Урок 4

Сетевой уровень. Часть 2

Бесклассовая маршрутизация, маски подсетей переменной длины (CIDR/VLSM). Динамическая маршрутизация. Протокол DHCP.

Сетевой уровень

Введение

Как мы помним, для того, чтобы выделить адрес сети из хоста используется маска сети. Состоит она из двух частей. Та часть, что идентифицирует сеть, содержит двоичные единицы. А та часть, что выделена под хост, содержит двоичные нули. Например, 255.0.0.0 – маска для сетей класса А.

Произведя двоичное умножение побитово, маски сети на IP-адрес, мы получим адрес сети.

Для сетей класса В – маска 255.255.0.0.

Для сетей класса С – маска 255.255.255.0.

На самом деле для классовой адресации явным образом маску указывать и не надо, ее вычислить можно из первых бит адреса, определив класс сети. Но сейчас такой подход устарел и маску нужно указывать явным образом.

Опыт использования классовой адресации показал, что выделение сетей такими крупными кусками, как сети класса А и В оказалось расточительным. Да и выделение сетей класса С по 254 хоста тоже может быть избыточным. Понадобился новый способ выделения адресов.

Если взглянуть на стандартные маски сетей классов А, В и С, приведя их к двоичному виду, не сложно заметить, что, фактически, маска состоит из двух половин, одна из которых содержит единицы, другая нули. Но в классовой адресации она ограничена была тем правилом, что число бит должно было быть кратно байту. Отказавшись от правила кратности байту, мы получаем бесклассовую адресацию.

Например, имея одну сеть класса С в распоряжении (маска 255.255.255.0, то есть 24 бита под адрес сети), выделив + еще один бит, мы сможем разбить ее уже на 2 сети, но не по 254 хоста (256–2) а по 126 адресов (256/2–2).

Такую маску также можно записать и в десятичном виде. В последнем случае у нас октет будет иметь значение 10000000 в двоичном виде, т.е. десятичное значение его 128.

Сравним.

255.255.255.0   = 1111 1111. 1111 1111. 1111 1111. 0000 0000

255.255.255.128 = 1111 1111. 1111 1111. 1111 1111. 1000 0000

Число бит также принято указывать через косую черту после адреса. Оно называется префикс.

255.255.255.0   = 1111 1111. 1111 1111. 1111 1111. 0000 0000 = /24

255.255.255.128 = 1111 1111. 1111 1111. 1111 1111. 1000 0000 = /25

Записи.

10.0.0.0/255.255.255.0 = 10.0.0.0/24

10.0.0.0/255.255.255.128 = 10.0.0.0/25

10.0.0.128/255.255.255.128 = 10.0.0.128/25

Если мы используем уже не 25 бит, а 26 мы можем разбить сеть /24 на 4 подсети.

Вы можете самостоятельно это проверить, используя калькулятор по ссылке.

: http://jodies.de/ipcalc?host=10.0.0.0&mask1=24&mask2=25

Такая адресация называется бесклассовой или CIDR-адресацией (Classless interdomain routing).

Фактически, сейчас не применяется классовая адресация, а блоки адресов выделяются с той или иной маской, которую затем указывают и на хостах.

IP-калькулятор: http://jodies.de/ipcalc

В качестве минизадания: поупражняйтесь с калькулятором, разберитесь с IP-адресацией и ее особенностями, в том числе с бесклассовой (CIDR – адресацией).

CIDR/VLSM

Название расшифровывается как концепция бесклассовой междоменной маршрутизации (Classless Inter - Domain Routing). Также в литературе встречается второй термин:

Variable length subnet masks – сетевая маска с переменным размером (использующая не только стандартные-классы 8/16/24, но и другие значения).

В маске количество используемых бит равных единицам, отвечающих за границу адреса сети, может быть не кратно 8.

Например: 255.255.255.192 = /26 или 255.255.192.0 = /18

IP-адрес 130.64.134.5/18 в двоичном виде будет выглядеть:

IP-адрес 130.64.134.5 - 10000010.01000000.10000110.00000101 Маска 255.255.192.0 - 11111111.11111111.11000000.00000000

Применив маску сети, мы получим при наложение сетевой адрес:

10000010. 01000000. 10000000. 00000000 или в десятичной форме записи - адрес сети 130.64.128.0, и 00000000.00000000.00000110.00000101 адрес узла 0.0.6.5 соответственно.

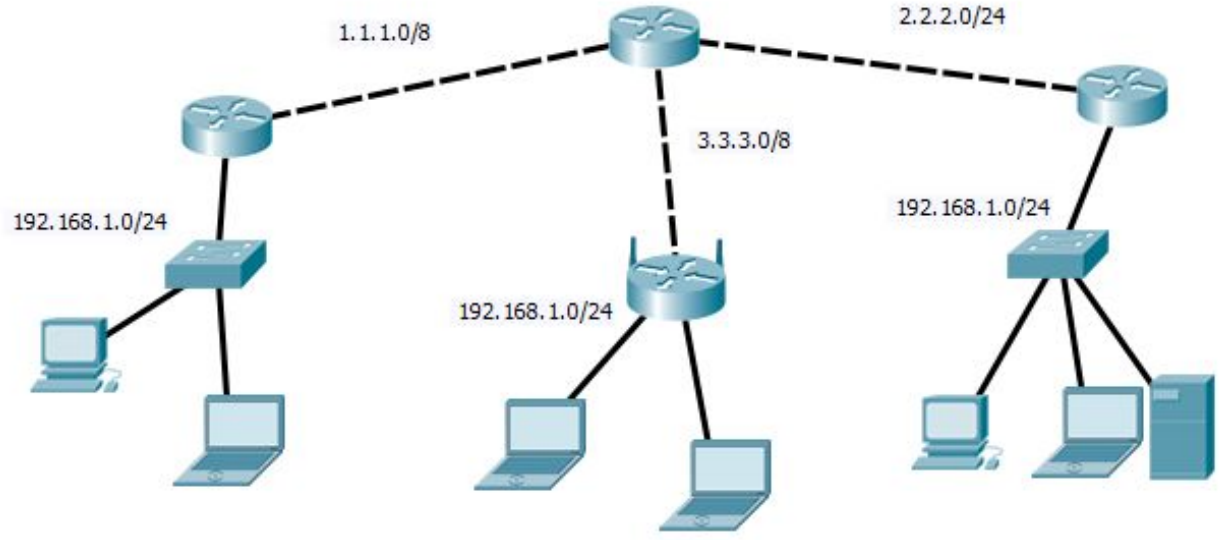
Развитие адресации в этом направлении и внедрение переменных масок/префиксов дает следующие преимущества:

- отказ от традиционного классового разделения адресов протокола IP. Как отмечалось ранее, это позволяет более эффективно распределить существующее адресное пространство между абонентами, создав большое количество сетей, частично решив проблему протокола IPv4, обладающего малым количеством адресов;
- суммаризация или объединение маршрутов. Запись маршрута к нескольким подсетям с помощью одного маршрута в таблице маршрутизации позволяет уменьшить объем сервисной

информации, пересылаемой между маршрутизаторами, что снижает нагрузку на сеть и аппаратные ресурсы телекоммуникационного оборудования. Также это позволяет снизить объем маршрутных таблиц на BGP маршрутизаторах, которые должны содержать таблицу маршрутизации для всех сетей Интернет.

IP адрес		Назначение
сетевые биты	хостовые биты	
номер сети	равны 0	текущая IP сеть
номер сети	номер хоста	хост в данной сети
равны 1	равны 1	все хосты в IP сети
номер сети	равны 1	все хосты в указанной IP сети
127	любые	адрес обратной связи (loopback)

На рисунке ниже приведен пример различных сетей. Как видно, соединения между маршрутизаторами входят в разные сети, а сетевые узлы, объединённые локальной сетью и подключенные к маршрутизатору, входят в одну сеть.

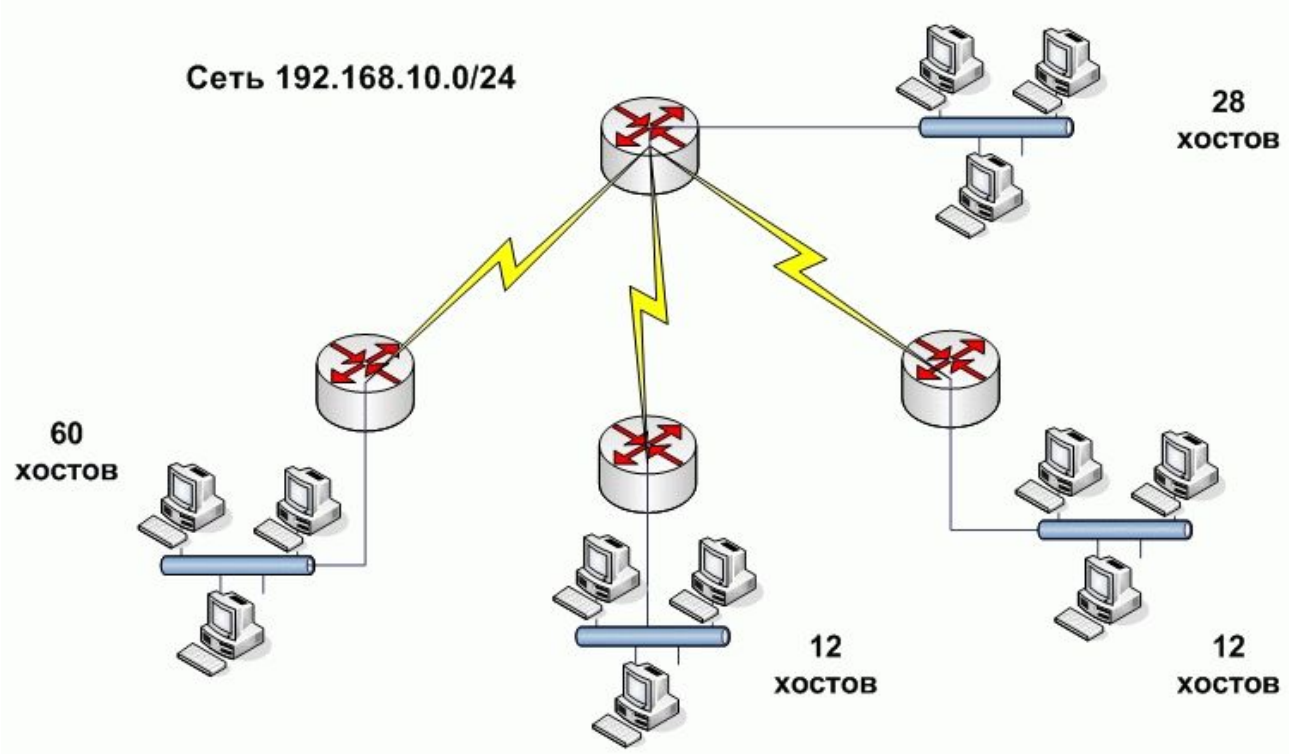


Разделение на подсети

Рассмотрим пример как можно разделить стандартную сеть класса С, в которую входит 254 адреса на 5 сетей с различным количеством узлов.

Необходимо определить, каких размеров сети нам нужны: 60, 28, 12 и 12. Записываем от большего к меньшему. Это важно.

Далее определяем по числу хостов кратному 2 в степени. Т.е. размер сети может быть 4, 8, 16, 32, 64 и т.д. Получается, нам нужно разбить сеть на диапазоны 64, 32, 16 и 16. Таким образом мы используем всего 128 узлов из всех нам доступных.



Адреса для получившихся сетей будут следующие:

192.168.10.0/26 – сеть на 62 узла;

192.168.10.64/27 – сеть на 30 улов;

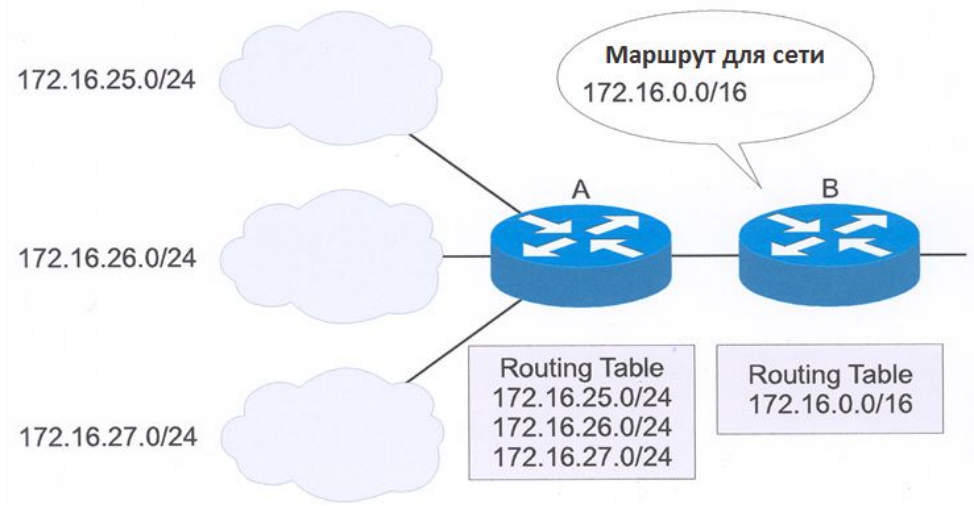
192.168.10.96/28 – сеть на 14 узлов;

192.168.10.112/28 – сеть на 14 узлов.

Объединение (суммаризация) маршрутов

Объединение маршрутов является путем к возможностям увеличения и масштабирования существующей сети. Суммаризация маршрутов решает несколько проблем: большой размер таблиц маршрутизации и время передачи маршрутной информации через автономную систему.

Суммаризация маршрутов снижает нагрузку на аппаратные ресурсы процессоров, оперативную память и загрузку каналов, которые используют службы маршрутизации. При отсутствии суммаризации при каждом обновлении информации о маршруте происходит передача по всем зонам, производя нагрузку на сеть и устройства.

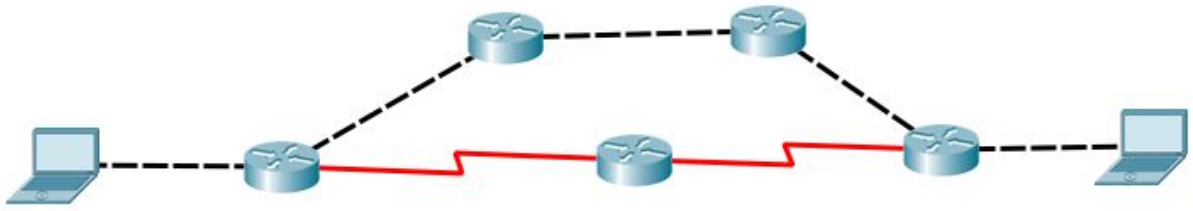


Динамическая маршрутизация

Динамическая маршрутизация — используется в средних и крупных сетях. Маршрутная информация вычисляется на основе данных, поступаюших от соседних маршрутизаторов. Для обмена данными используется протокол динамической маршрутизации.

- Преимущества: быстрее настройка и проще в администрирование;
- Недостатки: использование процессора и передача служебной информации между маршрутизаторами для вычисления оптимальных маршрутов, что также нагружает сеть.

В многосвязных сетях при использовании различных протоколов маршрутизации могут использоваться различные маршруты для передачи информации между двумя узлами. Все протоколы динамической маршрутизации делят на 2 группы: протоколы вектора расстояния и протоколы состояния связи.



Протоколы вектора расстояния (Distance vector) — также называемые дистанционно векторными, используют алгоритм кратчайшего пути для поиска маршрута до удаленной сети. Каждый переход (перенаправление) пакета с помощью маршрутизатора называют хопом (HOP). Протоколы этого типа вычисляют маршрут согласно количеству переходов без учета производительности канала. Примерами таких протоколов являются: RIP, IGRP.

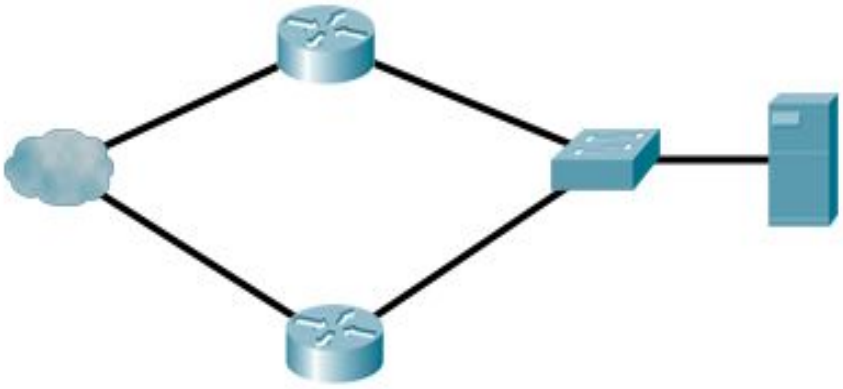
- К преимуществам можно отнести то, что они меньше нагружают процессоры маршрутизаторов и сеть, а недостаток - неэффективный учет пропускной способности и загруженности каналов.

Протоколы состояния связи (Link state) — также называются «протоколами состояния канала». Все маршрутизаторы в сети, на которых запущен протокол, содержат и постоянно обновляют три таблицы. Первая отслеживает соседние устройства, вторая содержит топологию всей сети и третья используется для маршрутизации пакетов. Данные протоколы более эффективно учитывают текущее состояние сети, но сильнее утилизируют каналы связи и аппаратные мощности устройств в связи с тем, что постоянно производят мониторинг состояния сети и обновления маршрутных таблицу. Устройства, использующие протокол состояния связи, обладает большей информацией о сети, чем протоколы вектора расстояния. Примерами протоколов состояния связи являются: OSPF, IS-IS.

- К недостаткам можно отнести то, что данная группа протоколов создает большую нагрузку на вычислительные ресурсы, и, в случае сбоя, тратится больше времени на конвергенцию в сети (конвергентная сеть – сеть, в которой все маршрутизаторы обладают актуальными данными о состояние сети).

Балансировка трафика

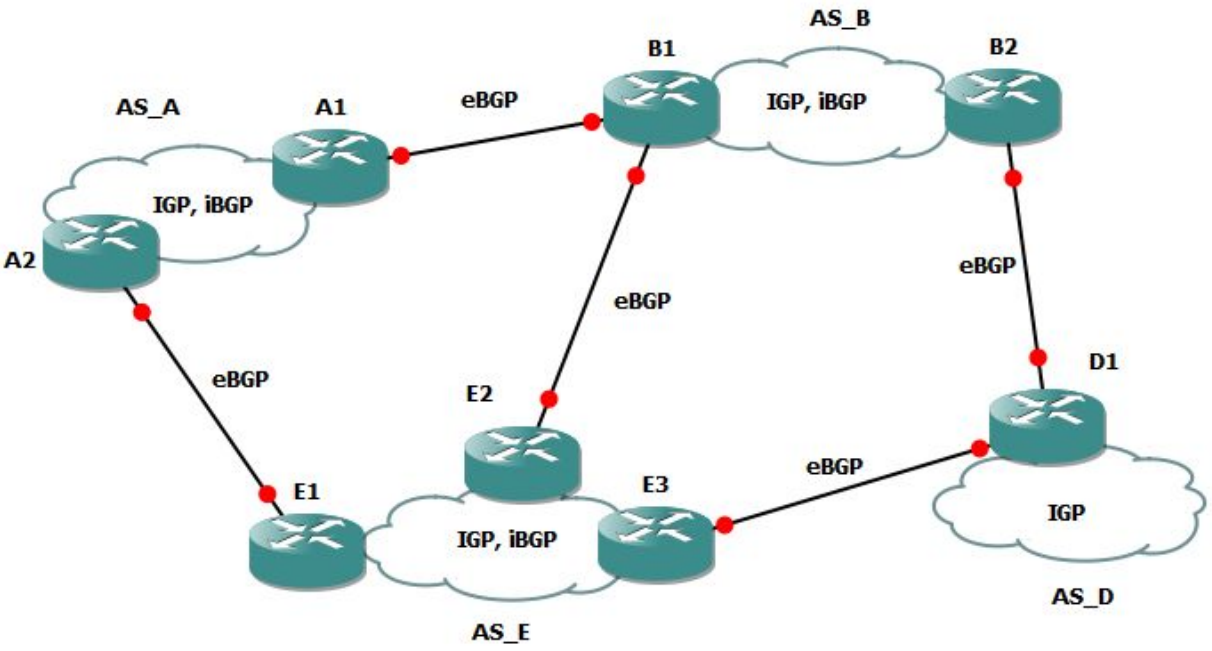
В терминологии компьютерных сетей балансировка нагрузки или выравнивание нагрузки (англ. load balancing) — метод распределения заданий между несколькими сетевыми устройствами (например, серверами) с целью оптимизации использования ресурсов, сокращения времени обслуживания запросов, горизонтального масштабирования кластера (динамическое добавление/удаление устройств), а также обеспечения отказоустойчивости (резервирования).



BGP

Border Gateway Protocol — это основной протокол динамической маршрутизации, который используется в Интернете. Маршрутизаторы, использующие протокол BGP, обмениваются информацией о доступности сетей.

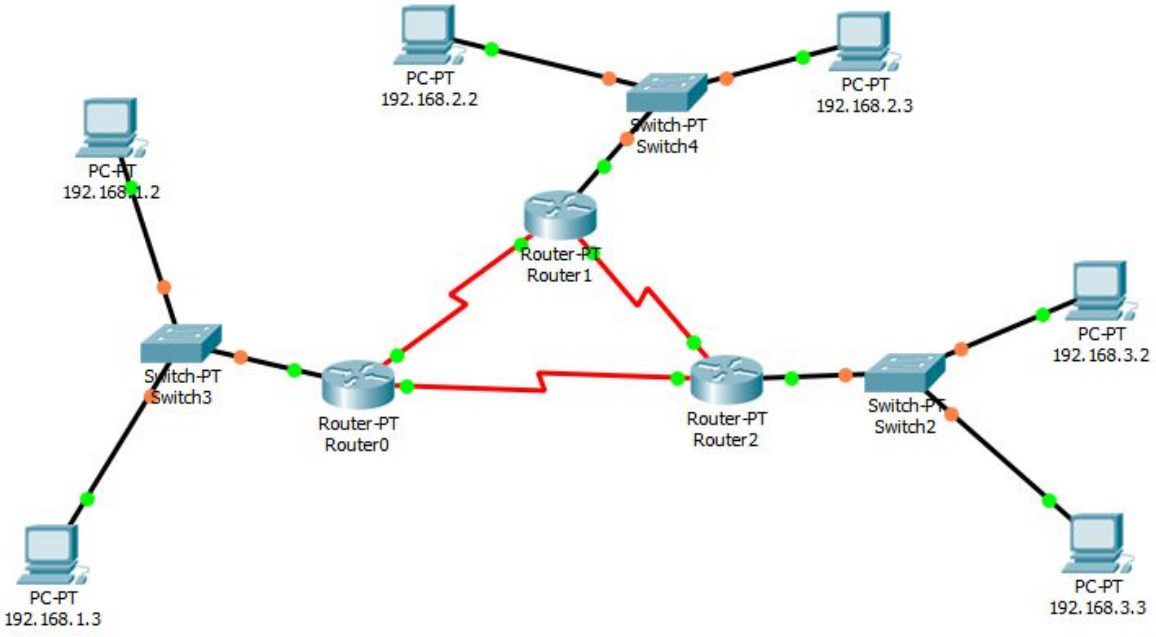
Протокол BGP нельзя отнести ни к дистанционно векторным, но он использует их идею. Основой для вычисления маршрута в BGP являются правила и приоритеты для трафика, настроенные администраторам. Данный протокол в основном используется провайдерами доступа в Интернет и организациями, чьи сети или сервера должны быть доступны извне.



RIP

***R**outing **I**nformation **P**rotocol* — один из известных, старейших и простых протоколов маршрутизации. Использует транспортный протокол UDP и 520 порт. Для того чтобы маршрутизатор работал с разными сетями, достаточно настроить использование RIP-протокола и указать, о каких из используемых сетей маршрутизатор будет уведомлять другие маршрутизаторы. Это можно сделать и из GUI-интерфейса Cisco Packet Tracer, но не сложно заметить, что вы не можете указать маску сети. Это неудобно даже в простом примере: вы не сможете выделить разным машинам подсети из сети 10.0.0.0.

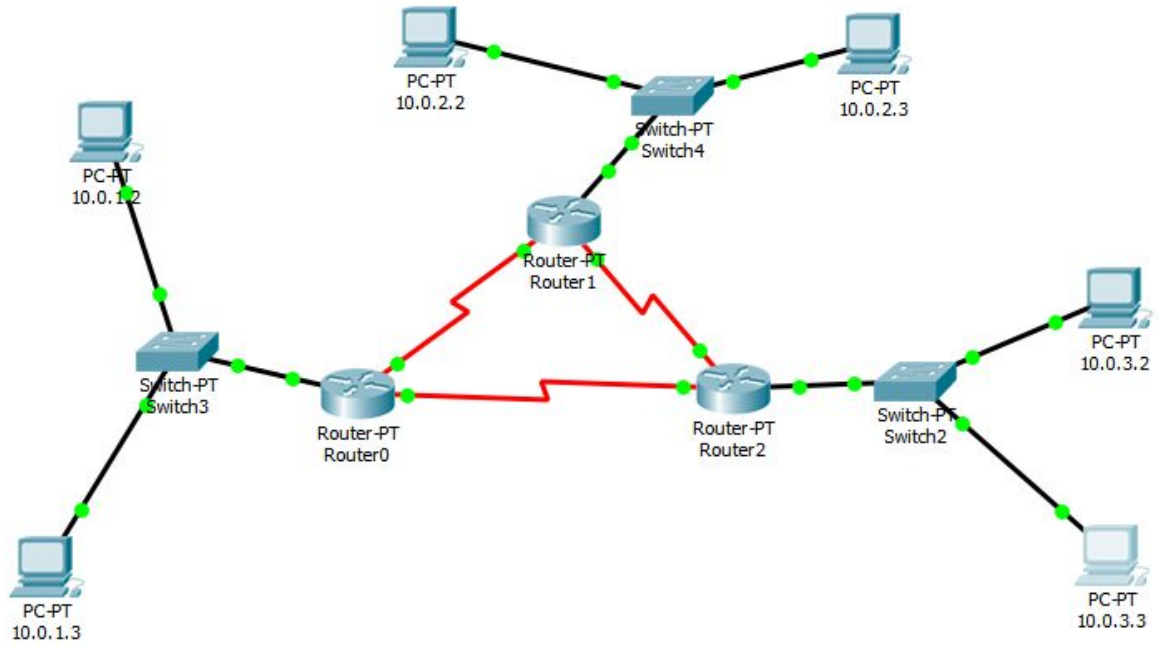
Макси в протоколе RIP не передаются, они определяются исходя из класса сети. Например, для 10.0.0.0 маска будет 255.0.0.0. Придется использовать, например, адреса вида 192.168.X.0, которые относятся к классу C.



Это привело к появлению следующей версии протокола - RIP2.

RIP2

Рассмотрим следующий пример:



Он почти не отличается от приведенного выше, но IP-адреса машин назначены в сетях 10.0.1.0/24, 10.0.2.0/24,10.0.3.0/24 (бесклассовая адресация).

В такой схеме невозможно настроить маршрутизацию с помощью RIP (поддерживает только классовую адресацию и не рассылает маски сетей), но зато можно использовать RIP-2.

В протоколе RIP-2 появилась возможность указывать маску сети, которая также рассылается вместе с адресом сети другим маршрутизаторам.

Настроим сетевые интерфейсы

```
Router0>ena
Router0#conf t
Router0(config)#int fa0/0
Router0(config-if)#int addr 10.0.1.1 255.255.255.0
Router0(config-if)#no shut
Router0(config-if)#int se2/0
Router0(config-if)#int addr 172.16.0.1 255.255.0.0
Router0(config-if)#no shut
Router0(config-if)#int se3/0
Router0(config-if)#int addr 172.17.0.1 255.255.0.0
Router0(config-if)#no shut
Router0(config-if)#exit
```

;

Перейдем в настройки протокола rip:

```
Router0(config)#route rip
```

Обязательно включим версию 2, и объявим те сети, о которых маршрутизатор будет оповещать (и через какие):

```
Router0(config-router)#version 2
Router0(config-router)#network 10.0.1.0
Router0(config-router)#network 172.16.0.0
Router0(config-router)#network 172.17.0.0
```

Если у данной машины имеется маршрут по умолчанию, можно рассылать и его:

```
Router0(config-router)# default-information originate
```

Осталось сам маршрут по умолчанию сделать (если опять же, допустим к схеме выше, у Router0 имеется еще маршрут)

```
Router0(config-router)# exit
Router0(config)ip route 0.0.0.0 0.0.0.0 100.64.0.1
```

(Но необходимо добавить и шлюз 100.64.0.1 и сетевой интерфейс на Router0, например, на fa5/0 в сети 100.64.0.0/24)

Такие же действия, кроме двух последних пунктов, необходимо проделать и на других маршрутизаторах.

После чего можно в привилегированном режиме посмотреть маршруты:

```
Router#show ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
* - candidate default, U - per-user static route, o - ODR
P - periodic downloaded static route
Gateway of last resort is not set
10.0.0.0/24 is subnetted, 2 subnets
C 10.0.1.0 is directly connected, FastEthernet0/0
R 10.0.3.0 [120/1] via 172.17.0.2, 00:00:06, Serial3/0
C 172.16.0.0/16 is directly connected, Serial2/0
C 172.17.0.0/16 is directly connected, Serial3/0
R 172.18.0.0/16 [120/1] via 172.17.0.2, 00:00:06, Serial3/0
```

DHCP

Dynamic Host Configuration Protocol или протокол динамической конфигурации сетевых узлов — протокол, позволяющий узлам в компьютерной сети в автоматическом режиме получить IP-адрес и дополнительные параметры (маска сети, основной шлюз, доменный сервер и другие), нужные для работы в компьютерной сети. Протокол построен на клиент-серверной архитектуре. В качестве сервера может выступать компьютер, маршрутизатор или коммутатор 3-го уровня. Во время инициализации сетевого интерфейса с включенным режимом автоматической конфигурации, клиент производит широковещательный запрос в сеть с целью обращения к DHCP-серверу. Сервер производит ответ, сообщая информацию о необходимых сетевых параметрах. Клиент отвечает серверу, подтверждая, что он готов принять сетевые параметры и нужно зарегистрировать IP-адрес из пула за ним. Сервер подтверждает регистрацию адреса, и клиент начинает использовать назначенный ему адрес. Администратор конфигурирует диапазон адресов (сетевой пул), которые будут назначены клиентам. Данный протокол ускоряет конфигурирование сетевых устройств, кроме того, существует возможность привязки адресов по MAC-адресам к каждому устройству. Протокол DHCP всегда используется в беспроводных сетях.

DHCP разработан на основе протокола BOOTP, который использовался для загрузки бездисковых терминалов и назначения им сетевых адресов. DHCP обратно совместим с BOOTP, но по сравнению с ним позволяет использовать динамические конфигурации.

Порт/ID: 67, 68/UDP.

Настройка DHCP-сервера на маршрутизаторе Cisco

Настроим на Router0 dhcp-сервер.

Посмотрим доступные сервисы (увидим, что dhcp активен), а также список команд для dhcp:

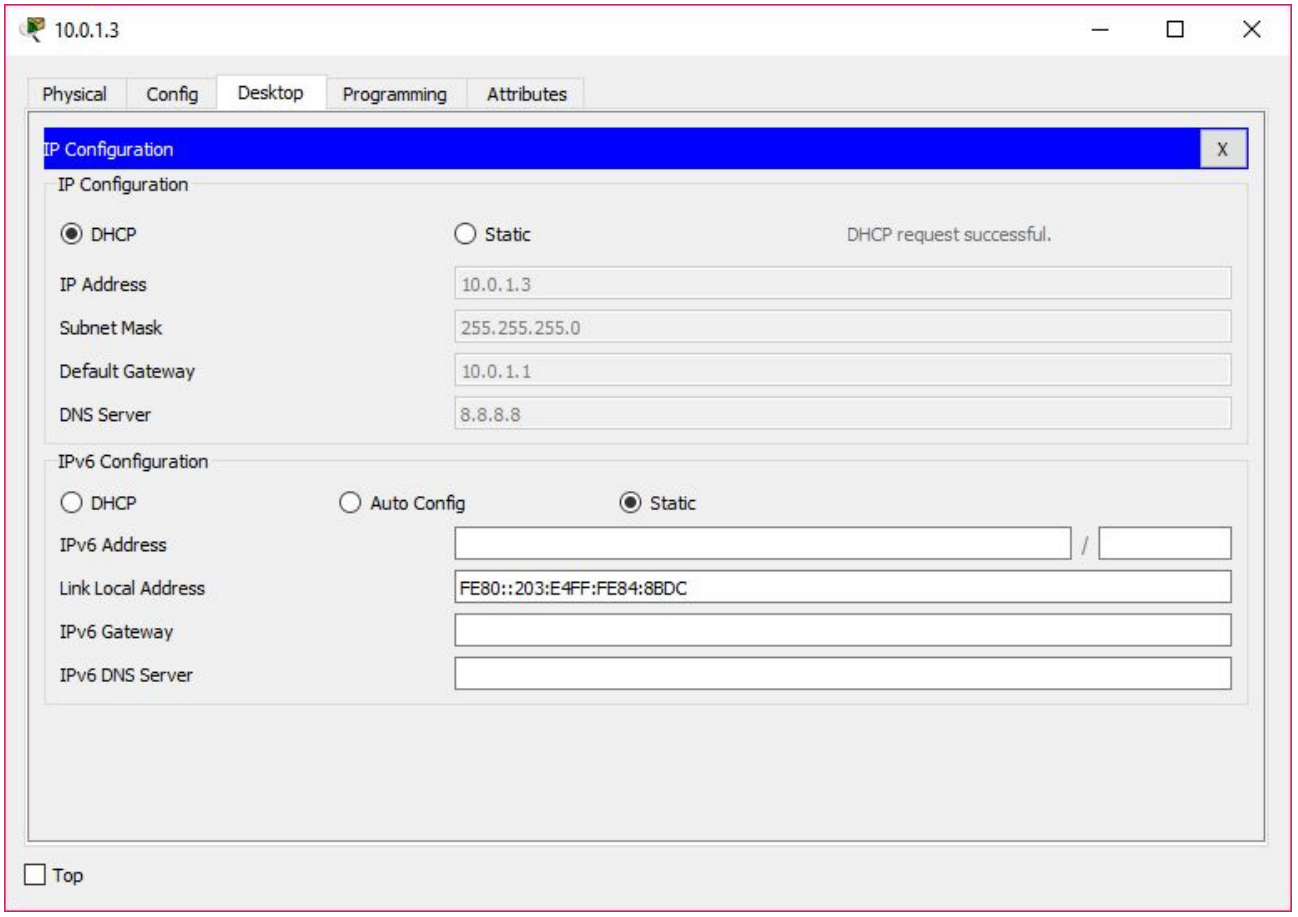
```
Router(config)#service ?
dhcp Enable DHCP server and relay agent
nagle Enable Nagle's congestion control algorithm
password-encryption Encrypt system passwords
timestamps Timestamp debug/log messages
Router(config)#ip dhcp ?
excluded-address Prevent DHCP from assigning certain addresses
pool Configure DHCP address pools
relay DHCP relay agent parameters
```

Зададим пул адресов, сначала дадим ему название, например, pool.10.0.1 а затем добавим диапазон адресов:

```
Router(config)#ip dhcp pool pool.10.0.1
Router(dhcp-config)#?
default-router Default routers
dns-server Set name server
exit Exit from DHCP pool configuration mode
network Network number and mask
```

```
no Negate a command or set its defaults
option Raw DHCP options
Router(dhcp-config)#network 10.0.1.0 255.255.255.0
Router(dhcp-config)#default-router 10.0.1.1
Router(dhcp-config)#dns-server 8.8.8.8
```

Теперь мы можем зайти в машину 10.0.1.3 и выбрать получение dhcp-адресов автоматически.



А в консоли роутера мы увидим, что были попытки назначит IP-адреса уже занятые другими машинами статически).

```
Router(dhcp-config)#%DHCPD-4-PING_CONFLICT: DHCP address conflict: server pinged 10.0.1.1.
%DHCPD-4-PING_CONFLICT: DHCP address conflict: server pinged 10.0.1.2.
```

Можно исключить адреса из диапазона (например, заранее присвоенные статически).

```
exit
Router(config)#ip dhcp ?
excluded-address Prevent DHCP from assigning certain addresses
pool Configure DHCP address pools
relay DHCP relay agent parameters
Router(config)#ip dhcp excl
Router(config)#ip dhcp excluded-address ?
A.B.C.D Low IP address
Router(config)#ip dhcp excluded-address ?
A.B.C.D Low IP address
Router(config)#ip dhcp excluded-address 10.0.1.1 ?
A.B.C.D High IP address
<cr>
Router(config)#ip dhcp excluded-address 10.0.1.1 10.0.1.2
Router(config)#
```

Теперь осталось разобраться, как работает DHCP.

Механизм получения настроек с помощью DHCP

Первый этап — обнаружение DHCP. Сообщение рассылается броадкастно, в качестве IP-адреса отправителя используется 0.0.0.0, в качестве получателя 255.255.255.255.

В качестве порта отправителя клиент использует UDP-порт 68, а в качестве порта получателя UDP-67. Сервер – наоборот.

Если у клиента ранее был назначен IP-адрес, он может указать эту информацию, но все равно так как сейчас этот адрес не присвоен, используется отправка пакета от 0.0.0.0 на 255.255.255.255. И даже если адрес сервера известен, может быть мы перешли в другую сеть.

Обнаружение DHCP

DHCPDISCOVER

UDP Src=0.0.0.0:68 Dest=255.255.255.255:67			
OP **(тип сообщения)**	**HTYPE** **(тип аппаратного адреса)**	**HLEN** **(длина аппаратного адреса)**	**HOPS** **(прыжки)**
0x01 (запрос серверу)	0x01 (MAC-адрес)	0x06 (длина MAC-адреса)	0x00 (количество промежуточных маршрутизаторов)
XID (ID транзакции)			

0x3903F326	
SECS	**FLAGS**
0x0000 (время в секундах с начала процесса получения адреса, 0 если не используется)	0x0000
CIADDR (IP-адрес клиента)	
0xC0A80164	
YIADDR	
0x00000000	
SIADDR	
0x00000000	
GIADDR	
0x00000000	
CHADDR (аппаратный, т.е. MAC-адрес)	
0x0000001d6057ed80	
SNAME	
(пустое поле)	
FILE	
(пустое поле)	
OPTIONS	
Опция DHCP 53: обнаружение DHCP	
Опция DHCP 50: запрос адреса 192.168.1.100 (указан присвоенный ранее адрес)	

Следующий этап — предложение в DHCP.

Север отвечает на порт 68 клиента, указывая в качестве IP-адреса отправителя свой IP-адрес, а в качестве получателя 255.255.255.255. Технически в RFC 2131, описывающем работу DHCP говорится, что сервер должен ответить юникастом на предложенный адрес, но на практике это не совсем верно.

Дело в том, что сетевой интерфейс, которому еще не присвоен IP-адрес, не обязан принимать сообщения, адресованные юникастом. Не все устройства могут поддерживать такую работу, потому в RFC имеется оговорка, что допускается броадкастная рассылка. На практике можно встретить ответы сервера как броадкастные, так и юникастные, но броадкастные встречаются чаще. Проверьте в wireshark, каким образом отправляет сообщения ваш сервер.

Предложение DHCP

DHCPOFFER

<table>
<tr><td colspan="4">UDP Src=192.168.1.1:67 Dest=255.255.255.255:68</td></tr>
<tr><td>OP

(тип сообщения)</td><td>HTYPE

(тип аппаратного адреса)</td><td>HLEN

(длина аппаратного адреса)</td><td>HOPS</td></tr>
<tr><td>0x02

(ответ клиенту)</td><td>0x01

(MAC-адрес)</td><td>0x06

(длина аппаратного адреса, то есть в данном случае для MAC-адреса – 6</td><td>0x00</td></tr>
<tr><td colspan="4">XID (идентификатор сессии)</td></tr>
<tr><td colspan="4">0x3903F326</td></tr>
<tr><td colspan="2">SECS</td><td colspan="2">FLAGS</td></tr>
<tr><td colspan="2">0x0000</td><td colspan="2">0x0000</td></tr>
<tr><td colspan="4">CIADDR</td></tr>
<tr><td colspan="4">0x00000000</td></tr>
<tr><td colspan="4">YIADDR (адрес, предложенный клиенту)</td></tr>
<tr><td colspan="4">0xC0A80164</td></tr>
<tr><td colspan="4">SIADDR (адрес сервера)</td></tr>
<tr><td colspan="4">0xC0A80101</td></tr>
<tr><td colspan="4">GIADDR</td></tr>
<tr><td colspan="4">0x00000000</td></tr>
<tr><td colspan="4">CHADDR (аппаратный адрес)</td></tr>
</table>

0x0000001d6057ed80
SNAME
(пустое поле)
FILE
(пустое поле)
OPTIONS
Опция DHCP 53: предложение DHCP
Опция DHCP 1: маска сети 255.255.255.0
Опция DHCP 3: шлюз по умолчанию 192.168.1.1
Опция DHCP 51: срок аренды IP-адреса — 1 день
Опция DHCP 54: DHCP-сервер 192.168.1.1

Теперь клиент может запросить у сервера предложенный адрес и другие параметры TCP/IP (а, теоретически, может и отказаться).

Запрос DHCP

DHCPREQUEST

UDP Src=0.0.0.0:68 Dest=255.255.255.255:67			
OP	**HTYPE**	**HLEN**	**HOPS**
0x01 (запрос серверу)	0x01 (MAC-адрес)	0x06 (6 октетов – для MAC)	0x00 (0 прыжков – 0 маршрутизаторов)
XID			
0x3903F326			
SECS		**FLAGS**	
0x0000		0x0000	
CIADDR			
0xC0A80164			

YIADDR
0x00000000
SIADDR
0x00000000
GIADDR
0x00000000
CHADDR
0x0000001d6057ed80
SNAME
(пустое поле)
FILE
(пустое поле)
OPTIONS
Опция DHCP 53: запрос DHCP
Опция DHCP 50: запрос адреса 192.168.1.100
Опция DHCP 54: DHCP-сервер 192.168.1.1

И четвертый этап – подтверждение настроек сервером.

Подтверждение DHCP

DHCPACK

UDP Src=192.168.1.1:67 Dest=255.255.255.255:68			
OP	**HTYPE**	**HLEN**	**HOPS**
0x02 (от сервера – клиенту)	0x01 (MAC-адрес)	0x06 (6 байт – для MAC-адреса)	0x00 (количество прыжков)
XID			

0x3903F326	
SECS	**FLAGS**
0x0000	0x0000
CIADDR	
0x00000000	
YIADDR	
0xC0A80164	
SIADDR	
0x00000000	
GIADDR	
0x00000000	
CHADDR	
0x0000001d6057ed80	
SNAME	
(пустое поле)	
FILE	
(пустое поле)	
OPTIONS	
Опция DHCP 53: подтверждение DHCP	
Опция DHCP 1: маска сети 255.255.255.0	
Опция DHCP 3: шлюз по умолчанию 192.168.1.1	
Опция DHCP 51: срок аренды IP-адреса — 1 день	
Опция DHCP 54: DHCP-сервер 192.168.1.1	

Только после этого клиент поднимает указанный адрес на сетевом интерфейсе и использует другие настройки.

Если срок аренды не истек, клиент может попытаться начать сразу с третьего шага.

DHCP позволяет не только получать IP-адрес, маску сети, адрес шлюза по умолчанию и DNS-сервер, но и другие параметры, такие как адрес NTP-сервера (для синхронизации времени по протоколу NTP – Network Time Protocol или SNTP – Simple Network Time Protocol), адрес TFTP-сервера (Trivial File Transfer Protocol) для загрузки бездисковых станций и т.д.

Домашнее задание

1. На всех маршрутизаторах настроить динамическую маршрутизацию с помощью протокола RIP2 и DHCP сервер для динамической настройки клиентов в LAN.

Дополнительные материалы

1. Таненбаум Э., Уэзеролл Д. Т18 Компьютерные сети. 5-е изд. — СПб.: Питер, 2012. — 960 с. (Глава 5)
2. https://tools.ietf.org/html/rfc2131

Используемая литература

Для подготовки данного методического пособия были использованы следующие ресурсы:

1. https://ru.wikipedia.org/wiki/RIP_(сетевой_протокол)
2. https://ru.wikipedia.org/wiki/DHCP