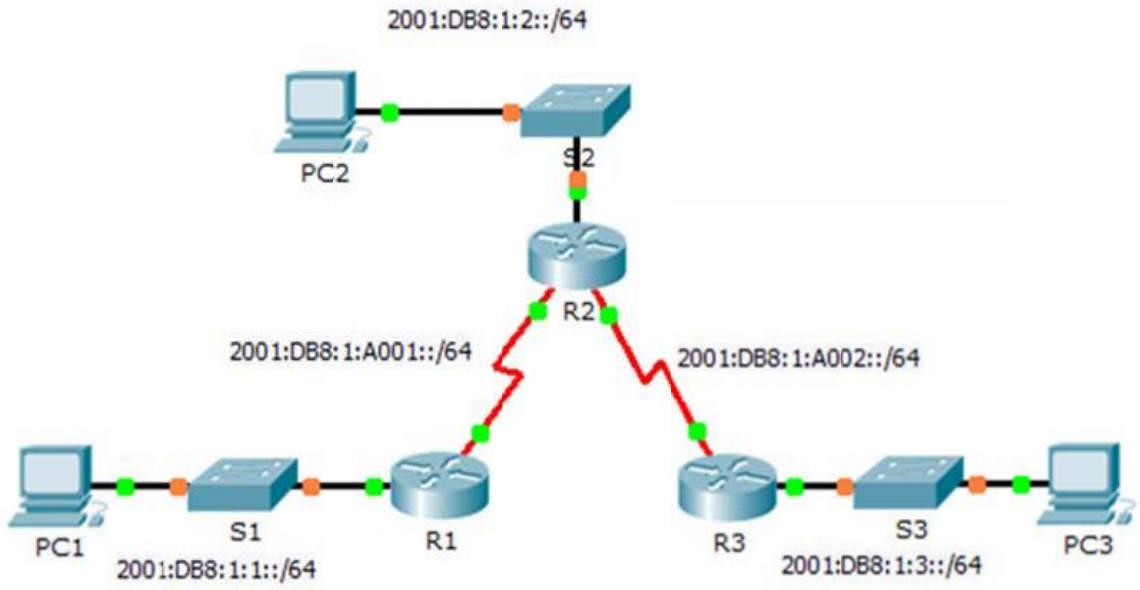
Въведение в IPv6.
Базови конфигурации на мрежови устройства

Топология



IP Addressing Table

Device	Interface	IP Address	Default Gateway
R1	FA0/0	2001:DB8:1:1::1/64	N/A
	S0/0/0	2001:DB8:1:A001::1/64	N/A
R2	S0/0/0	2001:DB8:1:A001::2/64	N/A
	S0/0/1	2001:DB8:1:A002::1/64	N/A
	FA0/0	2001:DB8:1:2::1/64	
R3	FA0/0	2001:DB8:1:3::1/64	N/A
	S0/0/1	2001:DB8:1:A002::2/64	N/A
PC1	NIC	2001:DB8:1:1::F/64	2001:DB8:1:1::1
PC2	NIC	2001:DB8:1:2::F/64	2001:DB8:1:2::1
PC3	NIC	2001:DB8:1:3::F/64	2001:DB8:1:3::1

Цел на упражнението

- **Част 1: Изследване и запознаване с мрежата**
- **Част 2: Конфигуриране на IPv6**
- **Част 3: Проверка на свързаността**

Теория

Част 1: Въведение в IPv6 протокола

IPv4 е издържал проверката на мащабиране както и всички условия,за да може да се използва вече толкова дълго в света, но този протокол не е бил проектиран да поддържа огромен на брой мрежово оборудване. Поради големият разтеж на интернет потреблението,IPv4 вече не е в състояние да задоволи огромното нарастване на броя на потребителите, както и географските нужди за интернет разширяването.Като резултат от всичко това, адресите на IPv4 започват да се изчерпват много бързо. Освен нововъзникващите приложения като интернет поддръжка на преносими устройства, домашни мрежи, мобилни ad hoc мрежи, безжични IP услуги и IP телефонни услуги изискват въвеждането на нов интернет протокол.

Експлотационният срок на IPv4 е бил удължен с помоща на различни техники, като например:

- Network Address Translation – накратко NAT
- Classless Inter-domain Routing – CIDR
- Dynamic Host Configuration Protocol- DHCP

Тези техники се появяват,за да увеличат адресното пространство и да удоволетворят традиционната сърват/клиент структура, но те немогат да отговарят на изискванията на реалната мрежа и на мобилността на потребителя. Приложенията се нуждаят от увеличаването на размера на честотната лента, тъй като предаването на адрес влияе върху производителността на межовото обурудване.

Освен това функцията „plug and play" играе съществена роля в това да се изисква разширение на IP протокола. Тя сама по себеси се характеризира с това, че всеки потребител на интернет трябва да може да се включи успешно към интернет мрежата и всичко да функционира нормално. Милионите нови технологични устройства като безжичните телефони, автомобили и битова техника няма да имат възможността да получат IPv4 адреси в световен мащаб още дълго време.IPv4 скоро ще достигне етап,когато ще трябва да се направи избор между това да имаме нови възможности на протокола или използването на по - големи мрежи но не и двете едновременно. С други думи ние се нуждаем от нов протокол, който да предостави нови и подобрени функции,за да може да се реши проблема с изчерпването на IP адресите. Този нов протокол е IPv6. IPv6 е проектиран да удоволетвори изискванията за огромното потенциално интернет потребление. Този протокол ще позволи възвръщане към една глобална среда, където правилата за адресиране на мрежата са отново прозрачни за приложенията. Чрез автоматичната конфигурация и „plug and play" подкрепата, мрежовите устройства ще имат възможността да се свържат към мрежата без да трябват ръчно конфигуриране и без каквито и да са фърмуер услуги като например - DHCP услугите.

IPv6 успява да извърши всичко това, като предоставя на мрежовите и ИТ специалисти следните ползи:

- Първо – IPv6 има по голямо адресно пространство за глобална достъпност и мащабируемост. Това ще даде като резултат неограничен брой IP адреси и йерархична мрежова архитектура за по-ефективна маршрутизация. Това елиминира проблемите свързание с NAT.

Способността за предоставяне на общодостъпни адреси за всяко устройство позволява достъпност от край до край. Така мрежовото управление ще бъде по-просто и по-лесно.

- Второ – опростен HEADER формат за ефективно управление на пакети. Шест от дванадесетте HEADER полета са отстранени в IPv6. Някои IPv4 полета са били пренесени с модифицирани имена и в същото време са добавени някои нови функции и полета, които да подобрят ефективността .
- Трето - йерархична мрежова архитектура за ефективна маршрутизация която следва някои от принципите на IPv4 CIDR(метод за разпределяне на IP адреси и маршрутизация на Internet Protocol пакети).
- Друго предимство на IPv6 е вградената сигурност,която задължително се изпълнява благодарение на IPSec. Разликата между IPv4 и IPv6 се характеризира в това че в IPv4 не е задължително използването на IPSec, докато при IPv6 е абсолютно задължително. IPsec е част от обвивката на IPv6 на протокола. Благодарение на това , ще имаме възможност да направи сигурен всеки един възел, което от своя страна ще направи мрежите много по-сигурни.
- Освен това, IPv6 предлага по-голям брой на мултикаст адресите. IPv6 няма да използва broadcast, което води до по-производителни мрежи.
- Поредното предисмство се изразява в това , че новият ICMP протокол познат още като ICMPv6 е много по мощен и включва нови функции които да подпомогнат автоматичното конфигуриране както и multicasting-а.
- И накрая,IPv6 ще бъде вграден в мобилността , защото се очаква голямо внедряване на безжичните услуги, които ще са основният двигател на IPv6.

Част 2: Адресиране на IPv6 протокола

IP адресирането значително се промени в IPv6 на протокола. Вместо да имаме 4 байтов адрес какъвто имаме в IPv4, в новата версия на протокола(IPv6) ние имаме вече 16 байтов адрес. Проучванията показват че за всеки човек на планетата ще има най-малко по 1000 адреса. Дори ако само част от пълното адресно пространство се използва на този протокол,IPv6 ще елиминира всякакви възможности за това да имаме изчерпване на IP адресите.

IP адресите на версия 6 на протокола обикновенно се изписват по следния формат:

XXXX:XXXX:XXXX:XXXX:XXXX:XXXX:XXXX:XXXX

Препоръчителния формат за представяне на адресите представлява осем 16 - битови полета, като тези полета се представят като стринг състоящ се от четири шеснайсетични числа. Може да дадем и един пример за да е по- нагледно:

1079:0005:AB45:5F4C:0010:BA97:0043:34AB

Шеснадесетичната номерация на адресите не е чувствителна към малки и големи букви:

- 1079:0005:AB45:5F4C:0010:BA97:0043:34AB - когато използваме числа и глвни букви
- 1079:0005:ab45:5f4c:0010:ba97:0043:34ab - когато използваме числа и малки букви
- 1079:0005:AB45:5f4c:0010:BA97:0043:34ab - когато използваме числа и смесица от малки и големи букви.

Примерите, които дадохме са абсолютно идентични и могат да се заменят един с друг.

Освен това,ако имаме водещи нули в полетата на адреса ние може да ги **компресираме**. Като пример който да ни позволи да разберем как точно става това може да дадем следното:

- 2001:ABC5:0000:556D:0000:983H:0000:2345 – нормален IPv6 адрес
- 2001:ABC5:0:556D:0:983H:0:2345 – компресиран IPv6 адрес

IPv6 на протокола използва друга много важна конвенкция за намаляване на адреса на IPv6,за да може да го направи по-лесен за представяне - може да направим **сливане** на две полета които съдържат нули и да ги представим по следния начин:

- 2001:ABC5:0:0:556D:983H:0:2345 □ 2001:ABC5::556D:983H:0:2345

Трябва обаче да запомним че всичко това е функционално и работи нормално, само ако имаме правилно въведен IPv6 адрес.

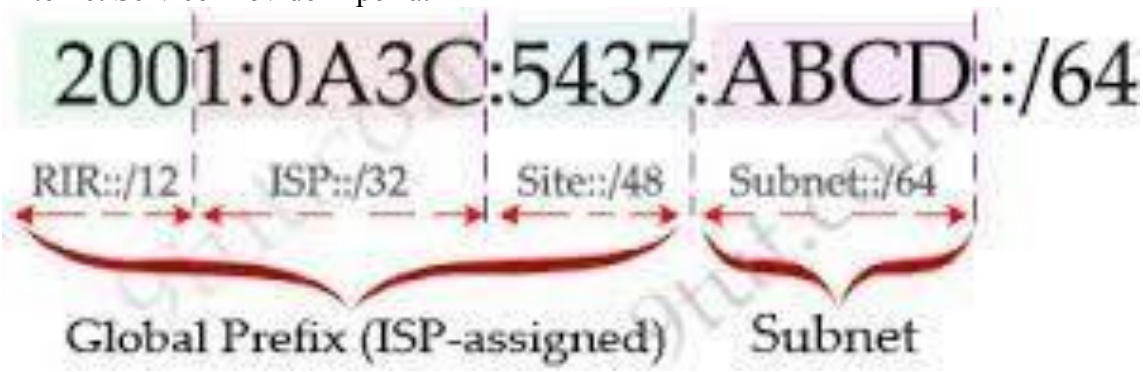
Друго съществено нещо, което трябва да запомним е, че неможе да изписваме по следния начин адреса:

• 2001:ABC5:0:0:556D:983H:0:2345 □ 2001:ABC5::556D:983H::2345 –това не е правилно,защото нямаме последователност от две полета, които да са изцяло изградени от нули, а имаме само едно поле и по този начин няма как да премахним нулата и да поставим две двойни точки.

Адресите на IPv6 могат да бъдат изразени и в следния формат: IPv6 **адрес/дължина на префикса**. По същият начин и адресите на IPv4 се представят в CIDR. Като пример този адрес, които сме изписа за IPv6 е напълно възможен и валиден:

2001:db81:8086:6502::/64

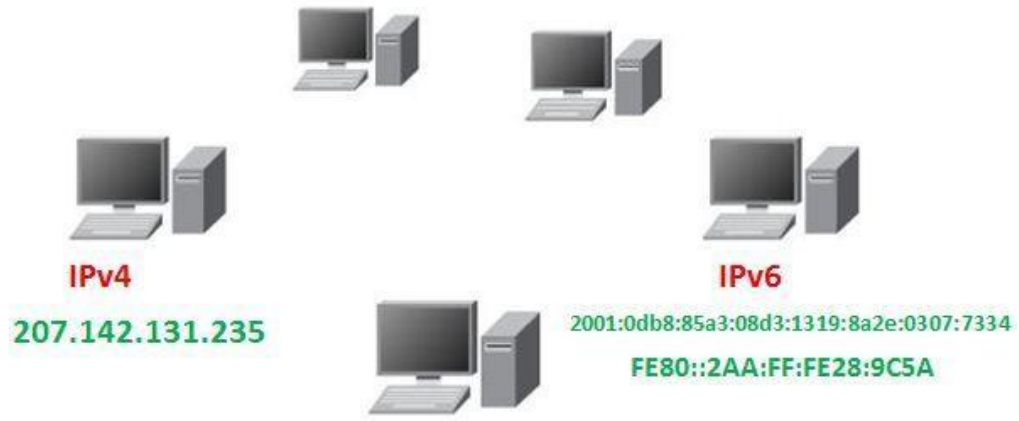
Дължината на префикса има десетична стойност , която показва колко от най- левите съседни бита на адреса включва префикса.Сам по себеси,префикса на IPv6 може да характеризира група от адреси и също така се изпозва за идентифициране на мрежа , като например линк,сайт дори и Internet Service Provider мрежа.



Линк като цяло има 64 бита дълъг префикс, докато един сайт има 48 бита дълъг префикс. В последния случай, 16 бита са разпределени свободно като подмрежа ID, за да може да се изградят различни подмрежи.

Видове адреси на IPv6:

Съществува огромна разлика между IP адресирането на възлите при IPv4 и IPv6. За всяка една възлова точка при IPv4 обикновенно има само един IP адрес,докато за IPv6 обикновенно има повече от един IP адрес за всяка възлова точка.



Имаме три важни типа за адресиране при IPv6:

- unicast
- multicast anycast.

Ще разгледаме всеки от типовете поотделно:

Unicast адрес на IPv6 - Един unicast адрес, идентифицира само един интерфейс. Unicast адресите на IPv6 на протокола могат да бъдат разделени на четири типа:

- Глбални unicast адреси(global unicast addresses)
- Unique local addresses или ULAs
- Link-local unicast addresses
- IPv4-mapped IPv6 addresses

Също така съществуват „специални“ unicast адреси,като например:

- unspecified адреси
- loopback адреси

Anycast адреси на IPv6 – представляват идентификатор присвоен на множество интерфейси, обикновенно на отделни хостове. Когато бъде изпратен пакет към anycast адрес, пакетът се предава само към един от интерфейсите асоциирани с адреса. Това обикновено е най – близкия адрес от маршрутната таблица. Anycast адресите изпозват същия синтаксис,какъвто изпозват и unicast адресите. Последните се превръщат в anucast адреси, когато бъдат присвоени на на повече от един мрежов интерфейс.

Multicast адреси на IPv6 - IPv6 multicast адрес е идентификатор за набор от интерфейси,който обикновено принадлежи на различни възли. Пакет,изпратен до IPv6 multicast адрес е доставен до всички хост интерфейси, които са описани от този multicast адрес. Той се повтаря във възлите по пътя между изпращащия и множеството получатели.

IPv6 не се възползва от “broadcast”. Broadcast адресите намаляваха мрежовата производителността на IPv4, като всеки възел от връзката трябва да обработва всички броудкасти за тази връзка, макар че повечето броудкасти са неподходящи за повечето възли. Обърнете внимание че при IPv6 нямаме broadcast адреси. Това е така, защото цялата функционалност предлагана от broadcast адресите при IPv4 е заменена с по-ефективните multicast адреси при IPv6.

Различни начини за представяне на адресите на IPv6:

Адресен тип	Оригинален адрес	Съкратен адресен синтаксис
Unicast	1090:0:0:0:0:876:AABC:1234	1090::876:AABC:1234
Multicast	FF01:0:0:0:0:0:0:67AB	FF01::67AB
Loopback	0:0:0:0:0:0:0:1	::1
Unspecified	0:0:0:0:0:0:0:0	::

Специални IPv6 адреси:

Необходимо нещо, което трябва да знаем за IPv6 са специалните unicast адреси:

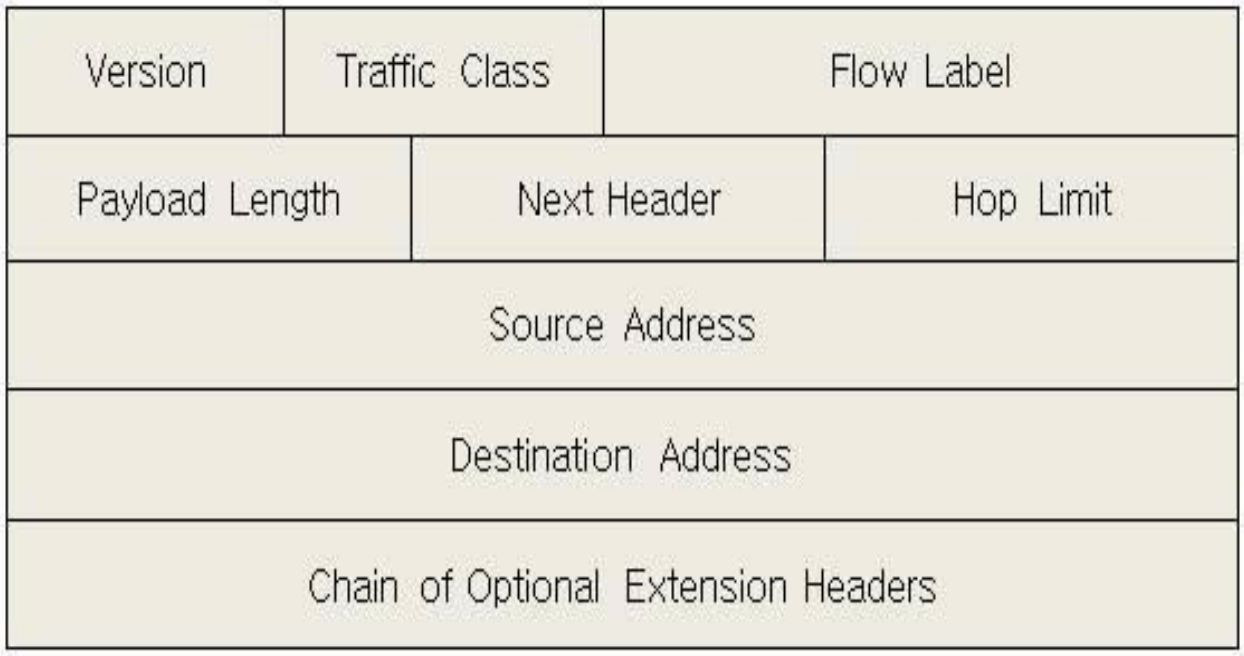
- **0:0:0:0:0:0:0:0** – този неопределен аддрес показва липсата на присвоен IPv6 адрес. Пример за това е DHCP клиент, който е инициализиран, но не е получил IP адрес от DHCP сървъра. Особеното тук, е че този аадрес може да бъде присвоен на дадена машина, но към него не могат да се правят обръщения.

- **0:0:0:0:0:0:0:1 –** този Loopback адрес се използва от IPv6 хоста, за да изпраща IPv6 пакети сам към себе си. Той може да бъде използван само в полето адрес на получателя на IPv6 пакета. Това е еквивалентно на loopback адреса 127.0.0.1 използван при IPv4
- **IPv6 адреси съвместими с IPv4 –** IPv6 хостовете, които ще комуникират с IPv4 хостовете се нуждаят от специален IPv6 unicast адрес, които съдържа валиден IPv4 адрес в младшите си 32 бита. В този случай първите 96 бита са нули.

Част 3: IPv6 хедър

Хедърът на IPv6 е доста опростен и много по-ефективен в сравнение с хеъра на IPv4. За да може всичко това да е така се направиха няколко прости неща - намали се дължината и се намали броя на полетата в него. Това направи:

- маршрутизирането по-ефективно
- увеличи прозводителността
- подпомогна мащабируемостта.



Ще разгледаме всички полета и техните функционалности свързани с IPv6 хеадъра:

- Version - Това 4-битово поле съдържа номера на IP версията и има стойност 6.
- Priority - Това 4-битово поле позволява предаващия хост да зададе приоритет на своите пакети. На ниско ниво на приоритетните пакети се присвоява стойност между 0 и 7. Пакетите от това ниво дават предимство на пакетите с ниво на приоритет между 7 и 15, ако настъпи натоварване на мрежовия трафик.
- Flow Label - Това 24- битово поле маркира пакетите, които изискват специална обработка от IPv6 маршрутизаторите. Тук могат да бъдат включени услуги за реално време или изисквания за нестандартно качество на услуга.
- Payload Length Това 16- битово поле указва дължината на остатъка от IP пакета.
  Това представлява цялата дължина на пакета без IP хедъра.
- Next header - Това 8- битово поле индицира незадължителен хедър, който се намира непосредствено следва IP хедъра. Стойностите в това поле са същите както при IPv4 протокола.

- Hop Limit - Това 8- битово поле е IPv6 еквивалента на TTL при IPv4. Всеки път, когато се изпраща пакет между мрежови сегменти, тази стойност се намалява с единица. Когато стойността на това поле стане нула пакета се отхвърля.
- Source Address - Това 128- битово поле съдържа IPv6 адреса на предаващия хост.
- Destination Address - Това 128- битово поле съдържа IPv6 адре- са на приемащия хост
- Chain of Optional Extension Headers-Верига незадължителни разширени хедъри,позиционирани веднага след хедъра на IPv6. Тези разширени headers притежават опции които спомагат за това да няма намаляне на производителността.
- Както може да видим, хедъра на IPv6 макар да е доста опростен дава много поголеми възможности в сравнение с хедъра на IPv4. Производителността е повишена, включени са услуги за реално време, проверка на качеството на самата услуга и също така може да правим подбор на пакети спрямо техния приоритет.

Двата протокола IPv4 и IPv6 се различават много в своя хедър.Както може да се види някои от полетата са премахнати други полета са заменени и само едно ново поле беше добавено в IPv6 хедъра в сравнение с по-старата версия на протокола.

Премахнати:

- „Header Checksum“-качеството на връзката е сега много по високо,а контролните суми(checksums) вече се извършват в горния и долния слой.
- Трите полета Identification , Flags и Fragment Offset - фрагментацията може да се осъществи изпозвайки подходящи разширения.
- Header Length - при IPv6 имаме фиксирана дължина на дължината на хедъра.

Заменени:

- В IPv4 имаме поле „type of service“ което е заменено в IPv6 от полето “Traffic Class”
- Полео „protocol type” е заменено от полето “Next Header” при IPv6.
- Полето „total length” е заменено от полето “Payload Length” при IPv6
- Полето „Time To Live” е заменено от полето „Hop Limit” при IPv6 на хедъра.

За разлика от хедъра на IPv4,който има 13 полета,хедъра на IPv6 съдържа само 8 такива с фиксирана дължина от 40 октет(единица за цифрова информация в компютрите,състоящ се от 8 бита)

IPv6 разширени хедъри

Противно на IPv4, който дефинира опции в хедъра,опциите в IPv6 са обхванати от разширените хедъри. Те могат да се добавят когато е необходино и да се пропускат ако има такава възможност. Осемте полета от хедъра на IPv6 са последвани от незадълвителните разширени хедъри.

Нямаме фиксиран брой на разширените хедъри в пакета на IPv6, но всеки един от тези разширени хедъри има дължина от 64 бита.

Съществена роля играе полето “Next header”. Благодарение на него се прави инициализация на самите разширени хедъри. Ако имаме повече от един хеадър това поле ги инициализира един след друг. По този начин последния разширен хеадър ще съдържа полето “Next header”.

Когато множество разширени хедъри са изпозвани в един и същ пакет, начина им на подреждане трябва да бъде следния:

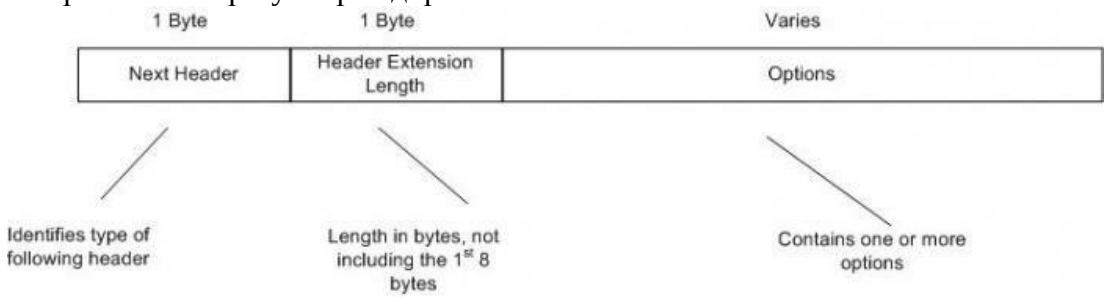
- Първо Hop-by-Hop Options header

- След това Destination Options header
- Следван от Routing header
- След това Fragment header
- Authentication header
- Encapsulating Security Payload header
- Upper-Layer header

Всеки разширен хедър трябва да се появява само един път в IPv6 пакета. Единственото изключение е хедъра Destination Options. Той може да бъде разположен преди хедъра Routing. Опциите в този хедър се обработват от всеки адрес на приемника указан в Routing header. Destination Options може да съществува и преди Upper-Layer header. Тогава той може да бъде обработен единствено от примащият хост, за който е предназначен пакета.

Сега ще разгледаме някои от най-използваните разширени хедъри малко по-подробно:

1. Този хедър носи информация, която трябва да бъде проверявана от всеки възел по пътя, през който минава пакета до достигане на приемника. Наличието му се оказва със стойност нула в полето Next Header на IPv6 хедъра. Този пакет също така може да указва т.нар. jumbo payload,които са IPv6 пакети с дължина по-голяма от 65536 октета без да включва дължината на IP хедъра. Формата на Hop-by-Hop хедъра е:

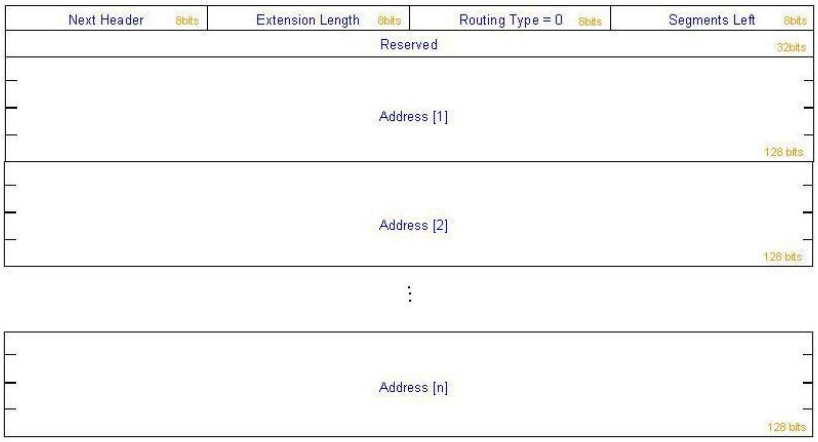


Хедъра съдържа следните полета:

- Next Header - Това 8-битово поле идентифицира типа на хедъра следващ непосредствено след Hop-by-Hop хедъра. Това поле има същите стойности като съответното поле при IPv4 прото¬кола.
- Header Extension Length - Това 8-битово поле указва дължината на Hop-byHop полето в 8-октетни единици (тук не се включват първите 8 октета).
- Options - Това поле е с променлива дължина зависеща от броя и типа на опциите. Тези опции по правило са във формат тип-дължина-стойност - type-length-value(TLV) (виж фигура 21.7),

Всяка една от опциите в Hop-by-Hop хедъра трябва да бъде обработена в последователен ред.

2. Routing хедър – този хедър се използва от IPv6 предаващият хост и служи за описание на маршрута на пакета до приемашия хост. Съществуването на Routing хедъра се указва чрез стойност 43 в полето Next Header на предшестващият го хедър. Формата на хедъра е следната:



- Next header – 8 битово поле, което идентифицира типа на хедъра следващ непосредствено след Routing хедъра. Това поле има същата стойност като съответното поле при IPv4 протокола.

3. Destination хедър - Този хедър съдържа информация, която може да бъде ползвана само от приемащия хост или от междинни хостове. Това зависи от разположението на този хедър по отношение на другите хедъри. Ако той е разположен след Hop-byHop хедъра всеки възел по пътя до приемащия хост може да види тази опционна информация. Формата на Destination хедъра е същият както на Hop-by-Hop хедъра

4. Authentication хедър - Този хедър осигурява механизъм за достоверност за IP датаграмите. Тази достоверност се осигурява чрез изчисления върху всички полета на IP датаграмите, които не се променят при предаването им. Тук не се включват полета съдържащи броячи. След като информацията за достоверност се изчисли по – горе на споменатите полета се присвоява стойност 0. Данните за достоверност се съхраняват в полето за данни на хедъра, така че това ще продължи да работи правилно без да се променя изградената инфраструктура на Интернет. Authentication хедъра се указва със стойност 51 в полето Next Header на предшестващия го хедър.

Част 4: Основни услуги на IPv6

ICMPv6: IP възлите се нуждаят от специален протокол за трансфер на съобщенията свързани с IP условията. Този протокол,интернет протокол за контрол на съобщенията,накратко ICMP, е един от основните протоколи в Интернет комуникацията. Използва се главно от операционните системи за изпращането на съобщения за грешка, показвайки недостъпност на Интернет услугата или че хостът в Интернет не може да бъде достигнат.

Генерирайки грешки и информационни съобщения,ICMP в IPv6 основно функционира по същият начин както ICMP в IPv4. Но допълнително,ICMP пакетите в IPv6 се използват също така и в IPv6 neighbour discovery process.

ICMP пакетите при IPv6 са подобни на транспортен слой,все едно че ICMP пакетите следват всички разширени хеадъри. Те съдържат както се казва последното пърче информация на самият IPv6 пакет.

ICMPv6 хедъра се идентифицира от полето “Next header” със стойност от 58 в предшестващият хеадър. В самия ICMPv6 пакет имаме две полета:

- Type поле-показва типът на съобщението,като : дестинация която неможе да бъде достъпена,прекалено голям пакет,параметричен проблем,изтекло време и други.
- Code поле -предоставящо допълнителна информация на специфичното съобщение.

Полето“Checksum” се сформира от полетата на ICMP пакета в IPv6 и IPv6 хедъра.

В Message Body-to на ICMPv6 се съдържа грешката или диагностичната информация отнесена към начина на действие на IP пакета. Подобно на ICMPv4,ICMPv6 е често блокиран от различните начини за сигурност в системата,тъй като този проткол е подлаган много пъти на хакерски атаки. Въпреки това,ICMPv6 е способен да използва IPSec , която предоставя начини за автентикация и криптиране. Тези услуги за сигурност намаляват възможността за хакерски атаки базирани на ICMPv6.

NEIGHBOUR DISCOVERY:

IPv6 Neighbour Discovery protocol използва ICMPv6 съобщенията и кореспондира с протоколите на IPv4 като например:ARP,ICMP Router Discovery и други.

Възлите като например хостове и рутери използват Neighbour Discovery за да определи най-долния слой от съседни адреси които пребивават в прикрепени свръзки и в същото време да може бързо да изчиства кешираните стойности,които са станали невалидни. Хостовете също използват Neighbour Discovery , за да намерят съседни рутери, които са готови да предадат пакетите от тяхно име. И накрая, възлите също използват този протокол , чрез който може да се следи връзката за това кои съседи могат да бъдат достигнати и кои не, и да може да се откриват променените адреси на най -ниско ниво.

Neighbour Discovery решава проблеми свързани с взаимодействието между възлите свързани към една и съща връзка. Той дефинира механизъм който решава следните проблеми:

- Router Discovery -
- Prefix Discovery-
- Parameter Discovery
- Address Autoconfiguration
- Address Resolution
- Next-hop Determination
- Neighbour Unreachability Detection
- Duplicate Address Detection
- Redirect

За да може да изпълни тези задачи и по този начин да реши проблемите Neighbour Discovery използва пет различни ICMPv6 пакетни типове:

- Router Solicitation
- Router Advertisement
- Redirect messages
- Neighbour solicitation
- Neighbour advertisement

IPv6 използва както stateful адресни автоматични конфигурационни механизми , така и stateless адресни автомаични конфигурационни механизми. Stateless автоматичната конфигурация позволява следните 3 неща:

- Не изисква ръчна конфгурация на хостовете
- Минимално конфигуриране на рутерите
- И никакви допълнителни сървъри

Този вид автоматична конфигурация е ключова характеристика на IPv6,която позволява на хостовете да генерират свои собствени адреси,като използват комбинация от локално наличната информация и информацията предадена им от рутерите.Stateless автоматичната конфигурация опростява дори преномерирането в някой от случаите.

Този вид конфигурация изисква да имаме локална връзка поддържаща мултикаст и в същото време мрежовият интерфейс да бъде в състояние да изпраща и получава такива мултикаст пакети.

IPv6 възлите като хостове и рутери ,автоматично създават валидни уникални адреси за всички интерфейси. И накрая IPv6 използва DAD-откриване на доблиращи адреси , за да определи дали адреса вече не се използва.

IPv6 използват получената информация от Router Advertisement за да направи автоматична конфигурация на:

- Маршрутизаторът по подразбиране
- Настройките за подразбиране на полето Hop Limit в хедъра на IPv6
- Таймерите в Neighbour Discovery прецесите
- MTU на локалният линк
- И списъкът от префикси,които са дефинирани за този линк

Трябва да отблележим две съществени неща свързани с Router Advertisement.

1. Всяко едно router advertisement съобщение съдържа в себе си две неща
   - IPv6 мрежовият префикс
   - Валидното му време на живот.

2. Router Advertisements съдържа два флага, които да ределят какъв вид stateful автоматична конфигурация трябва да се извърши , ако имаме изобщо такава:
   - Флагът за „managed адресна конфигурация“ ни показва дали хостът трябва да използва stateful автоматичната конфигурация , за да получи адреси или не.
   - И вторият флаг за „другият вид stateful конфигурацията“ ни показва дали хостовете трябва да използват този вид автоматична конфигурация , за да получат допълнителна информация, като например някакъв вид DNS сървърен адрес. Това е много важно , тъй като при stateless автоматичната конфигурация, няма абсолютно никакъв начин да изпратим такъв вид адрес до някой клиент.

DHCPv6:

DHCP за IPv6 познат още като DHCPv6 работи по модела клиент/сървър. Той позволява на DHCP сървърите да пропускат IPv6 адресите и други конфигурационни параметри към IPv6 възлите. Този протокол е stateful копие на IPv6 Stateless Address Autoconfiguration.

Процесът за придобиване на конфигурационните данни за клиентите е подобен на този който е при IPv4. DHCPv6 използва мултикастинг за много от неговите съобщения. Ако маршрутизатор е намерен , клиентът проучава router advertisements , за да определи дали DHCP трябва да бъде използван. Ако router advertisements позволи използването на DHCP или ако не е намерен този маршрутизатор, клиентът ще се свърже с DHCP сървъра.

Клиентите и сървърите обменят DHCP съобщения използвайки UDP.DHCP сървърите получават съобщения от клиенти , използващи запазени link -scoped мултикаст адреси. Те имат следния формат: DHCP клиента предава повечето съобщения на този запазен мултикаст адрес. За да позволи DHCP клиента да изпрати съобщение към DHCP сървъра , които не е свързан към същата връзка, DHCP препредаващият агент на клиентската връзка ще предаде съобщенията между клиента и сървъра. Работата на препредаващия агент е открита за клиента. При желание сървърът осигурява клента с IPv6 адреси и други конфигурационни параметри, като например:

- DNS сървър адреси,
- NTP сървър адреси
- други.

Но е невъзможно да се изпратят gateway адрес, защото тази информация трябва да е получена чрез stateless автоматична конфигурация.

DHCPv6 озигурява повече контрол отколкото stateless автоматичната конфигурация. За разлика от DHCPv6 stateless автоматичната конфигурация не позволява на мрежовия администратор да дефинира правила за контрол на достъпа. С автоматичната конфигурация, всеки хост свързан към мрежата може да получи IPv6 адрес. За разлика от това DHCP сървърите осигуряват средства за осигряване на контрол на достъпа до мрежовите ресурси, като първо проверява правилата за контрол на достъпа преди да отговори на заявката от клиета.

Част 5: Сигурност на новия протокол

Основните цели на IPv6 сигурността са същите като при всяка мрежова инфраструктура. Те включват следното:

- Здравина на инфраструктурата
- Автентикация, конфиденциалност и интегритет
- Невъзможност за отказ
- Контрол на достъпа
- IP accounting and billing

Заплахи за сигурността при IPv6

- Сканиране на gateways (шлюзове) и хостове за слабости
- Сканиране за мултикаст адреси
- Неоторизиран достъп
- Откиване на слабости с NAT(network address translation – преобразуване на мрежовите адреси) и слабости в защитните стени
- Атаки по производителността със фрагментирани хедъри
- Слабости на протокола
- Разпределена атака за отказ на услуга(DDoS)

Вижда се че има не малко атаки, които могат да повредят системата. Тези заплахи същесвуваха и при IPv4. Но има една съществена разлика меджу заплахите, които могат да се появят при IPv4 и IPv6. Тя се изразява в това, че IPv6 е протокол, при който сигурността е на много по – вискоко ниво в сравнение с IPv4 протокола.Ще разгледаме всяка една от атаките, като в същотот време покажем, какви мерси се взеха при IPv6 за повишаване на сигурността.

- Първата заплаха за сигурнстта е сканирането на шлюзовете и хостовете от хакери или системи които искат да пробият в мрежата или да я атакуват. Те сканират всички външни адреси на шлюзовете или хостовете на които попадат и търсят слабости в тяхната защита. Поради голямото адресно пространство на IPv6, сканирането на мрежата за уязвими системи е станало по-сложно. Изчерпателното сканиране на всеки адрес в подмрежа е станало много трудно. Освен това софтуер за сканиране на портовете като NMAP дори не поддържа сканиране на мрежата при IPv6. Но очевидно сканирането ще продължи да съществува. Поради нуждата публичните сървъри да са достъпни от DNS, хакерите все още имат хостове за атакуване. Освен това администраторите могат също да приемат easy-to-remember адреси. „Фиксираната част“ от адреса улеснява атакуващия. Нови техники за събиране на адреси могат да използвт информацията от DNS зони или логове. И накрая хакерите могат да намерят нови адреси за сканиране като компрометират рутери на ключови трянзитни точки в мрежата.
- Втарата заплаха е сканиране за мултикаст адреси; IPv6 очаква всички имплементации да поддържат мултикаст. Новите мултикаст адреси които поддържа IPv6 могат да дадат възможност на хакерите да идентифицират ключови ресурси в мрежата и да ги атакуват. „Всеки възел“ и „всеки рутер“ мултикаст адреси също могат да се използват като нови вектори за атака. За да се направят мултикаст адресите недостъпни отвън, те трябва да се филтрират на границата. Това е подразбиращата се ситуация ако IPv6 мултикаста е позволен. Сигурността на IPv6 адресите

може да се подобри като се използва Криптографски генерирани адреси. Те са IPv6 адреси които пренасят хеширана информация за публичния ключ в идентификаторната част. Криптографски генерираните адреси осигуряват свързване на IP адресите с публични ключове без нужда от управляваща инфраструктура.

- Неоторизиран достъп е третата заплаха - Мобилната IPv6,използва Protocol for Authentication and Network Access за предпазване от неоторизиран достъп. PANA осигурява решение което дава възможност за удостоверяване на достъпа до мрежата. В мобилната IPV4, мобилният възел взаимодесйства с външен агент за автентикацията си. В мобилната IPv6 тази автентикационна функция не се управлява от външен агент, а от PANA агент или PANA Authentication Agent(PAA).
- Слабости в защитната стена са четвъртята заплаха. В IPv6 защитните стени могат да се настроят по различни начини. Въпреки това, за да се избегнат слабости, архитектурата на IPv6 и самата защитна стена трябва да отговарят на определени изисквания. След като IPv6 не се нуждае от NAT, може да се използва същото ниво на сигурност и тайна както при IPv4. Това ниво дори е увеличено заради end-to-end сигурността предложена от задължителната имплементация на IPSec.И понеже няма нужда от NAT, слабостите при филтриране на пакети вече немогат да бъдат скрити. В допълнение архитектурата и защитната стена на IPv6 трябва да поддържат IPv6 поредици от хедъри и IPv4/IPv6 преходи и съжителства. Накрая те не трябва да чупят сигурността на IPv4. Трябва да се гарантира че въпреки допълнителната сложност на шлюзовете, няма действителна слабост.
- Петата заплаха се състои от атака по производителността с фрагментиране на хедъри. За да се избегне това, всеки администратор на IPv6 мрежа трябва да следва слените практики:
  - Отхвърляне на IPv6 фрагментите предназначени за междумрежови устройства които са използвни като DOS вектор за атака на инфраструктурата.
  - Осигуряване на адекватна филтрираща способност за фрагментации.
  - Всички фрагменти трябва да се доставят за 60 секунди. Ако това не може да стане те се пускат.
- Шестата заплаха се формира от слабости в протокола. В IPv4 тези слабости могат да доведат до spoofing на нива 3 и 4, или ARP и DHCP атаки. В IPv6 това вече не е така. Въпреки това шлюзовете между две среди остават сериозна мишена. В IPv4, ARP и DHCP са в състояние да разрушат хост инициализацията. В IPv6, ARP е заменен от Neighbour Discovery. С Neighbour Discovery, инструменти за атака като „ARP cache poisoning“ изчезват, но изчезват и инструменти за защита като DHCP snooping. Въпреки това Neighbour Discovery е по -добро решение.
- Последната заплаха е от DoS атака (Атака за отказ на услуга). Броудкаст усилване и “Smurf”атаки, които работят като изпращат ACMP пакети до броудкаст адреси, са елиминирани в IPv6, защото IPv6 използва глобални мултикаст адреси вместо броудкаст адреси.

Практическа задача

Част 1: Изследване и запознаване с мрежата

A. Разглеждайки схема топология, колко мрежи има общо?

B. Колко мрежи са свързани директно към R1, R2 и R3?

C. Коя команда се използва, за да изберете IPv6 статични маршрути?

Част 2: Конфигуриране на IPv6

Стъпка 1: Активиране на IPv6 маршрутизация на всички рутери.

Router> **enable**

Router# **configure terminal**
Router(config)# **ipv6 unicast-routing**

Стъпка 2: Основни настройки за всички рутери.

Конфигурирайте адреси на интерфейсите на рутерите, като използвате таблицата в началото на упражнението.

Примерна команда е:

R1> **enable**
R1# **configure terminal**
R1 (config)#**interface fastEthernet 0/0**
R1(config-if)#**ipv6 address 2001:DB8:1:1::1/64**
R1 (config-if)#**no shutdown**
R1 (config-if)#**exit**

Стъпка 3: Конфигуриране на рекурсивни статични маршрути за R1.

R1 (config)#**ipv6 route 2001:DB8:1:2::/64 2001:DB8:1:A001::2**
R1 (config)#**ipv6 route 2001:DB8:1:A002::/64 2001:DB8:1:A001::2**
R1 (config)#**ipv6 route 2001:DB8:1:3::/64 2001:DB8:1:A001::2**

Стъпка 4: Конфигуриране на директно прикачени и напълно определен статично маршрут на R2.

a. Конфигуриране на директно прикачени статичен маршрут от R2 до R 1 LAN.

   R2 (config)#**ipv6 route 2001:DB8:1:1::/64 Serial0/0/0**

b. Конфигуриране напълно определен маршрут от R2 до R3 LAN.

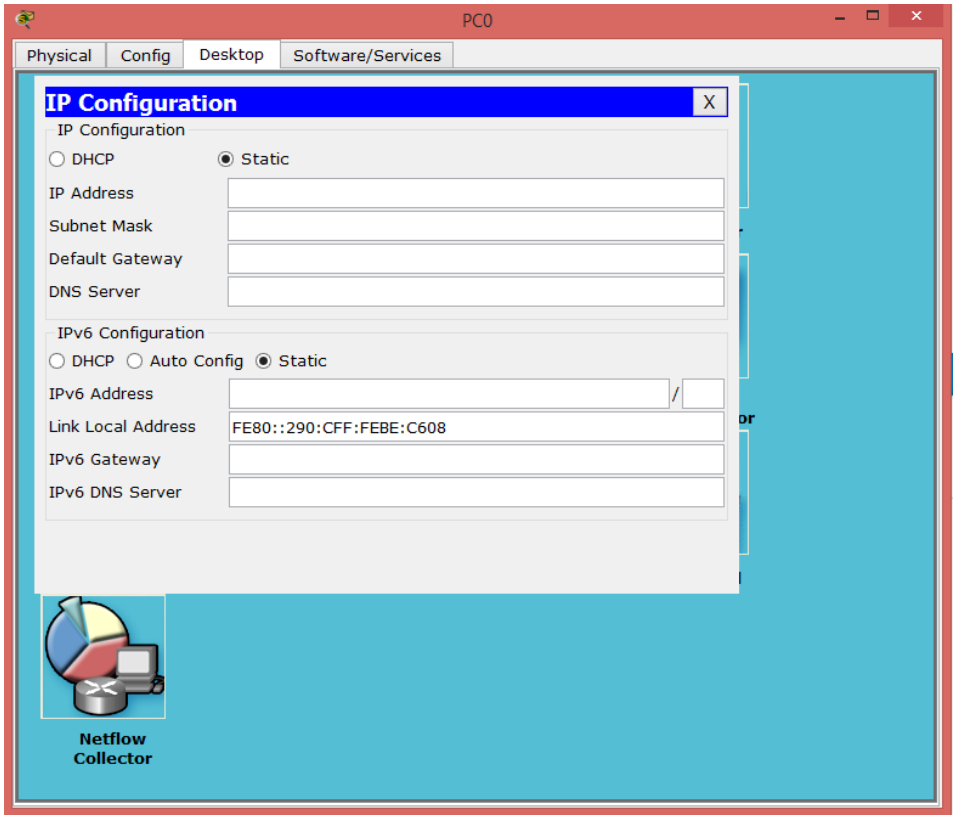
   R2 (config)#**ipv6 route 2001:DB8:1:3::/64 Serial0/0/1 2001:DB8:1:A002::2**

Стъпка 5: Конфигуриране маршрут по подразбиране на R3.

R3 (config)#i**pv6 route ::/0 2001:DB8:1:A002::1**

Стъпка 6: Конфигурирайте компютрите.

Конфигурирайте статични адреси. (в таблицата по-горе са показани адресите). Кликате на съответната машина и отивате на Deskop->IPconfiguration



Стъпка 7: Конфигуриране на пароли на R1, R2 и R3.

a. **Парола за конзолата**
   Router#**configure terminal**

   Router(config)#**line console 0**

   Router(config-line)# **password парола (за целта на упражнението ползвайте cisco)**

   Router(config-line)#**login**

b. **Парола на привилигирования режим**
   Router#**configure terminal**

   Router(config)#**enable password парола (за целта на упражнението ползвате cisco)**

   Router(config)#**enable secret парола (за целта на упражнението ползвате cisco2)**

c. **Парола за Telnet сесии**
   Router(config)#**line vty 0 4**

   Router(config-line)#**password парола (за целта на упражнението ползвате cisco)**

   Router(config-line)#**login**

Стъпка 9: Конфигуриране на банери

Router(config)#**banner motd # съобщение #**

Част 3: Проверка на свързаността

Стъпка 1: Направете пинг от PC-A до PC-C.

Стъпка 2: Направете пинг от PC-A до PC-B.

Стъпка 3: Направете пинг от PC-B до PC-C.

Използвана литература

1. Cisco Security v1.1
2. Компютърни мрежи и комуникации – Иван Цонев, Станимир Станев
3. Дебра Литълджон Шиндър – „Компютърни мрежи”
4. WWW
   - www.cisco.com