ФГБОУ ВО «Воронежский государственный технический университет»

Кафедра систем автоматизированного проектирования и информационных систем

ПРОТОКОЛЫ АДРЕСАЦИИ И МАРШРУТИЗАЦИИ В СЕТЯХ ПЕРЕДАЧИ ДАННЫХ

МЕТОДИЧЕСКИЕ УКАЗАНИЯ
к лабораторным работам по дисциплине "Протоколы передачи данных" для студентов направления 09.03.02 «Информационные системы и технологии» очной формы обучения

Воронеж 2019

1. ПРОТОКОЛ STP

1.1. Краткие теоретические сведения

Проблемы петлевой конфигурации. Петли, а значит, и параллельные пути в локальных Ethernet-сетях (LANs), являются причиной бесконечного движения по кругу:

– кадров с неизвестным мосту MAC-адресом назначения;

– широковещательных кадров;

– Unicast-кадров в фазе наводнения (Flooding).

Параллельные пути в более сложной топологии приводят к широковещательному шторму, переполнению всех буферных ресурсов и стагнации LANs.

Причины возникновения физических петель:

– намеренная попытка повысить надежность сети за счет избыточных соединений;

– ошибка администратора сети.

L2-петли доставляют намного больше проблем, чем L3-петли маршрутизации, так как IP-пакет уничтожается роутером при достижении времени жизни пакета TTL = 0, а Ethernet-кадр циркулирует в сети до тех пор, пока принудительно не будет отключено питание моста или не возникнут неисправности канала.

Назначение STP. Протокол связующего дерева STP (Spanning Tree Protocol, IEEE 802.3D) позволяет мостам общаться между собой протокольными блоками данных BPDU (Bridge Protocol Data Units) с групповым MAC-адресом назначения для приведения LANs с множественными связями к древовидной топологии, исключающей циклы движения кадров. Происходит это путем автоматического логического блокирования избыточных в данный момент портов на каждом мосте.

ФГБОУ ВПО «Воронежский государственный технический университет»

Кафедра систем автоматизированного проектирования и информационных систем

КРИПТОГРАФИЧЕСКИЕ МЕТОДЫ ЗАЩИТЫ ИНФОРМАЦИИ

МЕТОДИЧЕСКИЕ УКАЗАНИЯ
к лабораторным работам по дисциплинам "Информационная безопасность и защита информации", "Технологии защиты web-контента" для студентов направления 09.03.02 «Информационные системы и технологии» очной формы обучения

Воронеж 2019

Основное преимущество STP – можно построить LANs, в которой существует несколько параллельных путей, однако при этом гарантировать, что:

– резервные пути прохождения трафика при нормальном функционировании основного пути заблокированы;

– один из резервных путей автоматически активизируется при нарушении основного пути.

Главный недостаток STP – избыточные линии или избыточные сетевые компоненты не могут использоваться для балансирования загрузки.

Сервис STP согласно IEEE 802.3D:

– Конфигурирует произвольную топологию Bridge LAN в единственное распределенное связующее дерево. При наличии более одного пути для кадров между любыми двумя оконечными станциями все избыточные пути отключаются, таким образом устраняются циклы кадров.

– Предусматривает автоматическую отказоустойчивость посредством реконфигурации топологии распределенного связующего дерева в результате неисправности моста или неисправности в канале связи в пределах границ LAN без формирования циклов текущих данных.

– Распределенное связующее дерево образуется в LAN любой размерности с высокой вероятностью и за известный ограниченный интервал времени сходимости (конвергенции) протокола STP. В течение этого времени могут быть недоступны связи между любой парой оконечных станций.

– Активная топология предсказуема и воспроизводима. Активная топология может быть выбрана посредством управления параметрами алгоритма STP.

– Используемая STP-протоколом полоса пропускания каналов при установлении и поддержании распределенного связующего дерева использует малый процент от полной располагаемой полосы пропускания.

1.1.1. Ключевые параметры (сущности) STP

В вычислениях связующего дерева используются следующие основные параметры (сущности) в соответствии с рис. 1.1 (из IEEE):

– Bridge ID (BID) – идентификатор моста;

– Port ID (PID) – идентификатор порта;

– Path Cost – стоимость порта.

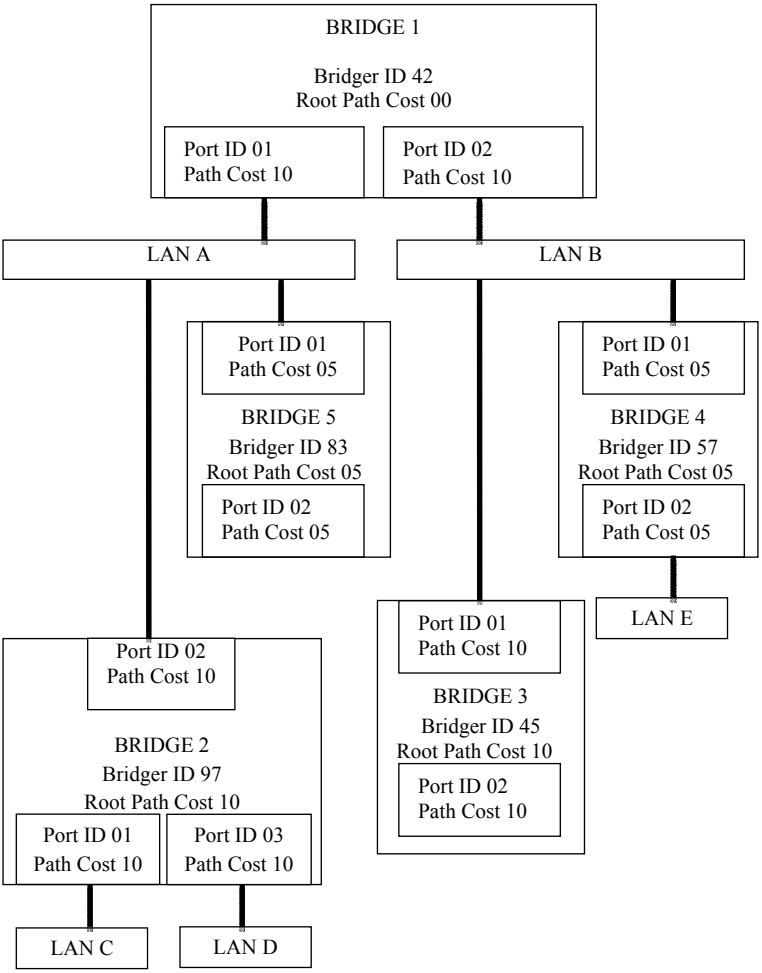


Рис. 1.1. Основные параметры STP

Идентификатор моста (BID – Bridge ID)

BID состоит из комбинации MAC-адреса моста и приоритета моста (рис. 1.2).

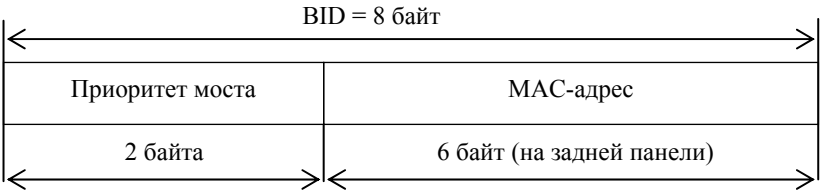


Рис. 1.2. BID

MAC-адрес моста:

– мост имеет один или несколько (по количеству портов) MAC-адресов;

– MAC-адрес моста назначается администратором или указывается на задней панели изготовителем устройства;

– если MAC-адрес не указан на задней панели, то используется самый маленький MAC-адрес из всех имеющихся.

Приоритет моста:

– конфигурируется администратором в диапазоне $0–2^{16}(65\,535)$, по умолчанию равен 32 768;

– в протоколе PVST данное поле разбито на два: приоритет моста (4 бита) и номер VLAN (12 бит);

– чем меньше BID моста, тем выше его приоритет;

– если сохранены значения приоритета моста по умолчанию, то мост с самым маленьким MAC-адресом будет корневым мостом.

Идентификатор порта (PID – Port ID)

Port ID уникален для каждого порта моста, состоит из двух полей (рис. 1.3).

Приоритет порта:

– 1 байт в 802.3D (диапазон 0–255, по умолчанию – 128);

– 6 бит в Cisco Catalist (диапазон 0–64, для коммутаторов с большой плотностью портов);

– Конфигурируется администратором.

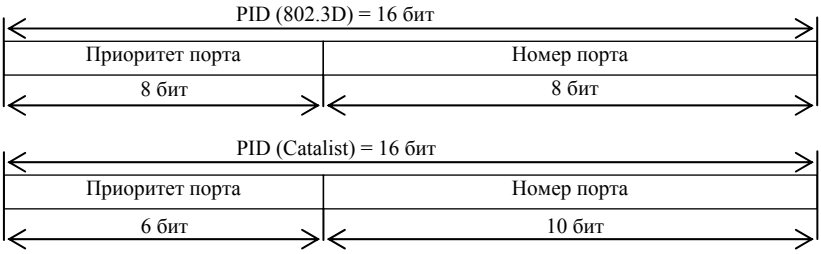


Рис. 1.3. PID

Номер порта:

– значение 1 присваивается порту 0/1, значение 2 – порту 0/2 и т.д.;

– 1 байт в 802.3D (диапазон 0–255);

– 10 бит в Cisco Catalist (диапазон 0–1023, для коммутаторов с большой плотностью портов);

– чем меньше PID порта, тем выше его приоритет относительно других портов моста.

Стоимость пути (Path Cost)

Это целое число, определяющее стоимость соединения между двумя смежными мостами. Значение стоимости пути:

Раньше: Path Cost = 1000/скорость порта.

Примеры: Path Cost (l0BaseT) = 100 (1000/10);

Path Cost (l00Base и FDD) = 10 (1000/100).

Сейчас, в связи с появлением Ethernet 1 Гбит/с и 10 Гбит/с, IEEE стандартизировала для STP нелинейную шкалу стоимостей, приведенную ниже. Значение стоимости пути может быть сконфигурировано администратором вручную для каждого порта моста.

Значение стоимости пути (Path Cost) в IEEE версии:	
Пропускная способность	Стоимость пути
4 Мбит/с	250
10 Мбит/с	100
16 Мбит/с	62
45 Мбит/с	39
100 Мбит/с	10
155 Мбит/с	14
622 Мбит/с	6
1 Гбит/с	4
10 Гбит/с	2

1.1.2. Состояние портов моста и таймеры STP

Каждый порт моста в ходе работы проходит STP первые четыре состояния (пять – если порт выключен вручную администратором):

1. Blocking (Заблокирован). При инициализации коммутатора все порты (за исключением отключенных) автоматически переводятся в состояние «Заблокирован». В этом случае порт принимает и обрабатывает только кадры BPDU. Все остальные кадры отбрасываются.

2. Listening (Прослушивание). В этом состоянии порт продолжает принимать, обрабатывать и ретранслировать только кадры BPDU. Из этого состояния порт может перейти в состояние «Заблокирован», если получит BPDU с лучшими параметрами, чем его собственные (BID, PID, Path Cost). В противном случае, при истечении таймера Forward-delay, порт перейдет в следующее состояние «Обучение».

3. Learning (Обучение). Порт начинает принимать все кадры и на основе адресов источника строить таблицу коммутации. Порт в этом состоянии все еще не продвигает кадры. Порт продолжает участвовать в работе алгоритма STA и при поступлении BPDU с лучшими параметрами переходит в состояние «Заблокирован». В противном случае, при истечении таймера Forward-delay, порт перейдет в следующее состояние «Продвижение».

4. Forwarding (Продвижение). В этом состоянии порт может обрабатывать кадры данных в соответствии с построенной таблицей коммутации. Также продолжают приниматься, передаваться и обрабатываться кадры BPDU.

5. Disable (Отключен). В это состояние порт переводит администратор. Отключенный порт не участвует ни в работе протокола STP, ни в продвижении кадров данных. Порт можно также вручную включить, и он сначала перейдет в состояние Blocking.

Таймеры STP представлены ниже.

Таймеры STP:

Hello timer	Интервал между передачей BPDU корневым коммутатором может изменяться от 1 до 10 с
Forward-delay timer	Время, в течение которого каждый порт коммутатора остается в состоянии прослушивания перед переходом либо в состояние продвижения кадров, либо в состояние блокирования. Изменяется от 6 до 40 с
Maximum-age	Время по истечении которого, если не были получены BPDU-кадры от корневого коммутатора, коммутатор начнет сам посылать кадры BPDU, объявляя себя в качестве корневого коммутатора
Message Age	Возраст конфигурационного сообщения BPDU (1–10 с). Служит для выявления устаревших сообщений

1.1.3. Три этапа начальной сходимости STP

Этап 1. Выбор корневого моста (Root Bridge):

– корневым выбирается мост с наименьшим Bridge ID (BID);

– процесс выбора моста с наименьшим BID называется «корневой борьбой»;

– все порты корневого моста становятся назначенными (Designated Port);

– исключением из этого правила являются физические петли к корневому мосту (например, когда два порта корневого моста подключены к концентратору или два порта соединены кабелем).

Этап 2. Выбор корневых портов (Root Port):

– каждый некорневой коммутатор просчитывает кратчайший путь к корневому мосту (Root Path Cost) для каждого своего подключенного к сети порта;

– ближайшие к корневому мосту порты (с наименьшим Root Path Cost) называются корневыми портами (Root Port);

– каждый некорневой мост должен иметь только один корневой порт (Root Port);

– совокупная стоимость всех каналов к корневому мосту называется корневой стоимостью (Root Path Cost);

– корневой мост отправляет сообщения BPDU, указывая корневую стоимость 0. Стоимость пути увеличивается при получении мостом BPDU, а не при отправке.

Этап 3. Выбор назначенных портов (Designated Port):

– идея назначенных портов – только один порт обрабатывает трафик для определенного сегмента сети;

– каждый сегмент в сети должен иметь хотя бы один назначенный порт;

– функцию назначенного порта выполняет обычный порт моста, который осуществляет обмен трафиком между сегментом сети и корневым мостом;

– мост, имеющий хотя бы один назначенный порт, называется назначенным мостом для данного сегмента сети;

– критерий выбора назначенного порта – минимальная стоимость маршрута к корневому мосту (Root Path Cost).

После завершения третьего этапа на всех мостах блокируются все порты (Blocking Port), не являющиеся корневыми и назначенными. В результате получается древовидная структура (математический граф) с вершиной в виде корневого коммутатора. Далее для отслеживания изменений в топологии корневой мост рассылает через Hello Time интервалы BPDU-сообщения, а все некорневые мосты их ретранслируют. В случае обнаружения изменений в топологии происходит перестройка древовидной структуры.

1.1.4. Формат BPDU-кадра

MAC/SAP-адрес отправителя

В Ethernet 802.3 адрес отправителя (SA – Source Address) – это MAC-адрес порта коммутатора, который отправил BPDU:

– каждый порт коммутатора Catalyst имеет свой уникальный (Unicast) MAC-адрес;

– MAC-адрес порта используется для формирования поля SA в заголовке кадра, в котором отправляется сообщение BPDU;

– SSAP (Source Service Access Point) – сервисная точки доступа отправителя. DSAP = SSAP = 0×42 (зарезервированы для STP).

Разница между MAC-адресом любого порта коммутатора и MAC-адресом используемого для идентификатора моста (BID):

– MAC-адрес моста, используемый при формировании поля BID, берется из настроек операционной системы коммутатора, либо используется значение по умолчанию (адрес, который написан на задней панели коммутатора);

– если на задней панели нет этого адреса, выбирается минимальный адрес порта коммутатора.

Пример:

Коммутаторы Cisco Catalyst всегда имеют на один MAC-адрес больше, чем количество портов: отдельный MAC-адрес на каждый порт, а также еще один дополнительный адрес – MAC-адрес всего устройства (для BID).

MAC/SAP-адрес получателя

MAC-адрес получателя (DA):

– используется групповой (Multicast) MAC-адрес = 01-80-C2-00-00-00;

– сервисная точка доступа получателя DSAP (Destination Service Access Point). DSAP = SSAP = 0×42 (зарезервированы для STP).

Два типа сообщений BPDU

Существует два типа сообщений BPDU:

1) конфигурационные BPDU. Создаются корневым мостом и далее распространяются по ветвям дерева;

2) сообщения об изменении топологии (TCN – Topology Change Notification). Распространяются в обратном направлении, чтобы сообщить корневому мосту об изменении в топологии. TCN в рамках этого пособия не рассматриваются.

Формат конфигурационного сообщения BPDU

Все мосты (коммутаторы) сети, в которой работает STP, обмениваются информацией посредством кадров BPDU (Bridge Protocol Data Units), поля которых представлены на рис. 1.4.

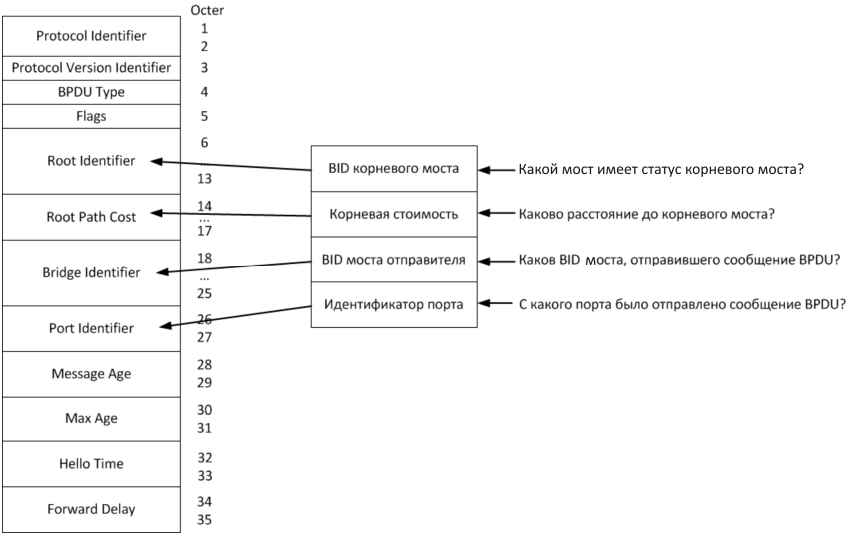


Рис. 1.4. Формат BPDU-сообщений

Назначение полей:

Protocol Identifier – идентификатор протокола

0 для STP 802.1D.

Protocol Version – версия

00 (hex) для версии 802.1D (1998).

BPDU Type – тип сообщения:

00 (hex) для конфигурационных BPDU;

80 (hex) для сообщения об изменении топологии TCN.

Flags – признаки:

бит 8 – подтверждение изменения топологии;

бит 1 – изменение топологии (TC);

используются в TCN BPDU для сигнализации об изменении топологии.

Root Identifier – идентификатор корневого моста:

при начальном запуске каждый мост LANs считает себя корневым и ставит свой BID в это поле;

в процессе обмена BPDU-сообщениями каждый мост записывает в это поле наименьшее значение из полученных от других мостов и своего BID.

Root Path Cost – стоимость маршрута к корневому мосту.

Стоимость пути в этом поле BPDU увеличивается при получении портом моста этого BPDU на величину Path Cost этого порта, а не при отправке через другие порты.

Bridge Identifier – идентификатор моста (отправителя).

Port Identifier – идентификатор порта.

Message Age – возраст конфигурационного сообщения BPDU (1–10 с). Служит для выявления устаревших сообщений.

Корневой мост при передаче конфигурационного BPDU устанавливает переменную в 0.

Каждая передача через другие мосты увеличивает это число на 1.

Max Age – максимальный срок хранения конфигурационных BPDU (6–40 с).

Ограничение жизни полученных конфигурационных BPDU.

Основной параметр для обнаружения IDLE-отказов (например, корневой мост «мертв»).

Поле оказывает влияние на таймер времени хранения таблицы моста в процессе уведомления об изменении топологии.

По умолчанию 20 с.

Hello Time – интервал времени между периодической отправкой корневым мостом конфигурационных сообщений BPDU.

Корневой мост отправляет конфигурационные сообщения каждые Hello Time секунд.

Мосты, получившие такое сообщение, отправляют его дальше в сеть.

По умолчанию 2 с.

Forward Delay (4–30 с) – временная задержка для перевода порта в состояние передача (Forward).

По умолчанию 15 с. Это означает 15 с состояний прослушивания плюс 15 с изучения топологии.

Рекомендации:

Hello Time, Max Age, Forward Delay специфицируются (конфигурируются) в корневом мосте.

1.1.5. Алгоритм обработки конфигурационных BPDU-сообщений

Все сообщения BPDU, полученные и отправленные через порт, сравниваются между собой. Мост сохраняет и передает через порт только наиболее приемлемое сообщение. Приемлемым считается сообщение с наименьшими параметрами.

Определение наилучшего конфигурационного сообщения BPDU. Каждый порт моста сохраняет копию наилучшего из полученных конфигурационных сообщений BPDU по следующему алгоритму принятия решения, в порядке убывания приоритета:

1) наименьшего идентификатора корневого моста (Root BID);

2) наименьшей корневой стоимости маршрута (Root Path Cost);

3) наименьшего идентификатора моста-отправителя (Bridge ID);

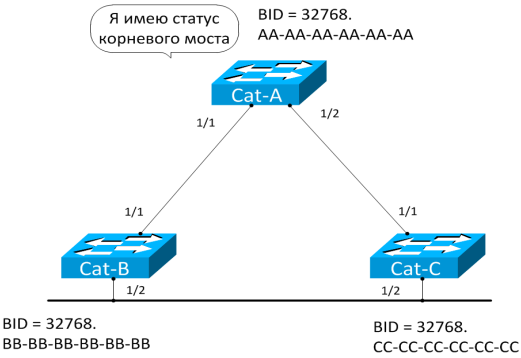
4) Наименьшего идентификатора порта отправителя (Port ID).

Если собственное конфигурационное сообщение BPDU порта является лучше принятого, отправление собственных сообщений в сеть через этот порт продолжается.

Если принятое конфигурационное сообщение BPDU порта является лучше собственного, порт останавливает отправку собственных сообщений BPDU и рассылает полученное сообщение.

1.1.6. Пример работы STP

Этап 1. Выбор корневого моста. Представлен на рис. 1.5.



… Фрагмент BPDU-сообщения	
Root ID – BID корневого моста	→ Какой мост имеет статус корневого моста?
Root path cost – корневая стоимость	→ Каково расстояние до корневого моста?
Sender ID – BID моста отправителя	→ Каков BID моста отправителя BPDU?
Port Identifier – идентификатор порта	→ С какого порта было отправлено BPDU?

Рис. 1.5. Выбор корневого моста

Процесс корневой борьбы:

– BPDU-сообщения стандартно отправляются каждые 2 с;

– сначала мосты в поля Root ID и Sender ID подставляют собственные значения BID;

– каждый мост в поле Root ID сохраняет лучшее из BPDU, полученных на каждый порт. Каждый приходящий BPDU сравнивается с ранее сохраненным. Если полученный BPDU более приемлем, то новое сообщение заменяет ранее записанное;

– мосты определяют, что наименьший BID у моста Cat-A, поэтому Cat-A становится корневым.

Этап. 2. Выбор корневых портов. Представлен на рис. 1.6.

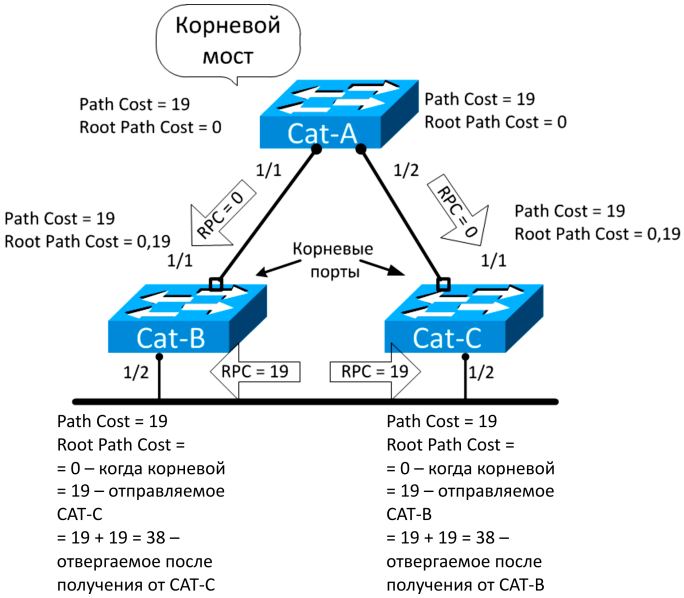


Рис. 1.6. Выбор корневых портов

Процесс выбора корневых портов:

– Cat-A (корневой мост) отправляет сообщения BPDU с корневой стоимостью, равной 0, через все порты;

– RPC Cat-A = 0.

– получив такое BPDU, мост Cat-B добавляет к значению корневой стоимости значение стоимости порта 1/1, равное для FE числу 19:

RPC Cat-B = RPC Cat-A + Path COST Cat-B = 0 + 19 = 19;

Cat-B отправляет BPDU с RPC Cat-B = 19 через другие порты.

– BPDU от моста Cat-B получает мост Cat-C на порту 1/2 и рассчитывает:

RPC Cat-C (1/2) = RPC Cat-B + Path COST Cat-C (1/2) = 19 + + 19 = 38;

– с другой стороны на порт 1/1 Cat-C от корневого моста приходят сообщения со значением стоимости, равным 0, и затем мост Cat-C увеличивает ее на 19:

RPC Cat-C (1/1) = RPC Cat-A + Path COST Cat-C (1/1) = 0 + + 19 =19;

– мост Cat-C выберет порт 1/1 в качестве корневого со значением RPC = 19;

– мост Cat-C отправляет BPDU с RPC Cat-C = 19 через другие порты.

Мост Cat-B выполняет аналогичные вычисления: стоимость пути от корневого моста до порта 1/1 устройства Cat-B равняется 19, в то время как стоимость пути от порта 1/2 моста Cat-B равняется 38, поэтому порт 1/1 становится корневым для коммутатора Cat-B.

Этап 3. Выбор назначенных портов. Представлен на рис. 1.7.

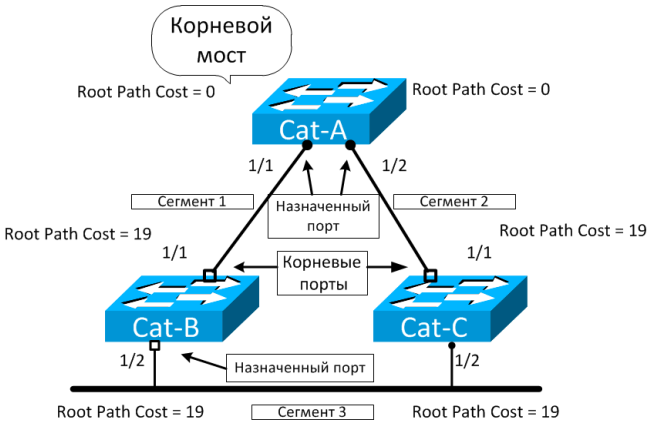


Рис. 1.7. Выбор назначенных портов

Процесс выбора назначенных портов

– Сегмент 1 имеет подключения по двум портам:

1) порт 1/1 Cat-A и порт 1/1 Cat-B;

2) порт 1/1 Cat-A имеет меньшую корневую стоимость, поэтому становится назначенным.

– Сегмент 2 имеет подключения также по двум портам:

1) порт 1/2 Cat-A и порт 1/1 Cat-C;

2) порт 1/2 Cat-A имеет меньшую корневую стоимость и он становится назначенным;

– Сегмент 3 подключен к двум коммутаторам, имеющим одинаковое значение корневой стоимости, равное 19. В такой ситуации срабатывает «Алгоритм принятия решения» протокола STP:

по наименьшему идентификатору корневого моста (Root BID);

по наименьшей стоимости маршрута к корневому мосту (RPC);

по наименьшему идентификатору моста-отправителя (BID);

по наименьшему идентификатору порта (Port ID).

Выбор назначенного порта в сегменте 3:

– Cat-B и Cat-C не корневые, поэтому переходим к 2.

– Cat-B и Cat-C имеют одинаковые значения стоимости, равные 19, поэтому переходим к 3.

Идентификатор коммутатора Cat-B (32768.BB-BB-BB-BB-BB-BB) меньше, чем идентификатор коммутатора Cat-C (32768.CC-CC-CC-CC-CC-CC), поэтому:

– порт 1/2 коммутатора Cat-B становится назначенным для сегмента 3;

– порт 1/2 коммутатора Cat-C получает статус блокированного (неназначенного) порта.

1.1.7. Развитие протокола STP

Технология PortFast и безопасность STP

На коммутаторах Cisco нижеописанные технологии по умолчанию отключены. Их необходимо вручную включать на коммутаторе администратору сети.

PortFast. Предназначен для портов доступа и транковых портов, не участвующих в формировании дерева STP. PortFast мгновенно переводит порт в состояние продвижения из блокированного состояния, минуя состояния прослушивания и обучения. PortFast применяется только для подключения компьютеров пользователей и серверов, а не коммутаторов, иначе может возникнуть петля. PortFast включается на уровне порта.

По умолчанию коммутатор рассылает и принимает кадры BPDU на всех портах. Поскольку STP не имеет механизмов аутентификации, то злоумышленник может подключиться к порту коммутатора и с помощью специального программного обеспечения подделать сообщения BPDU, что может привести к перестройке дерева STP, смене корневого моста и нарушению работоспособности сети. Для защиты STP от неверной конфигурации и атак на портах, рассчитанных на подключение компьютеров и серверов, были введены технологии BPDU Filter, BPDU Guard, Root Guard.

BPDU Filter. Запрещает (фильтрует) посылку и прием кадров BPDU на порту коммутатора. Может включаться как на уровне коммутатора, так и на уровне интерфейса, но существуют различия:

– на уровне коммутатора можно задействовать BPDU Filtering для предотвращения посылки/получения в/из портов PortFast кадров BPDU. При этом в случае получения BPDU-кадра портом PortFast порт потеряет свой PortFast статус и BPDU Filter выключается;

– на уровне интерфейса можно задействовать BPDU Filter на любом порту с PortFast и без него.

BPDU Guard. Запрещает порту получать кадры BPDU, т.е. при получении кадра BPDU портом переводит порт в состояние

Err-disable и отключает его. Может включаться как на уровне коммутатора, так и на уровне интерфейса, но существуют различия.

На уровне коммутатора (Global Level) можно задействовать BPDU Guard на PortFast портах. В нормальном режиме работы порты PortFast не будут получать BPDU. Получение кадров BPDU на портах PortFast говорит о неверной конфигурации сети или атаке злоумышленника.

На уровне интерфейса можно задействовать BPDU Guard на любом порту:

– *Root Guard.* Запрещает порту получать кадры BPDU с корневым мостом, отличным от текущего, т.е. при получении портом кадра BPDU с корневым мостом, отличным от текущего, переводит порт в состояние Root-Inconsistent (эквивалентно состоянию Listening). После того как порт перестает получать BPDU с корневым мостом отличным от текущего, он переходит в нормальное состояние. Данная функция включается на интерфейсе.

– *Loop Guard.* Обеспечивает дополнительную защиту на втором уровне от возникновения петель при сбое оборудования. STP-петля возникает, когда блокированный порт в избыточной топологии ошибочно переводится в состояние передачи. Это может возникнуть, например, когда блокированный STP-порт перестает получать кадры BPDU. Поскольку работа протокола STP полагается на постоянное присутствие BPDU-кадров в сети, то назначенный порт должен постоянно передавать BPDU-кадры, а заблокированный порт должен их получать. Как только на порт перестают поступать BPDU, STP понимает это как изменение топологии и исчезновение петли, после чего переводит порт в состояние Forwarding. В случае использования Loop Guard порт после прекращения получения кадров BPDU переводится в состояние Loop-Inconsistent и остается блокированным.

Протоколы PVST, PVST+

Эти протоколы разработаны и принадлежат компании Cisco. PVST, PVST+ строит для каждого VLAN свое дерево STP, в связи

с этим поле «Приоритет моста» на рис. 1.2 разбивается на два поля: «Приоритет моста» и «Номер VLAN». По умолчанию PVST+ включен на всех коммутаторах Cisco. В данной лабораторной работе применяется именно он. В нем не используется состояние порта Blocking, а используется состояние Alternate Blocking, что означает что этот порт включится, как только основной порт в состоянии Root Port перестанет работать. Отличие PVST от PVST+ в том, что последний, помимо ISL, поддерживает и транки 802.1Q.

Протоколы RSTP, Rapid-PVST+

Время сходимости STP от 30 до 50 с, что для современных сетей неприемлемо. Для решения это проблемы IEEE разработал протокол RSTP (802.1w). Стандарт 802.1w позже был включен в 802.1D – 2004. Данный протокол обеспечивает более быструю сходимость сети по сравнению с STP. Протокол Rapid-PVST+ строит дерево RSTP для каждого VLAN. Существенным отличием STP и RSTP является способ перехода портов в состояние пересылки (Forwarding) и то, каким образом этот переход влияет на роль порта в топологии. RSTP объединяет три состояния 802.10: Disabled, Blocking, Listening – в одно Discarding, в котором порт неактивен. Состояния портов в RSTP и STP представлены в табличной форме.

Сравнение состояний портов в STP и RSTP:

STP(801.1D)	RSTP(802.1w)	Порт передает user-кадры?	Порт самообучается по MAC-адресам?
Disabled	Discarding	Нет	Нет
Blocking	Discarding	Нет	Нет
Listening	Discarding	Нет	Нет
Learning	Learning	Нет	Да
Forwarding	Forwarding	Да	Да

Роли портов. Выбор активной топологии завершается присвоением протоколом RSTP определенной роли каждому порту. Роли «корневой порт» и «назначенный порт» включают порт в активную топологию. В RSTP появились две новые роли: «альтерна-

тивный порт» (Alternate) и «резервный порт» (Backup), соответствующие состоянию «Заблокирован» в STP и исключающие порт из активной топологии:

– Alternate (альтернативный) порт является резервным корневым портом;

– Backup (резервный) порт является резервным назначенным портом. Резервные порты существуют только в конфигурациях, где есть два или более соединения данного моста с данной сетью (сегментом сети).

Новые роли показаны на рис. 1.8.

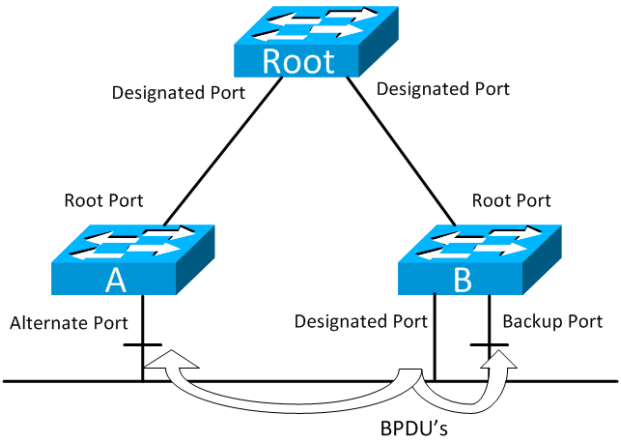


Рис. 1.8. Роли портов RSTP

В RSTP также изменены некоторые поля BPDU-сообщений:

– в поле Version и Type записывается значение 2;

– в поле Flags добавлено пять новых флагов (рис. 1.9).

RSTP внес изменения в обработку сообщений BPDU:

– BPDU после построения древовидной структуры отправляются через интервал Hello Time (2 с) всеми мостами, в отличие от STP, где мосты ретранслируют BPDU, полученные от корневого моста;

– если порт не получает BPDU в течение трех интервалов Hello Time, то порт считает, что связь с соседом потеряна, в отличие от STP, в котором связь считается утерянной, если мост не получил BPDU в течение интервала Max Age;

– если мост получает информацию через свой порт в роли «назначенный» или «корневой», то он принимает и сохраняет ее.

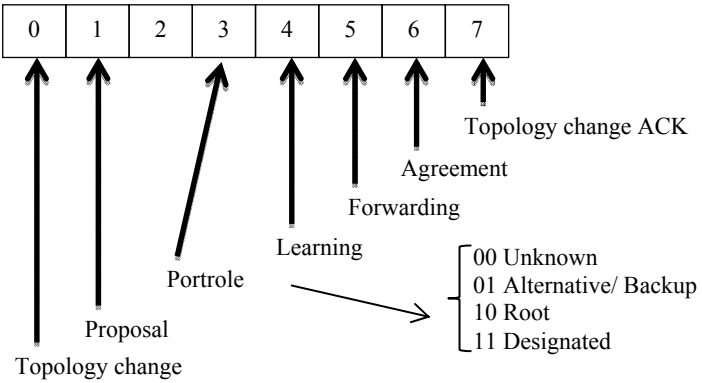


Рис. 1.9. Новые флаги RSTP

Процесс вычисления связующего дерева протоколов STP и RSTP одинаков. Однако при работе RSTP порт может перейти в состояние Forwarding значительно быстрее – он больше не зависит от конфигурации таймеров. Порты больше не должны ждать стабилизации топологии, чтобы перейти в режим Forwarding продвижения. Для того чтобы обеспечить быстрый переход в это состояние, протокол RSTP вводит две новые переменные: «пограничный порт» (Edge Port) и порт типа «точка-точка» (point-to-point, P2P).

Пограничным (Edge) портом объявляется порт, непосредственно подключенный к сегменту, в котором не могут быть созданы петли. Например, порт непосредственно подключен к рабочей станции. Порт, который определен как пограничный, мгновенно переходит в состояние Forwarding, минуя состояния Listening

и Learning. Пограничный порт теряет свой статус и становится обычным портом связующего дерева в том случае, если получит кадр BPDU.

P2P-порт, обычно используемый для подключения к другим мостам, также способен быстро перейти в состояние Forwarding. При работе RSTP все порты, функционирующие в полнодуплексном режиме, рассматриваются как порты P2P, до тех пор, пока не будут переконфигурированы вручную.

1.1.8. Настройка STP на коммутаторах Cisco

Начальное состояние командной строки – привилегированный режим EXEC Cisco IOS. Курсивом показаны переменные. В квадратных скобках опциональные атрибуты. В фигурных и без скобок – обязательные атрибуты; если их несколько и они отделены чертой, то при вводе команды выбирается только один из них. Чтобы отменить команду, ее вводят повторно, но с *no* в начале. В данном пособии не у всех команд указаны все атрибуты, для просмотра атрибутов пользуйтесь помощью IOS либо руководствами Command Reference Guide на нужное устройство Cisco.

Настройка протокола STP:

– вход в глобальный режим конфигурации

```
configure terminal
```

– выбор протокола STP

```
spaning-tree mode {mst | pvst | rapid-pvst}
```

Настройка приоритета BID коммутатора, таймеров:

– вход в глобальный режим конфигурации

```
configure terminal
```

– настройка приоритета BID, таймеров (у каждого VLAN свое дерево STP)

```
spanning-tree vlan vlan-id [forward-time seconds | hello-time seconds| max-age seconds |priority priority | root {primary | secondary} [diameter net-diameter [hello-time seconds]]]
```

Настройка Port Cost на интерфейсе:

– вход в глобальный режим конфигурации

```
configure terminal
```
– вход в режим конфигурации нужного интерфейса
```
interface interface-id
```
– настройка стоимости порта
```
spanning-tree [vlan vlan-id] cost cost
```
Настройка Port Priority на интерфейсе:

– вход в глобальный режим конфигурации
```
configure terminal
```
– вход в режим конфигурации нужного интерфейса
```
interface interface-id
```
– настройка приоритета порта
```
spanning-tree [vlan vlan-id] port-priority priority
```
Настройка PortFast на интерфейсе:

– вход в глобальный режим конфигурации
```
configure terminal
```
– вход в режим конфигурации нужного интерфейса
```
interface interface-id
```
– включение PortFast
```
spanning-tree portfast {disable | trunk}
```
Здесь Disable – отключить на данном интерфейсе;

Trunk – включить на транковом интерфейсе (если порт не транковый, его нужно перевести в состояние Access, командой Switchport Mode Access).

Настройка BPDU Filter на интерфейсе PortFast:

– вход в глобальный режим конфигурации
```
configure terminal
```
– вход в режим конфигурации нужного интерфейса
```
interface interface-id
```
– включение BPDU Filter
```
spanning-tree bpdufilter {disable | enable}
```
Настройка BPDU Guard на интерфейсе PortFast:

– вход в глобальный режим конфигурации
```
configure terminal
```
– вход в режим конфигурации нужного интерфейса
```
interface interface-id
```

– включение BPDU Filter

```
spanning-tree bpduguard {disable | enable}
```

Просмотр параметров работы и типа используемого протокола STP:

```
show spanning-tree [summary | detail | vlan vlan-id]
```

1.2. Лабораторная работа «Протокол STP»

1.2.1. STP-дерево «по умолчанию»

Соберите показанную на рис. 1.10 топологию, соединив разъемы на патч-панели патчкордами типа Straight-Touch согласно рис. 1.11.

Отметим, что по умолчанию:

– BID Priority всех коммутаторов установлено в значение 32 768;

– все порты находятся в VLAN 1;

– на коммутаторах запущен PVST, т.е. Bridge Priority = Bridge Priority + VLAN, в нашем случае 32 768 + 1 = 32 769.

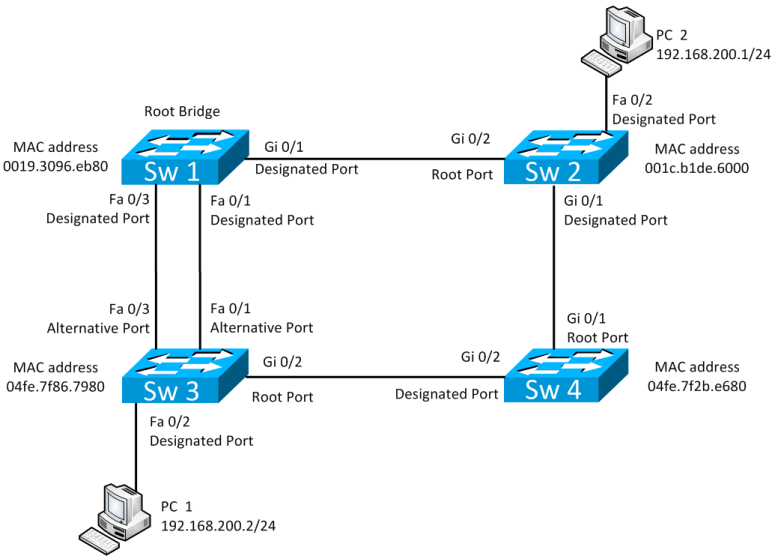


Рис. 1.10. Начальная топология

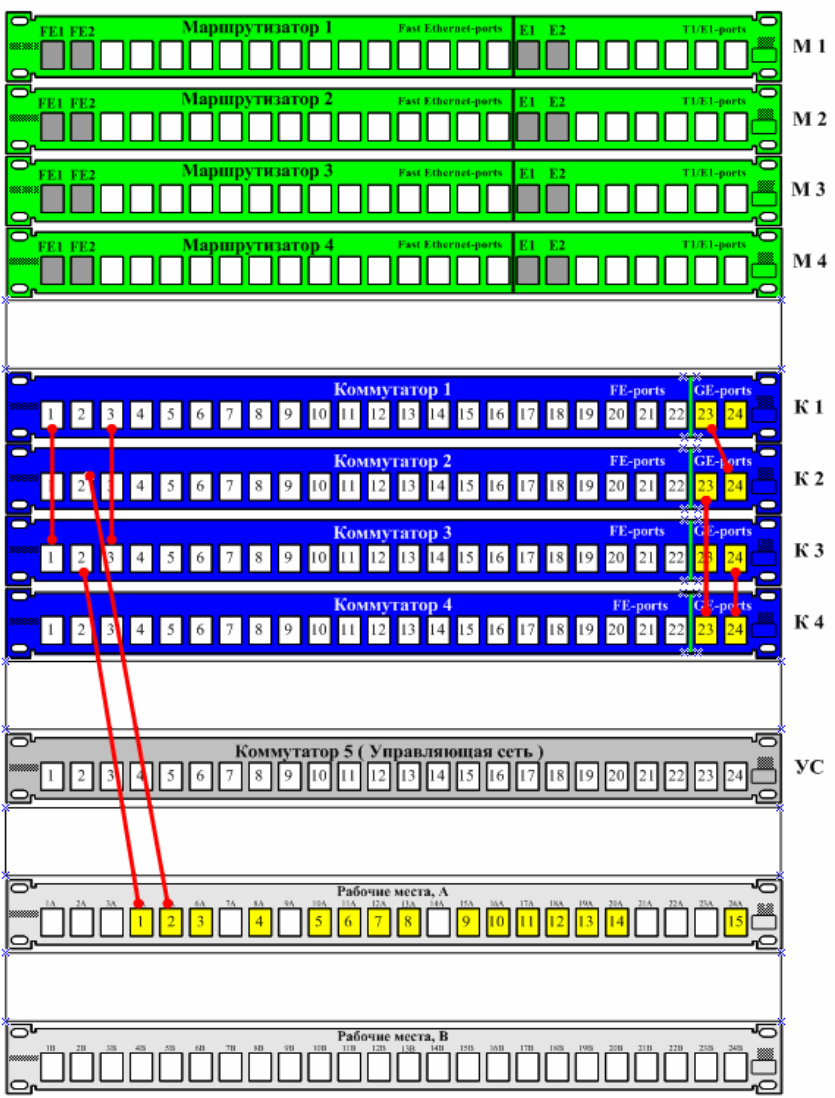


Рис. 1.11. Соединения на коммутационном поле

Проведите начальную конфигурацию коммутаторов. Для доступа к коммутаторам используйте терминальный сервер:

– для доступа к sw1.lab запустите telnet 192.168.0.110 2003;
– для доступа к sw2.lab запустите telnet 192.168.0.110 2004;
– для доступа к sw3.lab запустите telnet 192.168.0.110 2005;
– для доступа к sw4.lab запустите telnet 192.168.0.110 2006.
* Имя student, пароль student.

Если коммутаторы не настраивались ранее, выполните начальную конфигурацию коммутаторов (Имя устройства, шифрование паролей, логин (student) и пароль доступа (student) на терминальные и консольные линии доступа, баннер на вход), выполните приведенную ниже последовательность команд для каждого коммутатора из привилегированного режима EXEC Cisco IOS (меняя имя коммутатора):

```
conf t
hostname sw1.lab
service password-encryption
username student privilege 15 secret 0 student
no ip domain-lookup
banner motd ^C
sw1.lab

PERM, Russia,
Network technology lab. IT department. PSTU

Warning: Authorized access only!!!
Disconnect IMMEDIATELY if you are not an authorized
person!!!
Contact information:
web http://wrls.ru
email support@wrls.ru
tel +7(342)220-63-85

_____________________________________________________
^C
line con 0
login local
line vty 0 4
login local
line vty 5 15
login local
```

Убедимся в правильности приведенных на рис. 1.5 статусе и состоянии портов коммутаторов согласно разд. 1 пособия, используя вывод команд Show Spanning-Tree VLAN 1 и Show Spanning-Tree Detail. **Состояние коммутаторов будет выглядеть так:**

```
    Sw1:
    sw1.lab#show spanning-tree detail

    VLAN0001 is executing the ieee compatible Spanning
Tree protocol
    Bridge Identifier has priority 32768, sysid 1, ad-
dress 0019.3096.eb80
    Configured hello time 2, max age 20, forward delay 15
    We are the root of the spanning tree (здесь и далее
цветом выделены важные элементы, к некоторым будут даны
пояснения)
    Topology change flag not set, detected flag not set
    Number of topology changes 20 last change occurred
00:04:47 ago
    Times: hold 1, topology change 35, notification 2
    hello 2, max age 20, forward delay 15
    Timers: hello 0, topology change 0, notification 0,
aging 300
    * Этот коммутатор стал корневым (Root Bridge для
VLAN 1).

    Port 1 (FastEthernet0/1) of VLAN0001 is forwarding
    Port path cost 19, Port priority 128, Port Identi-
fier 128.1.
    Designated root has priority 32769, address
0019.3096.eb80
    Designated bridge has priority 32769, address
0019.3096.eb80
    Designated port id is 128.1, designated path cost 0
    Timers: message age 0, forward delay 0, hold 0
    Number of transitions to forwarding state: 5
    Link type is point-to-point by default
    BPDU: sent 627, received 1981
    * Path Cost для этого порта = 19, Port Priority =
= 128, PID = 128.1.
```

```
    Port 3 (FastEthernet0/3) of VLAN0001 is forwarding
    Port path cost 19, Port priority 128, Port Identifier
128.3.
    Designated root has priority 32769, address
0019.3096.eb80
    Designated bridge has priority 32769, address
0019.3096.eb80
    Designated port id is 128.3, designated path cost 0
    Timers: message age 0, forward delay 0, hold 0
    Number of transitions to forwarding state: 3
    Link type is point-to-point by default
    BPDU: sent 179, received 1149
    * Path Cost для этого порта = 19, Port Priority =
= 128, PID = 128.3.

    Port 25 (GigabitEthernet0/1) of VLAN0001 is for-
warding
    Port path cost 4, Port priority 128, Port Identi-
fier 128.25.
    Designated root has priority 32769, address
0019.3096.eb80
    Designated bridge has priority 32769, address
0019.3096.eb80
    Designated port id is 128.25, designated path cost 0
    Timers: message age 0, forward delay 0, hold 0
    Number of transitions to forwarding state: 3
    Link type is point-to-point by default
    BPDU: sent 169, received 2454
    * Path Cost для этого порта = 4, Port Priority =
= 128, PID = 128.25.

    sw1.lab#show spanning-tree vlan 1
    VLAN0001
    Spanning tree enabled protocol ieee
    Root ID Priority 32769
    Address 0019.3096.eb80
    This bridge is the root
    Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec

    Bridge ID Priority 32769 (priority 32768 sys-id-ext 1)
    Address 0019.3096.eb80
    Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec
```

```
    Aging Time 300
      Interface   Role      Sts      Cost   Prio.Nbr   Type
         Fa0/1    Desg      FWD      19     128.1      P2p
         Fa0/3    Desg      FWD      19     128.3      P2p
         Gi0/1    Desg      FWD      4      128.25     P2p
    * Role – роли портов на коммутаторе Sw1.lab.

    Sw2:
    sw2.lab#show spanning-tree detail

    VLAN0001 is executing the ieee compatible Spanning
Tree protocol
    Bridge Identifier has priority 32768, sysid 1, ad-
dress 001c.b1de.6000
    Configured hello time 2, max age 20, forward delay 15
    Current root has priority 32769, address
0019.3096.eb80
    Root port is 26 (GigabitEthernet0/2), cost of root
path is 4
    Topology change flag not set, detected flag not set
    Number of topology changes 24 last change occurred
00:04:59 ago
    from GigabitEthernet0/1
    Times: hold 1, topology change 35, notification 2
    hello 2, max age 20, forward delay 15
    Timers: hello 0, topology change 0, notification 0,
aging 300
    * Информация о том, что корневой Sw1, RPC = 4 от
Sw2 к Sw1.

    Port 2 (FastEthernet0/2) of VLAN0001 is forwarding
    Port path cost 19, Port priority 128, Port Identi-
fier 128.2.
    Designated root has priority 32769, address
0019.3096.eb80
    Designated bridge has priority 32769, address
001c.b1de.6000
    Designated port id is 128.2, designated path cost 4
    Timers: message age 0, forward delay 0, hold 0
    Number of transitions to forwarding state: 1
    Link type is point-to-point by default
```

```
    BPDU: sent 396, received 0
    Port 25 (GigabitEthernet0/1) of VLAN0001 is for-
warding
    Port path cost 4, Port priority 128, Port Identi-
fier 128.25.
    Designated root has priority 32769, address
0019.3096.eb80
    Designated bridge has priority 32769, address
001c.b1de.6000
    Designated port id is 128.25, designated path cost 4
    Timers: message age 0, forward delay 0, hold 0
    Number of transitions to forwarding state: 1
    Link type is point-to-point by default
    BPDU: sent 755, received 2008

    Port 26 (GigabitEthernet0/2) of VLAN0001 is for-
warding
    Port path cost 4, Port priority 128, Port Identi-
fier 128.26.
    Designated root has priority 32769, address
0019.3096.eb80
    Designated bridge has priority 32769, address
0019.3096.eb80
    Designated port id is 128.25, designated path cost 0
    Timers: message age 2, forward delay 0, hold 0
    Number of transitions to forwarding state: 1
    Link type is point-to-point by default
    BPDU: sent 2699, received 177

    Sw2.lab#show spanning-tree vlan 1
    VLAN0001
    Spanning tree enabled protocol ieee
    Root ID Priority 32769
    Address 0019.3096.eb80
    Cost 4
    Port 26 (GigabitEthernet0/2)
    Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec
    Bridge ID Priority 32769 (priority 32768 sys-id-ext 1)
    Address 001c.b1de.6000
    Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec
    Aging Time 300
```

Interface	Role	Sts	Cost	Prio.Nbr	Type
Fa0/2	Desg	FWD	19	128.2	P2p
Gi0/1	Desg	FWD	4	128.25	P2p
Gi0/2	Root	FWD	4	128.26	P2p

Sw3:
sw3.lab#show spanning-tree detail

VLAN0001 is executing the ieee compatible Spanning Tree protocol
Bridge Identifier has priority 32768, sysid 1, address 04fe.7f2b.e680
Configured hello time 2, max age 20, forward delay 15
Current root has priority 32769, address 0019.3096.eb80
Root port is 26 (GigabitEthernet0/2), cost of root path is 12
Topology change flag not set, detected flag not set
Number of topology changes 42 last change occurred 00:04:28 ago
Times: hold 1, topology change 35, notification 2
hello 2, max age 20, forward delay 15
Timers: hello 0, topology change 0, notification 0, aging 300

Port 1 (FastEthernet0/1) of VLAN0001 is alternate blocking
Port path cost 19, Port priority 128, Port Identifier 128.1.
Designated root has priority 32769, address 0019.3096.eb80
Designated bridge has priority 32769, address 0019.3096.eb80
Designated port id is 128.1, designated path cost 0
Timers: message age 1, forward delay 0, hold 0
Number of transitions to forwarding state: 4
Link type is point-to-point by default
BPDU: sent 2488, received 933

Port 2 (FastEthernet0/2) of VLAN0001 is designated forwarding

```
    Port path cost 19, Port priority 128, Port Identi-
fier 128.2.
    Designated root has priority 32769, address
0019.3096.eb80
    Designated bridge has priority 32769, address
04fe.7f2b.e680
    Designated port id is 128.2, designated path cost 12
    Timers: message age 0, forward delay 0, hold 0
    Number of transitions to forwarding state: 1
    Link type is point-to-point by default
    BPDU: sent 380, received 0

    Port 3 (FastEthernet0/3) of VLAN0001 is alternate
blocking
    Port path cost 19, Port priority 128, Port Identi-
fier 128.3.
    Designated root has priority 32769, address
0019.3096.eb80
    Designated bridge has priority 32769, address
0019.3096.eb80
    Designated port id is 128.3, designated path cost 0
    Timers: message age 2, forward delay 0, hold 0
    Number of transitions to forwarding state: 3
    Link type is point-to-point by default
    BPDU: sent 1149, received 170

    Port 26 (GigabitEthernet0/2) of VLAN0001 is root
forwarding
    Port path cost 4, Port priority 128, Port Identi-
fier 128.26.
    Designated root has priority 32769, address
0019.3096.eb80
    Designated bridge has priority 32769, address
04fe.7f86.7980
    Designated port id is 128.26, designated path cost 8
    Timers: message age 4, forward delay 0, hold 0
    Number of transitions to forwarding state: 1
    Link type is point-to-point by default
    BPDU: sent 993, received 1758

    Sw3.lab#show spanning-tree vlan 1
```

VLAN0001
Spanning tree enabled protocol ieee
Root ID Priority 32769
Address 0019.3096.eb80
Cost 12
Port 26 (GigabitEthernet0/2)
Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec

Bridge ID Priority 32769 (priority 32768 sys-id-ext 1)
Address 04fe.7f2b.e680
Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec
Aging Time 300

Interface	Role	Sts	Cost	Prio.Nbr	Type
Fa0/1	Altn	BLK	19	128.1	P2p
Fa0/2	Desg	FWD	19	128.2	P2p
Fa0/3	Altn	BLK	19	128.3	P2p
Gi0/2	Root	FWD	4	128.26	P2p

Sw4:
sw4.lab#show spanning-tree detail

VLAN0001 is executing the ieee compatible Spanning Tree protocol
Bridge Identifier has priority 32768, sysid 1, address 04fe.7f86.7980
Configured hello time 2, max age 20, forward delay 15
Current root has priority 32769, address 0019.3096.eb80
Root port is 25 (GigabitEthernet0/1), cost of root path is 8
Topology change flag not set, detected flag not set
Number of topology changes 18 last change occurred 00:04:12 ago
Times: hold 1, topology change 35, notification 2
hello 2, max age 20, forward delay 15
Timers: hello 0, topology change 0, notification 0, aging 300

Port 25 (GigabitEthernet0/1) of VLAN0001 is root forwarding

```
    Port path cost 4, Port priority 128, Port Identi-
fier 128.25.
    Designated root has priority 32769, address
0019.3096.eb80
    Designated bridge has priority 32769, address
001c.b1de.6000
    Designated port id is 128.25, designated path cost 4
    Timers: message age 3, forward delay 0, hold 0
    Number of transitions to forwarding state: 1
    Link type is point-to-point by default
    BPDU: sent 2008, received 730

    Port 26 (GigabitEthernet0/2) of VLAN0001 is desig-
nated forwarding
    Port path cost 4, Port priority 128, Port Identi-
fier 128.26.
    Designated root has priority 32769, address
0019.3096.eb80
    Designated bridge has priority 32769, address
04fe.7f86.7980
    Designated port id is 128.26, designated path cost 8
    Timers: message age 0, forward delay 0, hold 0
    Number of transitions to forwarding state: 1
    Link type is point-to-point by default
    BPDU: sent 1750, received 993

    sw4.lab#show spanning-tree vlan 1

    VLAN0001
    Spanning tree enabled protocol ieee
    Root ID Priority 32769
    Address 0019.3096.eb80
    Cost 8
    Port 25 (GigabitEthernet0/1)
    Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec
    Bridge ID Priority 32769 (priority 32768 sys-id-ext 1)
    Address 04fe.7f86.7980
    Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec
    Aging Time 300
```

Interface	Role	Sts	Cost	Prio.Nbr	Type
Gi0/1	Root	FWD	4	128.25	P2p
Gi0/2	Desg	FWD	4	128.26	P2p

1.2.2. Изменение места положения корня

Изменим место положения корневого коммутатора путем уменьшения поля приоритета в BID. Например, чтобы Root Bridge стал Sw2 (рис. 1.12), изменим его приоритет в BID.

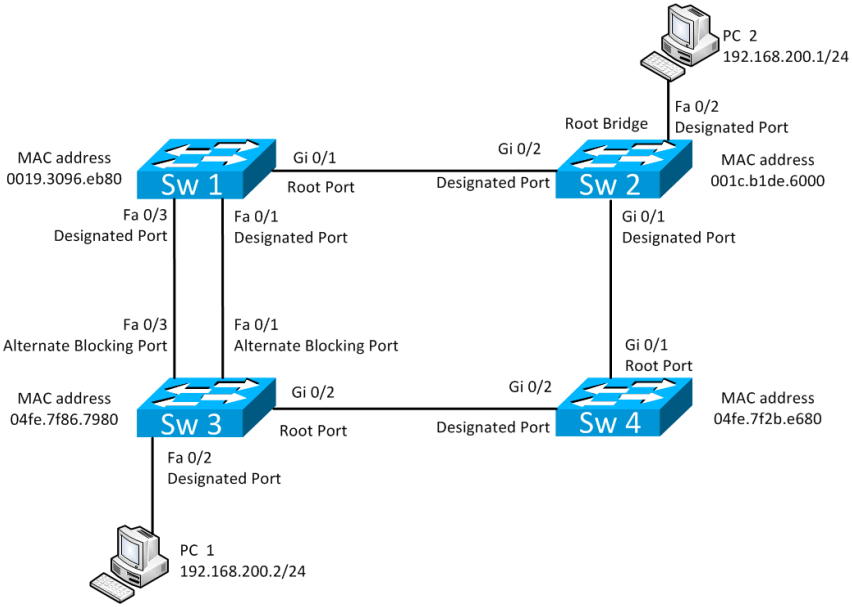


Рис. 1.12. Смена корневого моста

Настройте приоритет 4096 на Sw2:

```
Sw2:
sw2.lab#configure terminal
sw2.lab(config)# spanning-tree vlan 1 priority 4096
```

В результате вывод команды Show Spanning-Tree VLAN 1 на коммутаторах:

```
Sw1:
sw1.lab#show spanning-tree vlan 1

VLAN0001
Spanning tree enabled protocol ieee
Root ID Priority 4097
Address 001c.b1de.6000
Cost 4
Port 25 (GigabitEthernet0/1)
Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec

Bridge ID Priority 32769 (priority 32768 sys-id-ext 1)
Address 0019.3096.eb80
Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec
Aging Time 15

 Interface   Role     Sts     Cost   Prio.Nbr   Type
   Fa0/1     Desg     FWD      19     128.1     P2p
   Fa0/3     Desg     FWD      19     128.3     P2p
   Gi0/1     Root     FWD       4     128.25    P2p
*Информация о том, какой сейчас новый Root Bridge.

Sw2:
sw2.lab#show spanning-tree vlan 1
18w1d: %SYS-5-CONFIG_I: Configured from console by
console

VLAN0001
Spanning tree enabled protocol ieee
Root ID Priority 4097
Address 001c.b1de.6000
This bridge is the root
Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec

Bridge ID Priority 4097 (priority 4096 sys-id-ext 1)
Address 001c.b1de.6000
Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec
Aging Time 15
 Interface   Role     Sts     Cost   Prio.Nbr   Type
   Fa0/2     Desg     FWD      19     128.2     P2p
   Gi0/1     Desg     FWD       4     128.25    P2p
   Gi0/2     Desg     FWD       4     128.26    P2p
```

Sw3:

```
sw3.lab#show spanning-tree vlan 1

VLAN0001
Spanning tree enabled protocol ieee
Root ID Priority 32769
Address 0019.3096.eb80
Cost 12
Port 26 (GigabitEthernet0/2)
Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec

Bridge ID Priority 32769 (priority 32768 sys-id-ext 1)
Address 04fe.7f2b.e680
Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec
Aging Time 300

 Interface   Role      Sts     Cost   Prio.Nbr   Type
   Fa0/1     Altn      BLK      19     128.1     P2p
   Fa0/2     Desg      FWD      19     128.2     P2p
   Fa0/3     Altn      BLK      19     128.3     P2p
   Gi0/2     Root      FWD       4    128.26     P2p
```

Sw4:

```
sw4.lab#show spanning-tree vlan 1

VLAN0001
Spanning tree enabled protocol ieee
Root ID Priority 4097
Address 001c.b1de.6000
Cost 4
Port 25 (GigabitEthernet0/1)
Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec

Bridge ID Priority 32769 (priority 32768 sys-id-ext 1)
Address 04fe.7f86.7980
Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec
Aging Time 300

 Interface   Role      Sts     Cost   Prio.Nbr   Type
   Gi0/1     Root      FWD       4    128.25     P2p
   Gi0/2     Desg      FWD       4    128.26     P2p
```

Далее запустим tcpdump на PC1 или PC2. В выводе утилиты будут видны кадры BPDU STP.

1.2.3. Фильтрация BPDU

Теперь запретим коммутаторам отправлять кадры BPDU STP в порты, к которым подключены компьютеры.

Настроим PortFast и BPDU Filter и BPDU Guard на интерфейсе Fa0/2 на коммутаторах Sw2 и Sw3:

```
Sw2:
sw2.lab #conf t
sw2.lab (config)#interface fastEthernet 0/2
sw2.lab (config-if)#spanning-tree portfast
sw2.lab (config-if)#spanning-tree bpdugfilter enable
sw2.lab (config-if)#spanning-tree bpduguard enable
sw2.lab (config-if)#exit

Sw3:
sw3.lab #conf t
sw3.lab (config)#interface fastEthernet 0/2
sw3.lab (config-if)#spanning-tree portfast
sw3.lab (config-if)#spanning-tree bpdugfilter enable
sw3.lab (config-if)#spanning-tree bpduguard enable
sw3.lab (config-if)#exit
```

Теперь вывод tcpdump не будет показывать перехваченные кадры BPDU STP. Теперь вместо PC11 подключите коммутатор 5 управляющей сети к коммутатору Sw3 на 2 мин. В консоли Sw3 будет выведено сообщение о том, что BPDU Guard заблокирует порт Fa0/2:

– 18w1d: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/2, changed state to down

– 18w1d: %LINK-3-UPDOWN: Interface FastEthernet0/2, changed state to down

– 18w1d: %SPANTREE-2-BLOCK_BPDUGUARD: Received BPDU on port FastEthernet0/2 with BPDU Guard enabled. Disabling port

– 18w1d: %PM-4-ERR_DISABLE: bpduguard error detected on Fa0/2, putting Fa0/2 in err-disable state

Далее подключите PC1 обратно и выведете порт из этого состояния, включив и выключив его (для настройки выхода порта автоматически из этого состояния через 120 с введите в глобальном режиме конфигурации команду Errdisable Recovery Interval 40):

```
Sw2:
sw2#conf t
sw2(config)#interface FastEthernet 0/2
sw2(config-if)#shutdown
sw2#(config-if) #no shutdown
```

1.2.4. Изменение места корневого порта

Сменим роли на портах коммутатора Sw1, данные изменения касаются только Sw1 (рис. 1.13).

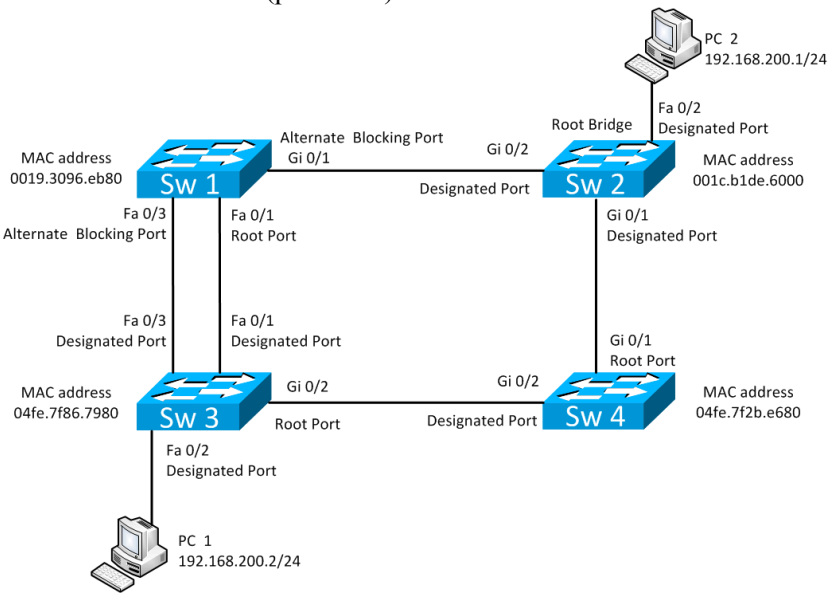


Рис. 1.13. Изменение места размещения корневого порта на коммутаторе Sw1

Для этого на коммутаторе Sw1 увеличим стоимость порта Ge0/1 с 4 на 100:

```
Sw1:
sw1#conf t
```

```
sw1(config)#int GigabitEthernet 0/1
sw1(config-if)#spanning-tree cost 100
```

Это приведет к тому, что путь от Sw1 к корню Sw2 будет короче через Sw3.

Вывод команды Show Spanning-Tree VLAN 1 на Sw1:

```
sw1.lab#show spanning-tree vlan 1
VLAN0001
Spanning tree enabled protocol ieee
Root ID Priority 4097
Address 001c.b1de.6000
Cost 27
Port 1 (FastEthernet0/1)
Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec

Bridge ID Priority 32769 (priority 32768 sys-id-ext 1)
Address 0019.3096.eb80
Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec
Aging Time 15

 Interface   Role     Sts     Cost   Prio.Nbr   Type
   Fa0/1     Root     FWD      19     128.1     P2p
   Fa0/3     Altn     BLK      19     128.3     P2p
   Gi0/1     Altn     BLK     100     128.25    P2p
*Стоимость порта Gi0/1 на Sw1.lab теперь равна 100.
```

1.2.5. Изменение роли портов

Теперь сменим на коммутаторе Sw1 роль Fa0/1 на Altn, а Fa0/3 на Root (рис. 1.14).

Для этого на коммутаторе Sw3 заменим Port Priority на порту Fa 0/3 с 128 на 16:

```
Sw3:
sw3.lab#conf t
sw3.lab(config)#int FastEthernet 0/3
sw3.lab(config-if)#spanning-tree port-priority 16
```

Вывод команд Show Spanning-Tree VLAN 1 на Sw1:

```
sw1.lab#show spanning-tree vlan 1
```

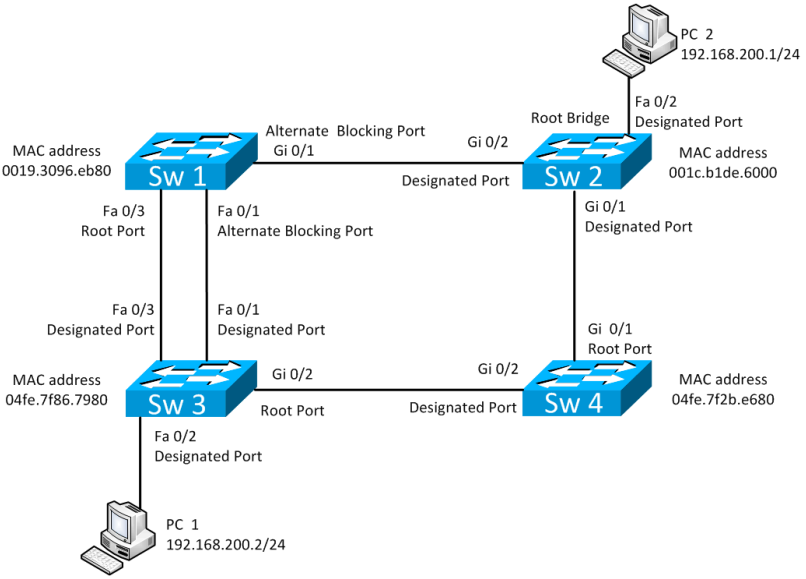


Рис. 1.14. Смена ролей портов FastEthernet на Sw1

```
VLAN0001
Spanning tree enabled protocol ieee
Root ID Priority 4097
Address 001c.b1de.6000
Cost 27
Port 3 (FastEthernet0/3)
Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec

Bridge ID Priority 32769 (priority 32768 sys-id-ext 1)
Address 0019.3096.eb80
Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec
Aging Time 15

  Interface    Role      Sts      Cost   Prio.Nbr   Type
    Fa0/1      Altn      BLK       19      128.1     P2p
    Fa0/3      Root      LRN       19      128.3     P2p
    Gi0/1      Altn      BLK      100     128.25     P2p
*Роли портов сменились.
```

Вывод команд Show spanning-tree VLAN 1 и Show Spanning-Tree Detail на Sw3:

```
sw3.lab#show spanning-tree detail

VLAN0001 is executing the ieee compatible Spanning Tree protocol
Bridge Identifier has priority 32768, sysid 1, address 04fe.7f2b.e680
Configured hello time 2, max age 20, forward delay 15
Current root has priority 4097, address 001c.b1de.6000
Root port is 26 (GigabitEthernet0/2), cost of root path is 8
Topology change flag set, detected flag not set
Number of topology changes 50 last change occurred 00:00:04 ago
from FastEthernet0/3
Times: hold 1, topology change 35, notification 2
hello 2, max age 20, forward delay 15
Timers: hello 0, topology change 0, notification 0, aging 15

Port 1 (FastEthernet0/1) of VLAN0001 is designated forwarding
Port path cost 19, Port priority 128, Port Identifier 128.1.
Designated root has priority 4097, address 001c.b1de.6000
Designated bridge has priority 32769, address 04fe.7f2b.e680
Designated port id is 128.1, designated path cost 8
Timers: message age 0, forward delay 0, hold 0
Number of transitions to forwarding state: 7
Link type is point-to-point by default
BPDU: sent 2551, received 1739

Port 2 (FastEthernet0/2) of VLAN0001 is designated forwarding
Port path cost 19, Port priority 128, Port Identifier 128.2.
Designated root has priority 4097, address 001c.b1de.6000
```

```
    Designated bridge has priority 32769, address
04fe.7f2b.e680
    Designated port id is 128.2, designated path cost 8
    Timers: message age 0, forward delay 0, hold 0
    Number of transitions to forwarding state: 1
    The port is in the portfast mode
    Link type is point-to-point by default
    Bpdu guard is enabled
    Bpdu filter is enabled
    BPDU: sent 0, received 0
    *Порт в режиме PortFast. BPDU-Guard и Filter включены.

    Port 3 (FastEthernet0/3) of VLAN0001 is designated
forwarding
    Port path cost 19, Port priority 16, Port Identi-
fier 16.3.
    Designated root has priority 4097, address
001c.b1de.6000
    Designated bridge has priority 32769, address
04fe.7f2b.e680
    Designated port id is 16.3, designated path cost 8
    Timers: message age 0, forward delay 0, hold 0
    Number of transitions to forwarding state: 4
    Link type is point-to-point by default
    BPDU: sent 1212, received 1197
    *Приоритет порта теперь 16 вместо 128.

    Port 26 (GigabitEthernet0/2) of VLAN0001 is root
forwarding
    Port path cost 4, Port priority 128, Port Identi-
fier 128.26.
    Designated root has priority 4097, address
001c.b1de.6000
    Designated bridge has priority 32769, address
04fe.7f86.7980
    Designated port id is 128.26, designated path cost 4
    Timers: message age 3, forward delay 0, hold 0
    Number of transitions to forwarding state: 1
    Link type is point-to-point by default
    BPDU: sent 1002, received 2851

    sw3.lab#show spanning-tree vlan 1
```

```
VLAN0001
Spanning tree enabled protocol ieee
Root ID Priority 4097
Address 001c.b1de.6000
Cost 8
Port 26 (GigabitEthernet0/2)
Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec

Bridge ID Priority 32769 (priority 32768 sys-id-ext 1)
Address 04fe.7f2b.e680
Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec
Aging Time 300

 Interface   Role      Sts     Cost   Prio.Nbr   Type
   Fa0/1     Desg      FWD      19     128.1     P2p
   Fa0/2     Desg      FWD      19     128.2   P2p Edge
   Fa0/3     Desg      FWD      19      16.3     P2p
   Gi0/2     Root      FWD       4     128.26    P2p
```

1.2.6. Корректное восстановление исходной конфигурации

Необходимо сохранить вашу конфигурацию на всех устройствах. Для этого выполним команды

```
Sw1.lab#copy running-config startup-config
Sw2.lab#copy running-config startup-config
Sw3.lab#copy running-config startup-config
Sw4.lab#copy running-config startup-config
```

Задания для самостоятельной работы

1. Сделайте коммутатор Sw4 корневым мостом.

2. По окончании работ сотрите свою конфигурацию (Erase Startup-Config) и перезагрузите оборудование (Reload) с помощью лаборанта.

Вопросы для самопроверки

1. Что такое сегмент сети?
2. Что означает Blocked Port?
3. Что означает Designated Port?
4. Что означает Root Port?
5. Из чего состоит BID?
6. Из чего состоит PID?
7. Как определяется значение стоимости пути?
8. Этапы начальной сходимости STP?
9. Сколько назначенных портов имеется в сети на рис. 1.15?
10. Сколько корневых портов имеется в сети на рис. 1.15?
11. Какой мост имеет статус корневого моста при том, что остальные параметры будут равны?

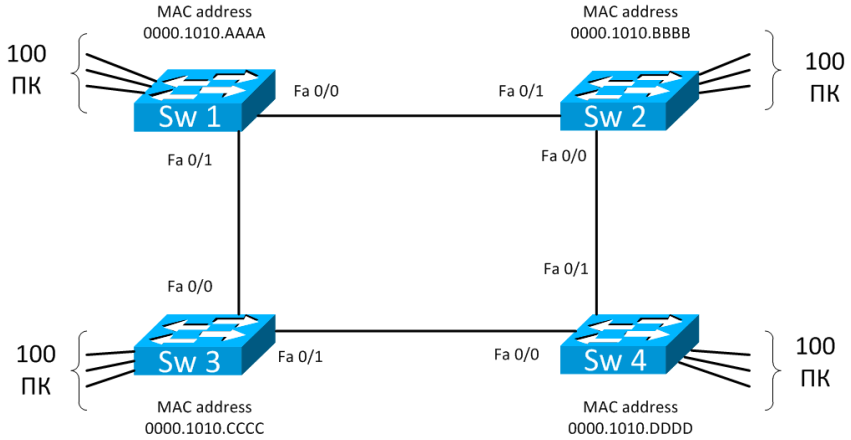


Рис. 1.15. Пример сети, состоящей из четырех коммутаторов и 400 станций

12. Сколько блокированных портов имеется в сети на рис. 1.15?
13. Каково время сходимости STP?
14. Каким образом вычисляется значение корневой стоимости?

15. В процессе работы алгоритма протокола STP каждый порт устройства сохраняет лучшее из сообщений BPDU, полученных через некоторый порт. По каким критериям оценивается полученная информация?

2. VLAN, 802.1Q, ETHERCHANNEL L2, VTP

2.1. Краткие теоретические сведения

2.1.1. VLAN-сети

Одной из важных функций, реализуемых в технологии Ethernet, являются виртуальные локальные сети (VLAN), в которых для объединения серверов и рабочих станций в логические группы используются коммутаторы. Связь устройств, принадлежащих к одной VLAN-сети, возможна только с устройствами этой же сети. VLAN-сети создаются на коммутаторах на L2-уровне для разбиения сети на широковещательные домены, масштабирования сети и усиления безопасности сети. Кадры данных передаются в пределах одной VLAN-сети без изменений в своей структуре.

Каждая сеть VLAN создается в локальной базе данных используемого коммутатора. Если в коммутаторе отсутствуют сведения о какой-либо VLAN-сети, то он не может передавать трафик для этой сети VLAN через свои порты. При создании VLAN-сети ей присваивается номер. Существует диапазон для использования VLAN-номеров: от 1 до 4094. При создании VLAN-сети можно также назначить ей определенные атрибуты, такие как имя, тип и операционное состояние.

Виды VLAN-сетей:

а) базирующиеся на портах – статические VLAN-сети;

б) базирующиеся на основе MAC-адресов – динамические VLAN-сети.

Последовательность настройки VLAN на коммутаторе:

а) создать VLAN-сеть, задать имя и MTU;

б) привязать отобранные порты коммутатора к созданной VLAN-сети (статический способ) либо привязать MAC-адрес хоста к созданной VLAN-сети (динамический способ).

Доступ к общесетевым ресурсам (например, почтовый сервер) в сетях с VLAN осуществляется путем настройки на порту сервера и коммутатора транкового интерфейса, способного поддерживать трафик нескольких VLAN. При этом на интерфейсе сервера создается по одному сабинтерфейсу с IP-адресом для каждого VLAN.

Маршрутизация между VLAN осуществляется либо с помощью коммутаторов, поддерживающих L3, либо путем настройки на маршрутизаторе сервера и коммутатора транкового интерфейса, способного поддерживать трафик нескольких VLAN. При этом на интерфейсе маршрутизатора создается по одному сабинтерфейсу с IP-адресом для каждого VLAN (рис. 2.8).

2.1.2. Транки

Под транком в Cisco понимается отдельный канал передачи данных между коммутаторами, способный нести данные нескольких VLAN-сетей. Для того чтобы различать фреймы разных VLAN в транке, 802.1Q помещает внутрь каждого фрейма *тег*, который передает информацию о принадлежности трафика к определенному VLAN. IEEE 802.1Q – открытый стандарт, который описывает процедуру тегирования трафика для передачи информации о принадлежности к VLAN. Поля тэга представлены на рис. 2.1.

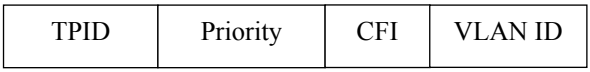


Рис. 2.1. Тег 802.1Q

Размер тега – 4 байта. Он состоит из полей:

– Tag Protocol Identifier (TPID) – идентификатор протокола тегирования. Размер поля – 16 бит. Указывает, какой протокол используется для тегирования. Для 802.1Q используется значение 0×8100.

– Priority – приоритет. Размер поля – 3 бита. Используется стандартом IEEE 802.1P для задания приоритета передаваемого трафика.

– Canonical Format Indicator (CFI) – индикатор канонического формата. Размер поля – 1 бит. Указывает на формат MAC-адреса: 1 – канонический (кадр Ethernet), 0 – неканонический (кадр Token Ring, FDDI).

– VLAN Identifier (VID) – идентификатор VLAN. Размер поля – 12 бит. Указывает, какому VLAN принадлежит кадр. Диапазон возможных значений VID от 0 до 4094.

При использовании стандарта Ethernet II 802.1Q вставляет тег перед полем «Тип протокола» (рис. 2.2). Поскольку кадр изменился, пересчитывается контрольная сумма.

Исходный фрейм

Адрес получателя	Адрес отправителя	Тип протокола	Данные	Контрольная сумма

Тегированный фрейм

Адрес получателя	Адрес отправителя	Тег	Тип протокола	Данные	Новая контрольная сумма

Рис. 2.2. Кадр до и после вставки тега

В стандарте 802.1Q существует понятие Native VLAN. По умолчанию это VLAN 1. Трафик, передающийся в этом VLAN, не тегируется. Важно заметить, что если коммутатор получает нетегированный фрейм на транк-порту, то он шлет его в Native VLAN. Native VLAN по умолчанию VLAN 1, но в целях безопасности его рекомендуется сменить. На обоих концах транка должны быть настроены одинаковые Native VLAN.

2.1.3. Агрегация портов EtherChannel

Агрегирование каналов – технология, которая позволяет объединить несколько физических каналов (до 8) в один логический.

Такое объединение позволяет увеличивать пропускную способность канала и его надежность. Агрегирование каналов может быть настроено как между двумя коммутаторами, так и между коммутатором и сервером, коммутатором и роутером. Существует агрегация каналов 2-го и 3-го уровней. В рамках данного пособия мы работаем только со 2-м уровнем. Существует два протокола, отвечающих за агрегацию каналов: стандартизированный IEEE – LACP и составляющий собственность Cisco – PAgP. EtherChannel не может быть одновременно настроен для работы в режиме PAgP и LACP.

Создание EtherChannel для портов 2-го и портов 3-го уровня отличается:

а) для интерфейсов 3-го уровня вручную создается логический интерфейс командой *Interface Port-Channel*;

б) для интерфейсов 2-го уровня логический интерфейс создается динамически;

в) для обоих типов интерфейсов необходимо вручную назначать интерфейс в EtherChannel. Для этого используется команда *Channel-group* в режиме настройки интерфейса. Эта команда связывает вместе физические порты в логический порт.

Агрегируются каналы с одинаковыми:

а) скоростями;

б) режимом дуплекса;

в) Native VLAN;

г) VLAN-диапазоном;

д) состоянием транкинга;

е) типом.

Последовательность настройки EtherChannel L2 на коммутаторе:

а) настроить порты, которые будут входить в один логический порт;

б) объединить порты в один логический порт.

2.1.4. Протокол VTP

С ростом сети добавление новых VLAN на коммутаторах и новых VLAN в список позволенных на транке становится существенной проблемой для администратора сети. VTP дает возможность сформировать один или несколько коммутаторов в режиме сервера, что позволяет им автоматически распространять обновления информации о VLAN по сети. Коммутаторы в режиме сервера становятся единой точкой управления информацией о VLAN в сети.

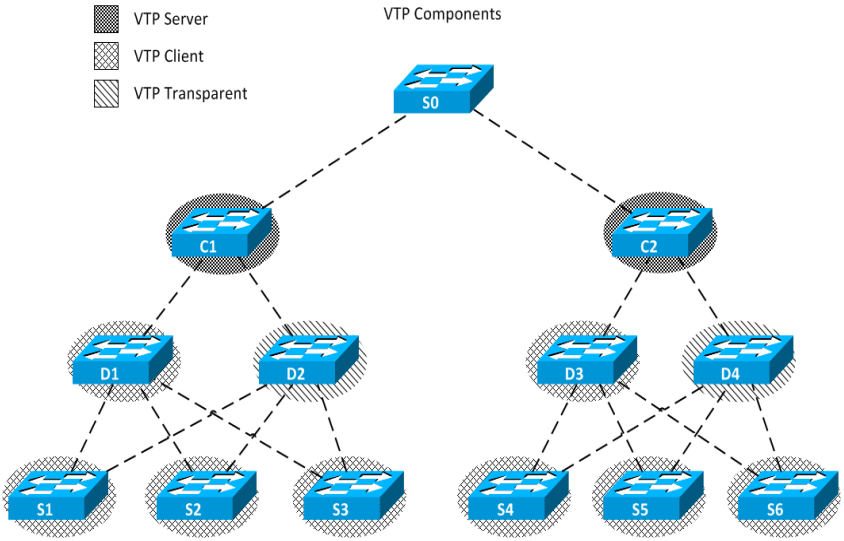


Рис. 2.3. Пример топологии VTP

Коммутатор в топологии VTP может быть в одном из трех режимов (рис. 2.3):

1. VTP Server. VTP сообщают VTP-информацию о VLAN другим коммутаторам с включенным VTP, находящимися в одном VTP-домене. Серверы VTP хранят информацию VLAN для всего домена в NVRAM. Сервер – то место, где VLAN может быть создан, удален или переименован для данного домена VTP.

2. VTP Client. VTP функционируют так же, как серверы VTP, но вы не можете создать, изменить или удалить VLAN на клиенте VTP. Клиент VTP только хранит информацию VLAN для всего домена, в то время как он запущен. Сброс коммутатора удаляет информацию о VLAN.

3. VTP Transparent. Прозрачные коммутаторы отправляют рекламные объявления VTP клиентам VTP и серверам VTP. Прозрачные коммутаторы не участвуют в процессе VTP. VLAN, которые созданы, переименованы или удалены на прозрачных коммутаторах, являются локальными только для этого коммутатора.

Сообщения, инкапсулированные в 802.1Q кадр, VTP передаются другим коммутаторам по транкам (рис. 2.4).

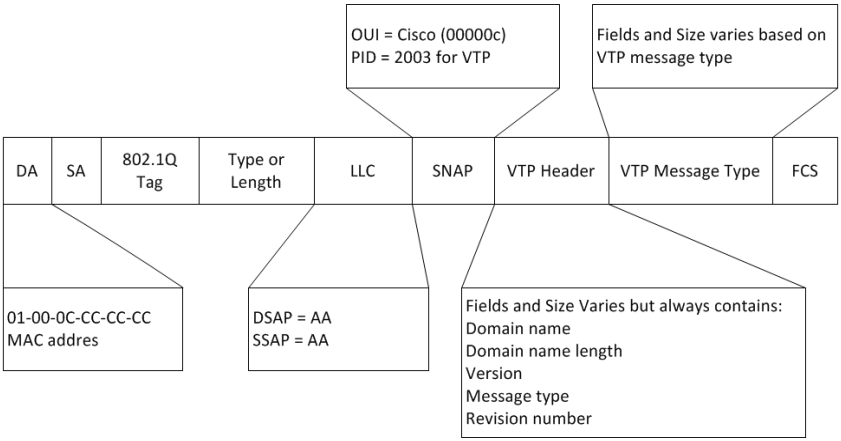


Рис. 2.4. Поля кадра VTP

Кадр VTP состоит из полей:

– Destination MAC address. Это поле установлено в Multicast-адрес 01-00-0C-CC-CC-CC, который зарезервирован для VTP-сообщений;

– LLC field Logical Link Control (LLC). Поле содержит значения DSAP и SSAP, установленные в AA;

– SNAP Field Subnetwork Access Protocol (SNAP). Поле имеет поле OUI, установленное в AAAA, и поле PID, установленное в 2003;

– VTP Header Field. Содержит различную информацию на основании поля VTP Message Type, но часто содержит данные VTP-поля:

- Domain Name. Имя домена VTP для данного коммутатора;
- Domain Name Length. Длина имени домена;
- Version. Версия VTP 1, VTP 2 или VTP 3. Коммутатор Cisco 2960 поддерживает только VTP 1 и VTP 2;
- Configuration Revision Number. Текущее значение Revision Number данного коммутатора. Данное поле увеличивается на 1, если на коммутаторе добавляется или удаляется VLAN;

– VTP Message Type. Тип сообщения VTP. VTP-кадр содержит данную информацию для каждого VLAN:

а) VLAN IDs (IEEE 802.1Q);

б) VLAN имя;

в) VLAN тип;

г) VLAN состояние;

д) дополнительные параметры VLAN, специфичные для каждого типа VLAN.

Типы сообщений VTP:

а) Summary Advertisements. Каждые 5 мин сервер посылает VTP соседним VTP-Enabled коммутаторам информацию о текущем VTP Configuration Revision Number для своего домена (рис. 2.5).

Описание полей Summary Advertisements:

- поле Followers указывает на то, что за этим пакетом следует пакет Subset Advertisements;
- Updater Identity – это IP-адрес последнего коммутатора, на котором был увеличен Revision Number;
- Update Timestamp – это дата и время последнего увеличения версии конфигурации;

- если включено использование алгоритма MD5, MD5 Digest содержит пароль VTP и используется для проверки подлинности обновления VTP;
- Code – для Summary Advertisements данное поле имеет формат 0×01.

Version	Code	Followers	MgmtD Len
Management Domain Name (zero-padded to 32 bytes)			
Configuration Revision Number			
Update Identity			
Update Timestamp (12 bytes)			
MD5 Digest (16 bytes)			

Рис. 2.5. Формат пакета Summary Advertisements

б) Subset Advertisements. Сервер VTP шлет «рекламу» подмножества, которая содержит информацию о VLAN-изменениях. Изменения, которые вызывают «рекламу» подмножества, также увеличивают на 1 Revision Number, включают создание, удаление, переименование, изменение параметров VLAN (рис. 2.6).

Version	Code	Followers	MgmtD Len
Management Domain Name (zero-padded to 32 bytes)			
Configuration Revisio			
VLAN-info field 1			
…….			
VLAN-info filed N			

Рис. 2.6. Формат пакета Subset Advertisements

Поля:

- Code – для Subset Advertisements данное поле имеет формат 0×02;
- VLAN-info field – это описание *n*-го VLAN.

в) Request Advertisements. Данный кадр шлет клиент VTP серверу VTP запрашивая информацию о VLAN, если клиент пропустил несколько обновлений, либо у него сменился домен VTP, либо он получил Summary Advertisements с VTP Configuration Revision Number больше, чем у себя (рис. 2.7).

Version	Code	Followers	MgmtD Len
Management Domain Name (zero-padded to 32 bytes)			
Start-Value			

Рис. 2.7. Формат пакета Request Advertisements

Поля:

- Code – для Request Advertisements данное поле имеет формат 0×03;
- Start Value – используется в случаях, когда было несколько Subset Advertisements. Если сначала получено *n*-е сокращенное объявление, а следующее *n* + 1-е – нет, то коммутатор запрашивает только объявления начиная с *n* + 1-го.

По умолчанию по транку разрешен широковещательный трафик всех VLAN, независимо от того, есть на соседнем коммутаторе хосты в данном VLAN или нет. Для того чтобы широковещательный трафик не шел по транку в коммутатор, на котором нет подсоединенных ПК в данной VLAN, используйте опцию VTP Pruning (рис. 2.8).

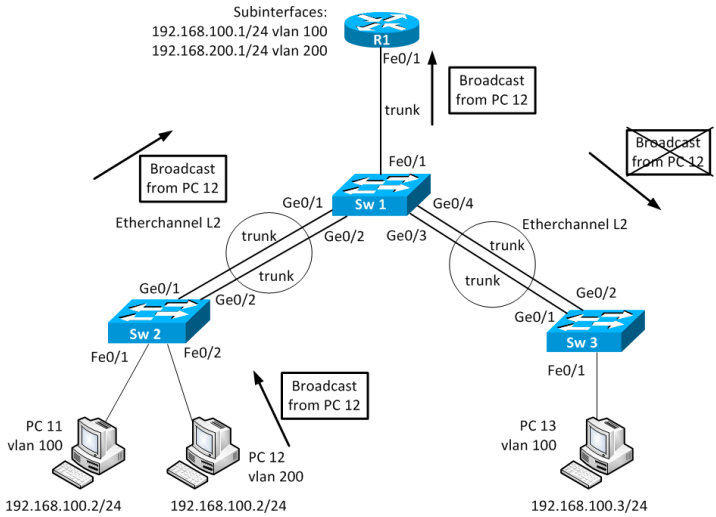


Рис. 2.8. Включение опции VTP Pruning

2.1.5. Настройки на оборудовании Cisco

Начальное состояние командной строки «привилегированный режим» EXEC Cisco IOS. Курсивом показаны переменные. Вертикальной чертой отделены различные варианты команд. Чтобы отменить команду, необходимо ввести ее повторно, но с *no* в начале.

Настройка VLAN на коммутаторах Cisco

Создание VLAN-сети:

– Вход в глобальный режим конфигурации

```
configure terminal
```

– Создание VLAN-сети и вход в режим конфигурации VLAN-сети

```
vlan «vlan-id»
```

– Настройка параметров VLAN-сети в режиме конфигурации VLAN-сети

```
[name vlan-nam] [state {suspend | active}] [mtu mtu-size]
```

Здесь name – описательное имя VLAN-сети длиной до 32 символов. Если имя не задано, принимается стандартное имя VLAN00XXX, где XXX – номер VLAN-сети;

– mtu – максимально возможная единица передачи данных (размер пакета в байтах), которая может использоваться в данной VLAN-сети. Стандартные значения находятся в диапазоне от 576 до 18 190. MTU-размер может быть увеличен до 1500 для Ethernet-сети и превышает это значение для сетей Token Ring и FDDI. Стандартное значение – 1500;

– state – используется для определения состояния VLAN-сети активное (Active) или приостановленное (Suspend). В последнем случае работа всех портов приостановлена и передача ими трафика не разрешена. Стандартное значение – Active.

Назначение сетям VLAN портов:

– вход в глобальный режим конфигурации

```
configure terminal
```

– вход в режим конфигурирования интерфейса порта. Указать физический интерфейс, который надо сконфигурировать для VLAN

```
interface «interface-id»
```

– сконфигурировать интерфейс порта в режим статического доступа

```
switchport mode access
```

– сопоставить порт с VLAN. Правильные идентификаторы VLAN от 1 до 4094; не начинайте ввод идентификатора с нуля

```
switchport access vlan «vlan-id»
```

– просмотреть настройки VLAN-режима на интерфейсе:

```
show running-config interface «interface-id»
```

– просмотреть настройки VLAN на коммутаторе:

```
show vlan
```

Настройка транков на коммутаторах Cisco

Создание транка на порту:

– вход в глобальный режим конфигурации

```
configure terminal
```

– вход в режим конфигурирования интерфейса порта

interface «interface-id»

– формируем транк на порту

switchport mode {dynamic {auto | desirable} | trunk}

Здесь dynamic auto установит интерфейс в состояние транка, если на соседнем интерфейсе установлен режим Trunk или Desirable. Включено по умолчанию;

- dynamic desirable установит интерфейс в состояние транка, если на соседнем интерфейсе установлен режим Trunk, Desirable или Auto;
- trunk установит интерфейс в перманентное состояние транка, даже если соседний интерфейс не транковый.

– меняем Native VLAN на VLAN, кроме 1

switchport trunk native vlan vlan id

– разрешаем или запрещаем трафику определенного VLAN идти по транку

switchport trunk allowed vlan {add | all | except | remove} vlan-list

– просмотр параметров настроенных транков

show interfaces trunk

Настройка EtherChannel на коммутаторах Cisco

Присоединение интерфейса в логический интерфейс Ether-Channel L2 (при L2 EtherChannel логический интерфейс (Port-Channel) создается автоматически):

– вход в глобальный режим конфигурации

configure terminal

– вход в режим конфигурирования интерфейса порта

interface «interface-id»

– присоединение интерфейса к EtherChannel

channel-group channel-group-number mode {auto [non-silent] | desirable [non-silent] | on} | {active | passive}

Здесь *channel-group-number* – номер от 1 до 6;

- для mode выберите один из ключей:
  - auto – позволяет PAgP только тогда, когда устройство PAgP обнаружено. Помещает порт в состояние Passive

Negotiating, в котором порт отвечает на PAgP-пакеты, которые он получает, но сам не инициирует переговоры PAgP, т.е. не отправляет пакеты PAgP;

- desirable – безусловно позволяет PAgP. Помещает порт в состояние Active Negotiating State, в котором порт начинает переговоры с портом на другой стороне путем отправки PAgP-пакетов;
- on – перманентно помещает порт в Port-Channel без переговоров PAgP или LACP. Данный режим работает, когда порты на обеих сторонах сконфигурированы в этом режиме;
- non-silent (Optional) – если ваш коммутатор подключен к партнеру, который PAgP-совместим, то сконфигурировать порт коммутатора для Non-Silent Operation, когда порт в режиме Auto или Desirable. Если вы не укажете Non-Silent, то Silent предполагается. Опция Silent для подсоединения к File Servers или Packet Analyzers. Эта опция позволяет PAgP работать, присоединять порт к Channel Group и использовать порт для передачи;
- active – позволяет LACP, только если устройство LACP обнаружено. Помещает порт в состояние Active Negotiating State, в котором порт начинает переговоры с портом на другой стороне путем отправки LACP-пакетов;
- passive – позволяет LACP на порту. Помещает порт в состояние Passive Negotiating State, в котором порт отвечает на запросы приходящих LACP-пакетов, но сам не инициирует переговоры LACP, т.е. не отправляет пакеты LACP.

Настройка транковых параметров интерфейса Port-channel:

interface portchannel «interface-id»

Настройка балансировки нагрузки на логическом интерфейсе EtherChannel:

– вход в глобальный режим конфигурации

configure terminal

– выбор критерия балансировки нагрузки

port-channel load-balance {dst-ip | dst-mac | src-dst-ip | src-dst-mac | src-ip | src-mac}

– просмотр краткой информации о параметрах интерфейсов EtherChannel, настроенных на коммутаторе:

show etherchannel summary

– просмотр подробной информации о параметрах интерфейсов EtherChannel, настроенных на коммутаторе:

show interfaces etherchannel или show etherchannel detail

– просмотр метода балансировки нагрузки:

show etherchannel load-balance

Настройка VTP на коммутаторах Cisco

Настройка VTP:

– вход в глобальный режим конфигурации

configure terminal

– настройка режима работы VTP на коммутаторе

VTP mode [server | client | transparent]

– настройка домена VTP

VTP domain «domain_name»

– настройка пароля VTP

VTP password «password»

– настройка версии VTP

VTP version «version»

– просмотр параметров работы VTP на коммутаторе:

show VTP status

show VTP password

Настройка Subinterfaces на маршрутизаторах Cisco

Создание сабинтерфейса в определенном VLAN, на порту маршрутизатора, подключенном к порту коммутатора, настроенному в режиме транка:

– вход в глобальный режим конфигурации

configure terminal

– вход в режим конфигурирования интерфейса порта

interface «interface-id»

– вход в глобальный режим конфигурации

configure terminal

– вход в режим конфигурирования сабинтерфейса

interface «interface-id. subinterface-id»

(рекомендуется, чтобы Subinterface-ID = VLAN-ID)

– настройка инкапсуляции 802.1Q для поддержки нужной VLAN

encapsulation dot1Q «vlan-id»

– настройка IP-адреса

ip address address netmask

После настройки всех сабинтерфейсов необходимо в режиме конфигурации основного интерфейса включить его командой No Shutdown.

– просмотр настройки и состояния интерфейсов на маршрутизаторе

show ip interface brief

– просмотр таблицы маршрутизации на маршрутизаторе

show ip route

2.2. Лабораторная работа «VLAN, 802.1Q, EtherChannel L2, VTP»

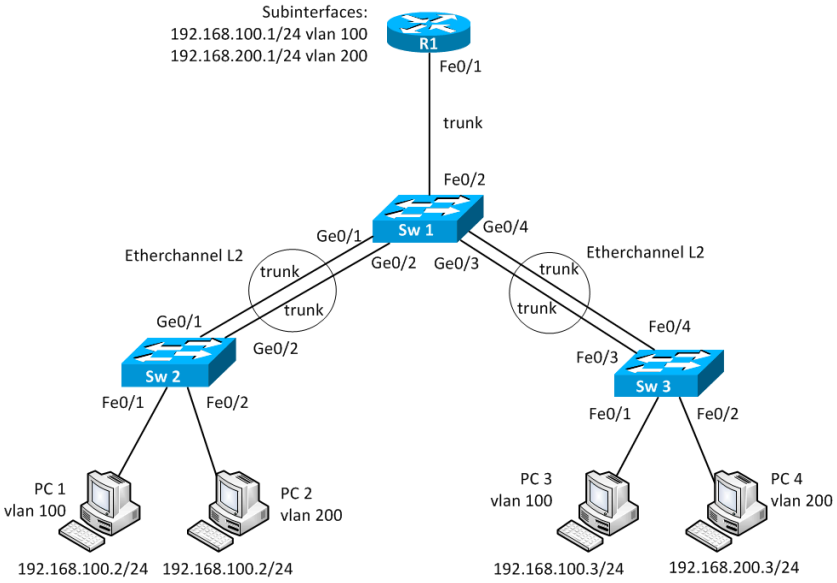


Рис. 2.9. Топология сети

Коммутационное поле

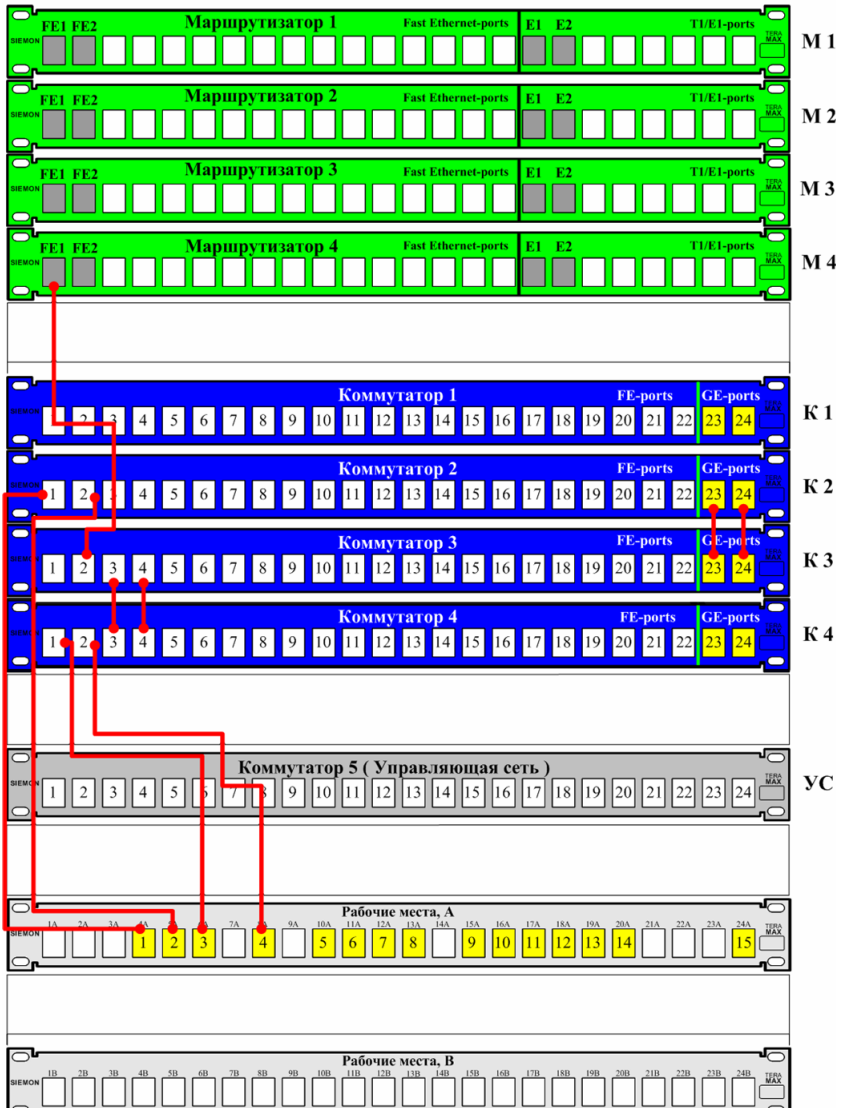


Рис. 2.10. Соединения на патч-панели

Соберите топологию, указанную на рис. 2.9, соединив разъемы на патч-панели патчкордами типа Straight-Touch (рис. 2.10). Проведите начальную конфигурацию коммутаторов и маршрутизатора. Для доступа к коммутаторам используйте терминальный сервер:

– для доступа к sw2.lab запустите telnet 192.168.0.110 2004;

– для доступа к sw3.lab запустите telnet 192.168.0.110 2005;

– для доступа к sw4.lab запустите telnet 192.168.0.110 2006;

– для доступа к r4.lab запустите telnet 192.168.0.110 2010.

* Имя student, пароль student.

Если коммутаторы и маршрутизаторы не настраивались ранее, выполните начальную конфигурацию коммутаторов (имя устройства, логин (student) и пароль доступа (student) на терминальные и консольные линии доступа). **Выполните данную последовательность команд для коммутатора из привилегированного режима EXEC Cisco IOS (меняя имя коммутатора естественно):**

```
conf t
hostname sw1.lab
service password-encryption
username student privilege 15 secret 0 student
no ip domain-lookup
banner motd ^C
_____________________________________________________
sw1.lab

PERM, Russia,
Network technology lab. IT department. PSTU

Warning: Authorized access only!!!
Disconnect IMMEDIATELY if you are not an authorized
person!!!

Contact information:
web http://wrls.ru
email support@wrls.ru
tel +7(342)220-63-85
_____________________________________________________^C
```

```
line con 0
login local
line vty 0 4
login local
line vty 5 15
login local
```

Для маршрутизатора из привилегированного режима EXEC Cisco IOS (меняя имя маршрутизатора естественно):

```
conf t
hostname r1.lab
service password-encryption
no ip domain-lookup
username student privilege 15 secret 0 student
banner motd ^C
_____________________________________________________

r1.lab

PERM, Russia,
Network technology lab. IT department. PSTU

Warning: Authorized access only!!!
Disconnect IMMEDIATELY if you are not an authorized
person!!!

Contact information:
web http://wrls.ru
email support@wrls.ru
tel +7(342)220-63-85
_____________________________________________________^C
line con 0
login local
line aux 0
line vty 0 4
login local
line vty 5 15
login local
```

Настройте тип media rj45 на гигабитных комбинированных портах и транки на коммутаторах с Native VLAN 99 согласно топологии:

```
Sw2:
sw2.lab#configure terminal
sw2.lab(config)#interface GigabitEthernet0/1
sw2.lab(config-if)#switchport trunk native vlan 99
sw2.lab(config-if)#switchport mode trunk
sw2.lab(config-if)#media-type rj45
sw2.lab(config-if)#interface GigabitEthernet0/2
sw2.lab(config-if)#switchport trunk native vlan 99
sw2.lab(config-if)#switchport mode trunk
sw2.lab(config-if)#media-type rj45

Sw3:
sw3.lab#configure terminal
sw3.lab(config)#interface FastEthernet0/3
sw3.lab(config-if)#switchport trunk native vlan 99
sw3.lab(config-if)#switchport mode trunk
sw3.lab(config-if)#interface FastEthernet0/4
sw3.lab(config-if)#switchport trunk native vlan 99
sw3.lab(config-if)#switchport mode trunk
sw3.lab(config)#interface GigabitEthernet0/1
sw3.lab(config-if)#switchport trunk native vlan 99
sw3.lab(config-if)#switchport mode trunk
sw3.lab(config-if)#media-type rj45
sw3.lab(config-if)#interface GigabitEthernet0/2
sw3.lab(config-if)#switchport trunk native vlan 99
sw3.lab(config-if)#switchport mode trunk
sw3.lab(config-if)#media-type rj45

Sw4:
sw4.lab#configure terminal
sw4.lab(config)#interface FastEthernet0/3
sw4.lab(config-if)#switchport trunk native vlan 99
sw4.lab(config-if)#switchport mode trunk
sw4.lab(config-if)#interface FastEthernet0/4
sw4.lab(config-if)#switchport trunk native vlan 99
sw4.lab(config-if)#switchport mode trunk
```

Объедините созданные транки в EtherChannel:

```
Sw2:
sw2.lab#configure terminal
sw2.lab(config)#interface GigabitEthernet0/1
sw2.lab(config-if)#channel-group 1 mode on
sw2.lab(config-if)#interface GigabitEthernet0/2
sw2.lab(config-if)#channel-group 1 mode on

Sw3:
sw3.lab#configure terminal
sw3.lab(config)#interface GigabitEthernet0/1
sw3.lab(config-if)#channel-group 1 mode on
sw3.lab(config-if)#interface GigabitEthernet0/2
sw3.lab(config-if)#channel-group 1 mode on
sw3.lab(config)#interface FastEthernet0/3
sw3.lab(config-if)#channel-group 2 mode on
sw3.lab(config-if)#interface FastEthernet0/4
sw3.lab(config-if)#channel-group 2 mode on

Sw4:
sw4.lab#configure terminal
sw4.lab(config)#interface FastEthernet0/3
sw4.lab(config-if)#channel-group 1 mode on
sw4.lab(config-if)#interface FastEthernet0/4
sw4.lab(config-if)#channel-group 1 mode on
```

Скорректируйте Native VLAN на созданных интерфейсах EtherChannel:

```
Sw2:
sw2.lab#configure terminal
sw2.lab(config)#interface Port-channel1
sw2.lab(config-if)# switchport trunk native vlan 99

Sw3:
sw3.lab#configure terminal
sw3.lab(config)#interface Port-channel1
sw3.lab(config-if)#switchport trunk native vlan 99
sw3.lab(config-if)#interface Port-channel2
sw3.lab(config-if)#switchport trunk native vlan 99
Sw4:
sw4.lab#configure terminal
```

```
sw4.lab(config)#interface Port-channel1
sw4.lab(config-if)#switchport trunk native vlan 99
```

Настройте метод балансировки нагрузки по MAC-адресу Destination на логических интерфейсах EtherChannel:

```
Sw2:
sw2.lab#configure terminal
sw2.lab(config)#port-channel load-balance dst-mac

Sw3:
sw3.lab#configure terminal
sw3.lab(config)#port-channel load-balance dst-mac

Sw4:
sw4.lab#configure terminal
sw4.lab(config)#port-channel load-balance dst-mac
```

Настройте VTP-server на Sw3, VTP-client на Sw2 и Sw4. Версия VTP – 2, домен – itas, пароль – mypass. Добавьте VLAN's 100 и 200 на Sw3:

```
Sw2:
sw2.lab(config)#vtp mode client
sw2.lab(config)#vtp version 2
sw2.lab(config)#vtp domain itas
sw2.lab(config)#vtp password mypass

Sw3:
sw3.lab(config)#vtp mode server
sw3.lab(config)#vtp version 2
sw3.lab(config)#vtp domain itas
sw3.lab(config)#vtp password mypass
sw3.lab(config)#vlan 100
sw3.lab(config-vlan)#name vl100
sw3.lab(config-vlan)#vlan 200
Switch(config-vlan)#name vl200

Sw4:
sw4.lab (config)#vtp mode client
sw4.lab (config)#vtp version 2
sw4.lab (config)#vtp domain itas
sw2.lab (config)#vtp password mypass
```

В случае если транки и EtherChannel настроены правильно, вывод команд Show Interfaces Trunk, Show EtherChannel Summary, Show EtherChannel Detail будет следующим:

```
Sw2:
sw2.lab#show interfaces trunk
Port Mode Encapsulation Status Native vlan
Po1 on 802.1q trunking 99
*На интерфейсе Port-Channel 1 настроен транк 802.1q с Native VLAN 99.
Port Vlans allowed on trunk
Po1 1-4094

Port Vlans allowed and active in management domain
Po1 1-3, 10, 17, 20, 100, 200

Port Vlans in spanning tree forwarding state and not pruned
Po1 1-3, 10, 17, 20, 100, 200
*Список VLAN, трафику которых разрешено идти по интерфейсу Port-Channell.
sw2.lab#show etherchannel summary
Flags: D - down P - in port-channel
I - stand-alone s - suspended
H - Hot-standby (LACP only)
R - Layer3 S - Layer2
U - in use f - failed to allocate aggregator
u - unsuitable for bundling
w - waiting to be aggregated
d - default port

Number of channel-groups in use: 1
Number of aggregators: 1

Group Port-channel Protocol Ports
------+-------------+--------+------
1 Po1(SU) - Gi0/1(P) Gi0/2(P)
* Интерфейс Port-Channell - работает на L2, состоит из портов Gi0/1 и Gi0/2, оба из которых работают.
```

```
sw2.lab#show etherchannel detail
Channel-group listing:
----------------------

Group: 1
----------
Group state = L2
Ports: 2 Maxports = 8
Port-channels: 1 Max Port-channels = 1
Protocol: -
Ports in the group:
-------------------
Port: Gi0/1
------------

Port state = Up Mstr In-Bndl
Channel group = 1 Mode = On/FEC Gcchange = -
Port-channel = Po1 GC = - Pseudo port-channel = Po1
Port index = 0 Load = 0x00 Protocol = -
*Режим работы EtherChannel - on.
Age of the port in the current state: 00d:00h:57m:21s

Port: Gi0/2
------------

Port state = Up Mstr In-Bndl
Channel group = 1 Mode = On/FEC Gcchange = -
Port-channel = Po1 GC = - Pseudo port-channel = Po1
Port index = 0 Load = 0x00 Protocol = -

Age of the port in the current state: 00d:00h:57m:34s

Port-channels in the group:
---------------------------

Port-channel: Po1
------------

Age of the Port-channel = 00d:00h:57m:34s
Logical slot/port = 2/1 Number of ports = 2
GC = 0x00000000 HotStandBy port = null
```

```
    Port state = Port-channel Ag-Inuse
    Protocol = -

    Ports in the Port-channel:

    Index Load Port EC state No of bits
    -----+----+----+--------+------------
    0  00 Gi0/1 On/FEC 0
    0  00 Gi0/2 On/FEC 0

    Sw3:
    sw3.lab#show interfaces trunk
      Port    Mode   Encapsulation  Status  Native  vlan
      Po1     on        802.1q     trunking   99
      Po2     on        802.1q     trunking   99

    Port Vlans allowed on trunk
    Po1 1-4094
    Po2 1-4094

    Port Vlans allowed and active in management domain
    Po1 1-3,10,17,20,100,200
    Po2 1-3,10,17,20,100,200

    Port Vlans in spanning tree forwarding state and
not pruned
    Po1 1-3,10,17,20,100,200
    Po2 1-3,10,17,20,100,200

    sw3.lab#show etherchannel summary
    Flags: D - down P - bundled in port-channel
    I - stand-alone s - suspended
    H - Hot-standby (LACP only)
    R - Layer3 S - Layer2
    U - in use f - failed to allocate aggregator

    M - not in use, minimum links not met
    u - unsuitable for bundling
    w - waiting to be aggregated
    d - default port
```

```
Number of channel-groups in use: 2
Number of aggregators: 2

Group Port-channel   Protocol Ports
------+-------------+---------+------
1  Po1(SU)  -  Gi0/1(P)  Gi0/2(P)
2  Po2(SU)  -Fa0/3(P)  Fa0/4(P)

sw3.lab#show etherchannel detail
Channel-group listing:
----------------------
Group: 1
----------
Group state = L2
Ports: 2 Maxports = 8
Port-channels: 1 Max Port-channels = 1
Protocol: -
Minimum Links: 0
Ports in the group:
-------------------
Port: Gi0/1
------------

Port state = Up Mstr In-Bndl
Channel group = 1 Mode = On Gcchange = -
Port-channel = Po1 GC = - Pseudo port-channel = Po1
Port index = 0 Load = 0x00 Protocol = -

Age of the port in the current state: 0d:01h:00m:53s

Port: Gi0/2
------------

Port state = Up Mstr In-Bndl
Channel group = 1 Mode = On Gcchange = -
Port-channel = Po1 GC = - Pseudo port-channel = Po1
Port index = 0 Load = 0x00 Protocol = -

Age of the port in the current state: 0d:01h:01m:00s

Port-channels in the group:
---------------------------
```

```
Port-channel: Po1
------------
Age of the Port-channel = 0d:01h:01m:00s
Logical slot/port = 2/1 Number of ports = 2
GC = 0x00000000 HotStandBy port = null
Port state = Port-channel Ag-Inuse
Protocol = -
Port security = Disabled

Ports in the Port-channel:

   Index       Load       Port      EC state  No of bits
     0         00         Gi0/1       On         0
     0         00         Gi0/2       On         0

Time since last port bundled: 0d:01h:00m:54s Gi0/1

Group: 2
----------
Group state = L2
Ports: 2 Maxports = 8
Port-channels: 1 Max Port-channels = 1
Protocol: -
Minimum Links: 0
Ports in the group:
-------------------
Port: Fa0/3
------------

Port state = Up Mstr In-Bndl
Channel group = 2 Mode = On Gcchange = -
Port-channel = Po2 GC = - Pseudo port-channel = Po2
Port index = 0 Load = 0x00 Protocol = -

Age of the port in the current state: 0d:00h:55m:25s

Port: Fa0/4
------------

Port state = Up Mstr In-Bndl
Channel group = 2 Mode = On Gcchange = -
Port-channel = Po2 GC = - Pseudo port-channel = Po2
```

```
    Port index = 0 Load = 0x00 Protocol = -

    Age of the port in the current state: 0d:00h:55m:17s

    Port-channels in the group:
    ---------------------------

    Port-channel: Po2
    ------------

    Age of the Port-channel = 0d:00h:55m:27s
    Logical slot/port = 2/2 Number of ports = 2
    GC = 0x00000000 HotStandBy port = null
    Port state = Port-channel Ag-Inuse
    Protocol = -
    Port security = Disabled

    Ports in the Port-channel:

       Index       Load       Port     EC state  No of bits
         0          00        Fa0/3       On          0
         0          00        Fa0/4       On          0

    Sw4:
    sw4.lab#show interfaces trunk
    Port Mode Encapsulation Status Native vlan
    Po1 on 802.1q trunking 99

    Port Vlans allowed on trunk
    Po1 1-4094

    Port Vlans allowed and active in management domain
    Po1 1-3,10,17,20,100,200

    Port Vlans in spanning tree forwarding state and not
pruned
    Po1 1-3,10,17,20,100,200

    sw4.lab#show etherchannel summary
    Flags: D - down P - bundled in port-channel
    I - stand-alone s - suspended
    H - Hot-standby (LACP only)
```

```
R - Layer3 S - Layer2
U - in use f - failed to allocate aggregator

M - not in use, minimum links not met
u - unsuitable for bundling
w - waiting to be aggregated
d - default port

Number of channel-groups in use: 1
Number of aggregators: 1

     Group        Port-channel     Protocol    Ports
       1            Po1(SU)         Fa0/3(P)   Fa0/4(P)

sw4.lab#show etherchannel detail
Channel-group listing:
----------------------

Group: 1
----------
Group state = L2
Ports: 2 Maxports = 8
Port-channels: 1 Max Port-channels = 1
Protocol: -
Minimum Links: 0
Ports in the group:
-------------------
Port: Fa0/3
------------

Port state = Up Mstr In-Bndl
Channel group = 1 Mode = On Gcchange = -
Port-channel = Po1 GC = - Pseudo port-channel = Po1
Port index = 0 Load = 0x00 Protocol = -

Age of the port in the current state: 0d:00h:45m:49s

Port: Fa0/4
------------

Port state = Up Mstr In-Bndl
Channel group = 1 Mode = On Gcchange = -
```

```
Port-channel = Po1 GC = - Pseudo port-channel = Po1
Port index = 0 Load = 0x00 Protocol = -

Age of the port in the current state: 0d:01h:00m:11s

Port-channels in the group:
---------------------------

Port-channel: Po1
------------

Age of the Port-channel = 0d:01h:00m:11s
Logical slot/port = 2/1 Number of ports = 2
GC = 0x00000000 HotStandBy port = null
Port state = Port-channel Ag-Inuse
Protocol = -
Port security = Disabled

Ports in the Port-channel:

   Index       Load       Port       EC state  No of bits
     0          00        Fa0/3        On          0
     0          00        Fa0/4        On          0
```

В случае если VTP настроен правильно, вывод команд Show VTP Status, Show VTP Password будет следующим:

```
Sw2:
sw2.lab#show vtp status
VTP Version : 2
Configuration Revision : 3
Maximum VLANs supported locally : 255
Number of existing VLANs: 12
VTP Operating Mode: Client
VTP Domain Name: itas
VTP Pruning Mode: Disabled
VTP V2 Mode: Enabled
VTP Traps Generation: Disabled
MD5 digest: 0xD9 0x1A 0x61 0x48 0x07 0x0B 0xC5 0x02
Configuration last modified by 0.0.0.0 at 7-7-93
06:25:16
```

*Домен VTP – itas, версия – 2, ревизия конфигурации – 3, режим работы – клиент.

```
sw2.lab#show vtp password
VTP Password: mypass
```

*Пароль VTP.

```
Sw3:
sw3.lab#show vtp status
VTP Version: running VTP2
Configuration Revision: 3
Maximum VLANs supported locally: 255
Number of existing VLANs: 12
VTP Operating Mode: Server
VTP Domain Name: itas
VTP Pruning Mode: Disabled
VTP V2 Mode: Enabled
VTP Traps Generation: Disabled
MD5 digest: 0xD9 0x1A 0x61 0x48 0x07 0x0B 0xC5 0x02
Configuration last modified by 0.0.0.0 at 7-7-93 06:25:16
Local updater ID is 0.0.0.0 (no valid interface found)

sw3.lab#show vtp password
VTP Password: mypass

Sw4:
sw4.lab#show vtp status
VTP Version: running VTP2
Configuration Revision: 3
Maximum VLANs supported locally: 255
Number of existing VLANs: 12
VTP Operating Mode: Client
VTP Domain Name: itas
VTP Pruning Mode: Disabled
VTP V2 Mode: Enabled
VTP Traps Generation: Disabled
MD5 digest: 0xD9 0x1A 0x61 0x48 0x07 0x0B 0xC5 0x02
Configuration last modified by 0.0.0.0 at 7-7-93 06:25:16
```

```
sw4.lab#show vtp password
VTP Password: mypass
```

Настройте порты Fa0/1 и Fa0/2 на коммутаторах Sw2 и Sw4 для работы с VLAN:

```
Sw2:
sw2.lab#configure terminal
sw2.lab(config)#interface FastEthernet0/1
sw2.lab(config-if)#switchport access vlan 100
sw2.lab(config-if)#switchport mode access
sw2.lab(config-if)#interface FastEthernet0/2
sw2.lab(config-if)#switchport access vlan 200
sw2.lab(config-if)#switchport mode access

Sw4:
sw4.lab#configure terminal
sw4.lab(config)#interface FastEthernet0/1
sw4.lab(config-if)#switchport access vlan 100
sw4.lab(config-if)#switchport mode access
sw4.lab(config-if)#interface FastEthernet0/2
sw4.lab(config-if)#switchport access vlan 200
sw4.lab(config-if)#switchport mode access
```

В случае если порты Fa0/1 и Fa0/2 на коммутаторах Sw2 и Sw4 настроены правильно, вывод команды Show VLAN будет следующим:

```
Sw2:
sw2.lab#show vlan
 VLAN   Name   Status             Ports
   1   default  active Fa0/3, Fa0/4, Fa0/5, Fa0/6
                       Fa0/7, Fa0/8, Fa0/9, Fa0/10
                       Fa0/11, Fa0/12, Fa0/13, Fa0/14
                       Fa0/15, Fa0/16, Fa0/17, Fa0/18
                       Fa0/19, Fa0/20, Fa0/21, Fa0/22
                       Fa0/23, Fa0/24
   2    VLAN_1  active
   3    VLAN_2  active
  10    vlan10  active
  17    test17  active
  20    test20  active
```

```
   100    vl100   active Fa0/1
   200    vl200   active Fa0/2
*Порт Fa0/1 помещен в VLAN vl100, порт Fa0/2 в vl200.
1002 fddi-default act/unsup
1003 trcrf-default act/unsup
1004 fddinet-default act/unsup
1005 trbrf-default act/unsup

VLAN  Type  SAID  MTU  Parent  RingNo  BridgeNo  Stp
BrdgMode Trans1 Trans2
--- --- ------- --- ---- ---- ----- --- ----- ---- ---

VLAN Type  SAID   MTU  Pa-  RingNo BridgeNo Stp  BrdgMode Trans1 Trans2
                       rent
  1  enet    1   1500 -     -       -      -      -       0      0
  2  enet 100002 1500 -     -       -      -      -       0      0
  3  enet 100003 1500 -     -       -      -      -       0      0
 10  enet 100010 1500 -     -       -      -      -       0      0
 17  enet 100017 1500 -     -       -      -      -       0      0
 20  enet 100020 1500 -     -       -      -      -       0      0
100  enet 100100 1500 -     -       -      -      -       0      0
200  enet 100200 1500 -     -       -      -      -       0      0
1002 fddi 101002 1500 -     -       -      -      -       0      0
1003 trcrf 101003 4472 1005  3276    -      -    srb       0      0
1004 fdnet 101004 1500 -     -       -    ieee     -       0      0
1005 trbrf 101005 4472 -     -      15    ibm      -       0      0

   VLAN    AREHops  STEHops         Backup CRF
   1003       7        7               off

Remote SPAN VLANs
------- ---- ------

Primary Secondary Type Ports
------- -------- ------ -------

Sw4:
sw4.lab#show vlan

  VLAN   Name   Status              Ports
    1   default  active Fa0/5, Fa0/6, Fa0/7, Fa0/8
                       Fa0/9, Fa0/10, Fa0/11, Fa0/12
                       Fa0/13, Fa0/14, Fa0/15, Fa0/16
```

```
                                  Fa0/17, Fa0/18, Fa0/19, Fa0/20
                                  Fa0/21, Fa0/22, Fa0/23, Fa0/24
                                  Gi0/1, Gi0/2
   2    VLAN_1  active
   3    VLAN_2  active
  10    vlan10  active
  17    test17  active
  20    test20  active
 100    vl100   active  Fa0/1
 200    vl200   active  Fa0/2
1002    fddi    default act/unsup
1003    trcrf   default act/unsup
1004    fddinet default act/unsup
1005    trbrf   default act/unsup

    VLAN  Type  SAID  MTU  Parent  RingNo  BridgeNo  Stp
BrdgMode Trans1 Trans2
     --- --- ------- --- ---- ---- ----- --- ----- ---- ---

VLAN Type  SAID   MTU  Pa-  RingNo BridgeNo Stp  BrdgMode Trans1 Trans2
                       rent
  1  enet    1   1500  -     -       -       -      -       0      0
  2  enet 100002 1500  -     -       -       -      -       0      0
  3  enet 100003 1500  -     -       -       -      -       0      0
 10  enet 100010 1500  -     -       -       -      -       0      0
 17  enet 100017 1500  -     -       -       -      -       0      0
 20  enet 100020 1500  -     -       -       -      -       0      0
100  enet 100100 1500  -     -       -       -      -       0      0
200  enet 100200 1500  -     -       -       -      -       0      0
1002 fddi 101002 1500  -     -       -       -      -       0      0
1003 trcrf 101003 4472 1005  3276    -       -    srb       0      0
1004 fdnet 101004 1500 -     -       -     ieee   -         0      0
1005 trbrf 101005 4472 -     -      15     ibm    -         0      0

        VLAN    AREHops  STEHops         Backup CRF
        1003       7        7               off

    Remote SPAN VLANs
    ------------------------------------------------------------

    Primary Secondary Type Ports
    ------- --------- -------------- ---------------------
```

Протестируйте работу VLAN-сетей

Компьютер PC1 с адресом 192.168.100.2:

– послать эхо-запросы ping к узлу PC3 с адресом 192.168.100.3 – работает (пинги пойдут не сразу, так как нужно время, чтобы заполнить таблицы MAC-адресов на всех коммутаторах);

– послать эхо-запросы ping к узлам PC4 и PC5 с адресами 192.168.200.2 и 192.168.200.3 – не работает.

Маршрутизация между VLAN. Существует два подхода к маршрутизации пакетов между VLAN. Первый – выделить на коммутаторе и роутере отдельный порт под каждую VLAN, но данный подход очень расточителен. Второй – создать между коммутатором и маршрутизатором транк, и на маршрутизаторе сделать виртуальные интерфейсы.

Настроим на коммутаторе Sw3 порт Fa0/2 в режим транка:

```
sw3.lab#configure terminal
sw3.lab#interface fastethernet0/2
sw3.lab#switchport mode trunk
```

Настроим на маршрутизаторе сабинтерфейсы на порту Fa0/1 согласно топологии:

```
r4.lab#configure terminal
r4.lab(config)#interface fa0/1.100
r4.lab(config-subif)#encapsulation dot1Q 100
r4.lab(config-subif)#ip    address    192.168.100.1
255.255.255.0
r4.lab(config-subif)#interface fa0/1.200
r4.lab(config-subif)#encapsulation dot1Q 200
r4.lab(config-subif)#ip    address    192.168.200.1
255.255.255.0
r4.lab(config-subif)#interface fa0/1
r4.lab(config-subif)#no shutdown
```

Не забудьте прописать шлюзы по умолчанию на всех PC!

В случае если порты на маршрутизаторе настроены правильно, вывод команд Show IP Int Brief и Show IP Route будет следующим:

```
r4.lab#show ip int brief

     Interface       IP-Address  OK? Method Status Protocol
  FastEthernet0/0    unassigned  YES  NVRAM   down     down
  FastEthernet0/1    unassigned  YES  unset   down     down
FastEthernet0/1.100 192.168.100.1 YES manual   up       up
FastEthernet0/1.200 192.168.200.1 YES manual   up       up
    Serial0/1/0      unassigned  YES manual   down     down
    Serial0/1/1      unassigned  YES  unset   down     down
                                     admini-
                                      stra-
                                     tively
    Serial0/1/2      unassigned  YES  unset   down     down
                                     admini-
                                      stra-
                                     tively
    Serial0/1/3      unassigned  YES  unset   down     down
                                     admini-
                                      stra-
                                     tively

    r4.lab#show ip route
    Codes: C - connected, S - static, R - RIP, M - mo-
bile, B - BGP
    D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF
inter area
    N1 - OSPF NSSA external type 1, N2 - OSPF NSSA ex-
ternal type 2
    E1 - OSPF external type 1, E2 - OSPF external type 2
    i - IS-IS, su - IS-IS summary, 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

    C    192.168.200.0/24    is    directly    connected,
FastEthernet0/1.200
    C    192.168.100.0/24    is    directly    connected,
FastEthernet0/1.100
```

Протестируйте работу маршрутизации между VLAN-сетями

Компьютер PC1 с адресом 192.168.100.2:

– послать эхо-запросы ping к узлу PC3 с адресом 192.168.100.3 – работает;

– послать эхо-запросы ping к узлам PC4 и PC5 с адресами 192.168.200.2 и 192.168.200.3 – работает (пинги пойдут не сразу, так как нужно время, чтобы заполнить таблицы MAC-адресов на всех коммутаторах и ARP-таблицу на маршрутизаторе).

Задания для самостоятельной работы

1. Скорректируйте настройки оборудования так, чтобы PC1 и PC3 были в VLAN 300. Проверьте работу VLAN и маршрутизации между VLAN.

2. Соберите топологию и настройте оборудование так, чтобы EtherChannel между Sw2 и Sw3 состоял не из Ge0/1 и Ge0/2, а из Fa0/6 и Fa0/7.

3. Запустите команду Show Spanning-Tree VLAN 100 Detail на Sw3. Как STP видит EtherChannel?

Вопросы для самопроверки

1. Что такое VLAN?
2. Зачем нужен VLAN?
3. Что такое транк?
4. Зачем нужен тег?
5. Какой размер имеет тег и какие поля он включает?
6. Что такое агрегирование каналов?
7. Что дает агрегирование каналов?
8. Каким образом можно объединить несколько VLAN?
9. Назовите основные способы образования VLAN?
10. Зачем нужен протокол VTP?
11. Назовите режимы коммутаторов в VTP.
12. Из каких полей состоит кадр VTP?
13. Как передаются VTP-кадры?

3. ПРОТОКОЛ IP

3.1. Краткие теоретические сведения

3.1.1. IP-адрес

Что такое адрес вообще

Адрес – идентификатор для нахождения объекта (согласно некоторым правилам его интерпретации). Адреса обычно имеют иерархический вид. Каждая часть имеет более специфическую подробность.

Пример. Способ нахождения МГФ:

- +7 342 2378376 (рис. 3.1)
- www.icmm.ru/~masich
- masich@icmm.ru
- 195.69.156.87

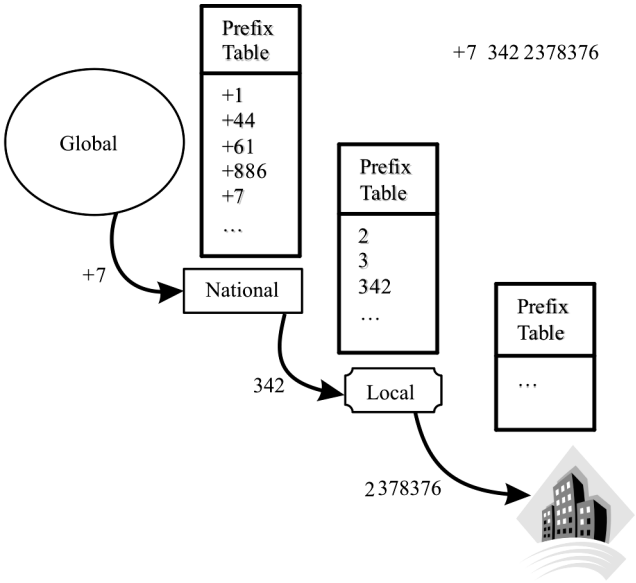


Рис. 3.1. Маршрутизация в телефонных сетях

Что такое IP-адрес

IP-адрес – идентификатор Интернета, информирующий о том, как достигнуть сетевой локализации через маршрутизирующую систему Интернета (СПД).

IPv4: 32-битовое число (4 байта). Байты пишутся в десятичной форме, разделяются точками. Пример: 172.16.58.7. В IPv4 могут быть 4 миллиарда различных хост-адресов (2^{32}).

IPv6: 128-битовое число (16 байт). Пишется в шестнадцатеричной-десятичной нотации. Пример: 2001:0503:0C27:0000:0000:0000:0000:0000. В IPv6 могут быть 16 миллиардов различных сетевых адресов (2^{128}).

Назначение IP-адреса:

– необходим для маршрутизации в Интернете;

– является конечным «Общественным ресурсом»; не находящийся в собственности пользователя адрес. Не свойство. Не может быть куплен, продан, передан. Предоставляется на непостоянной основе для использования. Возвращается, когда больше не требуется;

Иерархическая организация IP-адресов.

IP-адрес позволяет рассматривать группы адресов (сеть/подсеть) как единое целое до тех пор, пока не потребуется определить адрес индивидуального узла (порт хоста).

Иллюстрация IPv4 (рис. 3.2):

– Адрес сети – 172.16.0.0/16, где «/xx» – количество старших бит, используемых для нумерации сети и называемых префиксом сети.

– Адрес подсети – 172.16.14.0/24 в сети 172.16.0.0/16.

– Адрес хоста/порта – 172.16.14.15 в сети 172.16.0.0/16 (и подсети 172.16.14.0/24).

Пример работы IP-адреса

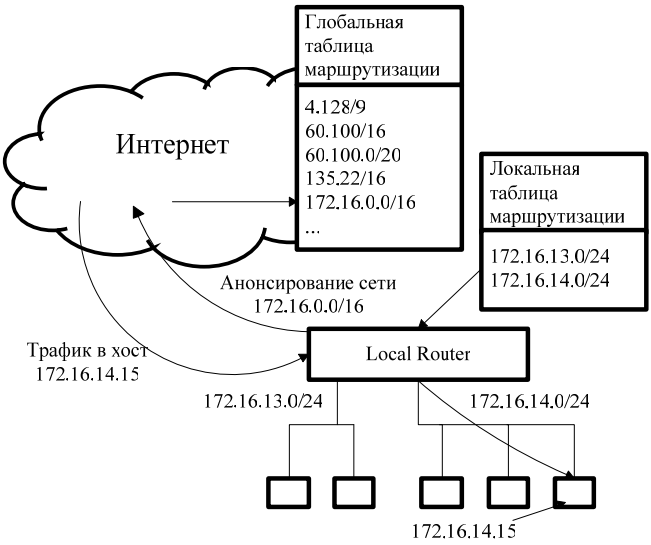


Рис. 3.2. Маршрутизация в Интернете

Кто распределяет IP-адреса

Региональные интернет-регистратуры (Regional Internet Registry – RIR) – организации, занимающиеся вопросами адресации и маршрутизации в Интернете. На 2006 год существуют пять RIR (рис. 3.3):

1. American Registry for Internet Numbers (ARIN) для Северной Америки.

2. RIPE Network Coordination Centre (RIPE NCC) для Европы, Ближнего Востока и Центральной Азии.

3. Asia-Pacific Network Information Centre (APNIC) для Азии и Тихоокеанского региона.

4. Latin American and Caribbean Internet Addresses Registry (LACNIC) для Латинской Америки и Карибского региона.

5. African Network Information Centre (AfriNIC) для Африки.

Рис. 3.3. Карта региональных интернет-регистратур

3.1.2. Основные понятия IP-маршрутизации

Маршрутизация (Routing) – это процесс перемещения пакета от источника к приемнику через сеть передачи данных.

Роутер (Router) – это устройство, передающее пакет в нужном направлении (нужный интерфейс).

Маршрутизируемый протокол (Routed Protocol, IP-протокол) существует в каждом роутере для передачи пакета в нужном направлении.

Нужное направление передачи роутер определяет на основании таблицы маршрутизации (Forwarding Tables). Таблицы маршрутизации формируются протоколами маршрутизации (Routing Protocol – RIP, OSPF, IGRP, IS-IS, BGP-4).

Протокол маршрутизации – это распределенный протокол, работающий координированно с другими роутерами.

Цели работы протокола маршрутизации – изучение и формирование глобального представления сети непротиворечивым и законченным способом.

Протоколы маршрутизации работают по алгоритмам маршрутизации (DVA – дистанционно-векторный, LSA – состояния связей).

Процесс формирования маршрутной таблицы

При инсталляции на роутерах запускаются протоколы маршрутизации, которые обмениваются маршрутной информацией с «соседями».

Информация о маршрутах «соседей» используется для формирования своих таблиц маршрутизации (табл. 3.1, 3.2). На основе таблиц выбирают один или несколько путей для доставки пакетов в пункт назначения.

Таблица 3.1

Таблица маршрутизации R1. Протокол RIP.
Метрика – число хопов

Сеть назначения	Следующий узел (Next Hop)	Исходящий интерфейс	Метрика
192.168.1.0/24	Подключен	e0	–
192.168.2.0/24	Подключен	s0	–
192.168.3.0/24	Подключен	s1	–
192.168.4.0/24	192.168.2.2	s0	1
192.168.4.0/24	192.168.3.2	s1	1
192.168.5.0/24	192.168.2.2	s0	1
192.168.6.0/24	192.168.3.2	s1	1

Таблица 3.2

Таблица маршрутизации R1. Протокол OSPF.
Метрика – скорость канала

Сеть назначения	Следующий узел (Next Hop)	Исходящий интерфейс	Метрика
192.168.1.0/24	Подключен (E0)	e0	–
192.168.2.0/24	Подключен (S0)	s0	–
192.168.3.0/24	Подключен (S1)	s1	–
192.168.4.0/24	192.168.3.2 (S1)	s1	60
192.168.5.0/24	192.168.2.2 (S0)	s1	130
192.168.6.0/24	192.168.3.2 (S1)	s1	70

Роутеры взаимодействуют при передаче трафика с соседями (следующими ближайшими устройствами – Next-Hop Devices).

Информация о пересылке до следующих ближайших устройств сети (IP-адреса соседних устройств и исходящий интерфейс) помещается в таблицу маршрутов (Forwarding Table).

Определение оптимального маршрута (метрика)

1. Решение о лучшем маршруте принимается на основании метрики.

2. Метрика – это стандарт измерения (число), используемый протоколами маршрутизации.

3. Когда в роутер поступает пакет, роутер анализирует заголовок и выделяет IP-адрес получателя.

4. Затем роутер сопоставляет IP-адрес получателя с информацией в таблице маршрутов пересылки (Forwarding Table) и получает сведения:

– об исходящем интерфейсе (через какой порт передавать);

– IP-адресе следующего ближайшего устройства, откуда можно попасть в пункт назначения.

5. Кроме того, роутер выполняет все необходимые дополнительные функции (уменьшение «времени жизни» – TTL, управление параметрами «тип сервиса» – TOS, фрагментацию и отработку опций при необходимости).

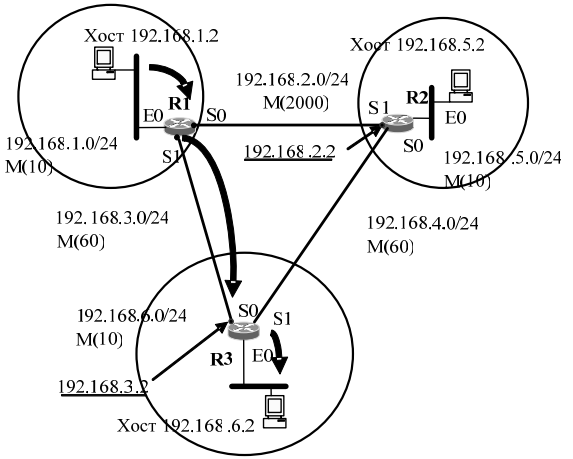


Рис. 3.4. Использование протоколов маршрутизации

Примеры маршрутизации

Движение: хост 192.168.1.2 –> хост 192.168.6.2 (рис. 3.4)

3.1.3. Две модели адресации и маршрутизации

Классовая модель. Фиксируется длина префикса («/xx» = const) подсетей, на которые разбита главная сеть. Одинаковый размер подсетей конфигурируется сетевым администратором.

Протоколам маршрутизации (RIPv1) не требуется передавать префикс подсети в сообщениях Routing Updates, поскольку все подсети в главной сети одинакового размера.

Бесклассовая модель (VLSM, CIDR). Допускает переменное (VLSM, CIDR) значение префикса («/xx» = var) подсетей, на которые разбивается главная сеть, поэтому протоколам маршрутизации (RIPv2, OSPF, BGP-4) требуется передавать длину префикса подсети в сообщениях Routing Updates.

3.1.3.1. Классовая модель адресации (Classful Model)

IP-адрес состоит из двух логических частей – номера сети и номера узла в сети. Значения первых битов адреса определяют границу логических частей и класс IP-адреса. На рис. 3.5 показана структура IP-адреса разных классов.

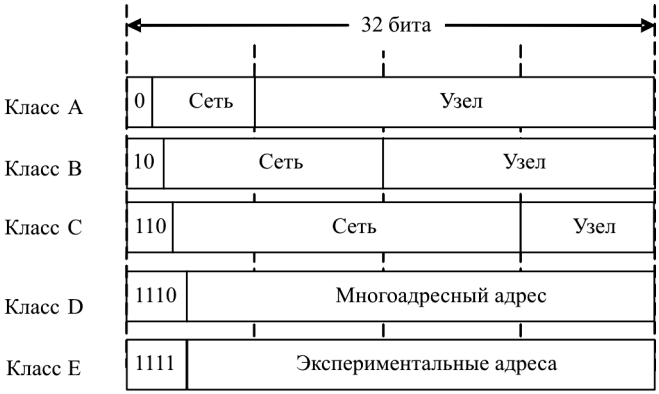


Рис. 3.5. Структура IP-адреса

Несколько адресов во всех классах зарезервированы для специальных целей.

Распределение специальных IP-адресов:

Диапазон адресов	Назначение
0.0.0.0	Неизвестная сеть (сеть по умолчанию)
10.0.0.0–10.255.255.255	Зарезервировано для частных сетей (RFC1918)
127.0.0.1–127.255.255.255	Зарезервировано для локальных адресов типа «петля»
172.16.0.0–172.31.255.255	Зарезервировано для частных сетей (RFC1918)
192.168.0.0–192.168.255.255	Зарезервировано для частных сетей (RFC1918)
255.255.255.255	Широковещательный адрес

Поскольку адрес 0.0.0.0 класса A не является нормальным, то реально в сетях класса A доступно $127 = (2^7 - 1)$ адресов.

Рассмотрим пример сети класса B:

Номер сети	Номер узла	Комментарий
172.17	0.0	IP-адрес сети
172.17	0.1	Первый IP-адрес хоста в этой сети
172.17	0.2	Второй IP-адрес хоста в этой сети
172.17	255.254	Последний IP-адрес хоста в этой сети
172.17	255.255	Направленный широковещательный IP-адрес для этой сети

Поэтому максимально возможное значение числа IP-адресов для назначения их хостам уменьшено на 2.

Организация подсетей

Идея – «заимствование» нескольких битов из узловой части адреса для разбиения сети на подсети.

Полный префикс сети, состоящий из сетевого префикса и номера подсети, получил название расширенного сетевого префикса.

Двоичное, или его десятичный эквивалент, содержащее единицы в разрядах, относящихся к расширенному сетевому префиксу, а в остальных разрядах – нули, назвали маской подсети. Такое представление не очень удобно, чаще используют обозначение

вида «/xx», где xx – количество бит в расширенном сетевом префиксе. Тогда классы IP-адресов по умолчанию используют маски, представленные на (рис. 3.6).

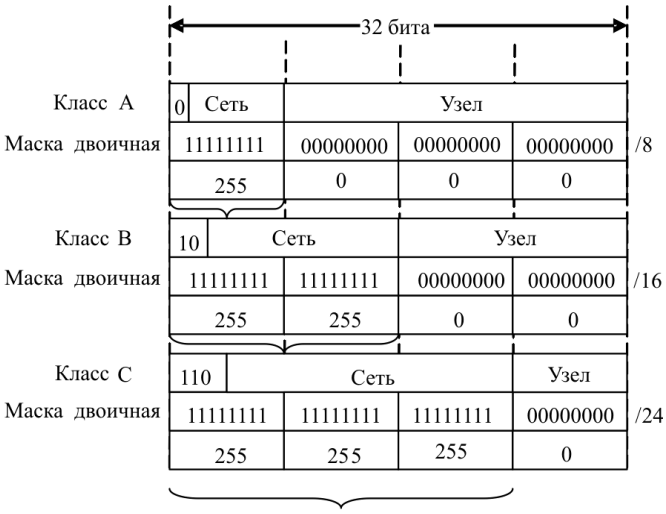


Рис. 3.6. Классовая модель адресации

Пример подсети в классовой модели «сеть, подсеть, хост»:

Главную сеть 10.0.0.0/8 (класс A) разобьем на псевдоподсети (размером класса B) с маской 255.255.0.0.

Подсети:

10.0.0.0/16 – нулевая подсеть. Нули в подсети никогда не используются для нумерации подсети в классовой модели маршрутизации (RFC 950).

10.1.0.0 /16 – адрес первой подсети.

10.1.0.0 – адрес подсети.

10.1.0.1 – первый хост в подсети 10.1.0.0.

10.1.255.254 – последний хост в подсети 10.1.0.0.

10.1.255.255 – направленное широковещание в подсеть 10.1.0.0.

10.2.0.0 /16 – адрес второй подсети.

10.3.0.0 /16 – адрес третьей подсети.

10.254.0.0/16 – адрес последней (254-й) подсети.

10.255.0.0/16 – направленное широковещание во все подсети. Никогда не используются для нумерации подсети в классовой модели маршрутизации (RFC 950).

Записи 10.0.0.0 для идентификации сети мало. Это либо сеть 10, либо подсеть 10.0. Записи 10.255.255.255 недостаточно для направленного широковещания для сети 10 либо для подсети 10.255.

Subnet Zero и Subnet Broadcast двусмысленны.

3.1.3.2. Классовая модель маршрутизации

Протоколы маршрутизации, не передающие вместе с каждым адресом сети/подсети информацию об ее маске, называются классовыми протоколами маршрутизации (RIPv1, IGRP). Поэтому все подсети одной главной сети (класс A, B и C) должны иметь одну и ту же маску подсети.

Подсетью (Subnet) называют IP-сеть, маска которой определяет часть адресного пространства главной сети путем расширения сетевой части адреса сети.

Не допускается использование маски переменной длины для подсетей. Сетевой администратор должен установить на портах маски одинаковой длины.

Получив пакет обновления (Routing Updates), классовый роутер выполняет следующие действия:

– Если информация в Routing Updates относится к тому же адресу основной сети, что и адрес сети, на который настроен принимающий интерфейс, роутер применяет маску подсети, установленную на принимающем интерфейсе (рис. 3.7).

– Если информация в Routing Updates относится к другой главной сети, роутер возьмет значение маски подсети по умолчанию (по классу адреса) (рис. 3.8).

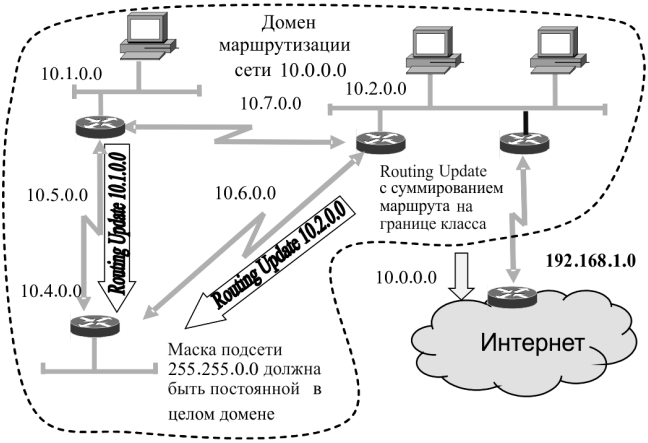


Рис. 3.7. Один домен маршрутизации

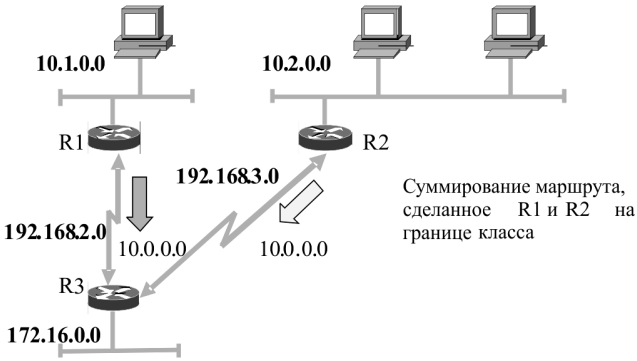


Рис. 3.8. Разобщенные подсети в классе

Это обстоятельство имеет несколько последствий. Если Routing Updates посылаются через интерфейс с сетевым номером, отличным от ее сетки (Subnetted Network), то только главный номер сети класса A, B или C будет объявлен, т.е.:

– суммирование маршрута будет выполнено на границах класса;

– область сеток должна быть непрерывна;

– маршрутизируются полные классы.

Проблемы классовой модели маршрутизации

R3 выберет:

– или один путь как лучший путь (RIP), тогда некоторые IP-хосты не могут быть достигнуты;

– или оба пути для балансировки нагрузки (IGRP). Следовательно, не все пакеты достигнут IP-хостов (то же самое с eIGRP-автосуммированием).

3.1.3.3. Бесклассовая модель IP-адресации

VLSM-маскирование обеспечивает:

– возможность создания более одной маски подсети в пределах одной главной сети;

– возможность разбивать на подсети уже разбитые на подсети IP-адреса.

Преимущества VLSM-маскирования:

– Более эффективное использование адресного пространства. Без VLSM-маскирования для всего адресного пространства сетей класса A, B или C можно применять только одну маску подсети (табл. 3.3).

– Возможность суммирования маршрутов.

– Возможно большое количество иерархических уровней в рамках одного плана адресации. Это позволяет производить оптимальное суммирование в таблицах маршрутизации.

Пусть имеем конкретный IP-адрес (относится к классу B):

– IP-адрес 172.16.113.205;

– маска подсети 255.255.255.192.

Какая сеть? Какой хост в сети?

Двоичный IP-адрес: 10101100 . 00010000 . 01110001 . 11001101

Двоичная маска: 11111111 . 11111111 . 11111111 . 11000000

Выполняем логическую операцию «И»:

Сеть: 10101100 . 00010000 . 01110001 . 11000000

Получаем в десятичном виде: сеть = 172.16.113.192.

Хост = 0.0.0.13 (эту запись обычно не приводят).

Таблица 3.3

Пример деления сети 172.16.0.0/16 на одинаковые подсети с маской 255.255.255.192

Сети	Байты				
	1-й	2-й	3-й	4-й	
Сеть класса B 172.16.0.0/16	10101100	00010000	00000000	00	000000
Разобьем маской 255.255.255.192	11111111	11111111	11111111	11	000000
Подсети	Сеть		Подсеть		Хост
172.16.0.0/26	10101100	00010000	00000000	00	000000
172.16.0.64/26	10101100	00010000	00000000	01	000000
172.16.0.128/26	10101100	00010000	00000000	10	000000
172.16.0.192/26	10101100	00010000	00000000	11	000000
172.16.1.0/26	10101100	00010000	00000001	00	000000
172.16.1.64/26	10101100	00010000	00000001	01	000000
…	...	...	…	…	…
172.16.255.128/26	10101100	00010000	11111111	10	000000
172.16.255.192/26	10101100	00010000	11111111	11	000000

3.1.3.4. Бесклассовая междоменная маршрутизация (CIDR)

Если дефицит класса B, следовательно, выделяют несколько классов C вместо одного адреса класса B.

Проблема: каждая сеть класса C нуждается в отдельной строке маршрутизации.

Решение: бесклассовая междоменная маршрутизация (Classless Inter-domain Routing (CIDR)), также называемая «суперсеть» (рис. 3.10–3.11).

Ключевой момент: так распределить адреса, чтобы они в итоге могли быть просуммированы, т.е. расположены рядом. Нужно совместно использовать те же самые биты верхнего уровня (т.е. префикс) (рис. 3.9)

Таблицы и протоколы маршрутизации должны быть способны к переносу маски подсети.

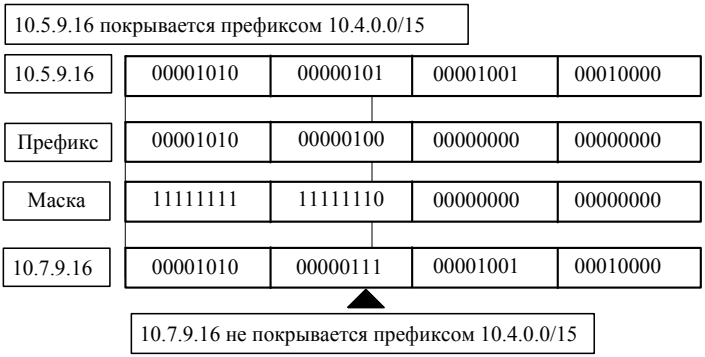


Рис. 3.9. Иллюстрация суммирования адресов (агрегации)

Междоменная маршрутизация без CIDR / с CIDR

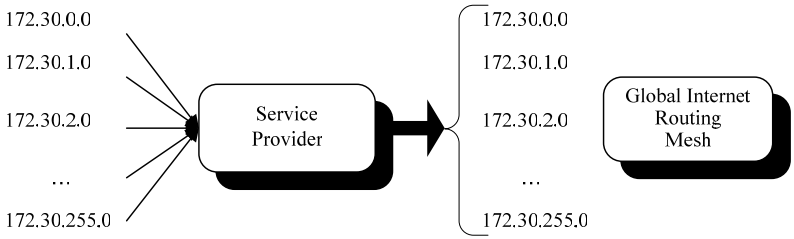


Рис. 3.10. Междоменная маршрутизация без CIDR

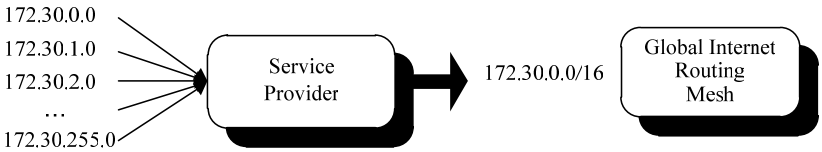


Рис. 3.11. Междоменная маршрутизация с CIDR

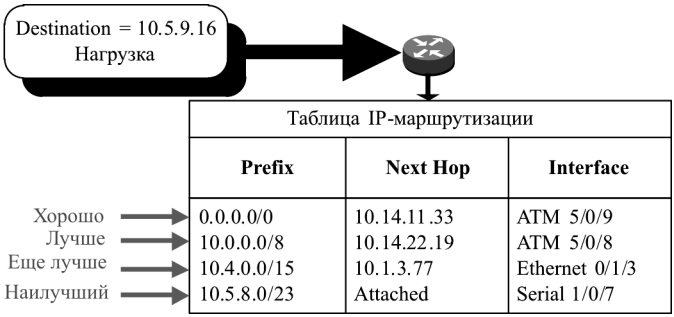


Рис. 3.12. Иллюстрация правила «длиннейшего» маршрута

Когда IP-адресу (10.5.9.16) соответствует много строк (записей), выбирается строка с самым длинным префиксным соответствием (рис. 3.12).

3.2. Лабораторная работа «Распределение IP-адресов»

Цель работы: получить навыки рационального распределения IP-адресов между подсетями корпоративной сети в заданном диапазоне адресного пространства.

Исходные данные: заданная преподавателем топология корпоративной сети с указанным числом компьютеров в каждой подсети.

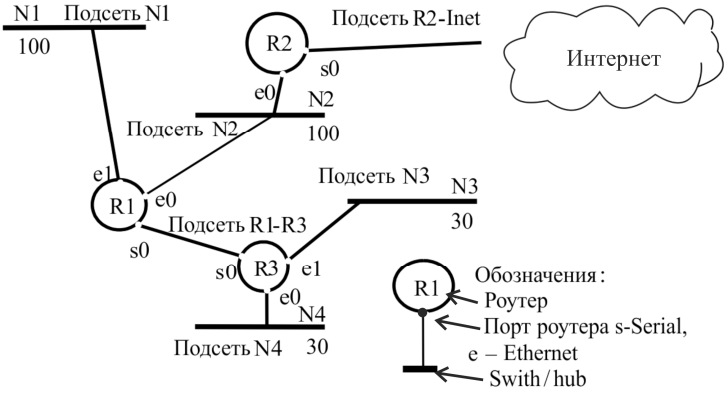


Рис. 3.13. Заданная топология корпоративной сети

Последовательность действий:

1. Нарисовать (Word) топологию, пронумеровать подсети, роутеры и порты (образец на рис. 3.13).

2. Рассчитать требуемое количество IP-адресов.

3. Задать необходимый диапазон IP-адресного пространства.

4. Распределить заданный диапазон между подсетями.

1. Нарисуем топологию, заданную преподавателем (см. рис. 3.13).

2. Рассчитаем необходимое количество IP-адресов.

Диапазон IP-адресов выбирается в зависимости от общего количества узлов всей сети и утверждается преподавателем.

Пусть топология корпоративной сети имеет вид, изображенный на рис. 3.13.

Общее число компьютеров – 260. Общее число портов роутеров – 9. Общее число подсетей – 6.

Для каждой подсети обязательно нужно учитывать два адреса: все нули (обозначение самой подсети) и все единицы (широковещательный адрес этой подсети). Поэтому к общей сумме всех компьютеров и портов роутеров нужно прибавить количество подсетей, умноженное на 2:

$$260 + 9 + 6 \cdot 2 = 281.$$

В итоге должно быть заказано пространство IP-адресов не менее 281.

При $N = 9$ имеем 512 адресов, что не меньше требуемого их количества, равного 281. Заметим, что размера одной сети класса C ($2^8 = 256$) недостаточно.

3. Зададим необходимый диапазон IP-адресного пространства.

Будем считать, что RIPE NCC выделил нам диапазон IP-адресов: 10.115.56.0–10.115.57.255.

Запишем начальный и конечный адреса в двоичном виде:

00001010.01110011.00111000.00000000

00001010.01110011.00111001.11111111

Неизменная часть адреса – 23 старших разряда ($32 – N = 32 – 9 = 23$). Маска сети в двоичном виде: 11111111.11111111.11111110.00000000, в десятичной форме: 255.255.254.0.

Запись выделенной сети RIPE NCC в слэш-формате: 10.115.56.0/23.

4. Распределим выделенный RIPE-диапазон IP-адресов.

Для подсети N1 необходимо 100 адресов для компьютеров и один адрес для порта роутера R1, к которому подсеть подключена, т.е. всего 101.

Количество выделенных адресов должно равняться степени двойки. Ближайшее большее число $128 = 2^7$.

Для подсети N2 нужно 102 адреса (100 + 2), т.е. выделим 128 адресов.

Для подсетей N3 и N4 требуется по 31 IP-адресу (30 +1). Ближайшая большая степень двойки $32 = 2^5$. Кажется, что это число нам вполне подходит, но вспомним, что номер узла не может состоять из одних двоичных нулей (это обозначение самой подсети) и единиц (широковещательный адрес этой подсети), т.е. начальный и конечный адреса не используются для нумерации хостов в подсети, и остается только 30 адресов для их присвоения хостам и портам роутеров. В нашем случае этого мало. Следующая ближайшая большая степень двойки $64 = 2^6$ – это слишком много, поэтому разобьем подсети N3 и N4 еще на подсети по 32 + 4 = 36 адресов.

Мы учли еще не все подсети. Роутеры R1 и R3 соединены между собой, и портам, через которые они подключены, тоже нужно назначить адреса. Для этой цели выделяется подсеть, состоящая всего из двух адресов. Согласно вышеизложенным соображениям в этой сети будет четыре IP-адреса.

В случае подсоединения корпоративной сети к Интернету в качестве канала связи используются два роутера. Одним из них будет R2 и какой-то роутер в облаке Интернета (на рисунке он не отмечен). Таким образом, у нас появится еще одна подсеть, состоящая из четырех IP-адресов.

Подсчитаем общее количество адресов и проверим, не выходим ли мы из заданного диапазона:

$$128 + 128 + 36 + 36 + 4 + 4 = 328.$$

Как видим 328 < 512, значит, все в порядке. Теперь разобьем диапазон IP-адресов корпоративной сети на вышеперечисленные подсети.

Разбиение на подсети представлено в табл. 3.1, желательно начинать с больших подсетей.

Сеть N1 включает в себя 128 адресов, т.е. для нумерации узлов необходимо семь младших разрядов IP-адреса, а старшие биты будут использованы для нумерации подсетей. Пусть старший бит (восьмой бит) четвертого байта адреса будет равен 0 (табл. 3.4).

Таблица 3.4

Расчет четвертого байта IP-адреса

Разряды	7	6	5	4	3	2	1	0
Вес	128	64	32	16	8	4	2	1
N1	0	*X*	*X*	*X*	*X*	*X*	*X*	*X*

Здесь «*X*» – разряды, выделенные под нумерацию узлов.

Тогда адрес IP-сети N1 – 10.115.56.0 /25, а маска – 255.255.255.128.

Пусть подсеть N4 состоит из 36 адресов и поделена на две подсети: 32 и 4. Определим адрес для первой подсети. Для нумерации 32 узлов необходимо пять разрядов младшего байта ($2^5 = 32$), следовательно, на номер сети остается три бита этого байта адреса. В старшем бите мы уже не можем поставить 0, так как этот диапазон уже занят. Два других разряда могут иметь произвольное значение (табл. 3.5).

Таблица 3.5

Расчет 4-го байта IP-адреса

Разряды	7	6	5	4	3	2	1	0
Вес	128	64	32	16	8	4	2	1
N4	1	0	1	*X*	*X*	*X*	*X*	*X*

Получим: IP-адрес подсети N4: 10.115.56.160/27.

Маска подсети: 255.255.255.224.

Следуя тем же рассуждениям и следя, чтобы диапазоны подсетей не пересекались, определим IP-адреса остальных подсетей (рис. 3.14).

Используем для перевода из двоичной в десятичную систему счисления →	**Байт 1**	**Байт 2**	**Байт 3**								**Байт 4**								→номер байта в IP-адресе
	1,2–8	9–16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32	→номер бита в IP-адресе
	7–0	7–0	7	6	5	4	3	2	1	0	7	6	5	4	3	2	1	0	→номер разряда в байте
	2^7–2^0	2^7–2^0	2^7	2^6	2^5	2^4	2^3	2^2	2^1	2^0	2^7	2^6	2^5	2^4	2^3	2^2	2^1	2^0	→вес разряда в байте (2^n)
	128–1	128–1	128	64	32	16	8	4	2	1	128	64	32	16	8	4	2	1	→вес разряда в байте (10)

Выделенная RIPE NCC IP-сеть 10.115.56.0/23	**Неизменяемая часть адреса (23 разряда)**									**Изменяемая (распределяемая) часть адреса**								IP-сеть (512 адресов)
	10	115	0	0	1	1	1	0	0	*X*	*X*	*X*	*X*	*X*	*X*	*X*	*X*	10.115.56.0/23

Номер подсети	Количество IP- адресов		**Распределение адресного пространства на подсети**																Комментарий
	Надо	Выделили	***Сеть***								***Подсеть***		***Хосты в подсети***						**IP-подсети**
*N*1	101	128	10	115	0	0	1	1	1	0	0	0	0	*X*	*X*	*X*	*X*	*X*	*X*	*X*	10.115.56.0/25
*N*4	31	32	10	115	0	0	1	1	1	0	0	0	1	0	1	*X*	*X*	*X*	*X*	*X*	10.115.56.160/27
		4	10	115	0	0	1	1	1	0	0	0	1	0	0	1	1	1	*X*	*X*	10.115.56.156/30
R2–*R3*	2	4	10	115	0	0	1	1	1	0	0	0	1	0	0	1	1	0	*X*	*X*	10.115.56.152/30
*N*2	102	128	10	115	0	0	1	1	1	0	0	1	0	*X*	*X*	*X*	*X*	*X*	*X*	*X*	10.115.57.0/25
*N*3	31	32	10	115	0	0	1	1	1	0	0	1	1	0	1	*X*	*X*	*X*	*X*	*X*	10.115.57.160/27
		4	10	115	0	0	1	1	1	0	0	1	1	1	0	1	1	1	*X*	*X*	10.115.57.220/30
R1–*In*	2	4	10	115	0	0	1	1	1	0	0	1	1	1	0	1	1	0	*X*	*X*	10.115.57.216/30
Всего	269	328	Получили IP-подсети, входящие в сеть →																10.115.56.0/23

Рис. 3.14. Разбиение распределения выделенного диапазона RIPE NCC IP-адресов

Следует еще всем портам роутеров присвоить MAC-адреса, которые могут быть абсолютно произвольными.

Результатом данной работы должна стать сеть, представленная на рис. 3.15.

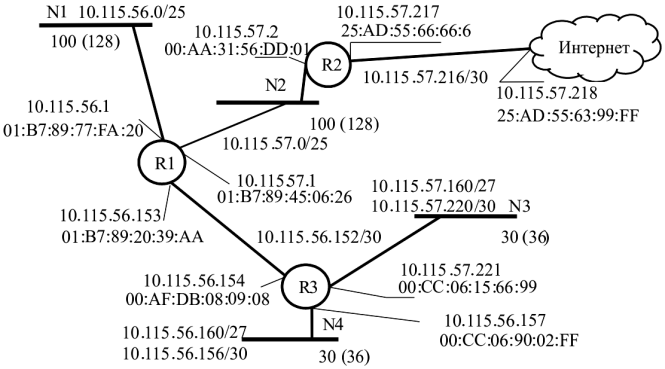


Рис. 3.15. Корпоративная сеть с назначенными IP-и MAC-адресами

10.115.56.0–10.115.57.255 размером 512 адресов.

10.115.56.0/23 – часто используемая запись сети или подсети.

Покажем распределение IP-адресов для данной корпоративной сети (см. рис. 3.14).

Задания для самостоятельной работы

1. Разделить подсеть на две или четыре части.
2. Объединить две или четыре подсети.
3. Привести максимальную свободную (нераспределенную подсеть).

3.3. Лабораторная работа «Движение пакетов в IP-сетях»

Цель работы: понять алгоритм работы средств сетевого уровня по продвижению пакета от хоста-источника к хосту-получателю, которые находятся в разных подсетях корпоративной сети.

Исходные данные:

– Присвоенные значения IP- и MAC-адресов портам роутеров и компьютеров предыдущей лабораторной работы.

– Заданное преподавателем направление движения пакетов.

– Сформированные (построенные) в рамках этой работы согласно теории вопроса системные таблицы, ARP-таблицы и таблицы маршрутизации.

Последовательность действий:

– Сформируем системные таблицы каждого устройства, показав в них имя порта, MAC-адрес и IP-адрес.

– Сформируем ARP-таблицы каждого устройства.

– Сформируем таблицы маршрутизации устройств, через которые проходит пакет.

Пример выполнения лабораторной работы

Рассмотрим движение пакета по нашей корпоративной сети (рис. 3.16) от компьютера 1 к компьютеру 2 (K1 → K2).

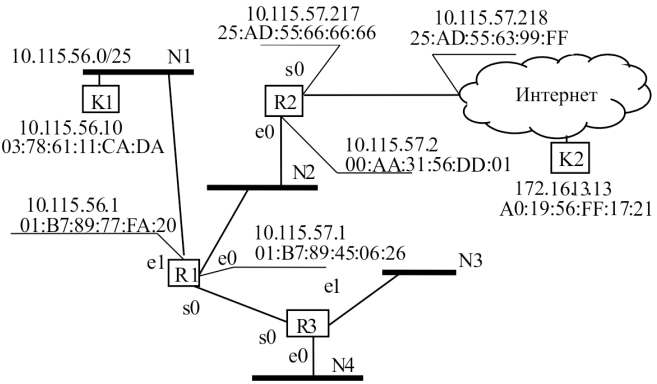


Рис. 3.16. Пример взаимодействия компьютеров через сеть

Построим таблицы маршрутизации в IP-сети

Цель работы: получить начальные навыки построения таблиц маршрутизации.

Краткие теоретические сведения:

Программные модули протокола IP устанавливаются на всех конечных станциях и роутерах сети. Для продвижения пакетов они используют таблицы маршрутизации (табл. 3.6–3.8).

Пример построения таблиц маршрутизации в IP-сети

Строка «Default» означает, что пакеты посылаются по умолчанию через данный порт роутера в том случае, если адрес сети назначения не принадлежит рассматриваемой корпоративной сети.

Таблица 3.6

Таблица маршрутизации роутера R1

IP-адрес подсети (Network Address)	Маска (Netmask)	Next Hop IP-адрес	Порт (Interface)	Расстояние (Metric)
10.115.56.0/25	255.255.255.128	–	e1	0
10.115.56.156/30	255.255.255.252	10.115.56.154	s0	1
10.115.56.160/27	255.255.255.224	10.115.56.154	s0	1
10.115.57.0/25	255.255.255.128	–	e0	0
10.115.57.160/27	255.255.255.224	10.115.56.154	s0	1
10.115.57.220/30	255.255.255.252	10.115.56.154	s0	1
10.115.57.216/30	255.255.255.252	10.115.57.2	e0	1
10.115.56.152/30	255.255.255.252	–	s0	0
0.0.0.0 (Default)	0.0.0.0	10.115.57.2	e0	–

Примечание. В качестве метрики использовалось количество линий соединений.

Таблица 3.7

Таблица маршрутизации роутера R2

IP-адрес подсети (Network Address)	Маска (Netmask)	Next Hop IP-адрес	Порт (Interface)	Расстояние (Metric)
10.115.56.0/25	255.255.255.128	10.115.57.1	e0	1
10.115.56.156/30	255.255.255.252	10.115.57.1	e0	2
10.115.56.160/27	255.255.255.224	10.115.57.1	e0	2
10.115.57.0/25	255.255.255.128	–	e0	0
10.115.57.160/27	255.255.255.224	10.115.57.1	e0	1
10.115.57.220/30	255.255.255.252	10.115.57.1	e0	1
10.115.57.216/30	255.255.255.252	–	s0	0
10.115.56.152/30	255.255.255.252	10.115.57.1	e0	1
0.0.0.0 (Default)	0.0.0.0	–	s0	–

Таблица 3.8

Таблица маршрутизации роутера R3

IP-адрес подсети (Network Address)	Маска (Netmask)	Next Hop IP-адрес	Порт (Interface)	Расстояние (Metric)
10.115.56.0/25	255.255.255.128	10.115.56.153	s0	1
10.115.56.156/30	255.255.255.252	–	e0	0
10.115.56.160/27	255.255.255.224	–	e0	0
10.115.57.0/25	255.255.255.128	10.115.56.153	s0	1
10.115.57.160/27	255.255.255.224	–	e1	0
10.115.57.220/30	255.255.255.252	–	e1	0
10.115.57.216/30	255.255.255.252	10.115.56.153	s0	2
10.115.56.152/30	255.255.255.252	–	s0	0
0.0.0.0 (Default)	0.0.0.0	10.115.56.153	s0	–

Вид таблицы IP-маршрутизации зависит от конкретного типа используемого протокола маршрутизации. Однако во всех таблицах есть ключевые параметры, присущие всем таблицам роутеров:

– IP-адрес сети (подсети) назначения (с маской – в бесклассовой модели маршрутизации; без маски – в классовой модели маршрутизации);

– IP-адрес следующего роутера (Next Hop);

– порт (интерфейс) роутера, через который нужно отправить пакет;

– метрика – расстояние до сети назначения, например в хопах.

Метрика – необязательный параметр. Если в таблице маршрутизации каждая сеть назначения упомянута только один раз, то поле метрики не будет приниматься во внимание при выборе маршрута, так как выбор отсутствует.

Метрика может использоваться как признак непосредственного подключения сети к роутеру.

Если сеть назначения подключена непосредственно к порту роутера, то пакет не будет передаваться следующему роутеру, а отправится на узел назначения.

Существуют протоколы маршутизации, в которых метрика измеряется хопами (например, протокол RIP). Хопы – количество промежуточных роутеров, через которые пакет пройдет по пути к узлу назначения. Также существуют протоколы, в которых метрика измеряется величинами, которые показывают состояния связи между роутерами, такие как скорость, надежность, стоимость (например, протокол OSPF).

В первом случае признаком непосредственного подключения сети будет значение поля метрики 0, во втором – 1. Другое значение метрики соответствует удаленной сети.

Существуют ситуации, когда роутер должен обязательно хранить значение метрики для записи о каждой удаленной сети. Эти ситуации возникают, когда записи в таблице маршрутизации являются результатом работы некоторых протоколов маршрутизации, например протокола RIP. В таких протоколах новая информация о какой-либо удаленной сети сравнивается с имеющейся в таблице, и если метрика новой информации лучше имеющейся, то новая запись вытесняет имеющуюся.

Иллюстрация процесса движения пакетов

Для начала покажем настройки компьютеров К1 и К2.

Настройки для компьютера К1	Настройки для компьютера К2
IP-адрес: 10.115.56.10	IP-адрес: 172.16.13.13
Маска подсети: 255.255.255.128	Маска подсети: 255.255.255.128
Основной шлюз: 10.115.56.1	Основной шлюз: 172.16.13.1
DNS: 193.0.14.129	DNS: 193.0.14.129
MAC-адрес: 03:78:61:11:CA:DA	MAC-адрес: A0:19:56:FF:17:21

Итак, пусть пользователь компьютера К1 (10.115.56.10), находящегося в подсети 10.115.56.0, по протоколу FTP обращается к компьютеру с IP-адресом 172.16.13.13.

Модуль FTP упаковывает свое сообщение в сегмент транспортного протокола TCP, который, в свою очередь, помещает свой сегмент в пакет протокола IP.

В заголовке IP-пакета должен быть указан IP-адрес отправителя и IP-адрес узла назначения:

Отправитель	10.115.56.10
Получатель	172.16.13.13

Модуль IP компьютера 10.115.56.10 проверяет, нужно ли маршрутизировать пакеты с адресом 172.16.13.13. Для этого он накладывает маску подсети на IP-адрес отправителя и получателя при помощи логической операции «И», а затем сравнивает получившиеся подсети.

IP-адрес хоста К1	10.115.56.10
Маска подсети	255.255.255.128
Логическая операция «И»	----------
Подсеть	10.115.56.0
IP-адрес хоста К2	172.16.13.13
Маска подсети	255.255.255.128
Логическая операция «И»	----------
Подсеть	172.16.13.0

Поскольку адрес сети назначения (172.16.13.0) не совпадает с адресом (10.115.56.0) сети, которой принадлежит компьютер-отправитель, то маршрутизация необходима.

Компьютер К1 начинает формировать IP-пакет роутеру (по умолчанию) R1, IP-адрес которого известен – 10.115.56.1, но неизвестен MAC-адрес, необходимый для перемещения пакета. Для определения MAC-адреса роутера R1 протокол IP обращается по протоколу ARP, который просматривает ARP-таблицу. Пусть в данном случае нужная запись была найдена по ARP-таблице хоста К1:

Порт	IP	MAC
Порт К1	10.115.56.1	01:B7:89:77:FA:20.

В результате компьютер К1 отправляет по сети пакет, зная IP- и MAC-адреса отправителя и получателя (табл. 3.9).

Таблица 3.9

Движение К1 → R1

Адрес	IP	MAC
Отправитель	10.115.56.10	03:78:61:11:CA:DA
Получатель	172.16.13.13	01:B7:89:77:FA:20

Роутер R1. Пакет принимается портом e1 роутера R1, так как MAC-узел этого порта распознает свой MAC-адрес. IP-пакет передается программному обеспечению роутера, реализующему протокол IP. Протокол IP извлекает из пакета адрес назначения 172.16.13.13 и просматривает записи своей таблицы маршрутизации. В роутере R1 не имеется записей в таблице маршрутизации (см. табл. 3.9) о сети 172.16.13.0/25.

Поэтому срабатывает строка по умолчанию

0.0.0.0 (Default)	0.0.0.0	10.115.57.2	e0	–

Эта строка говорит о том, что пакеты для сети 172.16.13.0/25 нужно передавать роутеру 10.115.57.2, находящемуся в сети, подключенной к порту e0 роутера R1.

Далее модуль IP определяет MAC-адрес следующего роутера по известному IP-адресу 10.115.57.2, для чего обращается к ARP-таблице (табл. 3.10).

Таблица 3.10

ARP-таблица роутера R1

Порт	IP	MAC
e1	10.115.56.10	03:78:61:11:CA:DA
e0	10.115.57.2	00:AA:31:56:DD:01
s0	10.115.56.154	02:A1:75:48:CC:10

Роутер R1 отсылает пакет роутеру R2.

Модуль IP на роутере R2 действует аналогично и определяет IP-адрес следующего роутера 10.115.57.218, по которому через ARP-таблицу выясняется MAC-адрес (табл. 3.11).

Таблица 3.11

ARP-таблица роутера R2

Порт	IP	MAC
2b	10.115.57.218	25:AD:55:63:99:FF
2a	10.115.57.1	01:B7:89:45:06:26

Пограничный роутер получает пакет. Нам неизвестно, как далее пакет движется по Интернету. Когда пакет поступит в роутер сети назначения, появится возможность передачи этого пакета компьютеру назначения с помощью всё тех же действий.

Задания для самостоятельной работы

1. Как роутер R1 сформировал IP- и MAC-адреса пакета и кадра при выполнении Forward в случае движения от К1 к К2?
2. Как компьютер К1 сформировал IP- и MAC-адреса пакета и кадра при выполнении Forward в случае движения от К1 к К2?

Вопросы для самопроверки

1. Является ли 192.168.156.0 адресом сети?
2. Для чего необходим IP-адрес?
3. Какая RIR занимается вопросами распределения IP в России?
4. Сколько различных хост-адресов может быть у IPv4?
5. Могут ли повторяться IP-адреса?
6. Что такое префикс сети?
7. Что такое маршрутизация, роутер, протокол маршрутизации?
8. Для чего нужны протоколы маршрутизации?
9. Что такое метрика?
10. Как осуществляется процесс передачи пакетов через роутеры?
11. Для чего нужны таблицы маршрутизации?

12. Как работают протоколы RIP и OSPF? Чем они отличаются?

13. Из чего состоит IP-адрес?

14. Какие есть классы IP-адресов? Чем они различаются?

15. Что такое подсеть? Какой размер может быть у самой маленькой подсети?

16. Могут ли сеть и подсеть иметь разные маски?

17. Как определить сеть, зная IP-адрес хоста и маску подсети?

18. Что такое CIDR? Какое у нее назначение?

19. Для чего нужно VLSM-маскирование?

4. ПРОТОКОЛЫ МАРШРУТИЗАЦИИ RIP И BGP-4

4.1. Краткие теоретические сведения

Маршрутизация (Routing) – это процесс перемещения пакета от источника к приемнику через сеть передачи данных.

Маршрутизатор (Router) – это устройство, передающее пакет в нужном направлении (через нужный интерфейс). В терминологии IETF маршрутизатор называют также шлюз (Gateway). По тексту пособия маршрутизатор называется роутером.

Маршрутизируемый протокол (Routed Protocol) существует в каждом роутере для передачи пакета в нужном направлении.

Нужное направление передачи роутер определяет на основании таблицы маршрутизации. *Таблицы маршрутизации* (Forwarding Tables) формируются протоколами маршрутизации

Протокол маршрутизации (Routing Protocol) – это распределенный протокол, работающий координированно с другими роутерами с целью изучения и формирования глобального представления сети непротиворечивым и законченным способом. Протоколы маршрутизации работают по алгоритмам маршрутизации

Обобщенная таксономия алгоритмов маршрутизации: одношаговые и многошаговые, статические и динамические, классовые и бесклассовые, дистанционно-векторные и состояния связей, внутренние и внешние.

4.1.1. Статическая маршрутизация

Статическая маршрутизация – вид маршрутизации, при котором маршруты указываются в явном виде при конфигурации роутера. Вся маршрутизация при этом происходит без участия каких-либо протоколов маршрутизации.

При задании статического маршрута указывается:

а) адрес сети (на которую маршрутизируется трафик), маска сети;

б) адрес шлюза (узла), который отвечает за дальнейшую маршрутизацию;

в) метрика (иногда именуется также «ценой») маршрута. При наличии нескольких маршрутов на одну и ту же сеть роутеры выбирают маршрут с минимальной метрикой.

В роутерах Cisco помимо метрики для выбора предпочитаемого маршрута используется параметр «Административное расстояние» (Administrative Distance), который характеризует степень предпочтения источника маршрута (у разных протоколов маршрутизации данный параметр разный). Чем меньше данный показатель, тем источник маршрута предпочтительней. У статических маршрутов Administrative Distance равно 1. У непосредственно подключенных сетей Administrative Distance равно 0.

Достоинства:

а) легкость отладки и конфигурирования в малых сетях;

б) мгновенная готовность (не требуется интервал для конфигурирования/подстройки);

в) низкая нагрузка на процессор роутера;

г) предсказуемость в каждый момент времени.

Недостатки:

а) очень плохое масштабирование;

б) низкая устойчивость к повреждениям линий связи;

в) отсутствие динамического балансирования нагрузки;

г) необходимость ведения отдельной документации к маршрутам, проблема синхронизации документации и реальных маршрутов.

4.1.2. Протокол маршрутизации RIP

RIP – дистанционно-векторный, внутренний протокол маршрутизации, использующий количество хопов в качестве метрики. Сети с метрикой более 15 недостижимы. По умолчанию протокол

рассылает широковещательные обновления маршрутизации каждые 30 с.

Номера портов UDP-, IP- и MAC-адреса источника и приемника, используемые при инкапсуляции сообщений RIP, показаны на рис. 4.1.

Версии RIP:

1. RIPv1:

– определен в RFC 1058;

– классовый протокол маршрутизации;

– поддерживает автосуммирование маршрутов в границе главных подсетей классов A, B, C.

2. RIPv2:

– определен в RFC 1723;

– бесклассовый протокол маршрутизации;

– поддерживает VLSM и CIDR;

– поддерживает автосуммирование маршрутов в границе главных подсетей классов A, B, C;

– поддерживает аутентификацию.

<table>
<tr><td colspan="4">Encapsulated RIPv1 Message</td></tr>
<tr><td>Data Link Frame Header</td><td>IP Packet Header</td><td>UDP Segment Header</td><td>RIP Message (504 bytes; Ip to 25 routes)</td></tr>
<tr><td colspan="4">Data Link Frame
MAC Destination Address = Broadcast: FF-FF-FF-FF-FF-FF
MAC Source Address = Address of sending interface
IP Packet
IP Source Address = Address of sending interface
IP Destination Address = Broadcast: 255.255.255.255
Protocol field = 17 for UDP
UDP Segment
Source Port = 520
Destination Port = 520
RIP Message:
Command: ReQuest(1); Response (2)
Version = 1
Address Family ID = 2 for IP
Routes: Network IP Address
Metric: Hop Count</td></tr>
</table>

Рис. 4.1. Инкапсулированное сообщение протокола RIPv1

Отличия в структуре сообщений разных версий протокола RIP показаны на рис. 4.2. *Первое новое поле в сообщении RIPv2 – Subnet Mask Field*, которое содержит 32-битную маску, которая включена в запись маршрута RIP. В результате роутер, получивший обновление, больше не зависит от маски подсети принявшего интерфейса или маски главной сети при определении маски подсети для маршрута.

Правило определения маски подсети в RIPv1. Если сеть в обновлении маршрутизации и IP-адрес принявшего обновление интерфейса роутера являются подсетями одной главной сети классов A, B или C, то к данной сети в обновлении применяется маска подсети интерфейса, иначе применяется маска соответствующей главной сети классов A, B, C. Классы подсетей приведены на рис. 3.6.

Второе новое поле в сообщении RIPv2 – Next Hop Address. Next Hop Address используется, чтобы идентифицировать лучший адрес следующего перелета (Next Hop). Если в данном поле есть только одна запись, то этот адрес используется как адрес Next Hop. Если поле содержит все нули (0.0.0.0), то адрес Next Hop – адрес роутера, отправившего сообщение RIP.

Comparing RIPv1 and RIPv2 Message Formats				
RIPv1				
Bit:	0 7	8 15	16 23	24 31
	Command = 1 or 2	Version = 1	Must be zero	
Route Entry	Address family identifier (2 = IP)		Must be zero	
	IP Address (Network Address)			
	Must be zero			
	Must be zero			
	Must be zero			
	Multiple Route Entries, up to a maximum of 25			
RIPv2				
Bit:	0 7	8 15	16 23	24 31
	Command = 1 or 2	Version = 2	Must be zero	
Route Entry	Address family identifier (2 = IP)		Route Tag	
	IP Address (Network Address)			
	Subnet Mask			
	Next Hop			
	Metric (Hops)			
	Multiple Route Entries, up to a maximum of 25			

Рис. 4.2. Различие в сообщениях RIPv1 и RIPv2

Поля сообщений RIP:

– Command – поле команды, если в поле 1, то это запрос, если 2, то ответ;

– Version – указывает на версию RIP: 1 или 2;

– Address Family Identifier – тип адреса, обычно поддерживается только запись AF_INET, которая равна 2 (т.е. используется для протокола IP);

– Route Tag – тег маршрута. Предназначен для разделения «внутренних» и «внешних» маршрутов, взятых, например, из другого IGP или EGP;

– IP Address – IP-адрес подсети назначения;

– Subnet Mask – маска подсети назначения (одно обновление содержит до 25 записей с маршрутами);

– Metric – метрика маршрута.

Таймеры протокола RIP представлены в табл. 4.1.

Таблица 4.1

Таймеры протокола RIP

Таймер	Значение по умолчанию, с	Описание
Update	30	Интервал между посылкой обновлений
Hold-Down	90	Период, по истечении которого маршрут удаляется из таблицы маршрутизации, чтобы предотвратить петли маршрутизации
Timeout	180	Интервал, в течение которого маршрут должен оставаться «живым» в таблице маршрутизации. Этот счетчик сбрасывается каждый раз, когда роутер получает обновления для этого маршрута
Flush	120	Как долго ждать, чтобы удалить маршрут из таблицы маршрутизации после того, как его время (Timeout) истекло

Алгоритм работы RIP:

1. При начальном запуске:

а) каждый RIP-сконфигурированный интерфейс роутера отсылает сообщение запроса (Request) соседям по RIP, чтобы они послали свои полные таблицы маршрутизации;

б) соседи по RIP отправляют сообщение ответа (Response) со своими таблицами маршрутизации;

в) когда запрашивавший роутер получает ответы, он просматривает каждую запись полученной таблицы маршрутизации. Если запись новая, роутер записывает этот маршрут в свою таблицу маршрутизации. Если маршрут уже есть в его таблице маршрутизации, существующая запись заменяется, если у новой записи метрика содержит меньшее число хопов.

2. Далее каждые 30 с каждый RIP-сконфигурированный роутер рассылает через свои RIP-сконфигурированные интерфейсы соседям свою полную таблицу маршрутизации. Могут также посылаться запросы роутерами при изменении их таблиц маршрутизации и Triggered-обновления маршрутизации, если какой-либо роутер обнаружил изменение в топологии.

При работе дистанционно-векторных протоколов маршрутизации с медленной конвергенцией (сходимостью) могут возникать петли маршрутизации. Для борьбы с петлями используются следующие правила:

1. Правило Split Horizon («расщепленный горизонт»). Роутер не должен направлять Update о маршрутах в адрес их источника. За этим правилом закрепилось название Split Horizon. Роутер, используя данное правило, разделяет свои маршруты на столько групп, сколько у него есть активных интерфейсов. При использовании правила Split Horizon обновления для маршрутов, которые были получены через некоторый интерфейс, не должны передаваться через этот же интерфейс.

2. Правило Poisoned Reverse («отравление маршрута»). Правило Split Horizon может быть использовано с незначительной модификацией. Правило Split Horizon with Poisoned Reverse разреша-

ет передачу обновлений маршрутизации для потенциально опасных, с точки зрения возникновения циклов, маршрутов. В данном случае для таких маршрутов устанавливается метрика, которая соответствует бесконечности, – 15.

3. Правило Triggered Update («управляемые модификации»). Использование данного правила предписывает необходимость формирования мгновенных модификаций в том случае, когда происходит изменение состояния сети.

Administrative Distance для протокола RIP равно 120.

4.1.3. Протокол маршрутизации BGP-4

BGP-4 – дистанционно-векторный, внешний протокол маршрутизации. Главная цель BGP – реализация политик маршрутизации между автономными системами AS. Протокол BGP включает в себя защиту от «зацикливания». AS – это набор роутеров, которые работают под управлением одного администратора или одной группы администраторов и используют общую стратегию маршрутизации. BGP используется в сетях между ISP (Inetrnet Service Providers). Местный трафик либо начинается, либо завершается в автономной системе (AS); в противном случае – это транзитный трафик. Системы без транзитного трафика не нуждаются в BGP (им достаточно EGP для общения с транзитными узлами).

Роутеры, которые принадлежат одной и той же AS и обмениваются BGP-обновлениями маршрутизации, работают по Internal BGP (iBGP). Роутеры, которые принадлежат разным AS, тоже обмениваются BGP-обновлениями маршрутизации, но работают по External BGP (eBGP).

Перед тем как обмениваться информацией о маршрутах с внешними AS, BGP должен гарантировать, что сети внутри его AS достижимы. Это обеспечивается комбинацией обмена информацией о маршрутах по iBGP между роутерами внутри AS и передачи информации о маршрутах BGP в один из Interior Gateway Protocols (IGPs), которые работают внутри AS (например, Intereior Gateway Routing Protocol IGRP, Intermediate System-to-Intermediate

System IS-IS, Routing Information Protocol RIP и Open Shortest Path First OSPF).

BGP использует TCP в качестве транспортного протокола (порт 179). Любые два роутера в BGP, между которыми открыто TCP-соединение для обмена информацией о маршрутизации, называются Peers или Neighbors. На приведенном ниже рис. 4.3 роутеры A и B являются BGP Peers, равно как и роутеры B и C, C и D. Роутеры A и B обмениваются информацией о маршрутизации по eBGP, а роутеры B и C – по iBGP. Заметим, что eBGP Peers соединены непосредственно, а iBGP – нет, но поскольку между ними работает IGP, он позволяет им достигать друг друга и обмениваться информацией.

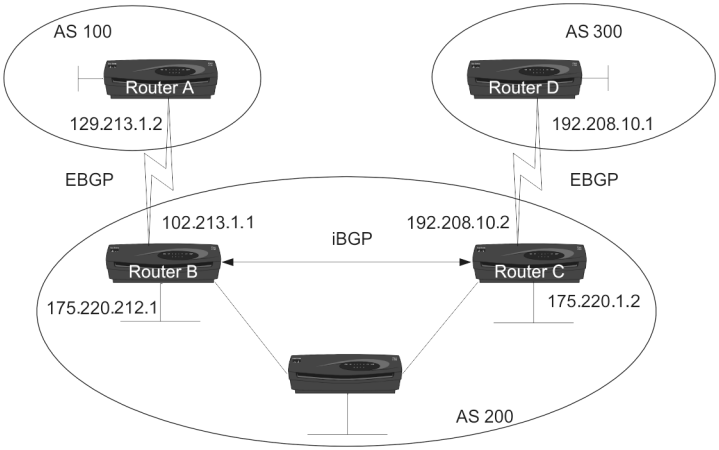


Рис. 4.3. Пример топологии BGP

BGP Peers инициируют обмен полными таблицами BGP-маршрутизации между собой. Позже они посылают лишь инкрементальные обновления маршрутизации. Кроме того, BGP Peers обмениваются Keepalive-сообщениями (чтобы удостовериться, что связь между ними не потеряна) и Notification-сообщениями (уведомления, сообщения об ошибках и другая служебная информация).

Формат BGP-сообщений:

1. Каждое BGP-сообщение имеет заголовок фиксированного размера. Формат заголовка представлен на рис. 4.4.

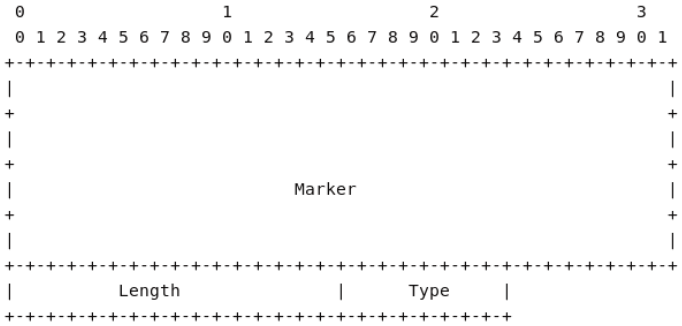


Рис. 4.4. Формат заголовка BGP-сообщения

Поле «Маркер» (Marker) содержит 16 байтов, и его содержимое может легко интерпретироваться получателем. Если тип сообщения открыть (OPEN) или если код идентификации в сообщении OPEN равен нулю, то поле Marker должно быть заполнено единицами. Marker может использоваться для обнаружения потери синхронизации в работе BGP-партнеров. Поле «Длина» (Length) имеет два байта и определяет общую длину сообщения в байтах, включая заголовок. Значение этого поля должно лежать в пределах 19–4096. Поле «Тип» (Type) представляет собой код разновидности сообщения и может принимать следующие значения:

1) OPEN (Открыть);

2) UPDATE (Изменить);

3) NOTIFICATION (Внимание);

4) KEEPALIVE (Еще жив).

BGP отличается от RIP и OSPF тем, что использует TCP в качестве транспортного протокола. Две системы, использующие BGP, связываются друг с другом и пересылают посредством протокола TCP полные таблицы маршрутизации.

2. После того как связь на транспортном протокольном уровне установлена, первое сообщение, которое должно быть послано, это

OPEN. При успешном прохождении этого сообщения партнер должен откликнуться сообщением KEEPALIVE. После этого возможны любые сообщения. Формат сообщения OPEN представлен на рис. 4.5.

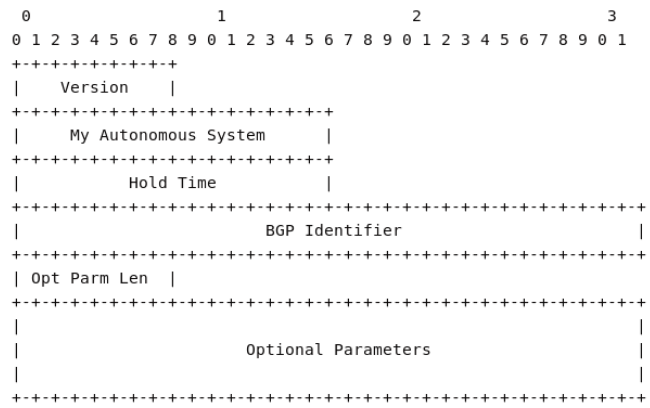


Рис. 4.5. Формат сообщения OPEN

Поле «Версия» (Version) описывает код версии используемого протокола, на сегодня для BGP он равен 4. Двухбайтное поле «Моя автономная система» (My Autonomous System) определяет код AS отправителя. Поле «Время сохранения» (Hold Time) характеризует время в секундах, которое отправитель предлагает занести в таймер сохранения (Hold Timer). После получения сообщения OPEN BGP-роутер должен выбрать значение времени сохранения (Hold Time). Обычно выбирается меньшее из полученного в сообщении OPEN и значения, определенного при конфигурации системы (0–3 с). Время сохранения определяет максимальное время в секундах между сообщениями KEEPALIVE и двумя UPDATE-сообщениями. Каждому узлу в рамках BGP приписывается четырехбайтный BGP-идентификатор (BGP-Identifier, задается при инсталляции и идентичен для всех интерфейсов BGP-роутера). Если два узла установили два канала связи друг с другом, то согласно правилам должен быть сохранен канал, начинающийся

в узле, BGP-идентификатор которого больше. Байт поля опциональных параметров (Opt Parm Len) указывает общую длину поля Optional Parameters. Если значение этого поля равно нулю, то поле Optional Parameters пустое. Поле Optional Parameters может содержать список необязательных параметров (таких, как параметры аутентификации), где каждый параметр состоит из трех частей: <Parameter Type, Parameter Length, Parameter Value>.

3. Сообщения типа UPDATE (Изменения) используются для передачи маршрутной информации между BGP-партнерами. Этот тип сообщения позволяет сообщить об одном новом маршруте или объявить о закрытии группы маршрутов, причем объявление об открытии нового и закрытии старых маршрутов возможно в пределах одного сообщения. Формат сообщения UPDATE представлен на рис. 4.6.

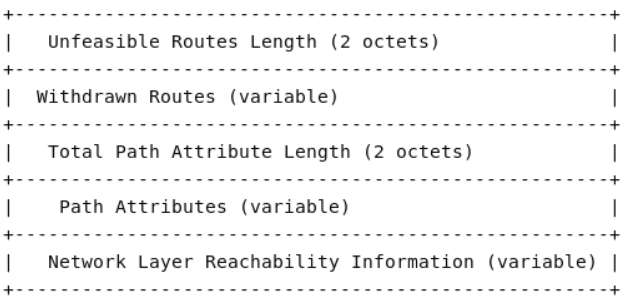


Рис. 4.6. Формат сообщения UPDATE

Сообщение UPDATE всегда содержит стандартный заголовок и может содержать другие поля. Если поле «Длина списка отмененных маршрутов» (Unfeasible Routes Length) равно нулю, т.е. ни один маршрут не отменен, то поле «Отмененные маршруты» (Withdrawn Routes) в сообщении отсутствует. Поле «Отмененные маршруты» имеет переменную длину и содержит список IP-адресных префиксов маршрутов, которые стали недоступны. Каждая такая запись имеет формат, показанный на рис. 4.7.

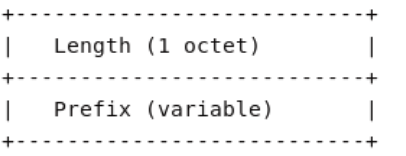


Рис. 4.7. Формат поля Withdrawn Routes

Здесь поле Length, равное нулю, означает, что префикс соответствует всем IP-адресам, а сам имеет нулевой размер. Поле Prefix содержит IP-адресные префиксы, за которыми следуют разряды, дополняющие их до полного числа байтов. Значения этих двоичных разрядов смысла не имеют. Двухбайтное поле полной длины списка атрибутов пути (Total Path Attribute Length) указывает на итоговую длину списка атрибутов пути (Path Attributes). Нулевое значение данного поля указывает на то, что информация о доступных сетях в UPDATE-сообщении отсутствует.

Поле «Список атрибутов пути» (Path Attributes) присутствует в любом UPDATE-сообщении. Это поле имеет переменную длину, а каждый атрибут содержит три составные части: <Attribute Type, Attribute Length, Attribute Value>. Тип атрибута (Attribute Type) представляет собой двухоктетное поле со структурой, показанной на рис. 4.8.

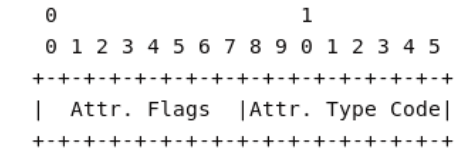


Рис. 4.8. Формат поля Attribute Type

Старший бит (бит 0) поля «Флаги атрибута» (Attr. Flags) определяет, является атрибут опционным (бит 0 = 1) или стандартным (бит 0 = 0). Бит 1 этого поля определяет, является атрибут переходным (бит 1 = 1) или непереходным (бит 1 = 0). Для обычных атрибутов этот бит должен быть равен 1. Третий бит (бит 2) поля

флагов атрибута определяет, является информация в опционном переходном атрибуте полной (бит 2 = 0) или частичной (бит 2 = 1). Для обычных и опционных непереходных атрибутов этот бит должен быть равен 0. Бит 3 поля флагов атрибута информирует о том, имеет длина атрибута один байт (бит 3 = 0) или два байта (бит 3 = 1). Бит 3 может быть равен 1 только в случае, когда длина атрибута более 255 байтов. Младшие четыре бита октета флагов атрибута не используются (и должны обнуляться). Если бит 3 = 0, то третий байт атрибута пути содержит длину поля данных атрибута в байтах. Если же бит 3 = 1, то третий и четвертый байты атрибута пути хранят длину поля данных атрибута. Остальные байты поля «Атрибут пути» характеризуют значение атрибута и интерпретируются согласно флагам атрибута.

Атрибуты пути бывают «стандартные обязательные» (Well-known Mandatory), «стандартные на усмотрение оператора» (Well-known Discretionary), «опционные переходные» (Optional Transitive) и «опционные непереходные» (Optional Non-transitive). Стандартные атрибуты должны распознаваться любыми BGP-приложениями. Опционные атрибуты могут не распознаваться некоторыми приложениями. Обработка нераспознанных атрибутов задается битом 1 поля флагов. Пути с нераспознанными переходными опционными атрибутами должны восприниматься как рабочие. Один и тот же атрибут может появляться в списке атрибутов пути только один раз.

4. Сообщение типа KEEPALIVE.BGP не использует никакой транспортный протокол для механизма Keepalive, чтобы определить достижимы ли Peers. Сообщения KEEPALIVE обмениваются между Peers с определенным интервалом сообщений KEEPALIVE, значение которого 1/3 от Hold Timer, но не чаще раза в секунду. Сообщение KEEPALIVE состоит из заголовка (Header) и имеет длину 19 байтов.

5. Сообщение NOTIFICATION. Формат сообщения представлен на рис. 4.9.

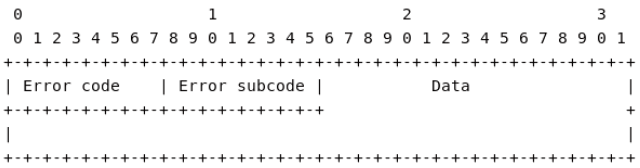


Рис. 4.9. Формат сообщения NOTIFICATION

Сообщение NOTIFICATION (Уведомление) отправляется, когда ошибки обнаружены, при этом соединение BGP закрывается сразу же после отправки. Однобайтное поле «Код ошибки» (Error Code) указывает на тип NOTIFICATION. Значения данного поля представлены ниже. Однобайтное поле «Подкод ошибки» (Error Subcode) обеспечивает более конкретную информацию о характере сообщения об ошибке. Значения данного поля представлены в табл. 4.2.

Таблица 4.2

Подкоды ошибок

Ошибка	Субкод	Описание
Заголовок	1	Соединение не синхронизовано
	2	Неверная длина сообщения
	3	Неверный тип сообщения
Сообщение OPEN	1	Неверный код версии
	2	Ошибочный код AS-партнера
	3	Ошибочный идентификатор BGP
	4	Ошибка в коде идентификации
	5	Ошибка при идентификации
	6	Неприемлемое время сохранения
Сообщение UPDATE	1	Ошибка в списке атрибутов
	2	Не узнан стандартный атрибут
	3	Отсутствует стандартный атрибут
	4	Ошибка в флагах атрибута
	5	Ошибка в длине атрибута
	6	Неправильный атрибут Origin
	7	Циклический маршрут
	8	Ошибка в атрибуте NEXT_HOP
	9	Ошибка в опционном атрибуте
	10	Ошибка в сетевом поле
	11	Ошибка в AS_PATH

Коды ошибок:

Код ошибки	Описание
1	Ошибка в заголовке сообщения
2	Ошибка в сообщении Open
3	Ошибки в сообщении Update
4	Истекло время сохранения
5	Ошибка машины конечных состояний
6	Прерывание

Атрибуты пути в BGP:

1. ORIGIN (код типа = 1) – стандартный обязательный атрибут, который определяет происхождение путевой информации. Генерируется автономной системой, которая является источником маршрутной информации. Атрибут в этом случае может принимать следующие значения:

– код атрибута = IGP, если информация достижимости сетевого уровня является внутренней по отношению к исходной автономной системе;

– код атрибута = EGP, если информация достижимости сетевого уровня получена с помощью внешнего протокола маршрутизации;

– код атрибута = Incomplete, если информация достижимости сетевого уровня получена каким-то иным способом.

2. AS_PATH (код типа = 2) также является стандартным обязательным атрибутом, который составлен из совокупности сегментов пути. Атрибут определяет автономные системы, через которые доставлена маршрутная информация. Когда BGP-роутер передает описание маршрута, которое он получил от своего BGP-партнера, он модифицирует AS_PATH-атрибут (добавляет номер своей AS в конец списка AS-маршрута), соответствующий этому маршруту, если информация передается за пределы автономной системы. Каждый сегмент AS_PATH состоит из трех частей <тип сегмента пути, длина сегмента пути и оценка сегмента пути>. Тип сегмента пути представляет, в свою очередь, однобайтное поле, которое может принимать следующие значения:

– код типа сегмента = AS_set: неупорядоченный набор маршрутов в UPDATE-сообщении;

– код типа сегмента = AS_sequence: упорядоченный набор маршрутов автономной системы в UPDATE-сообщении.

Длина сегмента пути представляет собой однобайтное поле, содержащее число автономных систем, записанных в поле «Оценка сегмента пути». Последнее поле хранит один или более кодов автономной системы, по два байта каждый.

3. NEXT_HOP (код типа = 3) – стандартный обязательный атрибут, определяющий IP-адрес пограничного роутера, который должен рассматриваться как цель следующего шага на пути к точке назначения.

4. MULTI_EXIT_DISC (MED) (код типа = 4) представляет собой опционный непереходной атрибут, который занимает четыре байта и является положительным целым числом. Величина этого атрибута может использоваться при выборе одного из нескольких путей к соседней автономной системе.

5. LOCAL_PREF (код типа = 5) является опционным атрибутом, занимающим четыре байта. Он используется BGP-роутером, чтобы сообщить своим BGP-партнерам внутри своей собственной автономной системы степень предпочтения объявленного маршрута.

6. ATOMIC_AGGREGATE (код типа = 6) представляет собой стандартный атрибут, который используется для информирования партнеров о выборе маршрута, обеспечивающего доступ к более широкому списку адресов.

7. AGGREGATOR (код типа = 7) – опционный переходной атрибут с длиной в шесть байтов. Атрибут содержит последний код автономной системы, который определяет агрегатный маршрут (занимает два байта), и IP-адрес BGP-роутера, который сформировал этот маршрут (четыре байта).

8. WEIGHT – это специальный атрибут, который используется только роутерами Cisco в процессе выбора наилучшего пути к какому-то роутеру или сети, если к нему ведет больше одного пути. Значение Weight Attribute является локальным для роутера,

на котором оно устанавливается. Это значение не передается в таблицах маршрутизации на другие роутеры.

9. COMMUNITY – опционный переходный атрибут, влияющий на принятие решения роутера о распространении полученного маршрута.

В Cisco используются следующие значения:

– No-Export – не передавать полученный маршрут к eBGP Peers. Распространять маршрут только в пределах AS;

– No-Advertise – не передавать полученный маршрут ни к Internal ни к External Peers;

– Internet – передавать полученный маршрут всем;

– Local-AS – ипользовать сценарии Confederation для предотвращения передачи маршрута вне локальной AS.

Алгоритм выбора наилучшего маршрута в BGP

BGP может получить различные обновления об одном маршруте от разных источников. BGP выбирает только один, самый лучший путь. Когда путь выбран, BGP помещает выбранный путь в свою таблицу маршрутизации и распространяет этот путь к своим «соседям». BGP использует следующие критерии, в указанном порядке, чтобы выбрать лучший путь:

1. Если у пути указан NEXT_HOP, который недоступен, то отбросить путь.

2. Выбирается путь с наибольшим атрибутом WEIGHT (только на устройствах Cisco).

3. Если вес одинаков, выбирается путь с наибольшим атрибутом Local Preference.

4. Если значения Local Preference одинаковы, то выбирается путь, который порожден локальным процессом BGP на данном роутере.

5. Если пути не порождены локальным BGP, то выбирается путь с кратчайшим атрибутом AS_PATH.

6. Если значения AS_PATH Length одинаковы, то выбирается путь с наименьшим атрибутом ORIGIN TYPE (где IGP меньше, чем EGP, а EGP меньше, чем Incomplete).

7. Если Origin Codes одинаковы, то выбирается путь с наименьшим атрибутом MED.

8. Если MED одинаковы, то путь External имеет предпочтение перед Internal.

9. Если оба пути External или Internal, то выбирается путь от ближайшего BGP соседа.

10. Выбирается путь с наименьшим IP-адресом (BGP Router ID).

Administrative Distance для протокола BGP равно 20.

4.1.4. Настройка оборудования Cisco

Начальное состояние командной строки – привилегированный режим EXEC Cisco IOS. Курсивом показаны переменные. В квадратных скобках – опциональные атрибуты. В фигурных и без скобок – обязательные атрибуты; если их несколько и они отделены чертой, то при вводе команды выбирается только один из них. Чтобы отменить команду, она повторно вводится с *no* в начале. В данном пособии не у всех команд указаны все атрибуты, для просмотра атрибутов пользуйтесь помощью IOS либо руководствами Command reference guide на нужное устройство Cisco.

4.1.4.1. Настройка статического маршрута на роутерах Cisco

Создание статического маршрута:

– вход в глобальный режим конфигурации

```
configure terminal
```

– создание статического маршрута.

```
ip route [vrf vrf-name] prefix mask {ip-address | interface-type interface-number [ip-address]} [dhcp] [distance] [name next-hop-name] [permanent | track number] [tag tag]
```

Здесь vrf – опциональный атрибут, который настраивает имя VRF (vrf-name), в которой статические маршруты должны быть указаны;

prefix – префикс маршрута;

mask – маска маршрута;

ip-address | interface-type interface-number – указывается либо IP-адрес Next Hop, либо исходящий интерфейс;

dhcp – опциональный атрибут, позволяет серверу Dynamic Host Configuration Protocol (DHCP) назначать этот маршрут как Default Route;

distance – Administrative Distance. По умолчанию для статических маршрутов равна 1;

name – опциональный атрибут, назначает имя на Next Hop Route (next-hop-name);

permanent – опциональный атрибут, при котором маршрут не будет удален из таблицы маршрутизации если Next Hop Interface будет выключен;

track – опциональный атрибут, который ассоциирует track object с этим маршрутом, number argument от 1 до 500;

tag – значение tag может быть использовано командами route map.

Просмотр таблицы маршрутизации на роутере

```
show ip route
```

4.1.4.2. Настройка протокола маршрутизации RIP

Включение протокола RIP на роутере:

– вход в глобальный режим конфигурации

```
configure terminal
```

– включение и вход в режим конфигурирования RIP

```
router rip
```

– настройка версии RIP

```
version {1 | 2}
```

– настройка сетей, участвующих в работе протокола RIP (указываются не только сети, участвующие в обновлении, но и сети, в которые будут посылаться сообщения RIP)

network ip-address

– перераспределение маршрута по умолчанию на роутере в обновления RIP

default-information originate

– включение автосуммирования маршрутов (суммирует в границах главных сетей)

auto-summary

– настрока таймеров RIP

`timers basic Interval_between_updates_for_RIP Invalid Holddown Flush Sleep`

– настройка интерфейса в Passive Mode (в него не отправляются сообщения

passive-interface interface-id

– просмотр запущенных протоколов маршрутизации

show ip protocols

– просмотр таблицы маршрутизации на роутере

show ip route

– запуск отладки работы протокола RIP

debug ip rip

Несколько слов о команде глобального режима конфигурации *IP Classless*. Данная команда влияет только на операцию посылки пакета. Иногда роутер получает пакеты для подсети, к которой нет маршрута и маршрут по умолчанию отсутствует, но у роутера есть маршрут для сети, в которую входит данная подсеть. Для пересылки этих пакетов по наилучшему маршруту (с наилучшим совпадением в таблице маршрутизации, а не с совпадением по маске, соответствующей классу сети A, B, C) используется команда глобального конфигурирования IP Classless.

Данная команда стандартно включена в конфигурации всех операционных систем Cisco IOS, начиная с версии 11.3 и выше. Для отключения этой функции используется форма данной коман-

ды с ключевым словом *no*. В случае, когда функция отключена и пакет пересылается в подсеть сети, к которой нет маршрута в таблице маршрутизации, – пакет отбрасывается. Принцип работы команды проиллюстрирован на рис. 4.10.

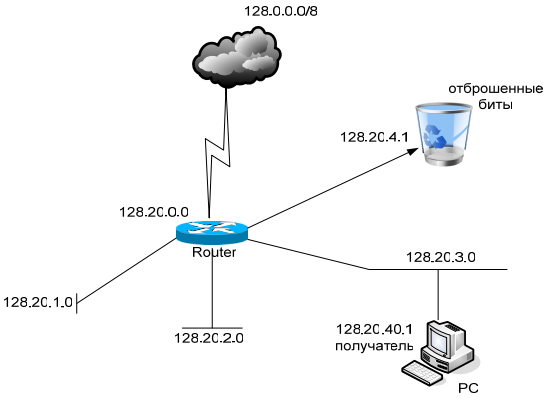


Рис. 4.10. No IP Classless

На рис. 4.10 у роутера (Router) есть четыре маршрута к сетям с префиксами: 128.0.0.0/8, 128.20.1.0/24, 128.20.2.0/24, 128.20.3.0/24, но к сети 128.20.4.0/24 маршрута нет и маршрута по умолчанию нет. При этом сеть 128.20.4.0/24 входит в сеть 128.0.0.0/8. Если роутер при выключенной функции IP Classless получит пакет к сети 128.20.4.1 и маршрут для данной подсети отсутствует, как в данном примере, то пакет отбрасывается. Если функция IP Classless включена, то пакет будет отправлен по маршруту с префиксом 128.0.0.0/8. Команда IP Classless воздействует только на операцию пересылки пакета, выполняемую операционной системой IOS. Она не влияет на построение таблиц маршрутизации. Описанный характер воздействия команды выражает сущность бесклассовой маршрутизации.

Несколько слов о команде глобального режима конфигурации *IP Subnet Zero*. Согласно документу RFC 950 подсети Subnet Zero (подсеть «все нули») и All-Ones Subnet (подсеть «все 1») использо-

вать не рекомендуется. Это полезно, чтобы сохранить и расширить толкование специальных адресов подсети и широковещательного адреса в подсетях. И все же, введя на роутере команду IP Subnet Zero, можно нарушить данное правило. В современных версиях IOS данная функция включена по умолчанию (начиная с версии 12.0).

Например, есть сеть класса B – 172.16.0.0/16. Разбиваем ее на подсети 172.16.0.0/24, 172.16.1.0/24–172.16.255.0/24. Подсеть 172.16.0.0/24 называется Subnet Zero (подсеть «все нули»), так как адрес данной подсети неотличим от адреса исходной сети. Подсеть 172.16.255.0/24 называется All-Ones Subnet, так как широковещательный адрес данной подсети неотличим от широковещательного адреса исходной подсети

4.1.4.3. Настройка протокола маршрутизации BGP-4

Включение протокола BGP-4 на роутере:

– вход в глобальный режим конфигурации

```
configure terminal
```

– включение и вход в режим конфигурирования BGP

```
router bgp AS_number
```

– отключение синхронизации

```
no synchronization
```

– настройка «соседей» по BGP

```
neighbor ip_address remote-as remote_AS_number
```

– настройка md5 авторизации с «соседом»

```
neighbor ip_address password 0 password
```

– настройка фильтрации маршрутов по AS_PATH к/от «соседа»

```
neighbor ip_address filter-list access_list_number_as_path {in | out}
```

– настройка фильтрации маршрутов и изменения атрибутов маршрута с помощью Route Map

```
- neighbor {ip-address | peer-group-name} route-map map-name {in | out}
```

– настройка фильтрации маршрутов по префиксам к/от «соседа»

`neighbor {ip-address | peer-group-name} distribute-list {access-list-number | expanded-list-number | access-list-name| prefix-list-name} {in | out}`

– настройка списка сетей, которые будут анонсироваться по BGP (в отличие от RIP в BGP данной командой объявляется только список анонсируемых сетей)

`network {network-number [mask network-mask] | nsap-prefix} [route-map map-tag]`

– отключение автосуммирования

`no auto-summary`

– настройка таймеров BGP

`timers bgp Keepalive_interval Holdtime Minimum_hold_time_from_neighbor`

– перераспределение статических маршрутов на роутере в обновления BGP

`redistribute static [metric {metric-value | transparent}]`

Настройка стандартных Access-List на роутере для IP-адресов

– вход в глобальный режим конфигурации

`configure terminal`

– команды создания строки Access-List, строки читаются последовательно; если обрабатываемая сеть и сеть в Access-List совпадают, то происходит обработка согласно строке, иначе читается следующая строка. В конце списка всегда предполагается правило, отбрасывающее все, что не совпало.

`access-list access-list-number {permit|deny} {host|source source-wildcard|any}`

Здесь Access-List-Number < 100.

Настройка стандартных Access-List на роутере для AS_Path:

– вход в глобальный режим конфигурации

`configure terminal`

– команды создания строки Access-List, строки читаются последовательно; если обрабатываемая сеть и сеть в Access-List совпадают, то происходит обработка согласно строке, иначе читается

следующая строка. В конце списка всегда предполагается правило, отбрасывающее все, что не совпало

ip as-path access-list-number {permit | deny} regexp

Здесь access-list-number < 100;

regexp – регулярное выражение.

Символы, которые используются в регулярных выражениях:

. – любой символ, включая пробел;

* – ноль или больше совпадений с выражением;

+ – одно или больше совпадений с выражением;

? – ноль или одно совпадение с выражением;

^ – начало строки;

$ – конец строки;

_ – любой разделитель (включая, начало, конец, пробел, табуляцию, запятую);

\ – не воспринимать следующий символ как специальный;

[] – совпадение с одним из символов в диапазоне;

| – логическое «или».

Примеры регулярных выражений:

_67_ – маршруты, проходящие через AS 67;

^67$ – маршруты из непосредственно присоединенной AS 67;

_67$ – маршруты отправленные из AS 67;

^67_ – сети находящиеся за AS 67;

^$ – маршруты локальной AS;

.* – любая строка.

Для просмотра маршрутов, которые попадают под ваше регулярное выражение, наберите команду

show ip bgp regexp regexp

Настройка Route Map на роутере:

– вход в глобальный режим конфигурации

configure terminal

– создание и вход в режим конфигурации Route Map. При создании нескольких Route Map с одинаковым именем, но разными Sequence-номерами они обрабатываются подряд, начиная с наименьшего Sequence Number.

route-map Name [[permit | deny] | [sequence-number]]

– настройка отбора маршрутов по AS_Path Access-List

match as-path access-list-number

– настройка отбора маршрутов по префиксу сетей

match ip address access-list-number

– установка атрибута пути к отобранным маршрутам

set {as-path tag | community | metric | local-preference | metric-type | origin | weight} attribite

– просмотр параметров работы BGP

show ip bgp summary

– просмотр соседей BGP

show ip bgp neighbors

– просмотр маршрутов BGP

show ip bgp

– просмотр маршрута BGP

show ip bgp prefix

– запуск отладки работы протокола BGP

debug ip bgp

4.2. Лабораторная работа «Протоколы маршрутизации RIP и BGP-4»

Соберите топологию, указанную на рис. 4.11. Соединив разъемы на патч-панели патчкордами типа Straight-Touch согласно рис. 4.12 (роутеры Router 1, Router 2, Router 3 и Router 4 соединяются кабелем типа Crossover). Попросите лаборанта соединить Serial-интерфейсы роутеров согласно топологии. Проведите начальную конфигурацию роутеров. Для доступа к роутерам используйте терминальный сервер:

– для доступа к r1.lab запустите *telnet 192.168.0.110 2007*;

– для доступа к r2.lab запустите *telnet 192.168.0.110 2008*;

– для доступа к r3.lab запустите *telnet 192.168.0.110 2009*;

– для доступа к r4.lab запустите *telnet 192.168.0.110 2010.*

* Имя student, пароль student.

Также подключите компьютеры (PC1, PC2, PC3, PC4), которые должны осуществлять связь с определенным роутером, и настройте вручную IP-адрес, маску подсети и основной шлюз согласно топологии.

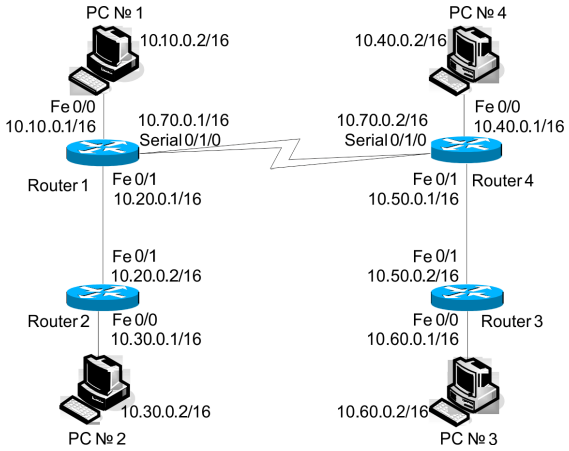


Рис. 4.11. Топология сети

Если роутеры не настраивались ранее, выполните начальную конфигурацию (Имя устройства, шифрование паролей, логин (student) и пароль доступа (student) на терминальные и консольные линии доступа, баннер на вход), для этого **выполните приведенную ниже последовательность команд для роутера из привилегированного режима EXEC Cisco IOS (меняя имя роутера естественно):**

```
conf t
hostname r1.lab
service password-encryption
no ip domain-lookup
username student privilege 15 secret 0 student
banner motd ^C
r1.lab
PERM, Russia,
Network technology lab. IT department. PSTU
Warning: Authorized access only!!!
```

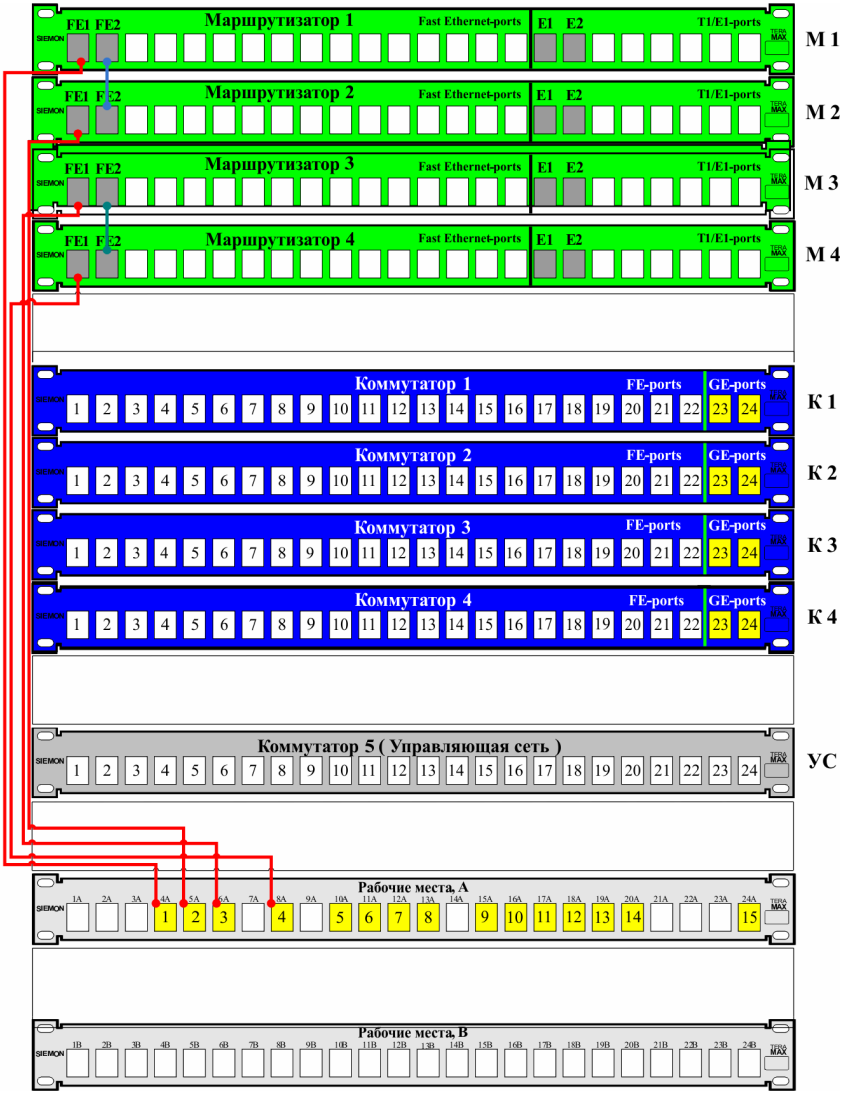


Рис. 4.12. Соединения на коммутационном поле

```
    Disconnect IMMEDIATELY if you are not an authorized
person!!!
    Contact information:
    web http://wrls.ru
    email support@wrls.ru
    tel +7(342)220-63-85
    ^C
    line con 0
    login local
    line aux 0
    line vty 0 4
    login local
    line vty 5 15
    login local
```

Настроим IP-адреса и маску подсети на интерфейсах Fast Ethernet. На интерфейсах Serial настроим инкапсуляцию PPP с протоколом авторизации CHAP и паролем Pass согласно топологии:

```
    R1:
    r1.lab#conf t
    r1.lab(config)#username r4 privilege 0 password 0 pass
    r1.lab(config)#interface FastEthernet0/0
    r1.lab(config-if)# ip address 10.10.0.1 255.255.0.0
    r1.lab(config-if)# duplex auto
    r1.lab(config-if)# speed auto
    r1.lab(config-if)#!
    r1.lab(config-if)#interface FastEthernet0/1
    r1.lab(config-if)# ip address 10.20.0.1 255.255.0.0
    r1.lab(config-if)# duplex auto
    r1.lab(config-if)# speed auto
    r1.lab(config-if)#!
    r1.lab(config-if)#interface Serial0/1/0
    r1.lab(config-if)# ip address 10.70.0.1 255.255.0.0
    r1.lab(config-if)# encapsulation ppp
    r1.lab(config-if)# ppp authentication chap
    r1.lab(config-if)# ppp chap hostname r1
    r1.lab(config-if)# ppp chap password 0 pass
```

```
R2:
r2.lab#conf t
r2.lab(config)#interface FastEthernet0/0
r2.lab(config-if)# ip address 10.30.0.1 255.255.0.0
r2.lab(config-if)# duplex auto
r2.lab(config-if)# speed auto
r2.lab(config-if)#!
r2.lab(config-if)#interface FastEthernet0/1
r2.lab(config-if)# ip address 10.20.0.2 255.255.0.0
r2.lab(config-if)# duplex auto
r2.lab(config-if)# speed auto

R3:
r3.lab#conf t
r3.lab(config)#interface FastEthernet0/0
r3.lab(config-if)# ip address 10.60.0.1 255.255.0.0
r3.lab(config-if)# duplex auto
r3.lab(config-if)# speed auto
r3.lab(config-if)#!
r3.lab(config-if)#interface FastEthernet0/1
r3.lab(config-if)# ip address 10.50.0.2 255.255.0.0
r3.lab(config-if)# duplex auto
r3.lab(config-if)# speed auto

R4:
r4.lab#conf t
r4.lab(config)#username r1 privilege 0 password 0 pass
r4.lab(config)#interface FastEthernet0/0
r4.lab(config-if)# ip address 10.40.0.1 255.255.0.0
r4.lab(config-if)# duplex auto
r4.lab(config-if)# speed auto
r4.lab(config-if)#!
r4.lab(config-if)#interface FastEthernet0/1
r4.lab(config-if)# ip address 10.50.0.1 255.255.0.0
r4.lab(config-if)# duplex auto
r4.lab(config-if)# speed auto
r4.lab(config-if)#!
r4.lab(config-if)#interface Serial0/1/0
r4.lab(config-if)# ip address 10.70.0.2 255.255.0.0
r4.lab(config-if)# encapsulation ppp
r4.lab(config-if)# clock rate 128000
r4.lab(config-if)# ppp authentication chap
```

```
r4.lab(config-if)# ppp chap hostname r4
r4.lab(config-if)# ppp chap password 0 pass
r4.lab(config-if)#clock rate 128000
```

* У Serial-кабеля один конец типа DTE, второй типа DCE, команда Clock Rate вводится на интерфейсе, к которому подключен DCE. Посмотреть, какой тип кабеля подключен, можно командой Show Controllers Interface_ID:

```
r4.lab#show controllers Serial 0/1/0
Interface Serial0/1/0
Hardware is PowerQUICC MPC860
DCE V.35, no clock
idb at 0x81081AC4, driver data structure at 0x81084AC0
SCC Registers:
General GSMR]=0x2:0x00000000, Protocol-specific
[PSMR]=0x8
Events [SCCE]=0x0000, Mask [SCCM]=0x0000, Status
[SCCS]=0x00
Transmit on Demand [TODR]=0x0, Data Sync [DSR]=0x7E7E
Interrupt Registers:
```

Удостоверимся, что роутеры могут пинговать своего соседа и подключенные PC. При проблемах выполним команду *Show IP Int Brief* для анализа того, какие порты сконфигурированы неправильно.

4.2.1. Статическая маршрутизация

Настроим статические маршруты на роутерах, для этого выполним команды:

```
R1:
r1.lab#conf t
r1.lab(config)#ip route 10.30.0.0 255.255.0.0
10.20.0.2
r1.lab(config)#ip route 10.40.0.0 255.255.0.0
10.70.0.2
r1.lab(config)#ip route 10.60.0.0 255.255.0.0
10.70.0.2
```

```
    R2:
    r2.lab#conf t
    r2.lab(config)#ip   route   10.10.0.0   255.255.0.0
10.20.0.1
    r2.lab(config)#ip   route   10.40.0.0   255.255.0.0
10.20.0.1
    r2.lab(config)#ip   route   10.60.0.0   255.255.0.0
10.20.0.1

    R3:
    r3.lab#conf t
    r3.lab(config)#ip   route   10.40.0.0   255.255.0.0
10.50.0.1
    r3.lab(config)#ip   route   10.10.0.0   255.255.0.0
10.50.0.1
    r3.lab(config)#ip   route   10.30.0.0   255.255.0.0
10.50.0.1

    R4:
    r4.lab#conf t
    r4.lab(config)#ip   route   10.60.0.0   255.255.0.0
10.50.0.2
    r4.lab(config)#ip   route   10.10.0.0   255.255.0.0
10.70.0.1
    r4.lab(config)#ip   route   10.30.0.0   255.255.0.0
10.70.0.1
```

В случае если статические маршруты настроены правильно, вывод команд Show IP Route будет следующим:

```
    R1:
    r1.lab#show ip route
    Codes: C -connected, S -static, R – RIP, M – mo-
bile, B – BGP, D -EIGRP, EX -EIGRP external, O -OSPF,
IA – OSPF inter area, N1 -OSPF NSSA external type1,
N2 -OSPF NSSA external type 2, E1 -OSPF external type
1, E2 – OSPF external type 2, i -IS-IS, su -IS-IS sum-
mary, 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
    10.0.0.0/8 is variably subnetted, 7 subnets, 2 masks
    C 10.10.0.0/16 is directly connected, FastEthernet0/0
    S 10.30.0.0/16 [1/0] via 10.20.0.2
    C 10.20.0.0/16 is directly connected, FastEthernet0/1
    S 10.40.0.0/16 [1/0] via 10.70.0.2
    S 10.60.0.0/16 [1/0] via 10.70.0.2
    C 10.70.0.0/16 is directly connected, Serial0/1/0
    C 10.70.0.2/32 is directly connected, Serial0/1/0
    * S – статический маршрут. В скобках – [Administra-
tive Distance/ Metric]. После Via – IP-адрес Next Hop.

    R2:
    r2.lab#show ip route
    Codes: C – connected, S – static, R – RIP, M – mo-
bile, B – BGP, …
    10.0.0.0/16 is subnetted, 5 subnets
    S 10.10.0.0 [1/0] via 10.20.0.1
    C 10.30.0.0 is directly connected, FastEthernet0/0
    C 10.20.0.0 is directly connected, FastEthernet0/1
    S 10.40.0.0 [1/0] via 10.20.0.1
    S 10.60.0.0 [1/0] via 10.20.0.1

    R3:
    r3.lab#show ip route
    Codes: C – connected, S – static, R – RIP, M – mo-
bile, B – BGP, …
    10.0.0.0/16 is subnetted, 5 subnets
    S 10.10.0.0 [1/0] via 10.50.0.1
    S 10.30.0.0 [1/0] via 10.50.0.1
    S 10.40.0.0 [1/0] via 10.50.0.1
    C 10.60.0.0 is directly connected, FastEthernet0/0
    C 10.50.0.0 is directly connected, FastEthernet0/1

    R4:
    r4.lab#show ip route
    Codes: C – connected, S – static, R – RIP, M – mo-
bile, B – BGP
    10.0.0.0/8 is variably subnetted, 7 subnets, 2 masks
    S 10.10.0.0/16 [1/0] via 10.70.0.1
    S 10.30.0.0/16 [1/0] via 10.70.0.1
    C 10.40.0.0/16 is directly connected, FastEthernet0/0
    S 10.60.0.0/16 [1/0] via 10.50.0.2
```

```
C 10.50.0.0/16 is directly connected, FastEthernet0/1
C 10.70.0.0/16 is directly connected, Serial0/1/0
C 10.70.0.1/32 is directly connected, Serial0/1/0
```

Протестируем работу статической маршрутизации:

Компьютер PC2 с адресом 10.30.0.2:

- Послать эхо-запросы ping к узлам: PC1 с адресом 10.10.0.2; PC4 с адресом 10.40.0.2; PC3 с адресом 10.60.0.2 – работает (пинги пойдут не сразу, так как нужно время, чтобы заполнить таблицы MAC-адресов на всех коммутаторах).

Удалим статические маршруты с роутеров:

```
R1:
r1.lab#conf t
r1.lab(config)#no ip route 10.30.0.0 255.255.0.0
10.20.0.2
r1.lab(config)#no ip route 10.40.0.0 255.255.0.0
10.70.0.2
r1.lab(config)#no ip route 10.60.0.0 255.255.0.0
10.70.0.2

R2:
r2.lab#conf t
r2.lab(config)#no ip route 10.10.0.0 255.255.0.0
10.20.0.1
r2.lab(config)#no ip route 10.40.0.0 255.255.0.0
10.20.0.1
r2.lab(config)#no ip route 10.60.0.0 255.255.0.0
10.20.0.1

R3:
r3.lab#conf t
r3.lab(config)#no ip route 10.40.0.0 255.255.0.0
10.50.0.1
r3.lab(config)#no ip route 10.10.0.0 255.255.0.0
10.50.0.1
r3.lab(config)#no ip route 10.30.0.0 255.255.0.0
10.50.0.1

R4:
r4.lab#conf t
r4.lab(config)#no ip route 10.60.0.0 255.255.0.0
10.50.0.2
```

```
    r4.lab(config)#no ip route 10.10.0.0 255.255.0.0
10.70.0.1
    r4.lab(config)#no ip route 10.30.0.0 255.255.0.0
10.70.0.1
```

4.2.2. RIP-маршрутизация

Настроим протокол RIPv1 на роутерах, для этого выполним команды:

```
    R1:
    r1.lab#conf t
    r1.lab(config)#router rip
    r1.lab(config-router)#version 1
    r1.lab(config-router)#network 10.10.0.0
    r1.lab(config-router)#network 10.20.0.0
    r1.lab(config-router)#network 10.70.0.0

    R2:
    r2.lab#conf t
    r2.lab(config)#router rip
    r2.lab(config-router)#version 1
    r2.lab(config-router)#network 10.30.0.0
    r2.lab(config-router)#network 10.20.0.0

    R3:
    r3.lab#conf t
    r3.lab(config)#router rip
    r3.lab(config-router)#version 1
    r3.lab(config-router)#network 10.60.0.0
    r3.lab(config-router)#network 10.50.0.0

    R4:
    r4.lab#conf t
    r4.lab(config)#router rip
    r4.lab(config-router)#version 1
    r4.lab(config-router)#network 10.40.0.0
    r4.lab(config-router)#network 10.50.0.0
    r4.lab(config-router)#network 10.70.0.0
```

Подождем несколько минут, пока RIP сойдется. Проверим правильность настроек командами Show IP Protocols, Show IP Route:

R1:

```
r1.lab#show ip protocols
Routing Protocol is "rip"
Outgoing update filter list for all interfaces is not set
Incoming update filter list for all interfaces is not set
```

* Фильтрация маршрутов не настроена.

```
Sending updates every 30 seconds, next due in 6 seconds
Invalid after 180 seconds, hold down 180, flushed after 240
```

* Таймеры RIP.

```
Redistributing: rip
Default version control: send version 1, receive version 1
      Interface    Send Recv Triggered RIP Key-chain
  FastEthernet0/0   1    1
  FastEthernet0/1   1    1
    Serial0/1/0     1    1
Automatic network summarization is in effect
```

* Autosummary включено по умолчанию.

```
Maximum path: 4
Routing for Networks:
10.0.0.0
```

* RIP работает для сети 10.0.0.0 (команда Network применяет маску главной сети).

```
Routing Information Sources:
      Gateway          Distance        Last Update
    10.20.0.2            120            00:00:19
    10.70.0.2            120            00:00:15
Distance: (default is 120)
```

* Gateway – «роутеры-соседи» по RIP. Administrative Distance равно 120.

```
r1.lab#show ip route
Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP
10.0.0.0/8 is variably subnetted, 8 subnets, 2 masks
C 10.10.0.0/16 is directly connected, FastEthernet0/0
R  10.30.0.0/16  [120/1]  via  10.20.0.2,  00:00:19, FastEthernet0/1
```

C 10.20.0.0/16 is directly connected, FastEthernet0/1
R 10.40.0.0/16 [120/1] via 10.70.0.2, 00:00:14, Serial0/1/0
R 10.60.0.0/16 [120/2] via 10.70.0.2, 00:00:14, Serial0/1/0
R 10.50.0.0/16 [120/1] via 10.70.0.2, 00:00:14, Serial0/1/0
C 10.70.0.0/16 is directly connected, Serial0/1/0
C 10.70.0.2/32 is directly connected, Serial0/1/0
* R – маршрут, изученный по RIP. В скобках – [Administrative Distance/ Metric]. После Via – IP-адрес Next Hop и исходящий интерфейс.

R2:
r2.lab#show ip protocols
Routing Protocol is "rip"
Outgoing update filter list for all interfaces is not set
Incoming update filter list for all interfaces is not set
Sending updates every 30 seconds, next due in 3 seconds
Invalid after 180 seconds, hold down 180, flushed after 240
Redistributing: rip
Default version control: send version 1, receive version 1
Interface Send Recv Triggered RIP Key-chain
FastEthernet0/0 1 1
FastEthernet0/1 1 1
Automatic network summarization is in effect
Maximum path: 4
Routing for Networks:
10.0.0.0
Routing Information Sources:
Gateway Distance Last Update
10.20.0.1 120 00:00:01
Distance: (default is 120)

r2.lab#show ip route
Codes: C – connected, S – static, R – RIP, M – mobile, B – BGP

```
    10.0.0.0/8 is variably subnetted, 8 subnets, 2 masks
    R   0.10.0.0/16   [120/1]   via   10.20.0.1,   00:00:13,
FastEthernet0/1
    C 10.30.0.0/16 is directly connected, FastEthernet0/0
    C 10.20.0.0/16 is directly connected, FastEthernet0/1
    R   10.40.0.0/16   [120/2]   via   10.20.0.1,   00:00:13,
FastEthernet0/1
    R   10.60.0.0/16   [120/3]   via   10.20.0.1,   00:00:13,
FastEthernet0/1
    R   10.50.0.0/16   [120/2]   via   10.20.0.1,   00:00:13,
FastEthernet0/1
    R   10.70.0.0/16   [120/1]   via   10.20.0.1,   00:00:13,
FastEthernet0/1
    R   10.70.0.2/32   [120/1]   via   10.20.0.1,   00:00:13,
FastEthernet0/1


    R3:
    r3.lab#show ip protocols
    Routing Protocol is "rip"
    Outgoing update filter list for all interfaces is not
set
    Incoming update filter list for all interfaces is not
set
    Sending updates every 30 seconds, next due in 26
seconds
    Invalid after 180 seconds, hold down 180, flushed
after 240
    Redistributing: rip
    Default version control: send version 1, receive
version 1
    Interface Send Recv Triggered RIP Key-chain
    FastEthernet0/0 1 1
    FastEthernet0/1 1 1
    Automatic network summarization is in effect
    Maximum path: 4
    Routing for Networks:
    10.0.0.0
    Routing Information Sources:
    Gateway Distance Last Update
    10.50.0.1 120 00:00:02
    Distance: (default is 120)
    r3.lab#show ip route
```

```
    Codes: C - connected, S - static, R - RIP, M - mo-
bile, B - BGP
    10.0.0.0/8 is variably subnetted, 8 subnets, 2 masks
    R  10.10.0.0/16  [120/2]  via  10.50.0.1,  00:00:00,
FastEthernet0/1
    R  10.30.0.0/16  [120/3]  via  10.50.0.1,  00:00:00,
FastEthernet0/1
    R  10.20.0.0/16  [120/2]  via  10.50.0.1,  00:00:00,
FastEthernet0/1
    R  10.40.0.0/16  [120/1]  via  10.50.0.1,  00:00:00,
FastEthernet0/1
    C 10.60.0.0/16 is directly connected, FastEthernet0/0
    C 10.50.0.0/16 is directly connected, FastEthernet0/1
    R  10.70.0.0/16  [120/1]  via  10.50.0.1,  00:00:00,
FastEthernet0/1
    R  10.70.0.1/32  [120/1]  via  10.50.0.1,  00:00:00,
FastEthernet0/1


    R4:
    r4.lab#show ip protocols
    Routing Protocol is "rip"
    Outgoing update filter list for all interfaces is not
set
    Incoming update filter list for all interfaces is not
set
    Sending updates every 30 seconds, next due in 17
seconds
    Invalid after 180 seconds, hold down 180, flushed
after 240
    Redistributing: rip
    Default version control: send version 1, receive
version 1
    Interface Send Recv Triggered RIP Key-chain
    FastEthernet0/0 1 1
    FastEthernet0/1 1 1
    Serial0/1/0 1 1
    Automatic network summarization is in effect
    Maximum path: 4
    Routing for Networks:
    10.0.0.0
    Routing Information Sources:
    Gateway Distance Last Update
```

```
    10.50.0.2 120 00:00:10
    10.70.0.1 120 00:00:16
    Distance: (default is 120)
    r4.lab#show ip route
    Codes: C - connected, S - static, R - RIP, M - mo-
bile, B - BGP
    10.0.0.0/8 is variably subnetted, 8 subnets, 2
masks
    R 10.10.0.0/16 [120/1] via 10.70.0.1, 00:00:22, Se-
rial0/1/0
    R 10.30.0.0/16 [120/2] via 10.70.0.1, 00:00:22,
Serial0/1/0
    R 10.20.0.0/16 [120/1] via 10.70.0.1, 00:00:22,
Serial0/1/0
    C 10.40.0.0/16 is directly connected, FastEthernet0/0
    R 10.60.0.0/16 [120/1] via 10.50.0.2, 00:00:16,
FastEthernet0/1
    C 10.50.0.0/16 is directly connected, FastEthernet0/1
    C 10.70.0.0/16 is directly connected, Serial0/1/0
    C 10.70.0.1/32 is directly connected, Serial0/1/0
```

Протестируем работу маршрутизации RIP:

С компьютера PC2 с адресом 10.30.0.2 послать эхо-запросы ping к узлам: PC1 с адресом 10.10.0.2; PC4 с адресом 10.40.0.2; PC3 с адресом 10.60.0.2; – работает (пинги пойдут не сразу, так как нужно время, чтобы заполнить таблицы MAC-адресов на всех коммутаторах).

Теперь создадим разобщенную сеть. Поменяйте IP-адреса согласно рис. 4.13. Если до этого роутер R1, получив обновление о сетях 10.40.0.0, 10.50.0.0, 10.60.0.0, согласно «Правилу определения маски подсети в RIPv1» применял к ним маску 255.255.0.0, то теперь он будет применять маску 255.0.0.0. Аналогично будет действовать роутер R4. В результате роутеры получат обновление о сети 10.0.0.0/8, которое проигнорируют, поскольку имеют непосредственно подключенные подсети из этой главной сети.

Для смены IP-адресов выполним команды:

```
R1:
r1.lab#conf t
r1.lab(config)#interface s0/1/0
```

```
    r1.lab(config-if)#ip      address      192.168.100.1
255.255.255.252
    r1.lab(config-if)#exit
    r1.lab(config)#router rip
    r1.lab(config-router)#network 192.168.100.0
    R4:
    r4.lab#conf t
    r4.lab(config)#int serial 0/1/0
    r4.lab(config-if)#ip      address      192.168.100.2
255.255.255.252
    r4.lab(config-if)#exit
    r4.lab(config)#router rip
    r4.lab(config-router)#network 192.168.100.0
```

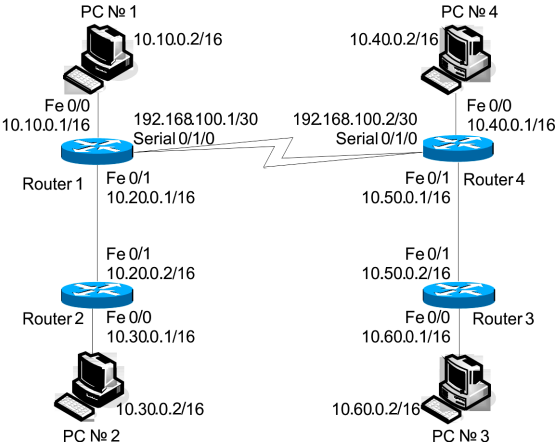


Рис. 4.13 Новая разобщенная топология сети

Подождем несколько минут, пока RIP сойдется, проверим содержимое таблиц маршрутизации командой *Show IP Route*:

```
    R1:
    r1.lab#show ip route
    Codes: C - connected, S - static, R - RIP, M - mo-
bile, B - BGP
    10.0.0.0/16 is subnetted, 3 subnets
    C 10.10.0.0 is directly connected, FastEthernet0/0
    R   10.30.0.0   [120/1]   via   10.20.0.2,   00:00:02,
FastEthernet0/1
```

```
    C 10.20.0.0 is directly connected, FastEthernet0/1
    192.168.100.0/24 is variably subnetted, 2 subnets,
2 masks
    C 192.168.100.0/30 is directly connected, Serial0/1/0
    C 192.168.100.2/32 is directly connected, Serial0/1/0
    * Количество маршрутов RIP уменьшилось.

    R2:
    r2.lab#show ip route
    Codes: C - connected, S - static, R - RIP, M - mo-
bile, B - BGP
    10.0.0.0/16 is subnetted, 3 subnets
    R   10.10.0.0   [120/1]   via   10.20.0.1,   00:00:16,
FastEthernet0/1
    C 10.30.0.0 is directly connected, FastEthernet0/0
    C 10.20.0.0 is directly connected, FastEthernet0/1
    R 192.168.100.0/24 [120/1] via 10.20.0.1, 00:00:16,
FastEthernet0/1

    R3:
    r3.lab#show ip route
    Codes: C - connected, S - static, R - RIP, M - mo-
bile, B - BGP
    10.0.0.0/16 is subnetted, 3 subnets
    R   10.40.0.0   [120/1]   via   10.50.0.1,   00:00:01,
FastEthernet0/1
    C 10.60.0.0 is directly connected, FastEthernet0/0
    C 10.50.0.0 is directly connected, FastEthernet0/1
    R 192.168.100.0/24 [120/1] via 10.50.0.1, 00:00:01,
FastEthernet0/1

    R4:
    r4.lab#show ip route
    Codes: C - connected, S - static, R - RIP, M - mo-
bile, B - BGP
    10.0.0.0/16 is subnetted, 3 subnets
    C 10.40.0.0 is directly connected, FastEthernet0/0
    R   10.60.0.0   [120/1]   via   10.50.0.2,   00:00:16,
FastEthernet0/1
    C 10.50.0.0 is directly connected, FastEthernet0/1
    192.168.100.0/24 is variably subnetted, 2 subnets,
2 masks
    C 192.168.100.0/30 is directly connected, Serial0/1/0
    C 192.168.100.1/32 is directly connected, Serial0/1/0
```

Включим отладку протокола RIP командой Debug IP RIP на R1.

Какие обновления маршрутизации он получает, почему?

Протестируем работу маршрутизации RIP.

С компьютера PC2 с адресом 10.30.0.2 послать эхо-запросы ping к узлам: PC4 с адресом 10.40.0.2; PC3 с адресом 10.60.0.2 – не работает; PC1 с адресом 10.10.0.2 – работает.

Для решения проблемы маршрутизации RIP в разобщенных сетях включим версию 2 протокола RIP, для этого выполним команды:

```
R1:
r1.lab#conf t
r1.lab(config)#router rip
r1.lab(config-router)#version 2

R2:
r2.lab#conf t
r2.lab(config)#router rip
r2.lab(config-router)#version 2

R3:
r3.lab#conf t
r3.lab(config)#router rip
r3.lab(config-router)#version 2

R4:
r4.lab#conf t
r4.lab(config)#router rip
r4.lab(config-router)#version 2
```

Подождем несколько минут, пока RIPv2 сойдется, проверим содержимое таблиц маршрутизации командой Show IP Route:

```
R1:
r1.lab#show ip route
Codes: C - connected, S - static, R - RIP, M - mo-
bile, B - BGP
10.0.0.0/8 is variably subnetted, 4 subnets, 2 masks
```

C 10.10.0.0/16 is directly connected, FastEthernet0/0
R 10.0.0.0/8 [120/1] via 192.168.100.2, 00:00:11, Serial0/1/0
R 10.30.0.0/16 [120/1] via 10.20.0.2, 00:00:08, FastEthernet0/1
C 10.20.0.0/16 is directly connected, FastEthernet0/1
192.168.100.0/24 is variably subnetted, 2 subnets, 2 masks
C 192.168.100.0/30 is directly connected, Serial0/1/0
C 192.168.100.2/32 is directly connected, Serial0/1/0
* Автосуммирование по умолчанию в версии 2 работает в границах главных подсетей. Как в данном случае влияет команда IP Classless?

R2:
r2.lab#show ip route
Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP
10.0.0.0/8 is variably subnetted, 4 subnets, 2 masks
R 10.10.0.0/16 [120/1] via 10.20.0.1, 00:00:20, FastEthernet0/1
R 10.0.0.0/8 [120/2] via 10.20.0.1, 00:00:20, FastEthernet0/1
C 10.30.0.0/16 is directly connected, FastEthernet0/0
C 10.20.0.0/16 is directly connected, FastEthernet0/1
R 192.168.100.0/24 [120/1] via 10.20.0.1, 00:00:20, FastEthernet0/1

R3:
r3.lab#show ip route
Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP
10.0.0.0/8 is variably subnetted, 4 subnets, 2 masks
R 10.0.0.0/8 [120/2] via 10.50.0.1, 00:00:24, FastEthernet0/1
R 10.40.0.0/16 [120/1] via 10.50.0.1, 00:00:24, FastEthernet0/1
C 10.60.0.0/16 is directly connected, FastEthernet0/0
C 10.50.0.0/16 is directly connected, FastEthernet0/1
R 192.168.100.0/24 [120/1] via 10.50.0.1, 00:00:24, FastEthernet0/1

```
R4:
r4.lab#show ip route
Codes: C - connected, S - static, R - RIP, M - mo-
bile, B - BGP
10.0.0.0/8 is variably subnetted, 4 subnets, 2 masks
R 10.0.0.0/8 [120/1] via 192.168.100.1, 00:00:06,
Serial0/1/0
C 10.40.0.0/16 is directly connected, FastEthernet0/0
R 10.60.0.0/16 [120/1] via 10.50.0.2, 00:00:09,
FastEthernet0/1
C 10.50.0.0/16 is directly connected, FastEthernet0/1
192.168.100.0/24 is variably subnetted, 2 subnets,
2 masks
C 192.168.100.0/30 is directly connected, Serial0/1/0
C 192.168.100.1/32 is directly connected, Serial0/1/0
```

Выполним команду *no IP Classless* и протестируем работу маршрутизации RIPv2.

С компьютера PC2 с адресом 10.30.0.2 послать эхо-запросы ping к узлам: PC4 с адресом 10.40.0.2; PC3 с адресом 10.60.0.2 – не работает. Почему?

Выполним команду *IP Classless* и протестируем работу маршрутизации RIPv2. Почему работает?

Отключим автосуммирование RIPv2, для этого выполним команды:

```
R1:
r1.lab#conf t
r1.lab(config)#router rip
r1.lab(config-router)# no auto-summary

R2:
r2.lab#conf t
r2.lab(config)#router rip
r2.lab(config-router)# no auto-summary
R3:
r3.lab#conf t
r3.lab(config)#router rip
r3.lab(config-router)# no auto-summary
```

```
R4:
r4.lab#conf t
r4.lab(config)#router rip
r4.lab(config-router)# no auto-summary
```

Подождем несколько минут, пока RIPv2 сойдется, проверим содержимое таблиц маршрутизации командой Show IP Route:

```
R1:
r1.lab#show ip route
Codes: C - connected, S - static, R - RIP, M - mo-
bile, B - BGP
10.0.0.0/8 is variably subnetted, 7 subnets, 2 masks
C 10.10.0.0/16 is directly connected, FastEthernet0/0
R 10.0.0.0/8 [120/1] via 192.168.100.2, 00:01:24,
Serial0/1/0
R 10.30.0.0/16 [120/1] via 10.20.0.2, 00:00:28,
FastEthernet0/1
C 10.20.0.0/16 is directly connected, FastEthernet0/1
R 10.40.0.0/16 [120/1] via 192.168.100.2, 00:00:24,
Serial0/1/0
R 10.60.0.0/16 [120/2] via 192.168.100.2, 00:00:24,
Serial0/1/0
R 10.50.0.0/16 [120/1] via 192.168.100.2, 00:00:24,
Serial0/1/0
192.168.100.0/24 is variably subnetted, 2 subnets,
2 masks
C 192.168.100.0/30 is directly connected, Serial0/1/0
C 192.168.100.2/32 is directly connected, Serial0/1/0
* После выключения автосуммирования маршрутов стало
больше.

R2:
r2.lab#show ip route
Codes: C - connected, S - static, R - RIP, M - mo-
bile, B - BGP
10.0.0.0/16 is subnetted, 6 subnets
R 10.10.0.0 [120/1] via 10.20.0.1, 00:00:22,
FastEthernet0/1
C 10.30.0.0 is directly connected, FastEthernet0/0
C 10.20.0.0 is directly connected, FastEthernet0/1
R 10.40.0.0 [120/2] via 10.20.0.1, 00:00:22,
FastEthernet0/1
```

```
    R   10.60.0.0   [120/3]   via   10.20.0.1,   00:00:22,
FastEthernet0/1
    R   10.50.0.0   [120/2]   via   10.20.0.1,   00:00:22,
FastEthernet0/1
    192.168.100.0/24 is variably subnetted, 3 subnets,
3 masks
    R 192.168.100.0/30 [120/1] via 10.20.0.1, 00:00:22,
FastEthernet0/1
    R 192.168.100.0/24 is possibly down,
    routing via 10.20.0.1, FastEthernet0/1
    R 192.168.100.2/32 [120/1] via 10.20.0.1, 00:00:22,
FastEthernet0/1

    R3:
    r3.lab#show ip route
    Codes: C - connected, S - static, R - RIP, M - mo-
bile, B - BGP
    10.0.0.0/16 is subnetted, 6 subnets
    R   10.10.0.0   [120/2]   via   10.50.0.1,   00:00:22,
FastEthernet0/1
    R   10.30.0.0   [120/3]   via   10.50.0.1,   00:00:22,
FastEthernet0/1
    R   10.20.0.0   [120/2]   via   10.50.0.1,   00:00:22,
FastEthernet0/1
    R   10.40.0.0   [120/1]   via   10.50.0.1,   00:00:22,
FastEthernet0/1
    C 10.60.0.0 is directly connected, FastEthernet0/0
    C 10.50.0.0 is directly connected, FastEthernet0/1
    192.168.100.0/24 is variably subnetted, 3 subnets,
3 masks
    R 192.168.100.0/30 [120/1] via 10.50.0.1, 00:00:22,
FastEthernet0/1
    R 192.168.100.0/24 is possibly down,
    routing via 10.50.0.1, FastEthernet0/1
    R 192.168.100.1/32 [120/1] via 10.50.0.1, 00:00:22,
FastEthernet0/1

    R4:
    r4.lab#show ip route
    Codes: C - connected, S - static, R - RIP, M - mo-
bile, B - BGP
    10.0.0.0/8 is variably subnetted, 7 subnets, 2 masks
```

```
    R 10.10.0.0/16 [120/1] via 192.168.100.1, 00:00:09,
Serial0/1/0
    R   10.0.0.0/8   is   possibly   down,routing   via
192.168.100.1, Serial0/1/0
    R 10.30.0.0/16 [120/2] via 192.168.100.1, 00:00:09,
Serial0/1/0
    R 10.20.0.0/16 [120/1] via 192.168.100.1, 00:00:09,
Serial0/1/0
    C 10.40.0.0/16 is directly connected, FastEthernet0/0
    R  10.60.0.0/16  [120/1]  via  10.50.0.2,  00:00:07,
FastEthernet0/1
    C 10.50.0.0/16 is directly connected, FastEthernet0/1
    192.168.100.0/24 is variably subnetted, 2 subnets,
2 masks
    C 192.168.100.0/30 is directly connected, Serial0/1/0
    C 192.168.100.1/32 is directly connected, Serial0/1/0
```

Запустив tcpdump на PC2, увидим сообщения RIP. Поясним поля в сообщениях RIP.

Отправлять сообщения RIP в интерфейсы, которые не участвуют в работе протокола, небезопасно. **Для запрета отправки сообщений в интерфейсы выполним следующие команды:**

```
    R1:
    r1.lab#conf t
    r1.lab(config)#router rip
    r1.lab(config-router)#passive-interface fa0/0

    R2:
    r2.lab#conf t
    r2.lab(config)#router rip
    r2.lab(config-router)#passive-interface fa0/0

    R3:
    r3.lab#conf t
    r3.lab(config)#router rip
    r3.lab(config-router)#passive-interface fa0/0
    R4:
    r4.lab#conf t
    r4.lab(config)#router rip
    r4.lab(config-router)#passive-interface fa0/0
```

Отключим протокол RIP, для этого выполните команды:

```
R1:
r1.lab(config)#no router rip

R2:
r2.lab#conf t
r2.lab(config)# no router rip

R3:
r3.lab#conf t
r3.lab(config)# no router rip

R4:
r4.lab#conf t
r4.lab(config)# no router rip
```

4.2.3. BGP-маршрутизация

Настройку BGP будем проводить согласно рис. 4.14.

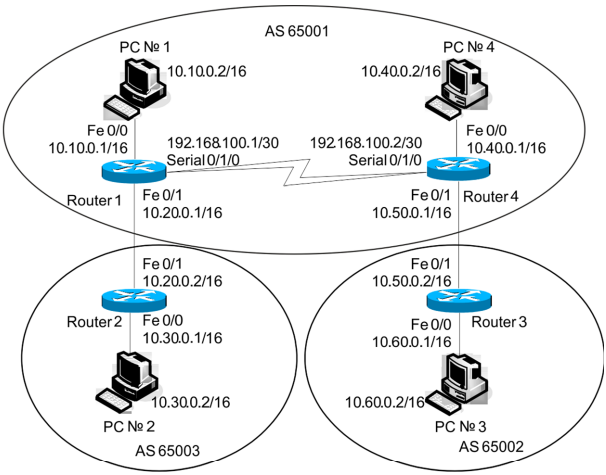


Рис. 4.14. Топология сети BGP

Несколько замечаний по поводу работы BGP в данной топологии:

1) роутеры R1 и R4 работают по iBGP (Internal);

2) роутеры R2 и R1, R4 и R3 работают по eBGP (External);

3) поскольку R1 и R4 находятся в одной AS (и работают по iBGP), то, для того чтобы роутер R4 посылал по eBGP обновление о сети 10.10.0.0 (информацию о которой он получил от R1), необходимо на R4 прописать команду Network 10.10.0.0. Аналогично поступаем для сети 10.40.0.0 на R1;

4) поскольку R1 и R4 находятся в одной AS (и работают по iBGP), то R1, получив обновление о сети 10.30.0.0 от R2 (AS65003), пошлет его к R4 с адресом Next Hop 10.20.0.2 (R2 Fa0/1). R4 не будет отправлять обновление о сети 10.30.0.0 к R3 до тех пор, пока у него не будет маршрута к 10.20.0.2 (R2 Fa0/1). В данной лабораторной работе мы прописываем статический маршрут к 10.20.0.2 (R2 Fa0/1) на роутере R4. Аналогично поступаем для сети 10.60.0.0 на R1.

Для начальной настройки BGP выполним следующую последовательность команд (пароль авторизации BGP: между R1 и R2 – bgppass1, между R1 и R4 – bgppass0, между R4 и R3 – bgppass2):

```
R1:
r1.lab#conf t
r1.lab(config)#ip route 10.50.0.0 255.255.0.0
192.168.100.2
r1.lab(config)#router bgp 65001
r1.lab(config-router)#no synchronization
r1.lab(config-router)# network 10.10.0.0 mask
255.255.0.0
r1.lab(config-router)# network 10.40.0.0 mask
255.255.0.0
r1.lab(config-router)# neighbor 10.20.0.2 remote-as
65003
r1.lab(config-router)# neighbor 10.20.0.2 password
0 bgppass1
r1.lab(config-router)# neighbor 192.168.100.2 re-
mote-as 65001
r1.lab(config-router)# neighbor 192.168.100.2 pass-
word 0 bgppass0
r1.lab(config-router)# no auto-summary
```

```
R2:
r2.lab#conf t
r2.lab(config)#router bgp 65003
r2.lab(config-router)# no synchronization
r2.lab(config-router)# network 10.30.0.0 mask
255.255.0.0
r2.lab(config-router)# neighbor 10.20.0.1 remote-as
65001
r2.lab(config-router)# neighbor 10.20.0.1 password
0 bgppass1
r2.lab(config-router)# no auto-summary

R3:
r3.lab# conf t
r3.lab(config)#router bgp 65002
r3.lab(config-router)# no synchronization
r3.lab(config-router)# network 10.60.0.0 mask
255.255.0.0
r3.lab(config-router)# neighbor 10.50.0.1 remote-as
65001
r3.lab(config-router)# neighbor 10.50.0.1 password
0 bgppass2

R4:
r4.lab#conf t
r4.lab(config)#ip route 10.20.0.0 255.255.0.0
192.168.100.1
r4.lab(config)#router bgp 65001
r4.lab(config-router)#no synchronization
r4.lab(config-router)# network 10.40.0.0 mask
255.255.0.0
r4.lab(config-router)# network 10.10.0.0 mask
255.255.0.0
r4.lab(config-router)# neighbor 10.50.0.2 remote-as
65002
r4.lab(config-router)# neighbor 10.50.0.2 password
0 bgppass2
r4.lab(config-router)# neighbor 192.168.100.1 re-
mote-as 65001
r4.lab(config-router)# neighbor 192.168.100.1 pass-
word 0 bgppass0
r4.lab(config-router)# no auto-summary
```

* Правило синхронизации: iBGP-маршрут считается лучшим в таблице BGP, только если он был получен по протоколу IGP (RIP, IGRP, OSPF) и находится в таблице маршрутизации. Или, другими словами, не использовать или не анонсировать внешним «соседям» маршрут, полученный по iBGP, до тех пор, пока соответствующий маршрут не будет получен от IGP. По этой причине синхронизация отключена.

В случае если настройки BGP на роутере правильные, вывод команд Show IP BGP Neighbors и Show IP BGP Summary будет следующим:

```
R1:
r1.lab#show ip bgp neighbors
BGP neighbor is 10.20.0.2, remote AS 65003, external link
*Описание «соседа» BGP.
BGP version 4, remote router ID 10.30.0.1
BGP state = Established, up for 00:01:57
*Версия и состояния сессии BGP с «соседом».
Last read 00:00:56, last write 00:00:26, hold time is 180, keepalive interval is 60 seconds
*Таймеры BGP «соседа».
Neighbor capabilities:
Route refresh: advertised and received(old & new)
Address family IPv4 Unicast: advertised and received
Message statistics:
InQ depth is 0
OutQ depth is 0
                         Sent               Rcvd
 Opens:                  1                  1
 Notifications:          0                  0
 Updates:                3                  1
 Keepalives:             4                  4
 Route Refresh:          0                  0
 Total:                  8                  6
Default minimum time between advertisement runs is 30 seconds

For address family: IPv4 Unicast
BGP table version 6, neighbor version 6/0
Output queue size : 0
Index 2, Offset 0, Mask 0x4
```

2 update-group member

	Sent	Rcvd
Prefix activity:	-	-
Prefixes Current:	3	1(Consumes 52 bytes)
Prefixes Total:	3	1
Implicit Withdraw:	0	0
Explicit Withdraw:	0	0
Used as bestpath:	n/a	1
Used as multipath:	n/a	0

	Outbound	Inbound
Local Policy Denied Prefixes:	---------	-------
Bestpath from this peer:	1	n/a
Total:	1	0

Number of NLRIs in the update sent: max 1, min 1

*Статистика работы BGP с «соседом».

Connections established 1; dropped 0

Last reset never

Connection state is ESTAB, I/O status: 1, unread input bytes: 0

Connection is ECN Disabled, Mininum incoming TTL 0, Outgoing TTL 1

Local host: 10.20.0.1, Local port: 17493

Foreign host: 10.20.0.2, Foreign port: 179

*Информация о TCP соединении BGP с «соседом».

Enqueued packets for retransmit: 0, inp: 0 mis-ordered: 0(0 bytes)

Event Timers (current time is 0x3C5CC508):

Timer	Starts	Wakeups	Next
Retrans	7	0	0x0
TimeWait	0	0	0x0
AckHold	5	3	0x0
SendWnd	0	0	0x0
KeepAlive	0	0	0x0
GiveUp	0	0	0x0
PmtuAger	0	0	0x0
DeadWait	0	0	0x0

iss:3010204380 snduna:3010204662 sndnxt:3010204662 sndwnd:16103

```
    irs:1440778602     rcvnxt:1440778794     rcvwnd:16193
delrcvwnd:191

    SRTT: 182 ms, RTTO: 1073 ms, RTV: 891 ms, KRTT: 0 ms
    minRTT: 0 ms, maxRTT: 300 ms, ACK hold: 200 ms
    Flags: active open, nagle, md5
    IP Precedence value: 6

    Datagrams (max data segment is 1460 bytes):
    Rcvd: 7 (out of order: 0), with data: 5, total data
bytes: 191
    Sent: 12 (retransmit: 0, fastretransmit: 0, partia-
lack: 0, Second Congestion: 0), with data: 7, total
data bytes: 281

    BGP neighbor is 192.168.100.2, remote AS 65001, in-
ternal link
    BGP version 4, remote router ID 192.168.100.2
    BGP state = Established, up for 00:06:06
    Last read 00:00:05, last write 00:00:05, hold time
is 180, keepalive interval is 60 seconds
    Neighbor capabilities:
    Route refresh: advertised and received(old & new)
    Address family IPv4 Unicast: advertised and received
    Message statistics:
    InQ depth is 0
    OutQ depth is 0

                         Sent               Rcvd
    Opens:                  1                  1
    Notifications:          0                  0
    Updates:                2                  2
    Keepalives:             9                  9
    Route Refresh:          0                  0
    Total:                 12                 12
    Default minimum time between advertisement runs is
0 seconds

    For address family: IPv4 Unicast
    BGP table version 6, neighbor version 6/0
    Output queue size : 0
    Index 1, Offset 0, Mask 0x2
    1 update-group member
```

	Sent	Rcvd
Prefix activity:	----	----
Prefixes Current:	2	2(Consumes 104 bytes)
Prefixes Total:	2	2
Implicit Withdraw:	0	0
Explicit Withdraw:	0	0
Used as bestpath:	n/a	2
Used as multipath:	n/a	0

	Outbound	Inbound
Local Policy Denied Prefixes:	--------	-------
Bestpath from this peer:	2	n/a
Total:	2	0

Number of NLRIs in the update sent: max 1, min 1
Connections established 1; dropped 0
Last reset never
Connection state is ESTAB, I/O status: 1, unread input bytes: 0
Connection is ECN Disabled, Mininum incoming TTL 0, Outgoing TTL 255
Local host: 192.168.100.1, Local port: 56649
Foreign host: 192.168.100.2, Foreign port: 179
Enqueued packets for retransmit:0, input:0 mis-ordered:0(0 bytes)
Event Timers (current time is 0x3C5CE078):

Timer	Starts	Wakeups	Next
Retrans	10	0	0x0
TimeWait	0	0	0x0
AckHold	9	2	0x0
SendWnd	0	0	0x0
KeepAlive	0	0	0x0
GiveUp	0	0	0x0
PmtuAger	0	0	0x0
DeadWait	0	0	0x0

iss:3182108986 snduna:3182109315 sndnxt:3182109315 sndwnd:16056
irs:1216351342 rcvnxt:1216351671 rcvwnd:16056 delrcvwnd:328

SRTT: 221 ms, RTTO: 832 ms, RTV: 611 ms, KRTT: 0 ms
minRTT: 12 ms, maxRTT: 300 ms, ACK hold: 200 ms

```
    Flags: active open, nagle, md5
    IP Precedence value : 6

    Datagrams (max data segment is 1460 bytes):
    Rcvd: 19 (out of order: 0), with data: 10, total
data bytes: 328
    Sent: 15 (retransmit: 0, fastretransmit: 0, partia-
lack: 0, Second Congestion: 0), with data: 11, total
data bytes: 328

    r1.lab#show ip bgp summary
    BGP router identifier 192.168.100.1, local AS num-
ber 65001
    *Настройки BGP на данном роутере.
    BGP table version is 6, main routing table version 6
    4 network entries using 468 bytes of memory
    4 path entries using 208 bytes of memory
    5/4 BGP path/bestpath attribute entries using 620
bytes of memory
    2 BGP AS-PATH entries using 48 bytes of memory
    0 BGP route-map cache entries using 0 bytes of memory
    0 BGP filter-list cache entries using 0 bytes of
memory
    BGP using 1344 total bytes of memory
    *Ресурсы роутера, используемые BGP.
    BGP activity 4/0 prefixes, 4/0 paths, scan interval
60 secs

      Neighbor    V   AS    Msg   Msg   Tbl  InQ OutQ   Up/   State/
                            Rcvd  Sent  Ver                Down  PfxRcd
       10.20.0.2  4 65003   7     9     6    0    0   00:02:15   1
    192.168.100.2 4 65001  12    12     6    0    0   00:06:15   2
    *Статистика работы BGP с «соседями».

    R2:
    r2.lab#show ip bgp neighbors
    BGP neighbor is 10.20.0.1, remote AS 65001, exter-
nal link
    BGP version 4, remote router ID 192.168.100.1
    BGP state = Established, up for 00:02:22
    Last read 00:00:22, last write 00:00:22, hold time
is 180, keepalive interval is 60 seconds
    Neighbor capabilities:
```

```
    Route refresh: advertised and received(old & new)
    Address family IPv4 Unicast: advertised and re-
ceived
    Message statistics:
    InQ depth is 0
    OutQ depth is 0
                                 Sent               Rcvd
     Opens:                         1                  1
     Notifications:                 0                  0
     Updates:                       1                  3
     Keepalives:                    5                  5
     Route Refresh:                 0                  0
     Total:                         7                  9
    Default minimum time between advertisement runs is
30 seconds

    For address family: IPv4 Unicast
    BGP table version 6, neighbor version 6/0
    Output queue size : 0
    Index 1, Offset 0, Mask 0x2
    1 update-group member

                             Sent               Rcvd
     Prefix activity:        ----               ----
     Prefixes Current:          1     3 (Consumes 156 bytes)
     Prefixes Total:            1                  3
     Implicit Withdraw:         0                  0
     Explicit Withdraw:         0                  0
     Used as bestpath:        n/a                  3
     Used as multipath:       n/a                  0

                                       Outbound Inbound
     Local Policy Denied Prefixes:    -------- -------
     Bestpath from this peer:                3      n/a
     Total:                                  3        0
    Number of NLRIs in the update sent: max 1, min 1

    Connections established 1; dropped 0
    Last reset never
    Connection state is ESTAB, I/O status: 1, unread
input bytes: 0
    Connection is ECN Disabled, Mininum incoming TTL 0,
Outgoing TTL 1
```

```
    Local host: 10.20.0.2, Local port: 179
    Foreign host: 10.20.0.1, Foreign port: 17493

    Enqueued packets for retransmit: 0, inp: 0 mis-
ordered: 0 (0 bytes)
    Event Timers (current time is 0x3C5B6588):
         Timer        Starts       Wakeups         Next
     Retrans             6             0          0x0
     TimeWait            0             0          0x0
     AckHold             6             1          0x0
     SendWnd             0             0          0x0
     KeepAlive           0             0          0x0
     GiveUp              0             0          0x0
     PmtuAger            0             0          0x0
     DeadWait            0             0          0x0

    iss:1440778602  snduna:1440778794  sndnxt:1440778794
sndwnd:16193
    irs:3010204380     rcvnxt:3010204662     rcvwnd:16103
delrcvwnd:281

    SRTT: 165 ms, RTTO: 1172 ms, RTV: 1007 ms, KRTT: 0 ms
    minRTT: 0 ms, maxRTT: 300 ms, ACK hold: 200 ms
    Flags: passive open, nagle, gen tcbs, md5
    IP Precedence value: 6

    Datagrams (max data segment is 1460 bytes):
    Rcvd: 12 (out of order: 0), with data: 7, total
data bytes: 281
    Sent: 7 (retransmit: 0, fastretransmit: 0, partia-
lack: 0, Second Congestion: 0), with data: 5, total
data bytes: 191

    r2.lab#show ip bgp summary
    BGP router identifier 10.30.0.1, local AS number
65003
    BGP table version is 6, main routing table version 6
    4 network entries using 468 bytes of memory
    4 path entries using 208 bytes of memory
    5/4 BGP path/bestpath attribute entries using 620
bytes of memory
    2 BGP AS-PATH entries using 48 bytes of memory
```

0 BGP route-map cache entries using 0 bytes of memory
0 BGP filter-list cache entries using 0 bytes of memory
BGP using 1344 total bytes of memory
BGP activity 4/0 prefixes, 4/0 paths, scan interval 60 secs

Neighbor	V	AS	Msg Rcvd	Msg Sent	Tbl Ver	InQ	OutQ	Up/ Down	State/ PfxRcd
10.20.0.1	4	65001	9	7	6	0	0	00:02:32	3

R3:
r3.lab#show ip bgp neighbors
BGP neighbor is 10.50.0.1, remote AS 65001, external link
BGP version 4, remote router ID 192.168.100.2
BGP state = Established, up for 00:01:11
Last read 00:00:11, last write 00:00:11, hold time is 180, keepalive interval is 60 seconds
Neighbor capabilities:
Route refresh: advertised and received (old & new)
Address family IPv4 Unicast: advertised and received
Message statistics:
InQ depth is 0
OutQ depth is 0

	Sent	Rcvd
Opens:	1	1
Notifications:	0	0
Updates:	1	3
Keepalives:	4	4
Route Refresh:	0	0
Total:	6	8

Default minimum time between advertisement runs is 30 seconds

For address family: IPv4 Unicast
BGP table version 6, neighbor version 6/0
Output queue size : 0
Index 1, Offset 0, Mask 0x2
1 update-group member

	Sent	Rcvd
Prefix activity:	----	----
Prefixes Current:	1	3 (Consumes 156 bytes)
Prefixes Total:	1	3
Implicit Withdraw:	0	0
Explicit Withdraw:	0	0
Used as bestpath:	n/a	3
Used as multipath:	n/a	0

	Outbound	Inbound
Local Policy Denied Prefixes:	--------	-------
Bestpath from this peer:	3	n/a
Total:	3	0

Number of NLRIs in the update sent: max 1, min 1
Connections established 1; dropped 0
Last reset never
Connection state is ESTAB, I/O status: 1, unread input bytes: 0
Connection is ECN Disabled, Mininum incoming TTL 0, Outgoing TTL 1
Local host: 10.50.0.2, Local port: 26648
Foreign host: 10.50.0.1, Foreign port: 179
Enqueued packets for retransmit: 0, input: 0 mis-ordered: 0 (0 bytes)
Event Timers (current time is 0x3C5CA47C):

Timer	Starts	Wakeups	Next
Retrans	5	0	0x0
TimeWait	0	0	0x0
AckHold	3	1	0x0
SendWnd	0	0	0x0
KeepAlive	0	0	0x0
GiveUp	0	0	0x0
PmtuAger	0	0	0x0
DeadWait	0	0	0x0

iss:3092581353 snduna:3092581526 sndnxt:3092581526 sndwnd:16212
irs:544266312 rcvnxt:544266575 rcvwnd:16122 delrcvwnd:262

SRTT: 146 ms, RTTO: 1283 ms, RTV: 1137 ms, KRTT: 0 ms
minRTT: 0 ms, maxRTT: 300 ms, ACK hold: 200 ms

```
    Flags: active open, nagle, md5
    IP Precedence value: 6

    Datagrams (max data segment is 1460 bytes):
    Rcvd: 6 (out of order: 0), with data: 4, total data
bytes: 262
    Sent: 8 (retransmit: 0, fastretransmit: 0, partialack:
0, Second Congestion: 0), with data: 5, total data
bytes: 172

    r3.lab#show ip bgp summary
    BGP router identifier 10.60.0.1, local AS number
65002
    BGP table version is 6, main routing table version 6
    4 network entries using 468 bytes of memory
    4 path entries using 208 bytes of memory
    5/4 BGP path/bestpath attribute entries using 620
bytes of memory
    2 BGP AS-PATH entries using 48 bytes of memory
    0 BGP route-map cache entries using 0 bytes of memory
    0 BGP filter-list cache entries using 0 bytes of
memory
    BGP using 1344 total bytes of memory
    BGP activity 4/0 prefixes, 4/0 paths, scan interval
60 secs
      Neighbor    V   AS    Msg    Msg    Tbl   InQ OutQ   Up/    State/
                            Rcvd   Sent   Ver             Down   PfxRcd
      10.50.0.1   4 65001   8      6      6     0    0   00:01:20   3

    R4:
    r4.lab#show ip bgp neighbors
    BGP neighbor is 10.50.0.2, remote AS 65002, exter-
nal link
    BGP version 4, remote router ID 10.60.0.1`
    BGP state = Established, up for 00:01:29
    Last read 00:00:29, last write 00:00:29, hold time
is 180, keepalive interval is 60 seconds
    Neighbor capabilities:
    Route refresh: advertised and received(old & new)
    Address family IPv4 Unicast: advertised and re-
ceived
    Message statistics:
    InQ depth is 0
```

```
  OutQ depth is 0
                                 Sent               Rcvd
  Opens:                            1                  1
  Notifications:                    0                  0
  Updates:                          3                  1
  Keepalives:                       4                  4
  Route Refresh:                    0                  0
  Total:                            8                  6
  Default minimum time between advertisement runs is
30 seconds
  For address family: IPv4 Unicast
  BGP table version 6, neighbor version 6/0
  Output queue size: 0
  Index 2, Offset 0, Mask 0x4
  2 update-group member
                               Sent               Rcvd
  Prefix activity:             ----               ----
  Prefixes Current:               3     1 (Consumes 52 bytes)
  Prefixes Total:                 3                  1
  Implicit Withdraw:              0                  0
  Explicit Withdraw:              0                  0
  Used as bestpath:             n/a                  1
  Used as multipath:            n/a                  0

                                    Outbound    Inbound
  Local Policy Denied Prefixes:     --------    -------
  Bestpath from this peer:                 1        n/a
  Total:                                   1          0
  Number of NLRIs in the update sent: max 1, min 1
  Connections established 1; dropped 0
  Last reset never
  Connection state is ESTAB, I/O status: 1, unread
input bytes: 0
  Connection is ECN Disabled, Mininum incoming TTL 0,
Outgoing TTL 1
  Local host: 10.50.0.1, Local port: 179
  Foreign host: 10.50.0.2, Foreign port: 26648
  Enqueued packets for retransmit: 0, input: 0 mis-
ordered: 0 (0 bytes)
  Event Timers (current time is 0x3C5C6788):
```

Timer	Starts	Wakeups	Next
Retrans	4	0	0x0
TimeWait	0	0	0x0
AckHold	4	1	0x0
SendWnd	0	0	0x0
KeepAlive	0	0	0x0
GiveUp	0	0	0x0
PmtuAger	0	0	0x0
DeadWait	0	0	0x0

iss:544266312 snduna:544266575 sndnxt:544266575 sndwnd:16122
irs:3092581353 rcvnxt:3092581526 rcvwnd:16212 delrcvwnd:172

SRTT: 124 ms, RTTO: 1405 ms, RTV: 1281 ms, KRTT: 0 ms
minRTT: 0 ms, maxRTT: 300 ms, ACK hold: 200 ms
Flags: passive open, nagle, gen tcbs, md5
IP Precedence value: 6

Datagrams (max data segment is 1460 bytes):
Rcvd: 8 (out of order: 0), with data: 5, total data bytes: 172
Sent: 6 (retransmit: 0, fastretransmit: 0, partialack: 0, Second Congestion: 0), with data: 4, total data bytes: 262
BGP neighbor is 192.168.100.1, remote AS 65001, internal link
BGP version 4, remote router ID 192.168.100.1
BGP state = Established, up for 00:07:03
Last read 00:00:03, last write 00:00:03, hold time is 180, keepalive interval is 60 seconds
Neighbor capabilities:
Route refresh: advertised and received(old & new)
Address family IPv4 Unicast: advertised and received
Message statistics:
InQ depth is 0
OutQ depth is 0

	Sent	Rcvd
Opens:	1	1
Notifications:	0	0
Updates:	2	2
Keepalives:	10	10
Route Refresh:	0	0
Total:	13	13

Default minimum time between advertisement runs is 0 seconds

For address family: IPv4 Unicast

BGP table version 6, neighbor version 6/0

Output queue size : 0

Index 1, Offset 0, Mask 0x2

1 update-group member

	Sent	Rcvd
Prefix activity:	----	----
Prefixes Current:	2	2(Consumes 104 bytes)
Prefixes Total:	2	2
Implicit Withdraw:	0	0
Explicit Withdraw:	0	0
Used as bestpath:	n/a	2
Used as multipath:	n/a	0

	Outbound	Inbound
Local Policy Denied Prefixes:	--------	-------
Bestpath from this peer:	2	n/a
Total:	2	0

Number of NLRIs in the update sent: max 1, min 1

Connections established 1; dropped 0

Last reset never

Connection state is ESTAB, I/O status: 1, unread input bytes: 0

Connection is ECN Disabled, Mininum incoming TTL 0, Outgoing TTL 255

Local host: 192.168.100.2, Local port: 179

Foreign host: 192.168.100.1, Foreign port: 56649

Enqueued packets for retransmit: 0, input: 0 mis-ordered: 0 (0 bytes)

Event Timers (current time is 0x3C5C78F8):

Timer	Starts	Wakeups	Next
Retrans	11	0	0x0
TimeWait	0	0	0x0
AckHold	10	9	0x0
SendWnd	0	0	0x0
KeepAlive	0	0	0x0
GiveUp	0	0	0x0
PmtuAger	0	0	0x0
DeadWait	0	0	0x0

iss:1216351342 snduna:1216351690 sndnxt:1216351690 sndwnd:16037
irs:3182108986 rcvnxt:3182109334 rcvwnd:16037 delrcvwnd:347

SRTT: 231 ms, RTTO: 769 ms, RTV: 538 ms, KRTT: 0 ms
minRTT: 8 ms, maxRTT: 300 ms, ACK hold: 200 ms
Flags: passive open, nagle, gen tcbs, md5
IP Precedence value: 6

Datagrams (max data segment is 1460 bytes):
Rcvd: 16 (out of order: 0), with data: 12, total data bytes: 347
Sent: 21 (retransmit: 0, fastretransmit: 0, partialack: 0, Second Congestion: 0), with data: 11, total data bytes: 347

r4.lab#show ip bgp summary
BGP router identifier 192.168.100.2, local AS number 650001
BGP table version is 6, main routing table version 6
4 network entries using 468 bytes of memory
4 path entries using 208 bytes of memory
5/4 BGP path/bestpath attribute entries using 620 bytes of memory
2 BGP AS-PATH entries using 48 bytes of memory
0 BGP route-map cache entries using 0 bytes of memory
0 BGP filter-list cache entries using 0 bytes of memory
BGP using 1344 total bytes of memory
BGP activity 4/0 prefixes, 4/0 paths, scan interval 60 secs

```
Neighbor        V    AS   Msg   Msg   Tbl  InQ OutQ   Up/   State/
                          Rcvd  Sent  Ver              Down  PfxRcd
10.50.0.2       4 65002    6     8     6    0    0 00:01:42    1
192.168.100.1   4 65001   13    13     6    0    0 00:07:13    2
```

В таблицах маршрутизации BGP содержатся записи, которые можно посмотреть с помощью команды Show IP BGP:

```
R1:
r1.lab#show ip bgp
BGP table version is 6, local router ID is 192.168.100.1
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,r RIB-failure, S Stale
Origin codes: i - IGP, e - EGP, ? - incomplete
     Network          Next Hop    Metric LocPrf Weight Path
 *>10.10.0.0/16    0.0.0.0          0         32768 i
 *>10.30.0.0/16    10.20.0.2        0      0  65003 i
 *>i10.40.0.0/16   192.168.100.2    0    100     0 i
 *>i10.60.0.0/16   10.50.0.2       0    100     0 i
                                                 65002
```

* Local Preference действует в пределах AS и равен 100 по умолчанию на маршрутах, полученных по eBGP.

Обратим внимание на Next Hop маршрута 10.60.0.0. Почему он такой?

```
R2:
r2.lab#show ip bgp
BGP table version is 6, local router ID is 10.30.0.1
     Network          Next Hop    Metric LocPrf Weight Path
 *>10.10.0.0/16    10.20.0.1        0      0  65001 i
 *>10.30.0.0/16    0.0.0.0          0         32768 i
 *>10.40.0.0/16    10.20.0.1        0         65001 i
 *>10.60.0.0/16    10.20.0.1        0  65001  65002 i
```

* Weight по умолчанию 32768 на непосредственно подключенных сетях, на маршрутах, полученных по eBGP, равно 0.

```
R3:
r3.lab#show ip bgp
BGP table version is 6, local router ID is 10.60.0.1
```

```
     Network          Next Hop    Metric LocPrf Weight Path
 *>10.10.0.0/16   10.50.0.1        0             65001   i
 *>10.30.0.0/16   10.50.0.1        0    65001    65003   i
 *>10.40.0.0/16   10.50.0.1        0        0    65001   i
 *>10.60.0.0/16   0.0.0.0          0             32768   i
```

R4:

```
r4.lab#show ip bgp
BGP table version is 6, local router ID is
192.168.100.2
     Network          Next Hop    Metric LocPrf Weight Path
 *>i10.10.0.0/16  192.168.100.1    0      100      0     i
 *>i10.30.0.0/16  10.20.0.2       0      100      0     i
                                                 65003
 *>10.40.0.0/16   0.0.0.0          0              32768   i
 *>10.60.0.0/16   10.50.0.2        0        0     65002   i
```

Добавим на R2 псевдомаршрут к сети 172.16.22.0. Настроим перераспределение статических маршрутов на R2 в BGP с метрикой (атрибут MED) = 500:

R4:

```
r2.lab#conf t
r2.lab(config)#ip route 172.16.22.0 255.255.255.128
Null0
r2.lab(config)#router bgp 65003
r2.lab(config-router)# redistribute static metric 500
```

В результате в таблицах маршрутизации BGP появится новая запись, которую можно посмотреть с помощью команды Show IP BGP:

R1:

```
r1.lab#show ip bgp
BGP table version is 7, local router ID is
192.168.100.1
     Network          Next Hop    Metric LocPrf Weight Path
 *>10.10.0.0/16   0.0.0.0          0              32768   i
 *>10.30.0.0/16   10.20.0.2        0        0     65003   i
 *>i10.40.0.0/16 192.168.100.2    0      100      0     i
 *>i10.60.0.0/16  10.50.0.2       0      100      0     i
                                                 65002
 *>172.16.22.0/25  10.20.0.2      500      0     65003   ?
```

```
R2:
r2.lab#show ip bgp
BGP table version is 7, local router ID is 10.30.0.1
     Network          Next Hop  Metric LocPrf Weight Path
  *>10.10.0.0/16   10.20.0.1     0      0    65001   i
  *>10.30.0.0/16    0.0.0.0      0           32768   i
  *>10.40.0.0/16   10.20.0.1     0           65001   i
  *>10.60.0.0/16   10.20.0.1     0    65001  65002   i
  *>172.16.22.0/25   0.0.0.0     500         32768   ?

R3:
r3.lab#show ip bgp
BGP table version is 7, local router ID is 10.60.0.1
     Network          Next Hop  Metric LocPrf Weight Path
  *>10.10.0.0/16   10.50.0.1     0           65001   i
  *>10.30.0.0/16   10.50.0.1     0    65001  65003   i
  *>10.40.0.0/16   10.50.0.1     0      0    65001   i
  *>10.60.0.0/16    0.0.0.0      0           32768   i
  *>172.16.22.0/25 10.50.0.1     0    65001  65003   ?
```

* MED'ы передаются на соседнюю AS, но не передаются за ее пределы (вернее, при передаче за пределы системы, получившей MED, это значение обнуляется).

```
R4:
r4.lab#show ip bgp
BGP table version is 7, local router ID is 192.168.100.2
     Network          Next Hop  Metric LocPrf Weight Path
  *>i10.10.0.0/16 192.168.100.1   0     100     0     i
  *>i10.30.0.0/16   10.20.0.2     0     100     0     i
                                                65003
  *>10.40.0.0/16     0.0.0.0      0           32768   i
  *>10.60.0.0/16    10.50.0.2     0      0    65002   i
  *>i172.16.22.0/25 10.20.0.2    500    100     0     ?
                                                65003
```

Существует два способа настройки Local Preference:

1) Установить Local Preference как значение по умолчанию для данного процесса BGP. Для этого на роутере R1 выполним следующие команды:

```
r1.lab#conf t
r1.lab(config)#router bgp 65001
r1.lab(config-router)#bgp default local-preference 150
```

2) Установить Local Preference с помощью Route Map. Для этого на роутере R4 выполним следующие команды (также на R4 параллельно Local Preference устанавливается атрибут локальный для роутера R4 Weight):

```
r4.lab#conf t
r4.lab(config)#ip as-path access-list 1 permit ^65002$
r4.lab(config)#route-map from_r3 permit 10
r4.lab(config-route-map)#match as-path 1
r4.lab(config-route-map)#set weight 2000
r4.lab(config-route-map)#set local-preference 250
r4.lab(config-route-map)#exit
r4.lab(config)#router bgp 65001
r4.lab(config-router)#neighbor 10.50.0.2 route-map from_r3 in
```

* На роутере R4 всем маршрутам (входящим), пришедшим от R3 (AS_PATH = 65002), устанавливаются атрибуты Weight и Local Preference. Запомните: Route Map не работают и не предназначены для обработки входящих маршрутов с командой Match IP Address Access_List_Number!!!

На роутере R4 выполним команду Show IP BGP Regexp ^65002$. Для чего нужна эта команда, что она выдает?

Для ускорения принятия изменений выполним команды Clear IP BGP* на роутерах R1 и R4.

В результате в таблицах маршрутизации BGP на R1 и R4 поменяются некоторые записи (Weight работает только на локальном роутере, Local Preference только в своей AS, поэтому таблицы BGP на R2 и R3 остаются без изменений).

R1:

```
r1.lab#show ip bgp
BGP table version is 28, local router ID is 192.168.100.1
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
r RIB-failure, S Stale
Origin codes: i - IGP, e - EGP, ? - incomplete
```

```
     Network          Next Hop    Metric LocPrf Weight Path
 *>10.10.0.0/16     0.0.0.0          0         32768 i
 *>10.30.0.0/16     10.20.0.2        0      0  65003 i
 *>i10.40.0.0/16    192.168.100.2    0    100      0 i
 *>i10.60.0.0/16    10.50.0.2        0    250      0 i
                                                65002
 *>172.16.22.0/25   10.20.0.2      500      0  65003 ?
```

* На роутере R4 всем маршрутам (входящим), пришедшим от R3 (AS_PATH = 65002), устанавливается атрибут Local Preference, равный 250.

R4:

```
r4.lab#show ip bgp
BGP table version is 20, local router ID is 192.168.100.2
     Network          Next Hop    Metric LocPrf Weight Path
 *>i10.10.0.0/16    192.168.100.1    0    150      0 i
 *>i10.30.0.0/16    10.20.0.2        0    150      0 i
                                                65003
 *>10.40.0.0/16     0.0.0.0          0         32768 i
 *>10.60.0.0/16     10.50.0.2        0   2000  65002 i
 *>i172.16.22.0/25  10.20.0.2      500    150      0 ?
                                                65003
```

* На роутере R1 всем маршрутам устанавливается атрибут Local Preference, равный 150, на роутере R4 всем маршрутам (входящим), пришедшим от R3, устанавливаются атрибуты Weight, равные 2000.

Есть второй способ установки атрибута Weight – указать в команде Neighbor значение атрибута Weight для маршрутов, приходящих от данного «соседа». На роутере R3 всем маршрутам (входящим), пришедшим от R4, устанавливаются атрибуты Weight. Для этого выполним команды:

```
r3.lab#conf t
r3.lab(config)#router bgp 65002
r3.lab(config-router)#neighbor 10.50.0.1 weight 3000
```

Для ускорения принятия изменений выполним команду Clear IP BGP 10.50.0.1 на роутере R3.

В результате в таблице маршрутизации BGP на R3 поменяется атрибут Weight у маршрутов, полученных от R4:

```
R3:
r3.lab#show ip bgp
BGP table version is 23, local router ID is 10.60.0.1
     Network          Next Hop    Metric LocPrf Weight Path
  *>10.10.0.0/16    10.50.0.1       3000         65001  i
  *>10.30.0.0/16    10.50.0.1       3000  65001  65003  i
  *>10.40.0.0/16    10.50.0.1          0   3000  65001  i
  *>10.60.0.0/16     0.0.0.0           0         32768  i
 *>172.16.22.0/25   10.50.0.1       3000  65001  65003  ?
```

Атрибут MED можно устанавливать не только на перераспределяемые статические маршруты, но и на остальные маршруты с помощью Route Map. Установим на маршрут 10.60.0.0 на R3 MED = 22:

```
r3.lab#conf t
r3.lab(config)#access-list 1 permit 10.60.0.0 0.0.255.255
r3.lab(config)#route-map to_r4
r3.lab(config-route-map)#match ip address 1
r3.lab(config-route-map)#set metric 22
r3.lab(config-route-map)#exit
r3.lab(config)#router bgp 65002
r3.lab(config-router)#neighbor   10.50.0.1   route-map
to_r4 out
```

Для сравнения настроим на R3 перераспределение статических маршрутов с MED = 122:

```
r3.lab#conf t
r3.lab(config)#ip route 172.28.22.0 255.255.255.128
Null0
r3.lab(config)#router bgp 65002
r3.lab(config-router)#redistribute static metric 122
```

Для ускорения принятия изменений выполним команду Clear IP BGP 10.50.0.1 на роутере R3.

В таблицах маршрутизации BGP появятся некоторые записи, вывод команд Show IP BGP:

```
R1:
r1.lab#show ip bgp
```

```
    BGP  table  version  is  33,  local  router  ID  is
192.168.100.1
         Network          Next Hop    Metric LocPrf Weight Path
 *>10.10.0.0/16     0.0.0.0          0         32768  i
 *>10.30.0.0/16     10.20.0.2        0      0  65003  i
 *>i10.40.0.0/16 192.168.100.2    0      100    0      i
 *>i10.60.0.0/16    10.50.0.2      22     250    0      i
                                                65002
 *>172.16.22.0/25   10.20.0.2      500    0      65003  ?
 >i172.28.22.0/25   10.50.0.2      122    250    0      ?
                                                65002
```

```
    R2:
    r2.lab#show ip bgp
    BGP table version is 26, local router ID is 10.30.0.1
         Network          Next Hop    Metric LocPrf Weight Path
 *>10.10.0.0/16     10.20.0.1        0      0      65001  i
 *>10.30.0.0/16     0.0.0.0          0         32768  i
 *>10.40.0.0/16     10.20.0.1        0         65001  i
 *>10.60.0.0/16     10.20.0.1        0      65001  65002  i
 *>172.16.22.0/25   0.0.0.0        500         32768  ?
 *>172.28.22.0/25   10.20.0.1        0      65001  65002  ?
```

```
    R4:
    r4.lab#show ip bgp
    BGP  table  version  is  39,  local  router  ID  is
192.168.100.2
         Network          Next Hop    Metric LocPrf Weight Path
 *>i10.10.0.0/16 192.168.100.1    0      150    0      i
 *>i10.30.0.0/16    10.20.0.2        0      150    0      i
                                                65003
 *>10.40.0.0/16     0.0.0.0          0         32768  i
 *>10.60.0.0/16     10.50.0.2      22     250    2000   i
                                                65002
 *>i172.16.22.0/25  10.20.0.2      500    150    0      ?
                                                65003
 *>172.28.22.0/25   0.50.0.2       122    250    2000   ?
                                                65002
```

Допустим, мы не хотим, чтобы R4 распространял маршрут о сети 172.28.22.0, полученный от R3. Для этого мы уста-

навливаем нужный атрибут Community на R3 (дописываем еще одно правило в Route Map с именем to_r4):

```
r3.lab(config)#router bgp 65002
r3.lab(config-router)#neighbor 10.50.0.1 sen
r3.lab(config-router)#neighbor 10.50.0.1 send-community
r3.lab(config-router)#exit
r3.lab(config)#access-list 2 permit 172.28.22.0 0.0.0.128
r3.lab(config)#exit
r3.lab(config)#route-map to_r4 permit 20
r3.lab(config-route-map)#match ip address 2
r3.lab(config-route-map)#set community no-advertise
```

* Отметим, что у нас теперь две Route Map с именем to_r4, но с разными Sequence Number.

Теперь все маршруты, отправляемые к R4, проходят следующую обработку:

1) начинаем с Route Map to_r4 10, в данном Route Map указано маршруту 10.60.0.0 установить MED = 22. Поскольку сеть 172.28.22.0 не попадает под этот Route Map, то идем на шаг 2;

2) в Route Map to_r4 20 маршруту 172.28.22.0 устанавливается Community No Adverse;

3) все остальные маршруты отбрасываются.

Для ускорения принятия изменений выполним команды Clear IP BGP* на роутерах R1 и R4.

В результате из таблиц маршрутизации BGP R1 и R2 удалится запись о маршруте 172.28.22.0, а на R4 в описании маршрута 172.28.22.0 будет указан атрибут Community:

```
R1:
r1.lab#show ip bgp
BGP table version is 40, local router ID is 192.168.100.1
     Network          Next Hop    Metric LocPrf Weight Path
 *>10.10.0.0/16     0.0.0.0          0         32768  i
 *>10.30.0.0/16    10.20.0.2         0      0  65003  i
*>i10.40.0.0/16 192.168.100.2       0    100      0  i
*>i10.60.0.0/16   10.50.0.2        22    250      0  i
```

```
                                                    65002
 *>172.16.22.0/25  10.20.0.2    500     0    65003   ?
```

R2:

```
r2.lab#show ip bgp
BGP table version is 29, local router ID is 10.30.0.1
     Network          Next Hop   Metric LocPrf Weight Path
 *>10.10.0.0/16   10.20.0.1     0      0    65001   i
 *>10.30.0.0/16    0.0.0.0      0           32768   i
 *>10.40.0.0/16   10.20.0.1     0           65001   i
 *>10.60.0.0/16   10.20.0.1     0    65001  65002   i
 *>172.16.22.0/25   0.0.0.0     500         32768   ?
```

R4:

```
r4.lab#show ip bgp 172.28.22.0
BGP routing table entry for 172.28.22.0/25, version 43
Paths: (1 available, best #1, table Default-IP-
Routing-Table, not advertised to any peer)
Flag: 0x820
Not advertised to any peer
65002
10.50.0.2 from 10.50.0.2 (10.60.0.1)
Origin incomplete, metric 0, localpref 250, weight
2000, valid, external, best
Community: no-advertise
```

```
r4.lab#show ip bgp
BGP table version is 49, local router ID is
192.168.100.2
     Network          Next Hop   Metric LocPrf Weight Path
 *>i10.10.0.0/16 192.168.100.1   0     150     0     i
 *>i10.30.0.0/16   10.20.0.2     0     150     0     i
                                                65003
 *>10.40.0.0/16    0.0.0.0      0           32768   i
 *>10.60.0.0/16   10.50.0.2     22    250    2000   i
                                                65002
 *>i172.16.22.0/25  10.20.0.2    500   150     0     ?
                                                65003
 *>172.28.22.0/25  10.50.0.2     0     250    2000   ?
                                                65002
```

Допустим, мы хотим, чтобы R1 распространял только определенные маршруты к R2, для этого выполним последовательность команд на R1 (аналогичным образом можно фильтровать получаемые маршруты, только в последней команде на конце будет filter-list in):

```
r1.lab#conf t
r1.lab(config)#access-list 1 permit 10.60.0.0 0.0.255.255
r1.lab(config)#access-list 1 permit 10.40.0.0 0.0.255.255
r1.lab(config)#router bgp 65001
r1.lab(config-router)#neighbor 10.20.0.2 distribute-list 1 out
sw3.lab# configure terminal
sw3.lab # interface fastethernet0/2
sw3.lab #switchport mode trunk
```

* Access-list читаются последовательно сверху вниз, сети, которые не попали ни под какую строку, отбрасываются.

Для ускорения принятия изменений выполним команды Clear IP BGP 10.20.0.2 на роутере R1.

В результате из таблиц маршрутизации BGP R2 удалятся все записи маршрутов, не удовлетворяющие правилам фильтрации на R1.

R2:

```
r2.lab#show ip bgp
BGP table version is 34, local router ID is 10.30.0.1
     Network          Next Hop    Metric LocPrf Weight Path
  *>10.30.0.0/16     0.0.0.0          0         32768 i
  *>10.40.0.0/16     10.20.0.1        0         65001 i
  *>10.60.0.0/16     10.20.0.1        0    65001 65002 i
  *>172.16.22.0/25   0.0.0.0        500         32768 ?
```

* R1 посылает R2 только маршруты о сетях 10.40.0.0 и 10.60.0.0.

Аналогично фильтрацию маршрутов можно сделать с помощью Route Map (все маршруты, не попавшие ни под какие Route Map, отбрасываются), но так, чтобы AS_Path для мар-

шрутов 10.40.0.0 и 10.60.0.0 был такой, как будто они прошли через AS 65222. Для этого выполним последовательность команд на R1:

```
r1.lab#conf t
r1.lab(config)#route-map to_r2
r1.lab(config-route-map)#match ip address 1
r1.lab(config-route-map)#set as-path prepend 65222
r1.lab(config-route-map)#exit
r1.lab(config)#router bgp 65001
r1.lab(config-router)#neighbor  10.20.0.2  route-map
to_r2 out
```

Для ускорения принятия изменений выполним команды Clear IP BGP 10.20.0.2 на роутере R1.

В результате в таблице маршрутизации BGP R2 у двух данных маршрутов будет новый AS_PATH:

```
R2:
r2.lab#show ip bgp
BGP table version is 42, local router ID is 10.30.0.1
     Network          Next Hop    Metric LocPrf Weight Path
 *>10.30.0.0/16     0.0.0.0          0         32768   i
 *>10.40.0.0/16    10.20.0.1         0    65001 65222   i
 *>10.60.0.0/16    10.20.0.1         0    65001 65222   i
                                                65002
 *>172.16.22.0/25    0.0.0.0       500         32768   ?
```

Сохраним вашу конфигурацию на всех устройствах, выполнив следующие команды:

```
sw1.lab# copy running-config startup-config
sw2.lab# copy running-config startup-config
sw3.lab# copy running-config startup-config
sw4.lab# copy running-config startup-config
r4.lab# copy running-config startup-config
```

Задания для самостоятельной работы

1. Ответьте на вопросы в тексте лабораторной работы.

2. Создайте на R3 маршрут к сети 172.16.22.0/25, скорректируйте настройки Route Map, чтобы они пропускали данный мар-

шрут с MED 22, проиллюстрируйте на R4 алгоритм BGP выбора маршрута к сети 172.16.22.0/25.

Вопросы для самопроверки

1. Виды классов сетей.
2. Какие данные указываются при статической маршрутизации?
3. Что означает метрика, IP Address, Subnet Mask в протоколе RIP?
4. Правило определения маски подсети в RIPv1.
5. Перечислите этапы алгоритма RIP.
6. Какие правила используются при борьбе с петлями?
7. Таймер Hold-Down.
8. Перечислите основные виды сообщений BGP-4.
9. Перечислите этапы алгоритма наилучшего маршрута в BGP-4.
10. Атрибут NEXT_HOP в BGP-4.
11. Атрибут AS_PATH в BGP-4.