър на пакета, добавеният от GRE хедър и хедърът, добавен от IPsec.

1.8 Протокол за определяне на следващия хоп (NHRP)

1.8.1 Основни понятия за NHRP

Протоколът за определяне на следващия хоп (Next Hop Resolution Protocol, NHRP)[9] е протокол от мрежовия слой, използван в мрежи с небраудкастов мултидостъп (Non-Broadcast Multi-Access, NBMA) за повишаване на ефективността на маршрутизацията. Той е особено полезен в среди, където множество устройства споделят общ гръбнак, като Frame Relay, ATM или MPLS мрежи. NHRP

позволява на устройствата да откриват най-краткия път до дадена дестинация, като динамично разрешават адреса на следващия хоп на слой 2 за даден адрес от слой 3.

1.8.2 Функционалност

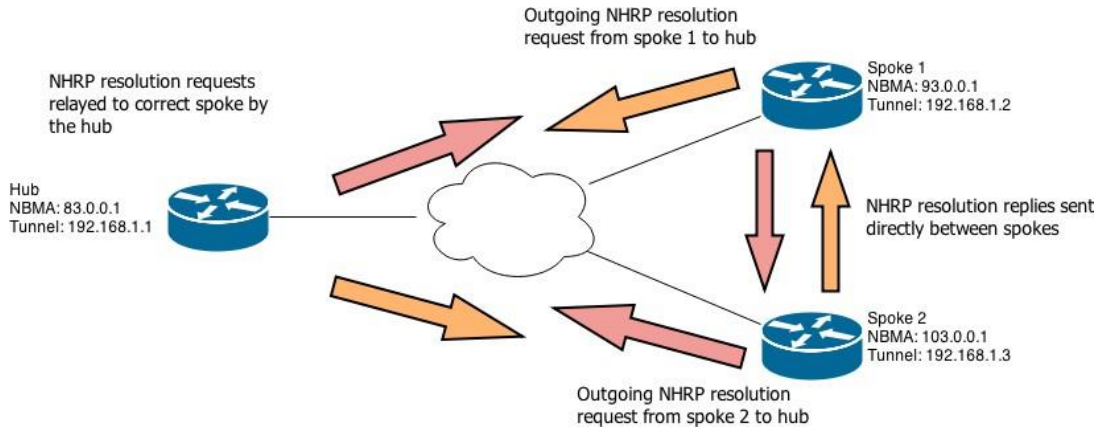
NHRP е създаден, за да адресира предизвикателствата в NBMA мрежите, където маршрутизацията обикновено разчита на статична конфигурация на адресите на следващия хоп. Чрез използването на NHRP устройствата (наричани клиенти) могат да се регистрират в централен сървър (наричан сървър за следващ хоп или NHS). Този централен сървър поддържа база данни, която свързва адреси от слой 3 (като IP адреси) с техните съответни адреси от слой 2. Когато клиент иска да комуникира с друго устройство в мрежата, той изпраща запитване към NHS за адреса от слой 2 на целевото устройство.

Този динамичен процес на разрешаване подобрява ефективността на мрежата, като позволява на устройствата да установяват директни връзки със своите партньори вместо да маршрутизират трафика чрез междинни устройства. Това минимизира закъсненията, намалява използването на честотната лента и оптимизира използването на ресурсите в мрежата.

1.8.3 Принцип на работа на NHRP

Клиентите регистрират своите адреси от слоеве 3 и 2 в NHS при присъединяване към мрежата. Тази регистрация гарантира, че

NHS разполага с актуална база данни за всички активни устройства и техните местоположения. Когато клиент трябва да комуникира с друго устройство, той изпраща запитване до NHS, за да поиска адреса от слой 2 на целевото устройство. NHS отговаря с подходящия адрес от слой 2, което позволява на клиента да установи директна връзка(фиг. 1.8.3.1).



фиг. 1.8.3.1

След като се извърши разрешаването, устройствата кешират локално съответствието на адресите. Освен това, NHRP включва механизми за поддържане на целостта на базата данни със съответствия на адресите. Клиентите периодично опресняват своите регистрации, а остарелите записи се премахват, за да се предотвратят грешки в маршрутизацията.

1.8.4 Приложения на NHRP

NHRP е основен компонент на динамичните многоточкови VPN (Dynamic Multipoint VPN или DMVPN), който позволява динамично създаване на тунели между клоновете в топология тип „star“. Това

позволява на периферните устройства да комуникират директно помежду си, без да маршрутизират трафика през централния възел.

1.8.5 Сравнение с други протоколи

Докато NHRP се фокусира върху динамичното разрешаване на адреси от слой 2 за следващия хоп, той се различава от протоколи като ARP и FHRP. Протоколът за разрешаване на адреси (ARP) се използва в мрежи с поддръжка на броудкаст за разрешаване на IP адреси в MAC адреси. ARP обаче е ограничен до локалните подмрежи и не поддържа NBMA среди. Протоколите за резервиране на първия хоп (FHRP), като HSRP, VRRP и GLBP, осигуряват резервираност за шлюзовете по подразбиране. Тези протоколи работят на слой 3, за да гарантират наличността на шлюзовете, но не разрешават динамично следващи хопове.

Втора глава - Използвани технологии

2.1 Основи на мрежовата архитектура

2.1.1 Изисквания към архитектурата, услугите и използваните протколи

Архитектурата на корпоративната мрежа трябва да бъде проектирана така, че да отговаря на няколко ключови изисквания.

На първо място, тя трябва да осигурява висока надеждност, като гарантира непрекъсваемост на връзката между централния офис (HQ) и отделните клонове (Branch_A, Branch_B, Branch_C). Това включва устойчивост на временни натоварвания или повреди на маршрутизатори, както и способност за бързо възстановяване на връзките при неизправности. Надеждността е от решаващо значение, за да се гарантира, че бизнес процесите няма да бъдат прекъснати поради мрежови проблеми.

Мрежата трябва също така да бъде мащабируема. Това означава, че проектираната архитектура трябва да поддържа лесно добавяне на нови клонове с минимални усилия и без сериозна намеса в съществуващата конфигурация. Тази възможност е особено важна за организации, които планират разширяване на дейността си, тъй като нови офиси могат да бъдат интегрирани

само чрез регистрация на техните тунелни интерфейси в Next Hop Server (NHS).

Друго изискване е оптимизация на маршрутизацията. За да се постигне това, мрежата трябва да използва динамичен маршрутизиращ протоколи, в случая EIGRP. Той осигурява автоматично изчисляване на оптималните маршрути, базирано на параметри като закъснение, честотна лента и разходи. Системата трябва също така да минимизира ненужния трафик чрез директни spoke-to-spoke тунели, което допълнително увеличава ефективността на мрежата.

За да се гарантира сигурността на комуникацията в корпоративната мрежа, DMVPN тунелите трябва да бъдат защитени чрез криптиране с IPsec. Това осигурява конфиденциалност, автентикация и защита на преносимите данни от външни заплахи, като прихващане, манипулация или неоторизиран достъп.

Всички DMVPN тунели трябва да използват криптиране чрез IPsec в транспортен режим, което позволява сигурност на нивото на GRE капсулирането, без да се добавя допълнителен overhead към IP заглавките. Криптографските алгоритми, използвани за шифроване и хеширане, трябва да гарантират високо ниво на защита. В този случай се използва AES за криптиране и SHA-256 за целостта на данните, като те осигуряват устойчивост срещу съвременни атаки.

Автентикацията между устройствата се извършва чрез предварително споделени ключове (pre-shared keys), което добавя

допълнителен слой сигурност към процеса на установяване на тунелите. В допълнение, IPsec профилите трябва да бъдат конфигурирани така, че да се прилагат към всички тунелни интерфейси, осигурявайки пълно криптиране на трафика между клоновете и централния офис.

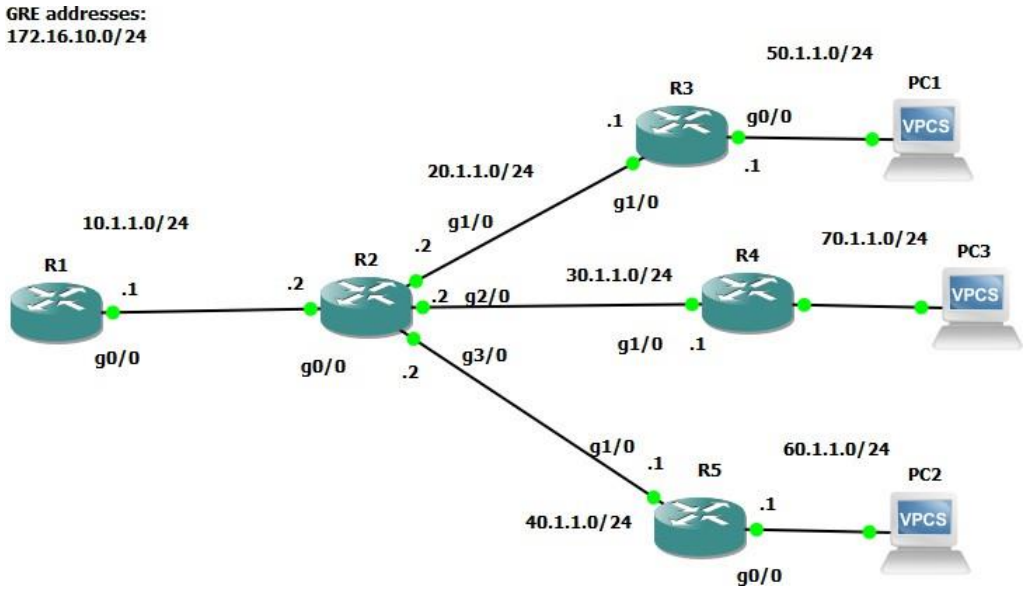
Друг важен аспект е защитата от атаки тип "man-in-the-middle" и неоторизирани устройства, които могат да се опитат да се включат в мрежата. Това се постига чрез използването на NHRP аутентикация, което гарантира, че само доверени устройства могат да регистрират своите адреси и да установяват директни spoke-to-spoke връзки.

И накрая, внедрената криптографска конфигурация трябва да осигурява баланс между сигурност и производителност. Използването на оптимизирани параметри за MTU и MSS настройките минимизира допълнителното натоварване върху маршрутизаторите, като същевременно поддържа висока ефективност на предаването на данни.

2.1.1 Проектиране на физическата свързаност на корпоративната мрежа

Физическата свързаност на корпоративната мрежа е проектирана в топология Hub and Spoke. Централният офис (HQ) действа като хъб, а всеки клон (Branch_A, Branch_B, Branch_C) е свързан към ISP маршрутизатора, който изпълнява ролята на посредник между хъба и клоновете. Тази топология(фиг. 2.1.1.1)

осигурява централизирано управление на мрежата и опростяване на маршрутизацията, като всички връзки между клоновете преминават през централния офис.



фиг. 2.1.1.1

Връзката между HQ и ISP маршрутизаторите се осъществява чрез интерфейсите g0/0, като използваното адресно пространство е 10.1.1.0/24. Всеки spoke маршрутизатор е свързан към ISP маршрутизатора чрез интерфейс g1/0 и отделни мрежи за всеки клон: 20.1.1.0/24 за Branch_A, 30.1.1.0/24 за Branch_B и 40.1.1.0/24 за Branch_C. За всяка връзка първият свободен адрес от мрежата се използва от маршрутизатора на клона, а вторият свободен адрес – от ISP маршрутизатора. Тази конфигурация осигурява ясно разграничение и управление на адресното пространство.

Архитектурата на DMVPN комбинира динамичните тунелни функции на multipoint GRE и разрешаването на адреси на NHRP. На всеки маршрутизатор е конфигуриран тунелен интерфейс, като

Spoke маршрутизаторите имат тунелна връзка само с Hub маршрутизатора. Протоколът NHRP позволява spoke маршрутизаторите да изпращат заявки за разрешаване на адреси към NHS, който в този случай е конфигуриран с underlay адреса на HQ маршрутизатора. След като HQ получи заявката, той връща тунелния адрес на крайния клон, позволявайки изграждането на spoke-to-spoke тунел при необходимост.

Маршрутизацията в overlay мрежата, която използва тунелните адреси, се управлява от EIGRP. Този протокол осигурява динамично обновяване на маршрутите и автоматично адаптиране към промени в мрежовата топология. От друга страна, underlay мрежата, която представлява основната инфраструктура на ISP, е симулирана чрез статични маршрути между интерфейсите на ISP и spoke маршрутизаторите. Тази двуслойна архитектура позволява ефективно разделяне на физическата и логическата свързаност, като същевременно оптимизира използването на мрежовите ресурси.

Трета глава - Конфигуриране и симулация

3.1 Конфигуриране на устройствата

Мрежата се разделя на две основни части: underlay и overlay. Underlay частта представлява основната инфраструктура на мрежата – физическата свързаност между хъба и клоновете, реализирана чрез интернет или, в случая, ISP. На това ниво маршрутизирането се осъществява чрез статични маршрути, които осигуряват базова свързаност между устройствата.

Overlay мрежата, от своя страна, е логическият слой, където се изграждат тунелни интерфейси и се използва маршрутизиращият протокол EIGRP. Този слой е фокусът на конфигурацията, тъй като предоставя динамично маршрутизиране и оптимизация на трафика между хъба и клоновете.

3.1.1 Конфигурация на тунелния интерфейс на hub маршрутизатора

Тунелният интерфейс на хъб маршрутизатора има следната конфигурация:

```
interface Tunnel0
 ip address 172.16.10.1 255.255.255.0
 no ip redirects
 ip mtu 1400
```

```
no ip next-hop-self eigrp 1
no ip split-horizon eigrp 1
ip nhrp authentication cisco
ip nhrp map multicast dynamic
ip nhrp network-id 1
ip nhrp redirect
ip tcp adjust-mss 1360
tunnel source GigabitEthernet0/0
tunnel mode gre multipoint
tunnel key 123
```

Мрежовото пространство, което се използва от overlay мрежата, е 172.16.10.0/24, като тунелният интерфейс на хъба (Tunnel0) е конфигуриран с първия използваем адрес - 172.16.10.1.

Командите `ip mtu 1400` и `ip tcp adjust-mss 1360` са критични за оптимизацията на размера на пакетите. Те настройват MTU (Maximum Transmission Unit) и MSS (Maximum Segment Size), за да предотвратят фрагментиране на пакети в тунелната мрежа, което би могло да доведе до загуба на пакети и нарушена комуникация.

Протоколът NHRP (Next Hop Resolution Protocol) е основен елемент от конфигурацията и е настроен по следния начин:

- `ip nhrp network-id 1` задава уникален идентификатор на NHRP мрежата, който помага за разграничаването ѝ от други мрежи.

- `ip nhrp authentication cisco` активира автентикация, като осигурява, че само легитимни устройства с коректна ключова дума ("cisco") могат да комуникират в мрежата.
- `ip nhrp map multicast dynamic` позволява динамично картографиране на multicast трафика, което е необходимо за правилното функциониране на EIGRP протокола върху тунелите.
- `ip nhrp redirect` активира механизма за пренасочване на NHRP, което позволява на хъба да указва на клоновете директни пътища към други клони (спиците), когато това е възможно.

Тунелна конфигурация:

- `tunnel source GigabitEthernet0/0` задава физическия интерфейс (GigabitEthernet0/0), който ще бъде използван като източник за тунела.
- `tunnel mode gre multipoint` активира режим multipoint GRE (mGRE), който позволява на хъба да поддържа множество spoke тунели чрез един общ тунелен интерфейс.
- `tunnel key 123` задава ключ за тунелите, осигурявайки допълнителен слой идентификация в мрежата.

Тази конфигурация гарантира, че хъбът може да служи като централен елемент на DMVPN мрежата, обработвайки ефективно заявките за разрешаване на адреси и маршрутизирайки трафика между отделните клони.

3.1.2 Конфигурация на тунелния интерфейс на spoke маршрутизатор

Конфигурацията на тунелния интерфейс на маршрутизаторите в клоновете гарантира правилната свързаност и комуникация с хъба в DMVPN мрежата:

```
interface Tunnel0
 ip address 172.16.10.2 255.255.255.0
 no ip redirects
 ip mtu 1400
 ip nhrp authentication cisco
 ip nhrp map multicast 10.1.1.1
 ip nhrp map 172.16.10.1 10.1.1.1
 ip nhrp network-id 1
 ip nhrp nhs 172.16.10.1
 ip nhrp shortcut
 ip tcp adjust-mss 1360
 tunnel source GigabitEthernet1/0
 tunnel mode gre multipoint
 tunnel key 123
```

На тунелния интерфейс на Branch_A е зададен IP адрес `172.16.10.2` с мрежова маска `255.255.255.0`, което позиционира маршрутизатора на клона в overlay мрежата заедно с хъба и другите клонове. Командата `no ip redirects` изключва ICMP redirect съобщенията, което подобрява сигурността и опростява

маршрутизацията. MTU размерът е настроен на 1400 байта с командата `ip mtu 1400`, а TCP MSS е зададен на 1360 с `ip tcp adjust-mss 1360`, за да се избегнат проблеми с фрагментацията в тунела.

Конфигурацията на NHRP е от съществено значение за динамичното мапване и ефективната маршрутизация в overlay мрежата:

- `ip nhrp authentication cisco` гарантира, че NHRP пакетите са автентифицирани с посочения ключ.
- `ip nhrp map multicast 10.1.1.1` мапва multicast трафика към underlay адреса на хъба (10.1.1.1), което позволява комуникация на маршрутизиращия протокол (EIGRP) през тунела.
- `ip nhrp map 172.16.10.1 10.1.1.1` мапва overlay адреса на хъба (172.16.10.1) към неговия underlay адрес, изграждайки необходимата връзка за комуникация между клона и хъба.
- `ip nhrp network-id 1` идентифицира NHRP домейна, като го синхронизира с този на хъба.
- `ip nhrp nhs 172.16.10.1` задава хъба като Next Hop Server (NHS), което позволява на маршрутизатора на клона да разрешава адресите динамично чрез хъба.
- `ip nhrp shortcut` позволява на клона да оптимизира маршрутизацията, като динамично научава директни пътища до други клонове при необходимост.

Източникът на тунела е зададен към физическия интерфейс `GigabitEthernet1/0`, който е свързан с ISP, а режимът GRE multipoint е активиран с `tunnel mode gre multipoint`, за да се позволят множество тунели от тип spoke-to-hub и spoke-to-spoke в рамките на DMVPN. Накрая, командата `tunnel key 123` предоставя допълнителен слой идентификация за тунела, гарантирайки съвместимост с конфигурацията на хъба.

Тази конфигурация позволява на маршрутизаторите на клоновете да комуникират ефективно с хъба и други клонове чрез overlay мрежата, като същевременно осигурява гъвкавост за бъдещо разширяване.

3.1.3 Конфигурация на маршрутизиращия протокол

EIGRP е избраният маршрутизиращ протокол за overlay мрежата. Той се използва за динамично разпространение на маршрути между Hub и Branch маршрутизаторите, като осигурява ефективност и минимизира ръчната конфигурация.
Конфигурация на Hub маршрутизатора:

Командите `no ip split-horizon eigrp 1` и `no ip next-hop-self eigrp 1` се използват, за да се осигури правилно рекламиране на маршрути между клоновете. Премахването на split-horizon позволява на хъба да рекламира маршрути, научени от един spoke, към останалите spokes, а деактивирането на next-hop-self гарантира, че next-hop адресите остават валидни.

Командата `router eigrp 1` активира EIGRP процеса с номер на автономната система (AS) 1. Всички маршрутизатори, участващи в EIGRP, трябва да използват същия номер на AS, за да могат да обменят маршрути. `network 172.16.10.0 0.0.0.255` позволява на Hub маршрутизатора да участва в EIGRP за overlay мрежата 172.16.10.0/24. Тази мрежа включва тунелните интерфейси на всички маршрутизатори. хъбът обявява тази мрежа, за да поддържа свързаност с клоновете.

Тази минимална конфигурация е достатъчна за Hub маршрутизатора, тъй като неговата основна роля е да действа като централен възел за маршрутизацията в overlay мрежата.

Конфигурация на Branch_A маршрутизатора(spoke):

Командата `router eigrp 1` активира EIGRP процеса с номер на автономната система 1, което осигурява съвместимост с Hub маршрутизатора, `network 50.1.1.0 0.0.0.255` обявява локалната LAN мрежа 50.1.1.0/24, която представлява офисната мрежа на клона, което позволява на останалите маршрутизатори в мрежата (хъба и другите клонове) да научат за тази мрежа и да осигурят свързаност до нея, а `network 172.16.10.0 0.0.0.255` активира EIGRP за overlay мрежата 172.16.10.0/24, свързана с тунелния интерфейс. Това позволява на Branch маршрутизатора да комуникира с хъба и другите клонове чрез тунелите.

- Описание на процеса

EIGRP динамично управлява маршрути между Hub-а и клоновете, като гарантира, че всички маршрутизатори имат

информация за локалните LAN мрежи на останалите клонове. Например, ако Branch_A обяви мрежата 50.1.1.0/24, хъбът ще разпространи този маршрут до Branch_B и Branch_C. Това позволява директна свързаност между офисите на различните клонове, като трафикът преминава през тунелите.

3.1.4 Конфигурация на IPsec тунел

IPsec конфигурацията осигурява криптиране и защита на данните, преминаващи през DMVPN мрежата, като прилага протоколите IKE и IPsec. Конфигурацията е съставена от няколко основни компонента:

```
crypto isakmp policy 10
 encryption aes
 hash sha256
 authentication pre-share
 group 14
 lifetime 86400
crypto isakmp key cisco123 address 0.0.0.0 0.0.0.0
crypto ipsec transform-set DMVPN-SET esp-aes
esp-sha-hmac
 mode transport
crypto ipsec profile DMVPN-PROFILE
 set transform-set DMVPN-SET
interface Tunnel0
 tunnel protection ipsec profile DMVPN-PROFILE
```

Първата стъпка е създаването на ISAKMP политика, която определя параметрите за фазата на преговори (Phase 1), в която се установява защитена комуникация между мрежовите възли. Командата `crypto isakmp policy 10` задава приоритет на политиката с номер 10. В конфигурацията се използва AES за криптиране, зададено чрез командата `encryption aes`, което гарантира висока степен на поверителност на данните. Хеширащият алгоритъм SHA-256 се избира с командата `hash sha256`, за да се осигури целостта на информацията. Методът за удостоверяване е базиран на предварително споделен ключ с `authentication pre-share`. Групата за алгоритъма Diffie-Hellman е зададена като 14 чрез командата `group 14`, което предоставя силна криптографска защита при обмен на ключове(2048-bit). Накрая, продължителността на фазата е определена на 24 часа чрез `lifetime 86400`.

Следващата стъпка е задаването на предварително споделен ключ между всички устройства в мрежата. Това се извършва с командата `crypto isakmp key cisco123 address 0.0.0.0 0.0.0.0`. Тук ключът „cisco123“ се задава за всички IP адреси, което позволява динамична връзка между възлите.

IPsec транспортният сет се създава, за да определи механизмите за криптиране и проверка на целостта на данните. Командата `crypto ipsec transform-set DMVPN-SET esp-aes esp-sha-hmac` създава трансформационен набор с име `DMVPN-SET`, който използва AES за криптиране и SHA за проверка

на целостта чрез HMAC. Режимът на работа е зададен като транспортен с `mode transport`, което осигурява криптиране само на полезния товар, като оставя IP хедъра непокътнат.

Създаването на IPsec профил се извършва с командата `crypto ipsec profile DMVPN-PROFILE`, която създава профил с име `DMVPN-PROFILE`. Този профил свързва трансформационния набор, зададен по-рано, чрез командата `set transform-set DMVPN-SET`. Това улеснява прилагането на IPsec настройките към мрежовите тунели.

Последната стъпка е активирането на защитата на тунелния интерфейс. Това се извършва чрез командата `tunnel protection ipsec profile DMVPN-PROFILE`, изпълнена на тунелния интерфейс, която активира IPsec криптиране, използвайки профила `DMVPN-PROFILE`.

Тази конфигурация комбинира ISAKMP за установяване на защитени сесии и IPsec за криптиране на тунелния трафик. Резултатът е сигурна DMVPN мрежа, която осигурява конфиденциалност, интегритет и удостоверяване на данните, преминаващи през тунелите. Тя е проектирана да защити чувствителната комуникация между възлите в мрежата, използвайки съвременни криптографски методи.

Четвърта глава - Доказване на работоспособност

4.1 Тестване на свързаността между устройствата

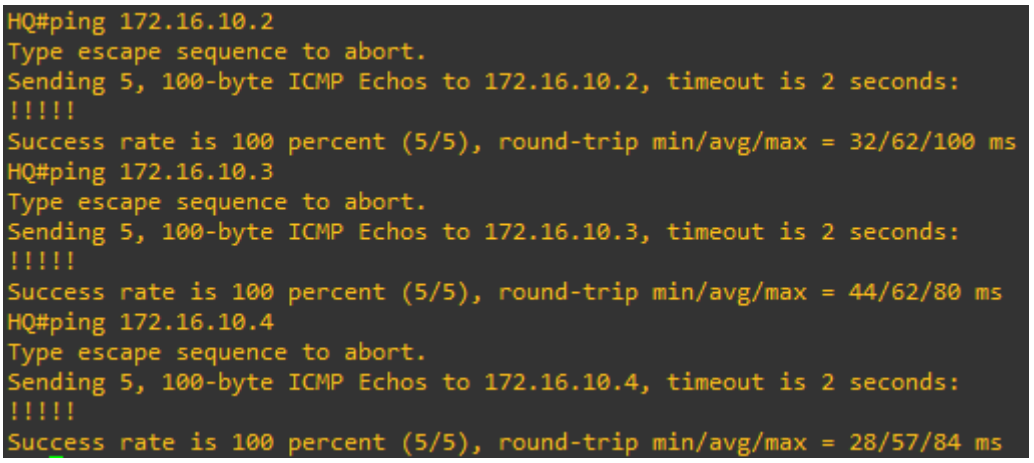
За проверка на свързаността и правилното функциониране на мрежата са изпълнени няколко команди, чиито резултати демонстрират коректно изградени тунели, налични EIGRP съседства и успешно маршрутизиране на трафика.

Най-напред, пинг тестовете от HQ маршрутизатора потвърждават, че той може да комуникира с всички мрежи от underlay слоя – адреси от диапазоните 10.1.1.0/24, 20.1.1.0/24, 30.1.1.0/24 и 40.1.1.0/24. Всеки пинг завършва с успех, което доказва правилна конфигурация на underlay мрежата и използваните статични маршрути.

```
HQ#ping 10.1.1.2
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.1.1.2, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 20/28/36 ms
HQ#ping 20.1.1.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 20.1.1.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 24/55/84 ms
HQ#ping 30.1.1.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 30.1.1.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 20/56/84 ms
HQ#ping 40.1.1.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 40.1.1.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 28/56/76 ms
```

фиг. 4.1.1

Втората серия пинг тестове е насочена към overlay мрежата, която използва тунелните адреси от 172.16.10.0/24. Пинг командите от HQ маршрутизатора успешно достигат всички Branch маршрутизатори (172.16.10.2, 172.16.10.3 и 172.16.10.4). Това потвърждава, че тунелите са изцяло функционални и че DMVPN инфраструктурата осигурява правилно маршрутизиране чрез EIGRP.



фиг. 4.1.2

На следващо място, EIGRP съседствата са проверени чрез командата show ip eigrp neighbors. На HQ маршрутизатора се виждат три EIGRP съседи – Branch_A, Branch_B и Branch_C, което показва, че EIGRP протоколът успешно установява и поддържа съседски отношения в overlay мрежата. На Branch_A, от друга страна, единственият EIGRP съсед е HQ маршрутизаторът, което е очаквано, предвид Hub and Spoke топологията на DMVPN.

```
HQ#sh ip eigrp ne
EIGRP-IPv4 Neighbors for AS(1)
H   Address                 Interface              Hold Uptime   SRTT   RTO  Q  Seq
                                                   (sec)         (ms)       Cnt Num
2   172.16.10.3             Tu0                      14 06:14:53  118  1398  0  3
1   172.16.10.4             Tu0                      10 06:14:53  138  1398  0  3
0   172.16.10.2             Tu0                      10 06:14:53  171  1398  0  3
HQ#sh ip eigrp top
EIGRP-IPv4 Topology Table for AS(1)/ID(172.16.10.1)
Codes: P - Passive, A - Active, U - Update, Q - Query, R - Reply,
       r - reply Status, s - sia Status

P 172.16.10.0/24, 1 successors, FD is 26880000
        via Connected, Tunnel0
P 50.1.1.0/24, 1 successors, FD is 26880256
        via 172.16.10.2 (26880256/2816), Tunnel0
P 60.1.1.0/24, 1 successors, FD is 26880256
        via 172.16.10.4 (26880256/2816), Tunnel0
P 70.1.1.0/24, 1 successors, FD is 26880256
        via 172.16.10.3 (26880256/2816), Tunnel0
```

фиг. 4.1.3

Допълнително, EIGRP топологията е проверена чрез командата show ip eigrp topology. Резултатите от HQ показват, че мрежите на Branch_A (50.1.1.0/24), Branch_B (60.1.1.0/24) и Branch_C (70.1.1.0/24) са правилно рекламирани и достъпни през тунелните интерфейси. Аналогично, Branch_A вижда мрежите от overlay слоя и собствената LAN мрежа (50.1.1.0/24) в EIGRP топологията.

```
Branch_A#sh ip eigrp ne
EIGRP-IPv4 Neighbors for AS(1)
H   Address                 Interface              Hold Uptime   SRTT   RTO  Q  Seq
                                                   (sec)         (ms)       Cnt Num
0   172.16.10.1             Tu0                      10 06:16:32  117  1398  0  6
Branch_A#sh ip eigrp top
EIGRP-IPv4 Topology Table for AS(1)/ID(172.16.10.2)
Codes: P - Passive, A - Active, U - Update, Q - Query, R - Reply,
       r - reply Status, s - sia Status

P 172.16.10.0/24, 1 successors, FD is 26880000
        via Connected, Tunnel0
P 50.1.1.0/24, 1 successors, FD is 2816
        via Connected, GigabitEthernet0/0
P 60.1.1.0/24, 1 successors, FD is 28160256
       172.16.10.4 via 172.16.10.1 (28160256/26880256), Tunnel0
P 70.1.1.0/24, 1 successors, FD is 28160256
       172.16.10.3 via 172.16.10.1 (28160256/26880256), Tunnel0
```

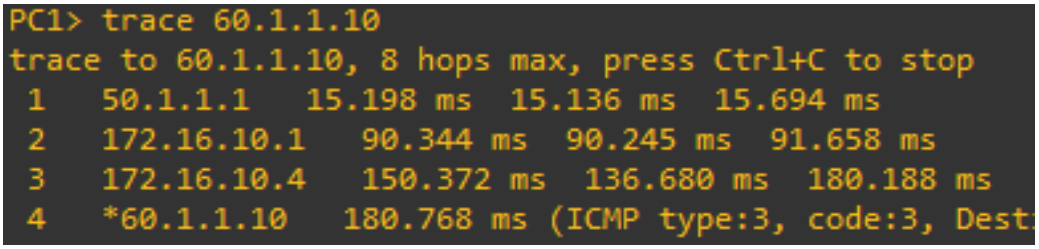
фиг 4.1.4

Тези тестове доказват, че всички елементи на мрежата – както underlay, така и overlay – са правилно конфигурирани и функционират според очакванията. DMVPN тунелите осигуряват свързаност между клоновете и HQ, а EIGRP гарантира ефективно маршрутизиране на трафика.

4.2 Тестване на работоспособност на DMVPN архитектурата

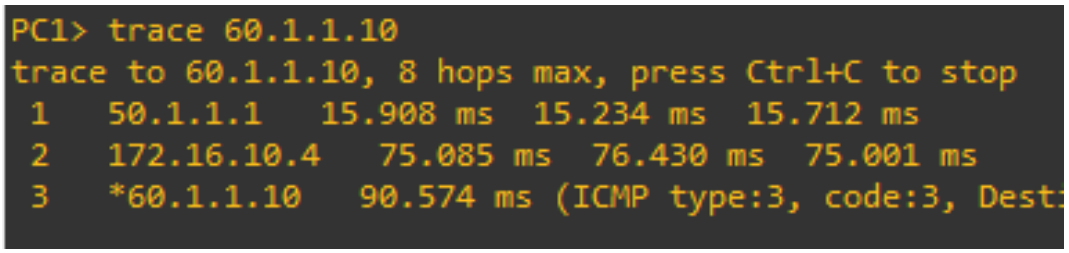
Резултатите от теста с traceroute ясно демонстрират ефективността на динамичните тунели в DMVPN и начина, по който работи протоколът NHRP (Next Hop Resolution Protocol). Проведеният тест включва проследяване на пътя между компютър PC1 в локалната мрежа на Branch_A и компютър PC2 в мрежата на Branch_C. Получените данни показват поведението на трафика при първоначално маршрутизиране през Hub-а и последващо директно комуникиране между клоновете.

При първото изпълнение на traceroute, трафикът стартира от PC1 (LAN на Branch_A с адрес 50.1.1.10) и първият хоп е локалният рутер на клона с IP адрес 50.1.1.1. След това пакетите преминават през Hub рутера с IP адрес 172.16.10.1. От хъба трафикът се пренасочва към DMVPN интерфейса на Branch_C (172.16.10.4), преди да достигне крайната точка – PC2 с адрес 60.1.1.10.



фиг. 4.2.1

При второто изпълнение на traceroute, трафикът отново стартира от PC1, но този път след първия хоп (локалният рутер с адрес 50.1.1.1) директно се свързва с DMVPN интерфейса на Branch_C (172.16.10.4), заобикаляйки хъба. След това пакетите достигат крайната точка PC2. Тази промяна в маршрута демонстрира преминаване от маршрутизиране през хъба към директна връзка между Branch_A и Branch_C (spoke-to-spoke). Това става възможно благодарение на NHRP, който по време на първото traceroute разрешава IP адреса на целевия рутер и позволява създаването на GRE тунел между двата клона.



фиг. 4.2.2

Тези резултати потвърждават, че DMVPN динамично оптимизира маршрутизирането на трафика след първоначалния процес на адресно разрешаване. Първоначалното маршрутизиране spoke-to-hub-to-spoke се заменя с директен тунел spoke-to-spoke, което значително намалява латентността и подобрява

ефективността на мрежата, като елиминира ненужните хопове през хъба при последващи комуникации.

Изходът от командата `show crypto ipsec sa` предоставя детайлна информация за състоянието на IPsec тунелите, включително броя на капсулираните (encaps) и декапсулираните (decaps) пакети. Тези параметри са от съществено значение за мониторинга на сигурността и ефективността на VPN връзките.

На hub устройството, в примера на *фиг. 4.2.3*, локалният идентификатор е 10.1.1.1, а отдалеченият 40.1.1.1. Партньорът на устройството е 40.1.1.1, чийто адрес отговаря на Branch_C, като броят на encapsulated пакетите е 67, а на decapsulated пакетите - 53. Устройството използва ESP-AES за криптиране и ESP-SHA-HMAC за проверка на целостта. Разликата в броя на изпратените и получените пакети се дължи на динамиката на трафика и факта, че хъбът комуникира с множество клони.

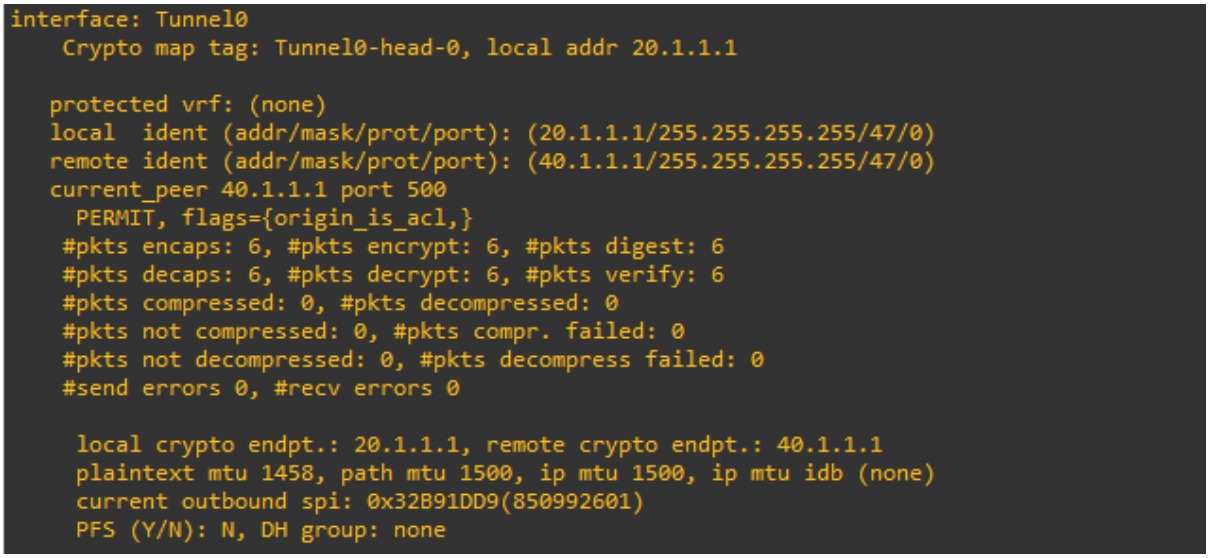
```
interface: Tunnel0
    Crypto map tag: Tunnel0-head-0, local addr 10.1.1.1

   protected vrf: (none)
   local  ident (addr/mask/prot/port): (10.1.1.1/255.255.255.255/47/0)
   remote ident (addr/mask/prot/port): (20.1.1.1/255.255.255.255/47/0)
   current_peer 20.1.1.1 port 500
     PERMIT, flags={origin_is_acl,}
    #pkts encaps: 63, #pkts encrypt: 63, #pkts digest: 63
    #pkts decaps: 58, #pkts decrypt: 58, #pkts verify: 58
    #pkts compressed: 0, #pkts decompressed: 0
    #pkts not compressed: 0, #pkts compr. failed: 0
    #pkts not decompressed: 0, #pkts decompress failed: 0
    #send errors 0, #recv errors 0

     local crypto endpt.: 10.1.1.1, remote crypto endpt.: 20.1.1.1
     plaintext mtu 1458, path mtu 1500, ip mtu 1500, ip mtu idb (none)
     current outbound spi: 0xFBA37613(4221793811)
     PFS (Y/N): N, DH group: none
```

фиг. 4.2.3

На Branch_A(*фиг. 4.2.4*) локалният идентификатор е 20.1.1.1, а отдалеченият 40.1.1.1, което означава, че този маршрутизатор също комуникира с Branch_C. Броят на encapsulated пакетите е 6, а на decapsulated пакети също е 6. Това означава, че има двупосочен трафик, в малки обеми, като тук също се използва ESP-AES и ESP-SHA-HMAC за защита на трафика.



фиг. 4.2.4

Encapsulated пакетите са тези, които устройството изпраща през IPsec тунела. Те се криптират и защитават преди да бъдат изпратени. Decapsulated пакетита са тези, които устройството получава през тунела и след това декриптира и проверява тяхната целостност.

Заключение

В хода на тази дипломна работа беше извършен детайлен анализ на Dynamic Multipoint Virtual Private Network (DMVPN) като технология за изграждане на мащабируеми, ефективни и сигурни виртуални частни мрежи. Бяха разгледани основните компоненти на DMVPN, включително използването на протокола NHRP за динамично разрешаване на адресите, маршрутизационния протокол EIGRP за осигуряване на оптимални маршрути и GRE over IPsec за защита на предаваните данни. Чрез тези технологии DMVPN предоставя надеждно решение за свързаност между множество отдалечени мрежови обекти.

По време на изследването беше демонстрирано как DMVPN позволява изграждането на динамични тунели, което значително намалява натоварването върху централния хъб и оптимизира маршрутизирането в мрежата. Тестовете показват, че след първоначалната комуникация през хъба крайните точки могат да установят директни връзки помежду си, като по този начин се подобрява латентността и се намалява използването на ресурси. Това прави DMVPN изключително ефективно решение за корпоративни среди, които изискват сигурна и динамична мрежова инфраструктура.

В заключение, дипломната работа показа, че DMVPN представлява надеждна и ефективна технология за изграждане на сигурни мрежови решения, които могат да се адаптират към динамично променящи се условия. Чрез използването на NHRP,

EIGRP и GRE over IPsec беше демонстрирано как DMVPN може да бъде приложен за оптимизиране на комуникацията между отдалечени мрежови обекти, като същевременно осигурява висока степен на сигурност и мащабируемост. Това го прави подходящ избор за организации, които търсят балансирано решение между производителност, сигурност и ефективност в управлението на мрежовата инфраструктура.

Съдържание

Използвана литература

1. **TCP/IP & OSI** - Acing the CCNA Exam Volume 1, Chapter 4 - The TCP/IP networking model

2. **Network topologies** - https://www.geeksforgeeks.org/types-of-network-topology

3. **Network devices** - Acing the CCNA Exam Volume 1, Chapter 2 - Network devices

4. **IP addressing** - Acing the CCNA Exam Volume 1, Chapter 7 - IPv4 addressing

5. **Routing** - Acing the CCNA Exam Volume 1, Chapter 9 - Routing fundamentals & Chapter 17- Dynamic routing

6. **Routing Protocol EIGRP** - https://www.cisco.com/c/en/us/td/docs/security/firepower/720/fdm/fptd-fd m-config-guide-720/fptd-fdm-eigrp.html https://www.cisco.com/c/en/us/support/docs/ip/enhanced-interior-gateway-routing-protocol-eigrp/13669-1.html

7. **Internet VPN & IPsec** - Acing the CCNA Exam Volume 2, Chapter 16, Section 16.3 - Internet VPNs

8. **IPsec** - https://www.cloudflare.com/learning/network-layer/what-is-ipsec/

9. **Next Hop Resolution Protocol(NHRP)** - https://www.techtarget.com/searchnetworking/definition/Next-Hop-Resolution-Protocol

Acing the CCNA Exam Volumes 1 & 2 - https://www.manning.com/books/acing-the-ccna-exam-fundamentals-an d-protocols https://www.manning.com/books/acing-the-ccna-exam-advanced-networ king-and-security