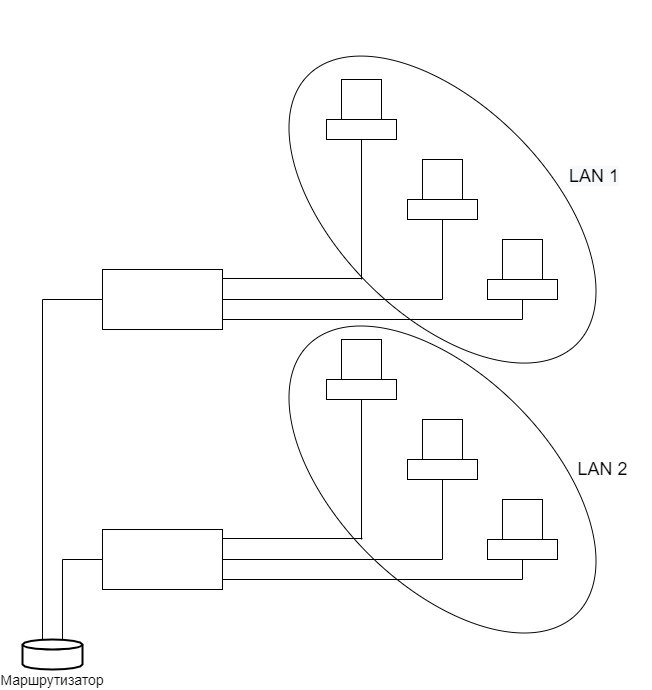
**ЗАЩИТА ИНФРАСТРУКТУРЫ КОММУТАЦИИ**

**Виртуальные локальные сети. Технология VLAN**

Технология VLAN позволяет объединять PC и сервера в логические группы с использованием коммутаторов. Связь (передача трафика) между устройствами возможна в пределах одной VLAN, т.е. сеть с коммутацией может функционировать как несколько не соединенных друг с другом ЛС. Таким образом, VLAN – средство (способ) логической группировки пользователей для обеспечения безопасной передачи трафика.

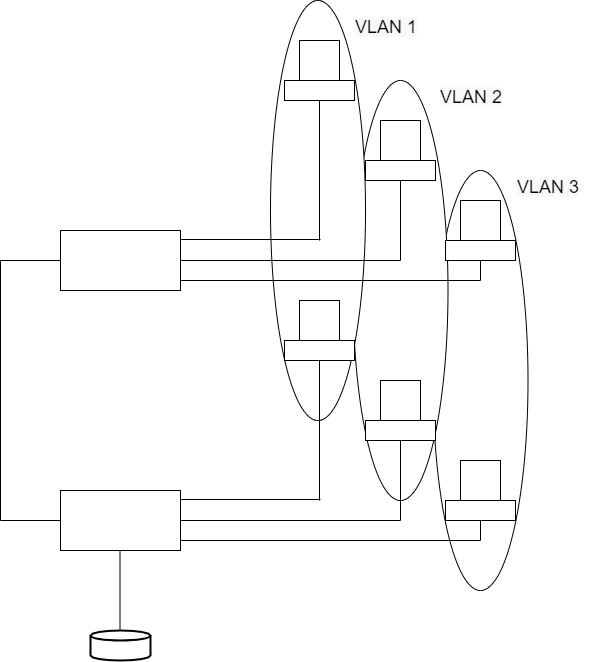
**Пример физического и логического группирования PC:**

Физическое группирование РС:

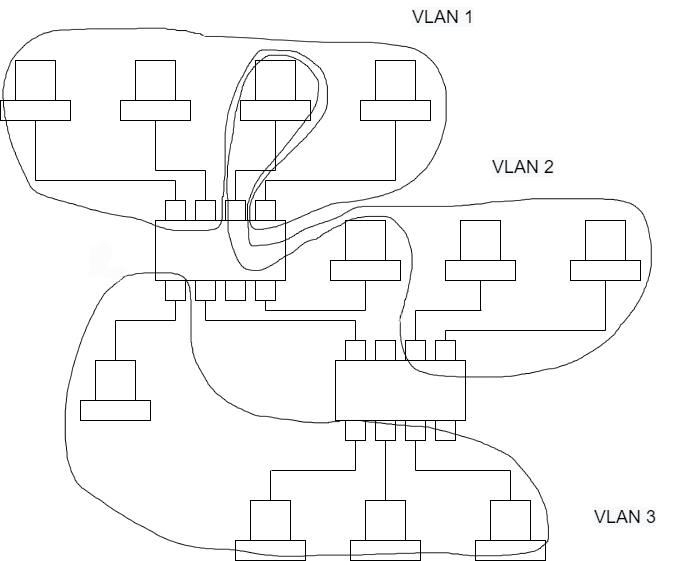


Маршрутизатор ограничивает доступ из одной LAN в другую.

Логическое группирование РС:



Сеть VLAN может рассматриваться как широковещательный домен для определенного набора коммутаторов (т.е. широковещательный трафик передается между PC одной VLAN).



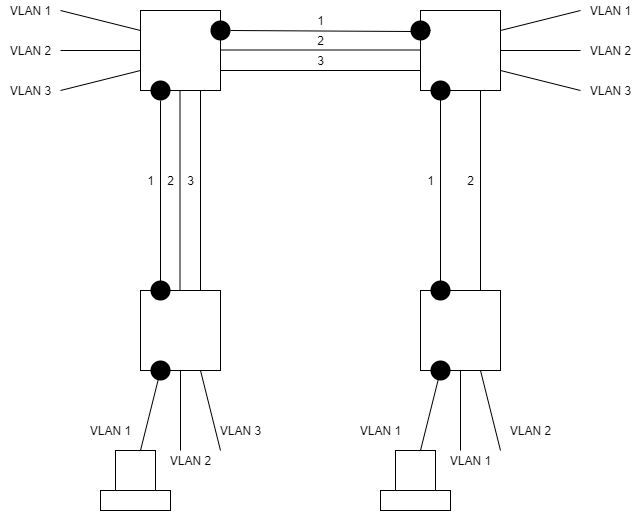
Имеем три широковещательных домена.

**Функционирование VLAN**

В сеть VLAN может быть включен любой порт коммутатора. Порты, выделенные одной и той же VLAN, имеют общее пространство широковещания (входят в один широковещательный домен). В результате повышается общая производительность сети (уменьшается количество широковещательных сообщений).

Рассматриваем статические VLAN:

Назначение портов сетям VLAN является статическим. Переключение порта на другую VLAN требует повторного … коммутатора.



Передача данных между коммутаторами по выделенным каналам:

1. Определение № VLAN, к которой принадлежит порт, в который пришел кадр от PC-источника;
2. На коммутаторе – определение портов, входящих в эту же VLAN;
3. Среди сформированного перечня портов определение того порта, который обеспечит передачу к соответствующему PC;
4. Выставление кадра в соответствующий порт.

**Особенность назначения портов в состав VLAN**

VLAN могут пересекаться, если порт входит в состав более, чем одной VLAN. То есть при создании VLAN на коммутаторе в ее состав включается его порт.

Таким образом, задачами, решаемыми за счет использования технологии VLAN, являются:

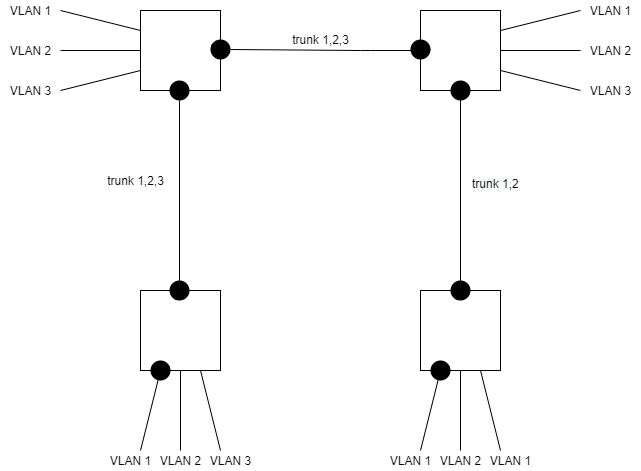
1. Повышение производительности (широковещание в рамках одной VLAN, уникальные экземпляры остовных деревьев для каждой VLAN);
2. Изоляция VLAN друг от друга для управления доступом пользователей к ресурсам сети.

**Варианты организации VLAN на нескольких коммутаторах**

1. Выделенные для каждой VLAN каналы между коммутаторами;

2. Магистральные каналы между коммутаторами (реализуется временное разделение канала для передачи трафика различных VLAN, трафик разных VLAN уплотняется в магистральном канале).

Организация сети с магистральными каналами между коммутаторами:

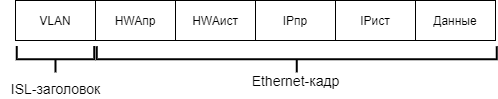


При создании trunk’а (магистрального канала), указывается трафик каких VLAN будет в нём уплотняться (то есть между трафиком каких VLAN этот магистральный канал будет разделён).

При передаче по магистрали данные (передаваемые кадры) инкапсулируются в дополнительные заготовки, содержащие номер VLAN, указывается номер VLAN отправителя.

Инкапсуляция кадра в дополнительные заготовки осуществляется протоколом ISL. Таким образом, ISL-инкапсуляция обеспечивает временное разделение каналов и позволяет использовать порт для связи коммутаторов с использованием магистрали.

Упрощенный формат кадра с ISL-инкапсуляцией:



**Алгоритм функционирования коммутатора при сконфигурированном магистральном канале**

1) На основе номера порта, на которой получен кадр от источника, номер VLAN;

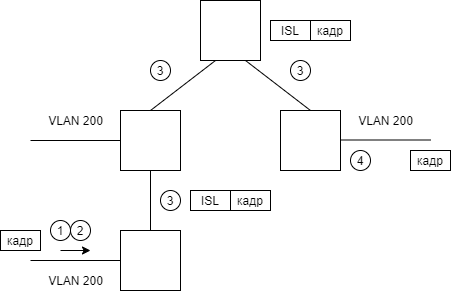
2) Определение совокупности портов, входящих в соответствующую VLAN;

3) Определение порта, обеспечивающего доступ к требуемой PC. Если этот порт магистральный, то реализация ISL-инкапсуляции, передача кадра по магистральному каналу;

4) Если порт не магистральный, то удаление ISL-заголовка и передача кадра на PC-приёмник;

При настройке магистрали ISL-инкапсуляция включается автоматически.

**Пример реализации передачи кадров с инкапсуляцией:**



Модифицированный формат MAC-таблицы:



Таким образом, в магистральных протоколах используется механизм добавления тегов (указателей, заголовков). Теги добавляются на одном конце магистрали и удаляются на другом. Кадры с тегами не являются широковещательными (предназначены одному устройству).

**Протокол магистральных соединений виртуальных локальных сетей (VTP-протокол)**

Протокол VTP является протоколом обмена сообщениями, обеспечивающим (на коммутаторах) автоматическое добавление, удаление, переименование VLAN в одном домене.

Функционирование протокола VTP возможно только при условии конфигурирования магистральных каналов между коммутаторами (то есть сообщения VTP инкапсулируются в заголовке протокола IS, то есть передаётся идентификатор VLAN).

Таким образом, назначение VTP-протокола – это автоматическое конфигурирование (переконфигурирование) VLAN на коммутаторах.

Перед созданием VLAN на коммутаторе создаётся VTP-домен (VTP-домен назначается коммутатору).

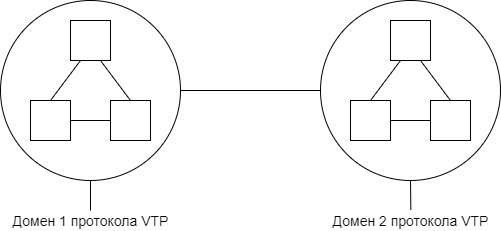
Если коммутаторы находятся в одном и том же VTP-домене, то они интерпретируют информацию о созданных и удалённых VLAN одинаковым образом. Коммутатор может принадлежать только одному домену VTP. Если коммутатор находится в двух доменах, то он не может использовать информацию о созданных или удаляемых VLAN. Таким образом, имя домена VTP указывает совокупность коммутаторов, которые будут интерпретировать VTP-сообщения, генерируемые в этом домене.

Формат сообщения протокола VTP:



В заголовке указывается длина на имени домена протокола VTP, имя домена протокола VTP.

**Пример организации доменов протокола VTP:**



Создание VLAN на одном из коммутаторов в VTP-домене приводит к автоматическому распространению информации об этой VLAN между коммутаторами домена

Режимы работы протокола VTP:

1) режим сервера

2) режим клиента

3) прозрачный режим

*Примечание*: использование VTP-доменов позволяет исключить распространение информации о созданных VLAN между всеми коммутаторами, то есть реализовать режим отключения трафика.

**Режим сервера протокола VTP**

Коммутатор в режиме сервера реализует:

1. Создание, удаление и изменение VLAN;
2. Рассылку информации о действиях с VLAN, которые были на ней выполнены (рассылка широковещательно через все магистральные каналы).

В результате информация о созданных VLAN будет размещена на всех коммутаторах, находящихся в том же домене, что и VTP-сервер. Таким образом, условием функционирования протокола VTP на коммутаторе является конфигурирование на них магистральных каналов.

**Прозрачный режим протокола VTP**

Коммутаторы, сконфигурированные в прозрачном режиме, не принимают участие в работе протокола VTP. Коммутаторы реализуют рассылку сообщений протокола VTP, сформированных клиентом (не анализируют поступившую информацию протокола VTP, не изменяют хранящуюся на них БД VLAN).

**Клиентский режим протокола VTP**

Клиенты реализуют обработку сообщений об изменениях в сетях VLAN, полученных от VTP-сервера. Также рассылает (широковещательно) полученные сообщения протокола VTP через свои магистральные порты.

**Функционирование протокола VTP**

Изменение конфигурации VLAN (создание, удаление и изменение VLAN) реализуется только на одном коммутаторе в домене (в данном случае – на VTP-сервере). Остальные устройства получают информацию о VLAN, интерпретируют её (вносят изменения в БД VLAN, которая находится на каждом коммутаторе).

Типы сообщений протокола VTP:

* Запрос анонсирования VLAN - запрос клиентом информации о созданных VLAN;
* Анонсирование общей информации – передача информации о созданных VLAN.

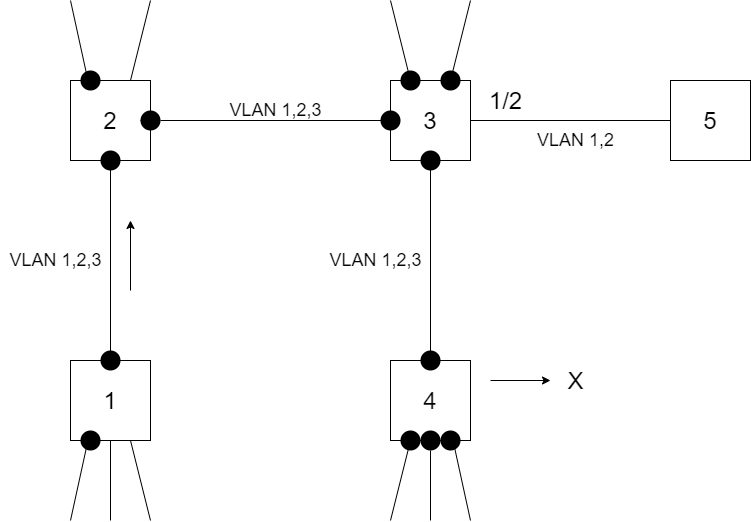
Таким образом, клиент запрашивает информацию об изменениях в составе VLAN, сервер информирует об изменениях в составе VLAN.

**Отсечение каналов в протоколе VTP**

Если в MAC-таблице на коммутаторе отсутствует MAC-адрес (время хранения в MAC-таблице истекло), то полученный одноадресный кадр широковещательно выставляется на все порты. Аналогичные действия выполняются с широковещательными кадрами.

Для исключения широковещания по магистральным каналам действует режим отсечения трафика протокола VTP. То есть, отсечение трафика действует только в магистральных каналах коммутаторов. По умолчанию отсечение выключено.

**Пример реализации отсечения трафика:**



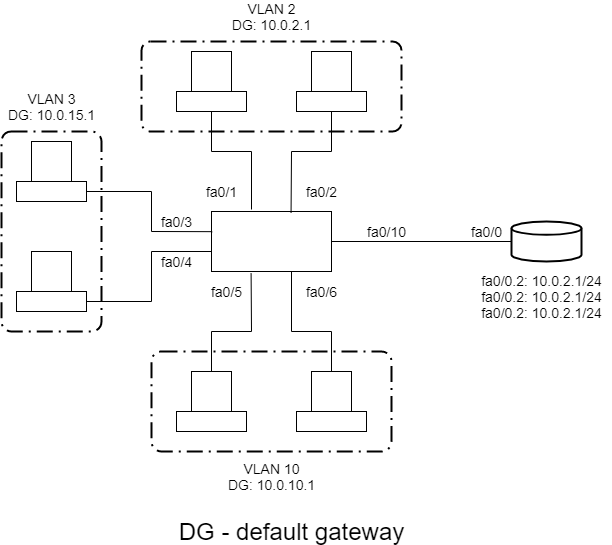
Если на коммутаторе 5 нет в VLAN3, то отсечение предотвращает рассылку на коммутаторе 3.

То есть коммутатор 3 из магистрального порта 1/2 (через магистральный порт 1/2) не реализует выставление широковещательного трафика VLAN3. VTP реализует отсечение трафика для VLAN с номерами от 2 до 1000.

**Туннелирование VLAN с использованием маршрутизатора**

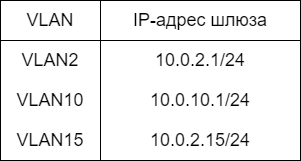
Передача данных между узлами, входящими в разные VLAN, реализуется с использованием маршрутизатора.

Для обеспечения туннелирования VLAN на одном физическом интерфейсе маршрутизатора создаются несколько логических под-интерфейс.



На коммутаторе порт, ведущий к маршрутизатору, является магистральным.

Таблица IP-адресов, использованных для устройств, входящих в разные VLAN:



**Пример конфигурирования под-интерфейс:**

interface fa0/0.2

encapsulation dot1q 2

/\* в интерфейсе инкапсулируется VLAN2 \*/

IP address 10.0.2.1 255.255.255.0

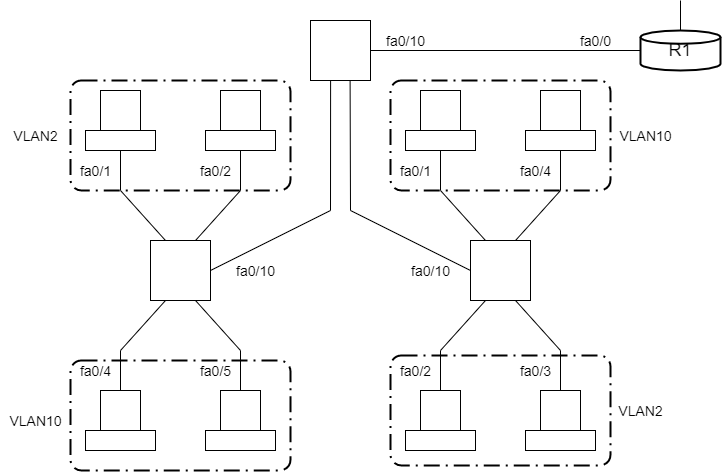
interface fa0/0.10

encapsulation dot1q 10

IP address 10.0.10.1 255.255.255.0

В результате у каждой VLAN будет свой логический под-интерфейс на маршрутизаторе (под-интерфейс назначается шлюзом для всех РС в соответствующей VLAN).

Архитектура туннелирования VLAN для нескольких коммутаторов:



На fa0/0 маршрутизатора R1 настроены под-интерфейсы

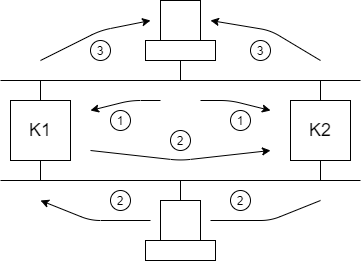
10.0.2.1, 10.0.10.1, маска: 255.255.255.0

**Протокол связующего (покрывающего) дерева (STP-протокол)**

Механизм протокола STP обеспечивает построение активной (логической) топологии без петель, то есть построение остовных деревьев. За счёт балансирования нагрузки STP позволяет формировать различные остовные деревья для разных VLAN и, как следствие, обеспечивает различные маршруты движения трафика разных VLAN (то есть построение различных остовных деревьев за счёт избыточных ИС позволяет повысить производительность работы сети без изменения состава оборудования). Изменение физической топологии связей между коммутаторами вызывает в протоколе STP перестроение логических топологий для разных VLAN (то есть обеспечивает сходимость сети и надежности её функционирования).

Беспетлевая топология - структура сети в виде дерева, покрывающего физическую топологию сети. Причины возникновения петель - наличие избыточных соединений, призванных повысить надежность функционирования сети.

**Пример образования широковещательной петли при наличии избыточных каналов:**



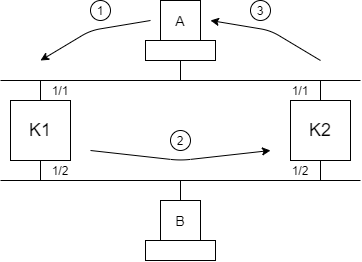
Станция А отправляет кадр с широковещательным MAC-адресом (пример с общей шиной).

*Первый этап* - кадр получают два коммутатора, так как адрес широковещательный, то коммутатор выставляет кадр на все свои физические порты.

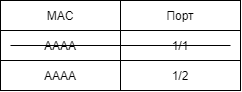
*Второй этап* - получив широковещательные кадры в другие порты, коммутаторы вновь выставят их на альтернативные порты.

*Третий этап* - действия второго этапа выполняются до бесконечности.

**Пример петли при адресной передаче:**



MAC-таблица на коммутаторе:



1) Станция А имеет запись в ARP-таблице о РС B. РС A отправляет одноадресный кадр.

2) Станция В временно отключена. Следовательно, в MAC-таблице на коммутаторе К1 отсутствует запись о РС В. Кадр поступает на порты 1/1 обоих коммутаторов.

3) В MAC-таблице на К1 отсутствует запись об адресе станции B, то К1 выставляет адресный кадр на 1/2.

4) Посланный кадр достигает порта 1/2 на К2. На К2 удаляется запись о подключении РС А к порту 1/1 и добавляется запись о подключении РС А к порту 1/2. После чего кадр выставляется на порт 1/1.

Таким образом, функции протокола STP предполагают построение остовных деревьев для VLAN, исключающих петли, а также за счет балансирования нагрузки - формирование различных экземпляров остовных деревьев для разных VLAN.

Построение разных экземпляров остовных деревьев разных VLAN возможно в случае наличия избыточных каналов между коммутаторами (избыточные каналы - повышение надежности и балансирование нагрузки).

Параметры, используемые протоколом STP при формировании остовных деревьев:

* идентификатор коммутатора Bridge ID (BID);
* стоимость маршрута до корневого коммутатора (корневого моста) остовного деревья.

Стоимость маршрута до корневого моста определяется для каждого порта коммутатора и характеризует степень удаленности порта (как следствие, коммутатора) от корневого моста.

Таким образом, стоимость маршрута - значение расстояния между коммутаторами – между корневым коммутатором и любым другим коммутатором сети. Стоимость маршрута определяется как сумма стоимостей участков, соединяющих коммутаторы. Стоимость участка определяется технологией связи между коммутаторами.

Значения стоимости участков:

1. 10 мб/с – 100;
2. 100 мб/с – 19;
3. 1 гб/с – 4.

Суммарная стоимость маршрута между коммутаторами должна быть минимальной.

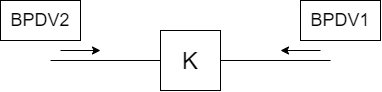
Идентификатор моста – BID – поле длиной 8 байт.

Формат BID:



В коммутаторе установлен один MAC-адрес. По умолчанию приоритет моста имеет значение 32768.

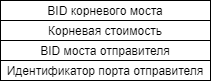
Функционирование протокола STP обеспечивается передачей сообщений. Передачу сообщений реализует протокол BPDV.



Коммутатор получает сообщения BPDV через все физические порты, интерпретирует и сохраняет только то сообщение, у которого значения параметров минимальны (минимален BID корневого моста, минимальная стоимость маршрута до корневого моста).

**Формат сообщения протокола BPDV**

(Формат сформирован (соответствует) алгоритму функционирования протокола STP).



BID корневого моста – идентификатор моста, являющегося основанием дерева. Корневая стоимость – расстояние от порта, который принял сообщение, до корневого моста.

При построении дерева анализируются последовательно следующие параметры (в случае равенства в сообщениях, принятых на разные порты, значений одного и того же параметра, реализуется переход к анализу следующего параметра в сообщении BPDV):

1. Значение корневого моста (выбирается min);
2. Значение стоимости маршрута до корневого моста (выбирается min);
3. Значение BID отправителя сообщения BPDV (выбирается min);
4. Значение идентификатора порта отправителя (выбирается min).

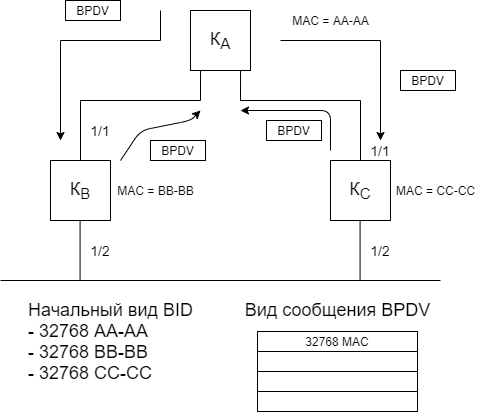
Алгоритм построения остовного дерева VLAN протоколом STP (с использованием передачи сообщения протокола BPDV):

1. Выбор корневого моста;
2. Выбор корневых портов – портов коммутаторов, наиболее близко расположенных по отношению к корневому мосту;
3. Выбор назначенных и не назначенных портов (назначенные порты – порты, через которые коммутатор передаёт кадры, не назначенные

порты – порты, через которые передачи кадров заблокирована).

**Пример первоначального выбора корневого моста**

При включении коммутаторов они обмениваются друг с другом сообщениями BPDV, в которых указывают собственный BID. Корневым выбирается мост с наименьшим значением BID.



Если мост получил через порт от другого моста более приемлемое сообщение, чем отправил в этот же порт, то отправка его сообщений через этот порт прекращается. Мост сохраняет сообщение с минимальным значением BID, которое он будет размещать в BPDV-сообщении на втором этапе.

Выборы корневого моста прекращаются, как только заканчивается обмен сообщениями BPDV.

*Второй этап -* Выбор корневых портов на каждом коммутаторе.

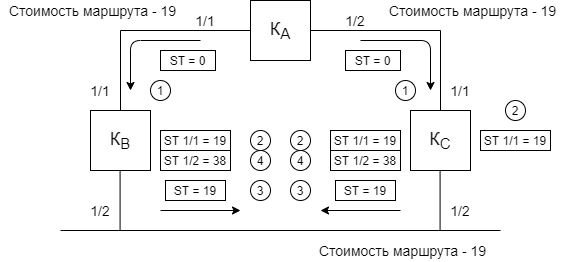
Корневой порт – это порт коммутатора, имеющий наименьшее значение корневой стоимости.

Виды стоимостей:

* Локальная стоимость – стоимость канала, к которому подключён порт;
* Корневая стоимость – сумма стоимостей всех каналов от корневого моста до текущего (рассматриваемого порта).

**Пример выбора корневых портов:**

Ближайший (с точки зрения корневой стоимости) порт на коммутаторе (к корневому мосту) назначается корневым потом. Каждый не корневой коммутатор должен иметь хотя бы один корневой порт. Используется понятие корневой стоимости.



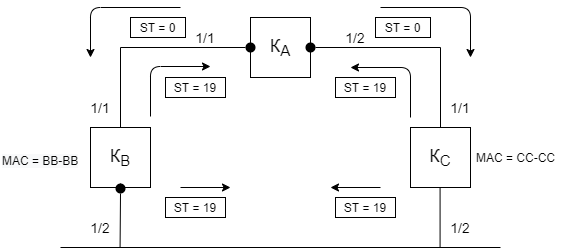
* 1. Корневой мост отправляет сообщения BPDV, содержащие корневую стоимость = 0;
  2. При получении сообщения коммутатор В сопоставляет с портами 1/1 стоимость 19;
  3. Коммутатор В рассылает сообщение BPDV с корневой стоимостью 19;
  4. Коммутатор С получив сообщение назначает порту 1/2 корневую стоимость 38;
  5. Коммутаторы В и С сравнивают корневые стоимости портов 1/1 и 1/2, выбирают в качестве корневых портов порты 1/1.

*Третий этап* - Выбор назначенных портов.

Выбор назначенных портов на коммутаторах выполняется для каждого сегмента сети (кабеля), соединяющего два коммутатора.

Назначенный порт – порт, который выполняет обмен трафиком между рассматриваемым сегментом сети и корневым мостом.

При выборе назначенных портов учитывается корневая стоимость, если корневая стоимость одинакова, то рассматриваются BID.



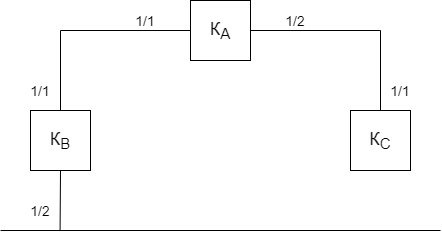
1. Обмен сообщениями BPDV между коммутаторами A и B, A и C. Коммутатор A выставляет стоимость 0, коммутаторы В и С – стоимость 19. Так как A получил стоимость 19, а выставленная стоимость 0, то его порты 1/1 и 1/2 идентифицируется как назначенные.
2. Обмен сообщениями BPDV между коммутаторами В и С.

Коммутатор В выставляет стоимость 19, коммутатор С – стоимость 19. Так как коммутатор В в порт 1/2 получил сообщение BPDV с ST=19, а в этот же порт он выставил BPDV с ST=19 (стоимости равны), он сравнивает свой BID с BID коммутатора С. Так как BIDB < BIDC, коммутатор B идентифицирует порт 1/2 как назначенный. Так как

BIDB < BIDC и STB = STC, то коммутатор С идентифицирует порт 1/2 как не назначенный, то есть он не будет выставлять в него кадры.

Таким образом, корневые и назначенные порты реализуют обмен кадрами между коммутаторами, не назначенные порты не реализуют обмен кадрами. Тогда на основе корневых, назначенных и не назначенных портов формируется новый вид таблиц коммутации.

Итоговый вид остовного дерева:



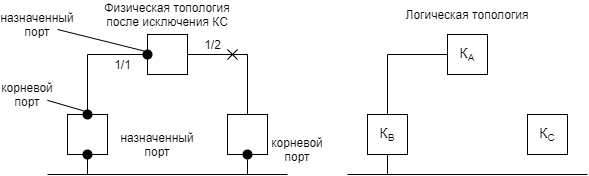
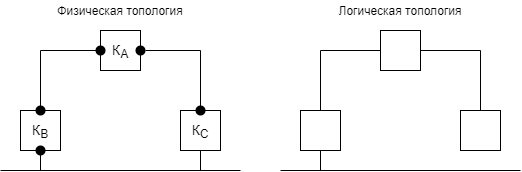
**Таймеры протокола STP. Формирование нового остовного дерева сети**

Контроль неизменности топологии обеспечивается периодической рассылкой сообщений BPDV корневым и не корневым мостам. Период рассылки сообщений BPDV – 2 секунды, возможная задержка – 20 секунд (возможное время ожидания).

Не корневые мосты отправляют сообщения BPDV после того, как получены сообщения от корневого моста.

Если сообщение BPDV не получено коммутатором, то он инициирует процедуру определения нового корневого моста (отправляет BPDV-сообщение с указанием своего ВID в поле корневого моста). Коммутаторы, получившие BPDV-сообщение, в котором ВID корневого моста не совпадает с корневым мостом, сохранённым у них, также реализуют процедуру построения нового остовного дерева.

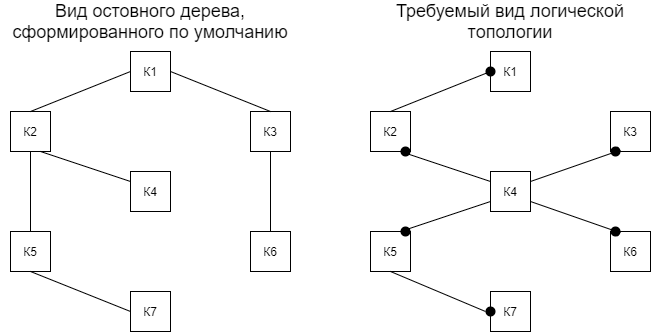
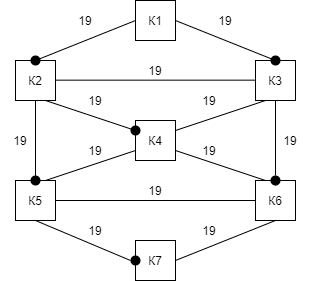
**Пример изменения логической топологии при изменении физической топологии:**



**Назначение местоположения корневого моста вручную**

При формировании остовного дерева корневой мост должен быть размещен в центре логической топологии, то есть коммутировать различные ветви дерева.

Вид логической топологии:



Таким образом, требуется чтобы коммутатор К4 был назначен корневым мостом. Так как К4 имеет MAC-адрес не минимальный среди всех MAC-адресов коммутаторов, то К4 корневым мостом назначен быть не может. При неэффективном расположение корневого моста в остовном дереве требуемый корневой мост должен быть назначен вручную. Чтобы корневой мост имел требуемое местоположение в остовном дереве, необходимо соответствующему коммутатору задать минимальный ВID. Для этого необходимо изменить приоритет соответствующего коммутатора в его ВID.

**Балансирование (распределение) нагрузки в сети**

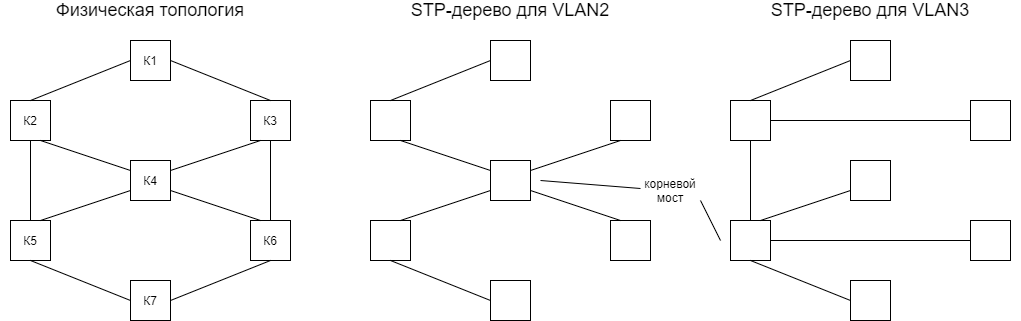
Для каждой VLAN должен быть сформирован свой экземпляр остовного дерева, не зависимый (не дублирующий) экземпляры остовных деревьев других VLAN.

В результате каждая VLAN будет иметь своё множество путей между коммутаторами, не пересекающиеся с множеством путей других VLAN (используется отдельный экземпляр остовного (связующего дерева).

Таким образом, реализуется изоляция экземпляров связующих деревьев для разных VLAN (недоступность трафика разных VLAN).

Итог: балансирование (распределение) нагрузки по различным экземплярам остовных деревьев разных VLAN.

**Пример различных конфигураций остовных деревьев для разных VLAN:**



Балансирование нагрузки позволяет удвоить пропускную способность без приобретения дополнительного оборудования.

Условия, наличие которых определяет возможность балансирования нагрузки:

* Наличие избыточных каналов, как следствие, наличие петлевых топологий;
* Наличие нескольких VLAN.

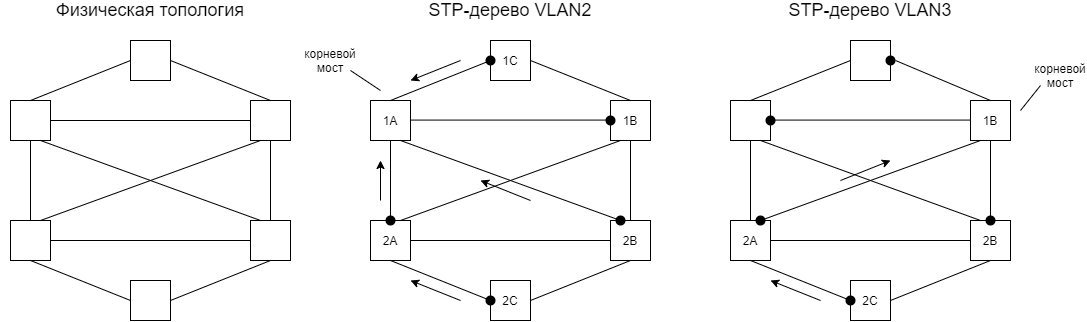
**Балансирование нагрузки за счет изменения приоритетов мостов**

Сформировать требуемую логическую топологию можно двумя способами:

* Разместить в нужном месте физической топологии мост с наименьшим MAC-адресом (с наименьшим BID моста);
* Изменить BID моста, который может быть назначен корневым, административно;
* Изменение BID моста реализуется путем уменьшения его приоритета. Таким образом, уменьшение приоритета моста позволит назначить новый корневой мост (местоположение нового корневого моста).

Однако, данный способ балансирования не гарантирует требуемого вида остовного дерева.

**Пример построения неэффективных топологий остовных деревьев после назначения нового местоположения корневого моста:**



В остовном дереве для VLAN3 ребро 2A-2C есть совпадающий маршрут (за счет меньшего значения идентификатора BID моста 2А).

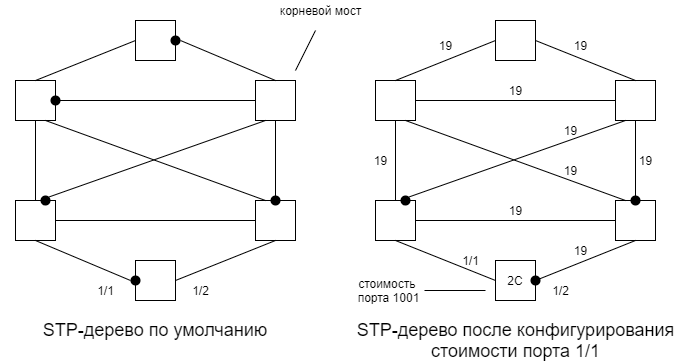
Для задания ветви 2С-2В в составе остовного дерева для VLAN3 необходимо указать приоритеты коммутаторов 1В и 2В следующим образом:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Priority 1B |  | Priority 2B |  | Priority default |
| 4096 | < | 8192 | < | 32768 |

Приоритеты изменяются на коммутаторах 1В и 2В соответственно.

**Балансирование нагрузки за счет изменения стоимости портов**

Предыдущий рисунок остовного дерева для VLAN3

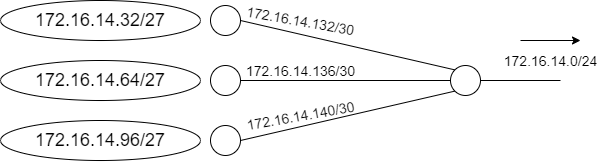


Таким образом, для изменения вида остовного дерева на коммутаторе 2C реализуется изменение стоимости порта 1/1 (задается значение 1001).

**Адресация устройств в объединённых сетях. VLSM-маcкирование**

VLSM-маcкирование - это способ формирования схемы адресации в объединённых сетях, который позволяет в рамках одной сети задавать более одной маски.

**Пример использования масок переменной длины в объединённых сетях:**



172.16.14.0/24 - суммарный адрес - задаётся административно, хранится в таблицах маршрутизации на удалённых устройствах.

Достоинства использования VLSM-маскирования:

* Более эффективное (полное) использование адресного пространства;
* Возможность использования суммирования маршрутов.

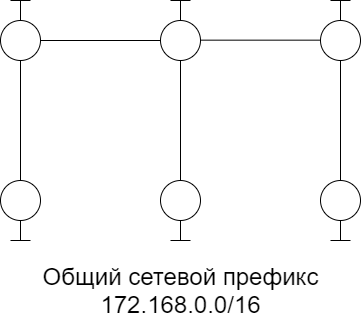
VLSM-маскирование позволяет задавать несколько уровней IP-адресов (иерархическая адресация подсетей в рамках сети). Задание иерархической адресации (иерархической схемы адресации) позволяет сформировать обобщённый адрес - суммировать все префиксы сетей в одной области (зоне).

Таким образом, VLSM-маскирование - для увеличения адресного пространства.

Алгоритм VLSM-маскирования:

1. Определение количества устройств в сети;
2. Определение количества бит в IP-адресе, которое должно быть выделено для адресации требуемого количества устройств;
3. Определение размера сетевого префикса и значения сетевого префикса (с учетом принципа наибольшего соответствия при маршрутизации);
4. Определение значения маски;
5. Определение значений IP-адресов отдельных устройств.

**Пример топологии сети для реализации VLSM-маскирования:**



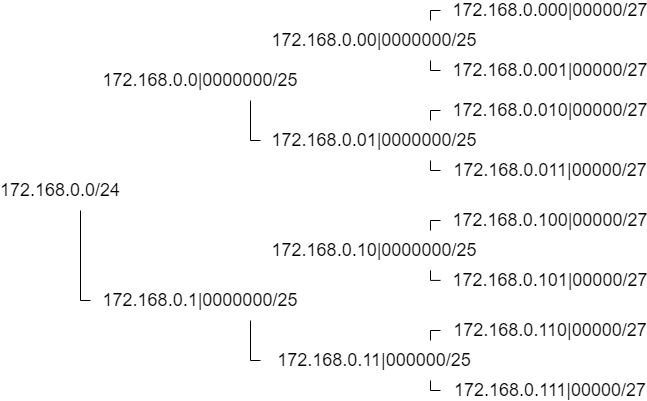
**CIDR-технология**

CIDR-технология - способ разделения адресного пространства в некоторой объединенной сети.

**Пример формирования схемы адресации:**

Общий адрес 172.168.0.0/24

Адресное пространство должно быть разделено в следующих пропорциях:



Итоговые значения адресов:

1/4, 1/4: 172.168.0.0/26,

172.168.0.64/26;

1/8, 1/8, 1/8: 172.168.0.128/27,

172.168.0.160/27,

172.168.0.192/27;

1/16, 1/16: 172.168.0.224/28,

172.168.0.240/28;

Последний сетевой префикс может быть использован для адресации каналов “точка-точка”.

**ЗАЩИТА ДАННЫХ НА УСТРОЙСТВАХ С ИСПОЛЬЗОВАНИЕМ СПИСКОВ ДОСТУПА**

Особенности использования списков доступа:

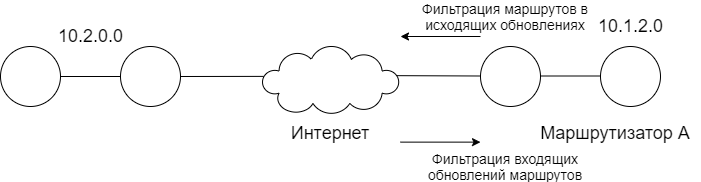
* Используются для того, чтобы заблокировать или разрешить передачу трафика на портах/интерфейсах маршрутизаторов;
* Фильтрация реализуется на основе адреса сети получателя, адреса сети отправителя, приложения, которому предназначен трафик (порта получателя), приложения, которое реализует передачу трафика (порта отправителя).

Использование фильтрации на маршрутизаторах обеспечивает:

* Запрет рассылки информации о к/п сети, чтобы исключить хранение маршрутной информации о ней и ограничить доступ к ней (фильтрация распространения информации о сети):
* Запрет на получение маршрутной информации - исключает получение ложной маршрутной информации, которая может привести к перенаправлению трафика.

Для реализации указанных функций список доступа связывается с портом (сетевым интерфейсом) с помощью команды *distribute-list* (то есть командой *distribute-list* список доступа привязывается к интерфейсу маршрутизатора).

**Пример схемы фильтрация пакетов:**



**Фильтрация входящих обновлений маршрутов**

Запрет объявления маршрутов в обновлениях маршрутизации (запрет исходящих обновлений). Цель - невозможность сторонним пользователям получить доступ к сети (то есть запрет объявления внутренних сетей внешним устройствам).

Сеть доступна только своим пользователям. Конфигурация сети и устройства в сети не могут быть определены сторонними пользователями.

Запрет обеспечивается указанием протокола маршрутизации.

Формат списка доступа (стандартного):

access-list <номер> <deny|permit>

<источник [групповой адрес источника]

*deny|permit* - определяет действие (запрет или разрешение), которое должно применяться к трафику с указанным адресом.

*источник* - указывает адрес источника.

*групповой адрес* *источника* - может быть использовано слово они для указания адреса источника.

Чтобы применить созданный список доступа к определенному интерфейсу применяется команда *IP access-group*.

Формат команды:

IP access-group <номер списка> {in|out}

*in -* фильтрация входящих пакетов, *out* - фильтрация исходящих пакетов. Команда *no access-list <номер списка доступа>* позволяет удалить список из конфигурации.

Вид списка доступа, запрещающего объявление маршрутов (указание отдельных сетей) в обновлениях маршрутизаторов:

accsess-list 45 deny 10.1.2.0 0.0.0.255

accsess-list 45 permit any

router eigrp 200

distribute-list 45 out serial 0

Реализуется запрет на указание сети в обновлениях, формируемых маршрутизатором. Требуется применение списка к обновлениям протокола EIGRP.

Таким образом, маршрутизатор в обновлениях протокола EIGRP не указывается сеть 10.1.2.0.

**Запрет обработки маршрутов, указанных в обновлениях (запрет на получение маршрутов)**

Реализуется запрет использования сетей, указываемых в обновлениях протоколов маршрутизации, таким образом на устройствах не будут использоваться маршруты, которые могут оказаться фиктивными. Тогда могут быть использованы только обновления, исходящие от маршрутизаторов, информация о которых уже имеется в таблице маршрутизации на устройстве (то есть используются обновления только от “надежных” сетей).

**Пример списка доступа для запрета обработки маршрутов:**

accsess-list 45 permit 10.2.0.0 0.0.255.255

router eigrp 200

distribute-list 46 in serial 0

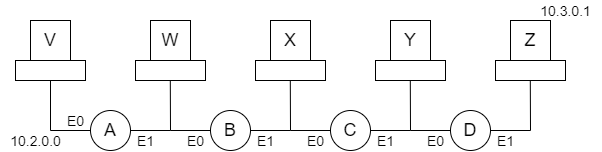
Список допускает возможность использования обновлений, исходящих от надежной сети 10.2.0.0 (список применяется к входящему в порт serial 0 трафику).

Рассмотренные списки доступа относятся к стандартным спискам доступа.

**Размещение стандартных списков доступа**

Стандартные списки доступа размещаются как можно ближе к маршрутизатору адресата (то есть к маршрутизатору, к которому подключение защищается PC).

**Пример организации объединенной сети:**



Задание списка доступа с целью запретить обращаться станции Z к станции V. В этом случае список должен быть размещен на маршрутизаторе А и привязан к интерфейсу Е1 (запрет входящего в Е1 трафика от станции 10.3.0.1)

Вид списка доступа:

accsess-list 3 deny 10.3.0.1

accsess-list 3 permit any

interface e1

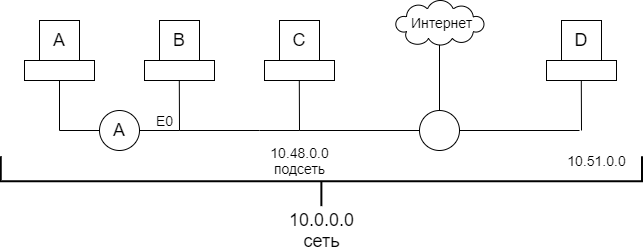
IP access-group 3 IN

Список доступа лучше привязать к входному порту, чтобы маршрутизатор А не обрабатывал входящий трафик.

Возможные варианты конфигурирования списка доступа на других маршрутизаторах:

* Маршрутизатор В: РС Z не соединяется с PC W и РС V;
* Маршрутизатор C: РС Z не соединяется с PC V, W, X;
* Маршрутизатор D: РС Z не соединяется с PC W, V, X, Y.

**Пример реализации стандартного списка доступа:**



Список доступа настраивается на маршрутизаторе A и привязывается к порту E0.

accsess-list 2 permit 10.48.0.1 //(неявная маска)

accsess-list 2 deny 10.48.0.0 0.0.255.255

accsess-list 2 permit 10.0.0.0 0.255.255.255

accsess-list 2 deny any

interface e0

IP accsess-group 2 in

*Первая строка* - разрешение для хоста В передачи данных на хост А (маска не указана / неявная маска, указан IP-адрес хоста и атрибут *permit).*

*Вторая строка* - запрет на доступ РС из сети 10.48.0.0 на доступ к РС А (РС С не имеет доступа к РС А) - *deny* - запрет передачи.

*Третья строка* - доступ PC, находящихся в сети 10.0.0.0/8 разрешён К РС А (то есть рабочая станция D имеет доступ к РС А).

Для пользователей из других сетей доступ к РС А запрещен (четвёртая строка).

**Расширенные списки доступа**

Стандартные списки доступа выполняют фильтрацию сетевого трафика только на основе адресов источников.

Возможности, предоставляемые расширенными списками доступа:

* Фильтрация на основе протокола транспортного уровня;
* Фильтрация на основе адреса получателя;
* Фильтрация на основе номера порта приложения, трафик которого передается.

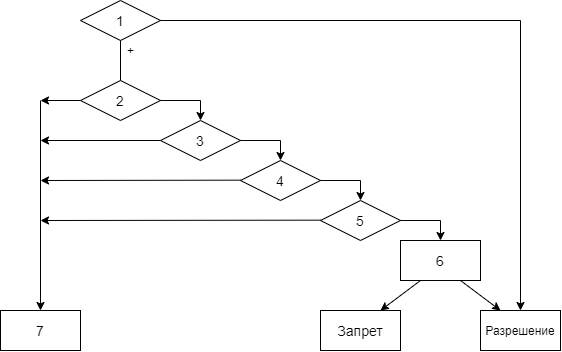
Стандартные списки доступа - быстрая обработка входящего трафика (анализируется малое количество параметров).

Таким образом, расширенные списки доступа применяются для контроля (проверки) адресов источника и получателя, протокола, данные которого передаются (в частности, проверяются идентификаторы портов TCP и UDP, что позволяет фильтровать данные на прикладном уровне).

При контроле трафика с использованием расширенного списка доступа проверяется совпадение параметров в списке и параметров пакета. Если совпадение по к/п параметру найдено, то реализуется переход к анализу следующего параметра (совпадение этого параметра в списке и параметра в пакете).

Если хотя бы одно условие нарушается, то реализуется переход к следующей строке списка (следующему списку).

Алгоритм реализации фильтрации:



1. Настроен ли список доступа;
2. Адрес получателя;
3. Адрес источника (отправителя);
4. Проверка протокола;
5. Проверка опций протокола.

Синтаксис расширенного списка доступа:

access-list номер {deny|permit}

протокол источник | групповой адрес источника получатель | групповой адрес получателя [precedence приоритет] [to s тип сервиса]

Значение приоритетов:

0 – routine, 1 – priority,

2 – immediate (немедленный),

3 – flash, 4 – flash-override,

5 – critical, 6 – internet, 7 – network.

Тип сервиса:

normal (0)

min – monetary cost (1)

max – reliability (2) (max – надежность)

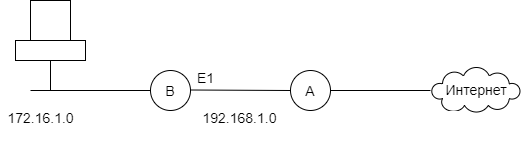
max – throughput (4)

min – delay (8)

В качестве идентификатора протокола могут быть заданы ключевые слова: *eiqrp*, *icmp*, *iqmp*, *iqrp*, *ip*, *ospt*, *tcp*.

Чтобы указать соответствие? любому протоколу Интернет (в том числе TCP и UDP) следует указать IP.

**Пример реализации расширенного списка доступа:**



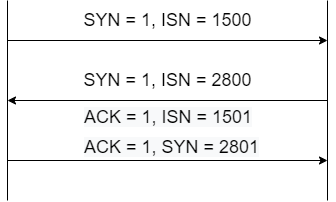
access-list 103 permit tcp any host 172.16.1.0 0.0.255.255 established

access-list 103 permit tcp any host 172.16.1.3 eq smtp

*established* - ключевое слово для протокола TCP, указывает на установленное соединение.

Чтобы SMTP-сообщение было передано узлу 172.16.1.3 в заголовке TCP-пакета должны быть установлены биты ACK или RST (установленные биты ACK и RST указывают на установленное соединение). Если установлен бит SYN, указывающий на инициализацию сеанса, то SMTP-сообщение отбрасывается.

Три фазы установления соединения в протоколе TCP:



ISN - номер первого байта в очереди на передающей и приемной сторонах.

**Пример 2 расширенного списка доступа:**

access-list 100 permit 192.168.1.0

0.0.0.255 eq 80 //указание на порт отправителя

10.1.1.0 0.0.0.255 eq 443

*eq –* атрибут, указывающий на равенство значений портов в TCP-заголовке и в списке.

access-list 100 deny tcp any host 172.16.1.5 qt 5000

Команда запрещает весь TCP трафик от любого хоста на хост с адресом 172.16. 1.5 с идентификаторами портов от 5001 и выше.

То есть *qt-атрибут* превышения значения порта в TCP-заголовке указанного в списке значения.

Альтернативные варианты операторов для идентификаторов портов.

*lt -* пакеты с более низким номером.

*ncq* - пакеты, нt соответствующие заданному номеру порта.

*range* - диапазон портов.