СПбГЭТУ «ЛЭТИ»
ПЕРВЫЙ ЭЛЕКТРОТЕХНИЧЕСКИЙ

Р.Р. Фаткиева

Основы построения защищенных компьютерных сетей

Протоколы идентификации, аутентификации и авторизации

СПбГЭТУ «ЛЭТИ», 2021 г.

4. ПРОТОКОЛЫ ИДЕНТИФИКАЦИИ, АУТЕНТИФИКАЦИИ И АВТОРИЗАЦИИ. ПОСТРОЕНИЕ МАРШРУТИЗИРУЕМОЙ ЛВС. ЗАЩИТА СЕТЕВОЙ ИНФРАСТРУКТУРЫ. НАСТРОЙКА АУТЕНТИФИКАЦИИ МАРШРУТИЗАТОРОВ

Цель работы: изучение теоретического материала о маршрутизации сетевого трафика, формирование практических навыков использование методов аутентификации по технологии AAA на основе протокола TACACS.

4.1. Построение маршрутизируемой ЛВС. Защита сетевой инфраструктуры.

При получении пакета из сети маршрутизатор решает следующие задачи:

1. Определение, что необходимо сделать с полученным пакетом, согласно установленным администратором правилам фильтрации;
2. Оценивание какой сети и по какому маршруту необходимо передать пакет согласно полученному IP-пакет.

При передаче пакета по сети возникает необходимость выбора оптимального пути передачи. Для решения этой задачи используются протоколы маршрутизации. Выбор оптимального пути передачи основан на анализе метрик передачи. *Метрика* –это условная стоимость передачи по сети. Полное измерение конкретного маршрута равно сумме метрик сетей, которые включают в себя маршрут. Задача маршрутизатора заключается в том, чтобы вычислить маршрут с наименьшей метрикой. Для выбора маршрута используют протоколы маршрутизации RIP,OSPF, BGP и др.

4.1.1 Протокол RIP (Routing Information Protocol)

Протокол инкапсулируется в UDP пакеты, при передаче используется порт 520. Протокол основан стоимости метрик, равнозначных для каждого участка сети.

При первоначальной установке маршрутизатора инициализируется таблица маршрутизации. Таблица содержит только сети, связанные напрямую и счет участков, значение которых равно 1. Рассмотрим таблицу маршрутизации маршрутизатора A, представленного на Рис.4.1

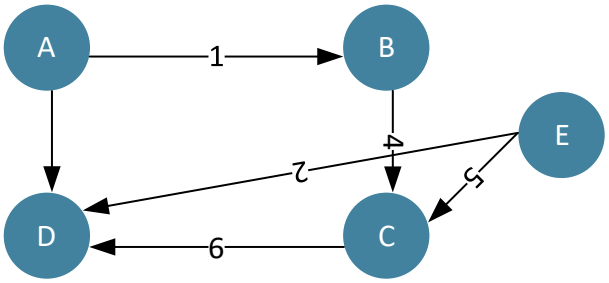


Рис. 4.1

1. При инициализации маршрутизатора A запись в таблице маршрутизации содержится следующая информация:

От A к	Канал	Вектор
A	Локальный	0

2. Маршрутизатор B получив сообщение от маршрутизатора A по каналу 1 изменяет свою таблицу маршрутизации.

От B к	Канал	Вектор
B	Локальный	1
A	1	1+1=2

3. Маршрутизатор D получив сообщение от маршрутизатора A с метрикой равной 3 изменяет свою таблицу маршрутизации

От D к	Канал	Вектор
D	Локальный	1
A	3	3+1=4

4. В свою очередь маршрутизаторы B, C и D формируют сообщения для маршрутизатора A. Рассылка сообщений происходит до того, пока не наступит момент схождения.
5. Маршрутизатор A изменяет собственную таблицу маршрутизации согласно следующим правилам:
   5.1 Если в таблице маршрутизации нет записи о маршрутизации, то формируется запись на основе присланного сообщения.
   5.2 Сообщения сведений от самого узла имеет приоритет (то есть запись в таблица, сформированной на этапе инициализации в п.1 имеет приоритет при получении сведений от других маршрутизаторов).

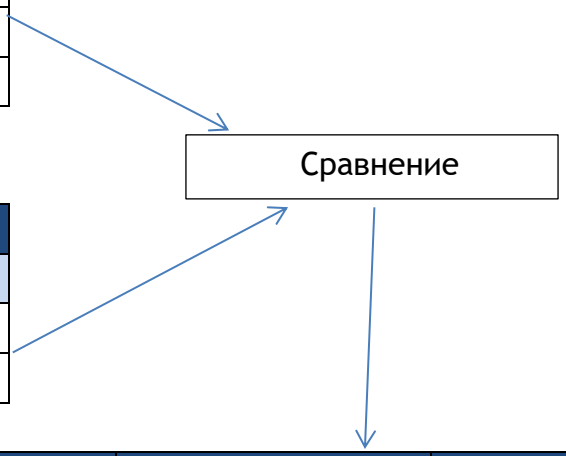
5.3Из присланных сообщений при построении таблицы маршрутизации выбирается наименьший маршрут и заносится в таблицу маршрутизации, как показано на Рис. 4.2.

Таблица маршрутизации A

От A к	Канал	Вектор
A	Локальный	1
B	1	2
D	3	4

Таблица маршрутизации E

От E к	Канал	Вектор
A	1+2+3	6
A	1+5+6+3	15
A	1+5+4+1	11



От A к	Канал	Вектор
A	Локальный	1
B	1	2
D	3	4
E	1+2+3	6

Рис. 4.2

Процесс построение указанных динамических таблиц маршрутизации называется процессом сходимости.

Формат сообщения RIP. Все сообщения протокола RIP состоят из заголовка фиксированной длины и следующего за ним списка сетей, которые могут быть достижимы с использованием данных передающего маршрутизатора (Рис. 4.3).

Команда	Версия	Зарезервировано
Семейство		Все нули
Сетевой адрес		
Все нули		
Расстояние		

Рис. 4.3

Команда-поле в 8 бит задает тип сообщения, запрос соответствует 1, ответ -2.

Версия- поле в 8 бит определяет версию протокола.

Семейство- поле в 16 бит определяет семейство используемых протоколов.

Сетевой адрес – поле в 14 бит определяет адрес пункт назначения.

Расстояние - поле в 32 бита определяет счетчик участков для каждого объявленного маршрутизатора к сети назначения

Виды сообщений RIP

1. **Инициализация таблицы маршрутизации** при установке и первом включении маршрутизатора. Таблица описана выше.
2. **Запрос/Ответ** об обновлении таблицы маршрутизации запущенный по таймеру (таймеры бывают трех видов: *периодический таймер*-установлен на случайную величину и посылает таблицу обновления всем маршрутизаторам по окончанию срока установленного по таймеру; *таймер истечения срока*-при получении сообщения обновления у маршрутизатора устанавливается таймер окончания для полученных маршрутов, когда счетчик таймера заканчивается, маршрутам присваивается вектор недостижимости; *таймер сбора мусора*-при поступлении некорректной информации о недостижимости маршрута информация не сразу стирается, а находится в таблицы маршрутизации то время, которое установлено на счетчике мусора. Это сделано для того, чтобы соседи смогли получить сведения о недействительности маршруты).
3. **Запускаемое обновление** – каждый маршрутизатор, который получает обновление рассылает новые таблицы маршрутизации соседним маршрутизаторам, раньше срока установленного по периодическому таймеру, это позволяет избежать проблем зацикливания.

Проблемы при маршрутизации

Представим сеть состоящую из 4 маршрутизаторов, представленных на Рис. 4.4.

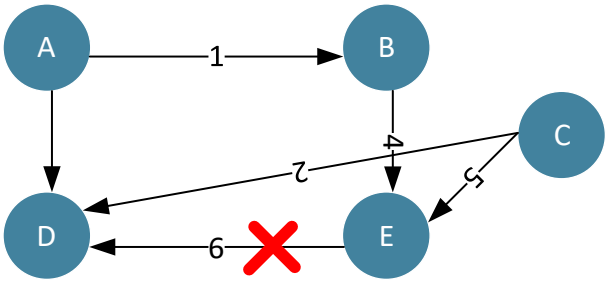


Рис. 4.3

Рассмотрим ситуацию, когда произошел обрыв каналов между маршрутизаторами A и B, и D и E. Представим ситуацию, когда маршрутизатор D первый обновил таблицу маршрутизации, в этом случае она будет выглядеть следующим образом:

От D к	Канал	Вектор
D	Локальный	1
A	3+1	4
B	3+1+1	5
C	2+1	3
E	6+1	16

Если маршрутизатор D передаст сообщение о недостижимости маршрута к E, раньше, чем это сделает любой другой маршрутизатор, то трафик в сети будет работать корректно. Если же маршрутизаторы успеют передать таблицы маршрутизации, сформированные до обрыва маршрута, то возникает **маршрутизация по петеле**. Соответственно таблица маршрутизации примет при передаче сообщения от маршрутизатора A вид:

От D к	Канал	Вектор
D	Локальный	1
A	3+1	4
B	3+1+1	5
C	2+1	3
E	6+1	7

После изменения таблицы маршрутизации D перешлет обновленную таблицу маршрутизации A и процесс может затянутся до бесконечности. Поэтому при авариях например между A и B, маршрутизатор A должен исключить все нарушенные сети, то есть убрать передачу маршрута сеть. Если связь восстановиться, то запись в таблице поменяется. При этом полученные

по сети маршруты не отправляются обратно по тому же интерфейсу, по которому получили.

Обеспечение безопасности протокола RIP. Используя возможности широковещательной рассылки, злоумышленник может создать атаки типа flood, поскольку сообщения инкапсулируются в UDP –протокол. Данный протокол позволяет осуществить атаку подмены IP адреса, подмену содержимого поля данных. Недостатком протокола также является то, что пакет передается по сети в открытом виде, что позволяет прослушать трафик.

Для защиты сети от перегрузки трафика и борьбы с подменой IP адреса используют статическую таблицу маршрутизации внутри локальной сети, настраиваемую администратором сети «вручную».

Для борьбы с перегрузками в сети возможно увеличить время передачи обновлений таблиц маршрутизации (это позволяет уменьшить время сходимости).

Использование механизмов аутентификации позволяют провести проверку маршрутизатора и защитить от неполномочного объявления. Формат сообщения показан ниже

Команда	Версия	Зарезервировано
FFFF		Тип аутентификации
Данные для аутентификации		

Тип аутентификации- поле показывает метод, используемый для аутентификации, например аутентификация может быть осуществлена по алгоритму MD5.

Данные для аутентификации –поле содержит данные необходимые для прохождения успешной аутентификации и зависеть от установленного механизма аутентификации, в частности, хеш от пароля, случайное число, метка времени и т п.

4.1.2 Протокол OSPF

Протокол (Open Shortest Paht First) инкапсулируется в IP- дейтограммы, содержит извещающий механизм для управления потоком и контролем ошибок. Его область автономные системы. Протокол позволяет осуществлять

маршрутизацию в районе одной зоне. Зона –это набор всех сетей, хостов и маршрутизаторов, содержащихся в автономной системе.

Маршрутизаторы внутри зоны содержат зоновую информацию маршрутизации, каждая зона имеет идентификатор зоны на границе которой установлены пограничные маршрутизаторы. Протокол позволяет администратору назначать стоимость, называемую метрикой. Для каждого маршрута. Метрика основана на типе сервиса, наиболее значимого для указанной

Виды метрик:

1. Вектор расстояния (число транзитных участков, число пакетов в очереди);
2. Таймер времени (время задержки, время жизни пакета);
3. Пропускная способность канала.

Для того чтобы выстроить маршрут с наименьшей метрикой маршрутизатору необходимо определить топологию сети. Для этого имеется 4 типа связей:

Связь точка -точка. Связь соединяет два маршрутизатора напрямую, метрика для этого маршрута одинаковая для обоих маршрутизаторов.

Транзитная связь. Это сеть с несколькими маршрутизаторами, соединенными линиями, каждый маршрутизатор имеет несколько соседей. Транзитная связь бывает нескольких видов – линейная связь, связь «каждый с каждым», связь с использованием узлового маршрутизатора. Построение указанных сетей зависит от количества хостов в подсети. Протокол позволяет делить их на области (Рис. 4.4).

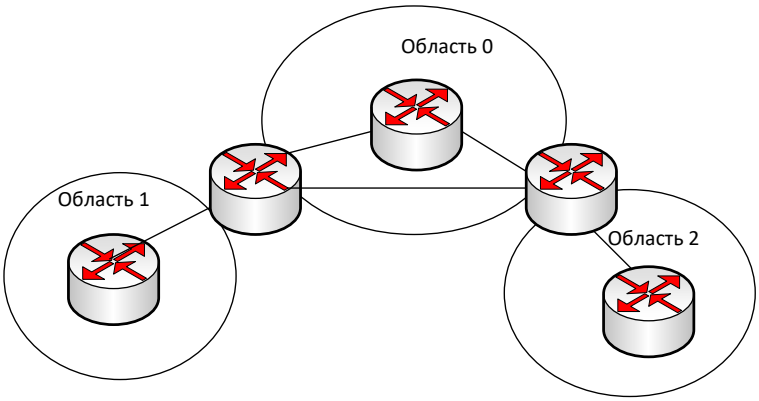


Рис. 4.3

Области 1, 2 –автономные, область 0- магистральная. Работа маршрутизатора заключается в расчете кратчайшего пути от источника до всех остальных точек сети. Рассмотрим выбор наикратчайшего маршрута от точки A до точки H в соответствии с алгоритмом Дейкстры (Рис. 4.5)

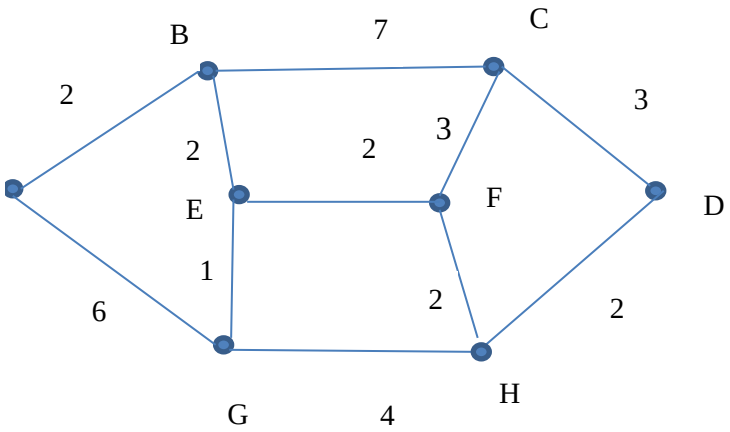
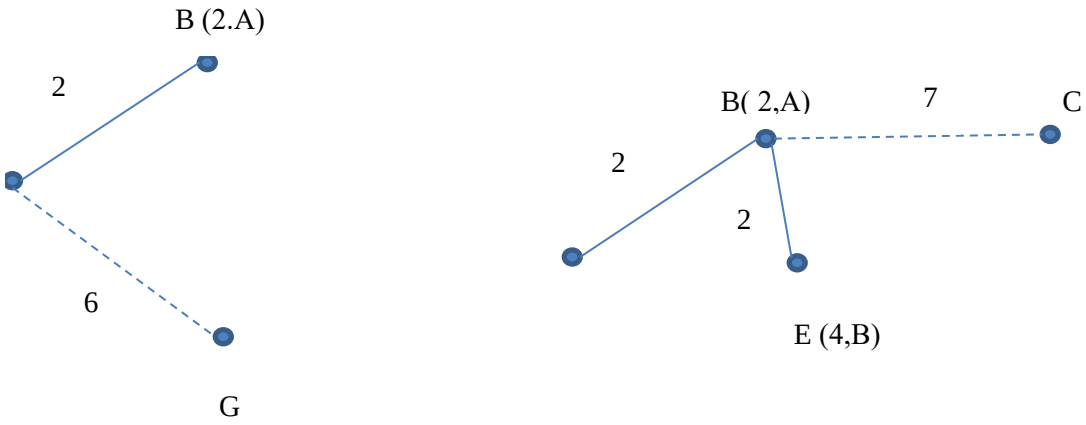


Рис. 4.4

Построение маршрута передачи сетевого трафика осуществляется с использованием алгоритма Дейскстры. Формирование наикратчайшего маршрута показано на Рис. 4.5.



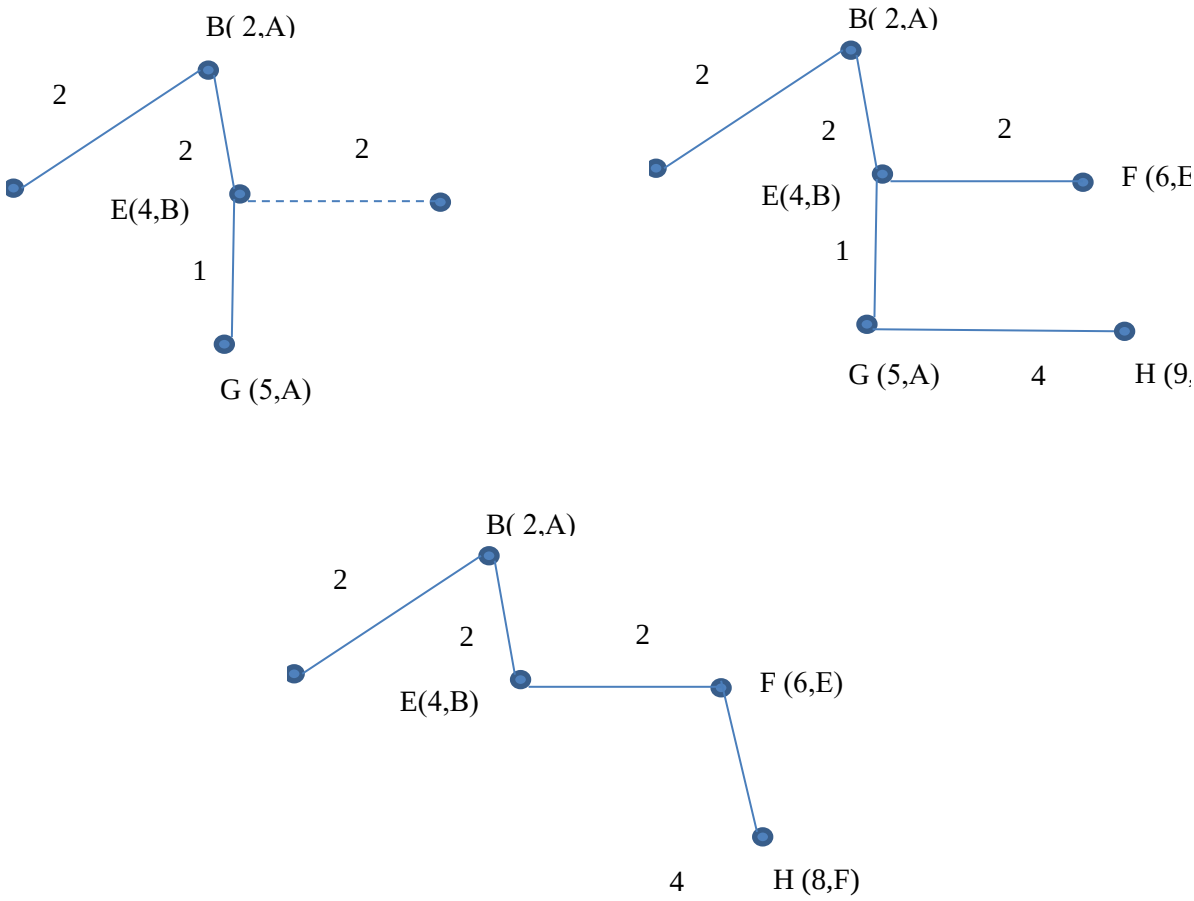


Рис. 4.5

Виды сообщений OSPF:

1. Инициализация таблицы маршрутизации при установке и первом включении маршрутизатора.
2. Извещение о состоянии связи представляют собой следующие виды сообщений:
   - 2.1 связь маршрутизатора- используется для извещения обо всех связях маршрутизатора;
   - 2.2 сетевая связь- используется узловым маршрутизатором для извещения о состоянии всех маршрутизаторов, подключенных к сети;
   - 2.3 суммарная связь к сети-информация о линиях маршрутизации и сетевых линиях внутри зоны, что позволяет выбрать наикратчайший путь;
   - 2.4 суммарная связь к пограничному маршрутизатору-информация о стоимости и маршруте к пограничному маршрутизатору;

2.5 внешняя связь- извещения о том, какая сеть доступна вне автономной системы.

Для формирования маршрутной информации используются **базы данных состояний линии,** которые представляют собой таблицу, характеризующую топологию внутри зоны, а также связи между соседними маршрутизаторами и метрики. На основании данной информации маршрутизатор применяя алгоритм поиска наикратчайшего пути, используя присланные метрики строит собственную таблицу маршрутизации.

При первом подключении маршрутизатор посылает пакет «hello» для оповещения соседних маршрутизаторов (Рис. 4.6).

Общий заголовок 24 байта				
Маска сети				
Интервал посылки	Все нули	E	T	Приоритет
Интервал неисправности				
IP адрес назначенного маршрутизатора				
IP адрес резервного назначенного маршрутизатора				
IP адрес соседа				

Рис. 4.6

Маска сети- поле 32 бита определяет маску сети, по которой посылается сообщение.

Интервал посылки- поле 16 бит определяет число секунд между сообщениями "hello".

E-флаг- установка флага означает, что зона является ответвлением.

T-флаг- установка флага означает, что маршрутизатор поддерживает множество метрик.

Приоритет. Это поле определяет приоритет, маршрутизатор с наивысшим приоритетом выбирается как назначенный, второй наивысший приоритет, выбирается как резервный назначенный маршрутизатор.

Интервал неисправности - поле 32 бита определяет число секунд до момента, когда маршрутизатор предположит, что сосед неисправен.

Получив сообщение «hello» соседние маршрутизаторы посылаю пакеты обновления с описанием собственных баз данных (но не

содержащих полную версию таблицы), на основании присланных данных маршрутизатор анализирует имеется ли в его таблице данная информация, при ее отсутствии посылает запрос о состоянии связи.

Использование механизмов аутентификации

Позволяет провести проверку маршрутизатора и защитить от неполномочного объявления. Формат сообщения представлен на Рис.4.7

Версия	Тип	Длина сообщения
IP-адрес источника		
Идентификатор зоны		
Контрольная сумма		Тип аутентификации извещения
Аутентификация данных		
Аутентификация типа		

Рис. 4.7

и содержит поля:

-Версия- поле 6 бит, определяющее версию протокола OSPF.

-Тип -поле 8 бит определяет тип пакета

-Длина сообщения- поле 16 бит определяет длину всего сообщения, включая заголовок.

-IP-адрес маршрутизатора источника- поле 32 бита определяет IP-адрес маршрутизатора, посылающего пакет.

-Идентификация зоны -поле 32 бит определяет зону, в которой работает маршрутизатор.

-Контрольная сумма- поле 16 бит используется для обнаружения ошибок во входящем пакете, исключая поля "аутентификация типа" и "аутентификация данных".

-Тип аутентификации-поле 16 бит, определяющее метод аутентификации, который используется в этой зоне. Иногда определяют два типа опознавания: 0 для отсутствия и 1 для пароля.

-Аутентификация данных- поле 64 бита для действующего значения данных. В настоящее время, если тип опознавания 0, это поле заполнено нулями. Если тип 1 — поле содержит пароль длиной восемь символов.

4.1.3 Протокол пограничной маршрутизации

Протокол маршрутизации (BGP — Border Gateway Protocol) функционирует между автономными системам, основан на методах маршрутизации, называемых "маршрутизация вектором пути". Вектор пути настраивается системным администратором в соответствии с политикой безопасности. Пакеты инкапсулируются в TCP-сегменты, используется порт 179.

Маршрутизация с помощью вектора пути применяется в случаях когда маршрут, вычисленный с наименьшим числом участков, не является предпочтительным (в случае запрета на передачу через автономную систему, которая не обеспечивает безопасности по наикратчайшему маршруту, перегрузки участков или ведение огромной базы данных состояний в случае использования ее в сети Интернет, что приводит к длительному времени работы каждого маршрутизатора для вычисления его таблицы маршрутов с использованием алгоритма Дейкстры).

Протоколом предусмотрено 3 типа связей:

1. Тупиковые сети.
2. Транзитивные сети (магистральные).
3. Многосвязные сети.

Рассмотрим выбор маршрута в многосвязной сети, представленной на Рис. 4.8.

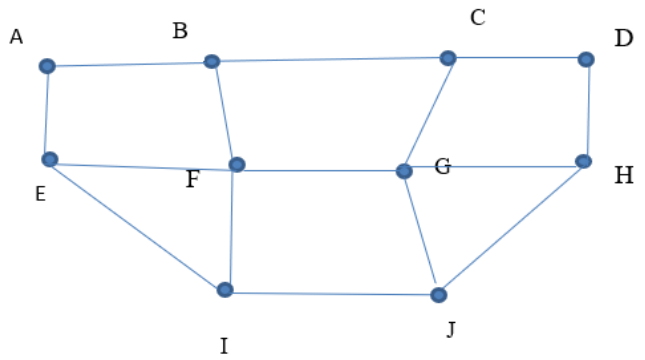


Рис. 4.8

Маршрутизатору F необходимо передать пакет маршрутизатору D. Маршрутизатор F извещает о достижимости сетей в их собственной автономной системе для соседних маршрутизаторов. Для этого он

устанавливает TCP-соединение с соседями и посылает сообщение "открытие". Если политики безопасности соседних маршрутизаторов совпадают, то соседний маршрутизатор отвечает «дежурным сообщением», которое означает, что связь между двумя маршрутизаторами установлена. На указанные сообщение маршрутизатор F получить следующие пути:

От B путь BCD

От G путь GCD

От B путь IFCD

От B путь EFCD

Последние 2 пути отбрасываются, поскольку использую узел F, оптимальным маршрутом будет признан FBCD. При этом политика маршрутизации подразумевает, что, когда маршрутизатор получает сообщение, он проверяет путь. Если одна из автономных систем, указанных в списке, не совпадет с его политикой, он может игнорировать этот путь и этот конечный пункт. Маршрутизатор не обновляет свою таблицу маршрутизации в части этого пути и не посылает сообщения своим соседям, соответственно соседи также игнорирует это путь передачи. Это означает, что таблицы маршрутизации в методе маршрутизации с использованием вектора путей не основываются на политике, навязываемой маршрутизатору администратором.

Виды сообщений BGP:

1. Сообщение "открытие"-формируется для создания информации об окружении и инициализации маршрутизатора.
2. Сообщение "обновление" —используется маршрутизатором для изменения пункта назначения, который был заявлен раньше, объявления маршрута к новому конечному пункту или замены обоих пунктов назначения.
3. Дежурное сообщение -используется для сообщения о том, что маршрутизаторы находятся в сети в работоспособном состоянии.
4. Сообщение уведомления - посылаются маршрутизатором при обнаружении признаки ошибки или завершении соединения.

Безопасность протокола BGP. Протокол маршрутизации и BGP, входя в стек протокола TCP/IP наследует все его уязвимости. Некорректно

настроенные или преднамеренно искаженные источники могут внести существенные искажения в работу маршрутизации путем вставки ложной маршрутной информации (путем изменения, подмены или повторного использования пакетов BGP).

Любой сторонний узел может включить в сообщения BGP обманные маршруты или разорвать соединение между соседними маршрутизаторами. При этом обрыв связи между соседними маршрутизаторами приводит к изменению распространяемой картины маршрутизации. Более того, внешние узлы могут также разрывать соединения между соседними маршрутизаторами, обрывая для них сессии TCP с помощью обманных пакетов.

4.2. Задание

На основании спроектированной в лабораторной работе 1 сетевой инфраструктуре настроить статическую и динамическую маршрутизацию и обеспечить защиту маршрутизаторов с применением механизмов аутентификации.

4.3. Порядок выполнения работы

4.3.1. Настройка протоколов маршрутизации

На основании спроектированной в лабораторной работе 1 сетевой инфраструктуре настроить статическую маршрутизацию на router1, router2 и router 3, для ограничения доступа злоумышленников (Рис. 4.9).

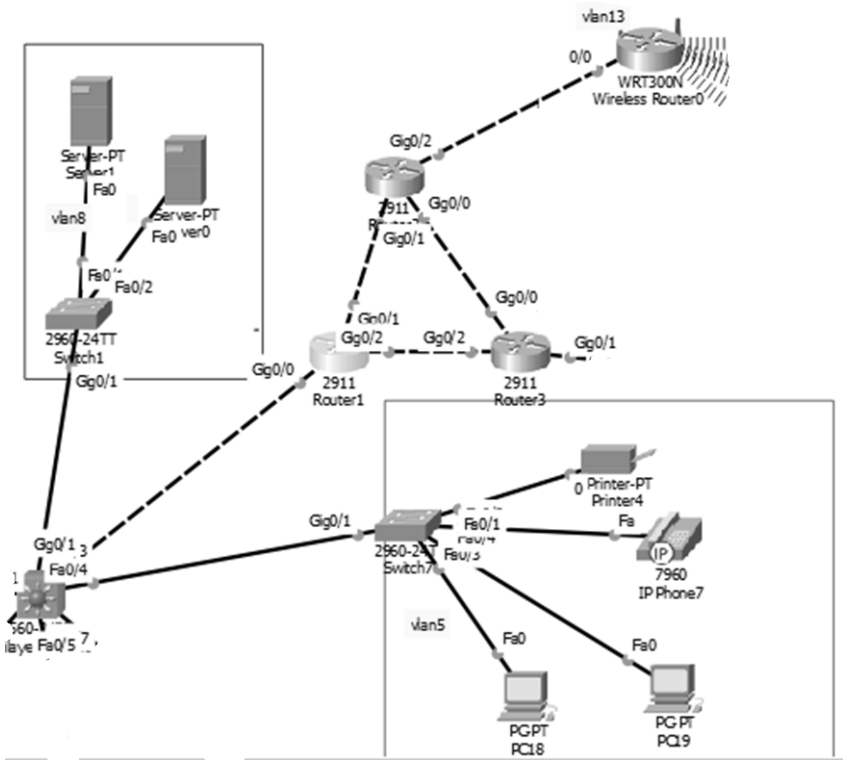


Рис. 4.9

Статическая маршрутизация —- вид маршрутизации, при котором маршруты указываются в явном виде при конфигурации маршрутизатора. Вся маршрутизация при этом происходит без участия каких-либо протоколов маршрутизации [1]. Такой способ требует вмешательства администратора каждый раз, когда происходят изменения в топологии сети. К **достоинствам** статической маршрутизации можно отнести:

- гибкость отладки и конфигурирования в малых сетях;
- увеличение производительности сети за счет отсутствия дополнительных накладных расходов на передачу служебного трафика:
- низкая нагрузка на процессор маршрутизатора;
- предсказуемость маршрутов сетевого трафика.

К недостаткам статической маршрутизации можно отнести:

- плохое масштабирование сети;

- низкая устойчивость в ситуациях, когда обрыв происходит между устройствами;
- отсутствие динамической балансировки нагрузки;
- необходимость в ведении отдельной документации к маршрутам, проблема синхронизации документации и реальных маршрутов.

1. Осуществить настройку интерфейсов для передачи трафика между L3 и router 1, с возможностью передачи трафик из VLAN 9. Для этого настроить работу коммутатора L3 согласно Рис. 4.10. Если соединение с VLAN настроено в предыдущих практических работах, то данный шаг можно пропустить.

```
Switch>
Switch>en
Switch#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#vlan 9
Switch(config-vlan)#name Vlan9
Switch(config-vlan)#int vlan 9
Switch(config-if)#
%LINK-5-CHANGED: Interface Vlan9, changed state to up

Switch(config-if)#ip address 192,168.9.2 255.255.255.0
                             ^
% Invalid input detected at '^' marker.

Switch(config-if)#ip address 192.168.9.2 255.255.255.0
Switch(config-if)#no shu
Switch(config-if)#exit
Switch(config)#int gb0/1
                  ^
% Invalid input detected at '^' marker.

Switch(config)#int g
Switch(config)#int gigabitEthernet 0/1
Switch(config-if)#swi
Switch(config-if)#switchport mode
Switch(config-if)#switchport mode acc
Switch(config-if)#switchport mode access
Switch(config-if)#switchport ac
Switch(config-if)#switchport access vlan 9
Switch(config-if)#exit
Switch(config)#ip route 0.0.0.0 0.0.0.0 192.168.9.1
Switch(config)#
```

Рис. 4.10

2. Настроить интерфейс маршрутизатора Router 1 (Рис. 4.11) и аналогично, согласно IP адресам для остальных маршрутизаторов.

```
Router>en
Router#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#int g
Router(config)#int gigabitEthernet 0/0
Router(config-if)#ip address 192.168.9.1 255.255.255.0
Router(config-if)#no shutdown

Router(config-if)#
%LINK-5-CHANGED: Interface GigabitEthernet0/0, changed state to
up
```

Рис. 4.11

3. Настроить работу Wi-Fi модуля WRT300N Wireless Router 0 согласно характеристикам, представленным на рисунке 4.12.

Рис. 4.12

4. Сформировать маршрутные пути с помощью команды ip route для маршрутизаторов router 0, 1, 3 (Рис. 4.13-4.15).

```
ip classless
ip route 192.168.12.0 255.255.255.0 210.210.0.2
ip route 0.0.0.0 0.0.0.0 192.168.13.1
ip route 0.0.0.0 0.0.0.0 192.168.11.2
!
```

Рис. 4.13

```
ip route 192.168.2.0 255.255.255.0 192.168.9.2
ip route 192.168.3.0 255.255.255.0 192.168.9.2
ip route 192.168.4.0 255.255.255.0 192.168.9.2
ip route 192.168.5.0 255.255.255.0 192.168.9.2
ip route 192.168.6.0 255.255.255.0 192.168.9.2
ip route 192.168.7.0 255.255.255.0 192.168.9.2
ip route 192.168.8.0 255.255.255.0 192.168.9.2
ip route 192.168.12.0 255.255.255.0 192.168.13.2
ip route 0.0.0.0 0.0.0.0 192.168.13.2
ip route 0.0.0.0 0.0.0.0 192.168.10.2
!
```

Рис. 4.14

```
ip route 192.168.2.0 255.255.255.0 192.168.10.1
ip route 192.168.3.0 255.255.255.0 192.168.10.1
ip route 192.168.4.0 255.255.255.0 192.168.10.1
ip route 192.168.5.0 255.255.255.0 192.168.10.1
ip route 192.168.6.0 255.255.255.0 192.168.10.1
ip route 192.168.7.0 255.255.255.0 192.168.10.1
ip route 192.168.8.0 255.255.255.0 192.168.10.1
ip route 192.168.12.0 255.255.255.0 192.168.11.1
ip route 210.210.0.0 255.255.255.0 192.168.11.1
!
```

Рис. 4.15

5. Осуществить проверку работоспособности статической маршрутизации отправкой эхо-пакетов с ip адреса 192.168.12.3 (Рис. 4.16).

Рис. 4.15

В случае, если проверка отправки эхо-пакетов завершилась успехом, то можно сделать вывод, что статическая маршрутизация работает правильно.

6. На маршрутизаторе Router1 выполнить настройку протокола маршрутизации OSPF, обеспечивающего регистрацию событий маршрутизации, аутентификацию соседей и активацию пассивных интерфейсов. Для этого формируем команды:

Conf t

Int looback 0

Ip address 192.168.100.1 255.255.255.255 выбор определенной сети, для всех looback-интерфейсов маршрутизаторов, и присваиванием значение 100.2, 100.3 и т.д последующим маршрутизаторам)

No shutdown

Exit

Rouster ospf 1

Network 192.168.2.0 0.0.0.255 area 0 (перечисляются все VLAN сети, что подключены к настраиваемому маршрутизатору, и записывается обратная маска)

Network 192.168.3.0 0.0.0.255 area 0

Network 192.168.4.0 0.0.0.255 area 0

Network 192.168.5.0 0.0.0.255 area 0

Network 192.168.6.0 0.0.0.255 area 0

Network 192.168.7.0 0.0.0.255 area 0

Network 192.168.8.0 0.0.0.255 area 0

Network 192.168.10.0 0.0.0.3 area 0 (перечисляются все маршрутизаторы, которые подключены к настраиваемому роутеру, в нашем случае это Router 2, Router 3)

Network 192.168.11.0 0.0.0.3 area 0

End

Wr mem

Результат настройки протокола маршрутизации OSPF на маршрутизаторе router1 представлен на Рис. 4.16.

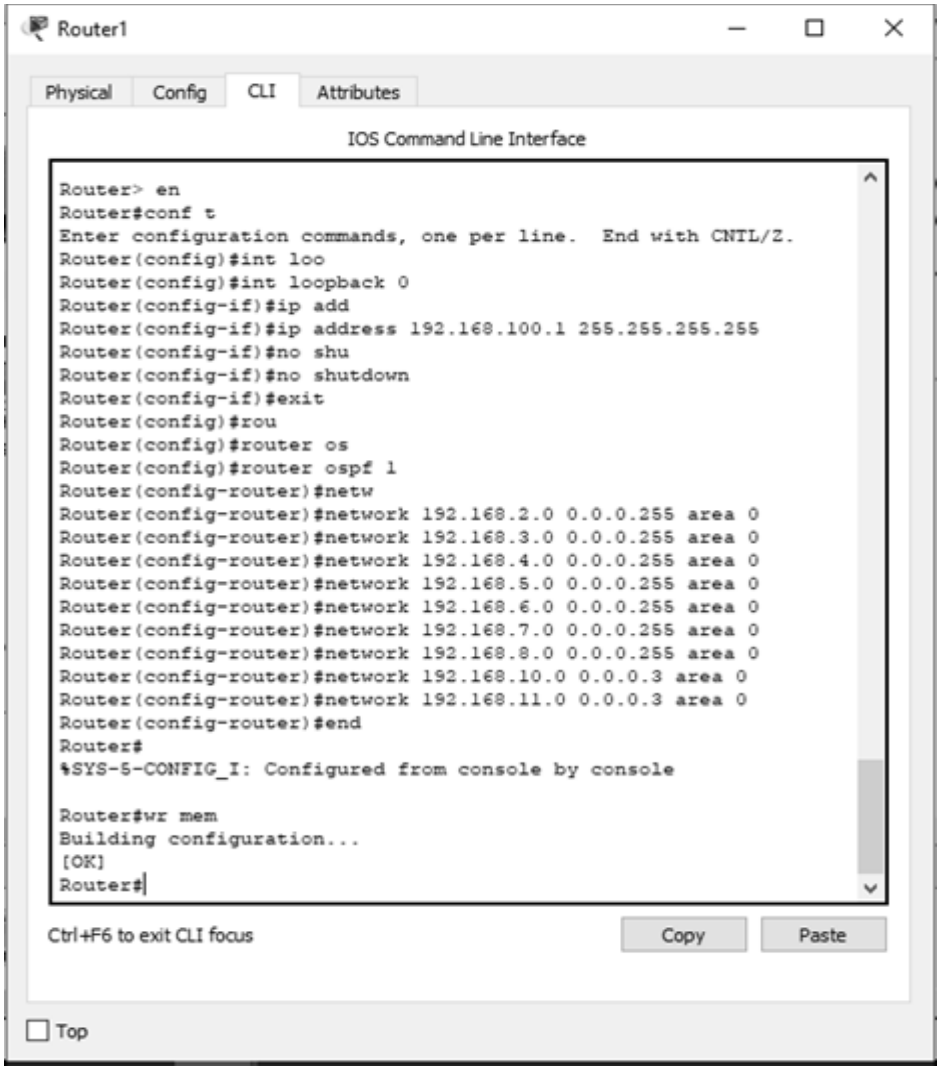


Рис. 4.16

7. Выполнить аналогичные настройки на двух других маршрутизаторах.

8. Проверить, что интерфейс, настроенный на протокол маршрутизации OSPF поднялся, для этого прописать команду:

show ip ospf neighbor

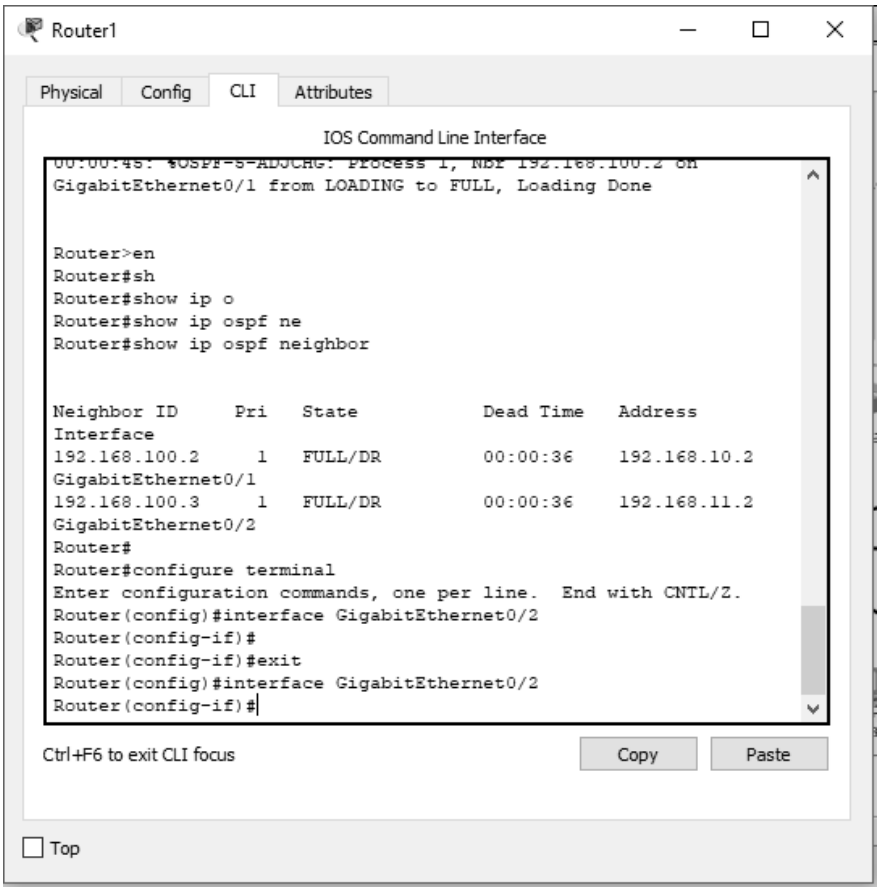


Рис. 4.17

На Рис. 4.17 показано, что на Router 1 отображаются соединения OSPF с Router 2(100.2) и Router 3(100.3).

9. Проверить, что OSPF сети поднялись на маршрутизаторах, для этого выполнить в консоли команду:

show ip route

и проверить IP адресацию сетей, обозначенных O.

Рис. 4.18

10. Убедиться в корректности настроек маршрутизаторов, проверить возможность использования резервных маршрутов при разрыве основных каналов связи.
11. Применить механизмы идентификации и аутентификации протокола OSPF, который поддерживает 2 типа аутентификации: открытым текстом и MD5. Механизм аутентификации с использованием MD5 добавляет в каждый пакет увеличивающийся номер последовательности, защищая тем самым участников обмена от атак, использующих повторную пересылку захваченных ранее

пакетов. Для включения механизмов аутентификации применить команды

router(config-if)#ip ospf authentication-key пароль
router(config-if)# ip ospf authentication [message-digest | null]

12. Осуществить н**астройку DHCP,** который сервер располагается на Server0 (Рис. 4.9 и Рис.4.19).

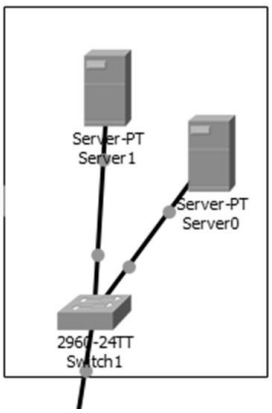


Рис. 4.19

Открыть интерфейс настройки сервера и выбрать вкладку Services->DHCP (Рис 4.20).Задать имя, шлюз, которым является порт на свитче 3560, DNS сервер 1.1.1.1 (или 8.8.8.8), стартовый адрес и маску (Рис. 4.20). Сделать это для всех VLAN в контролируемых сетях.

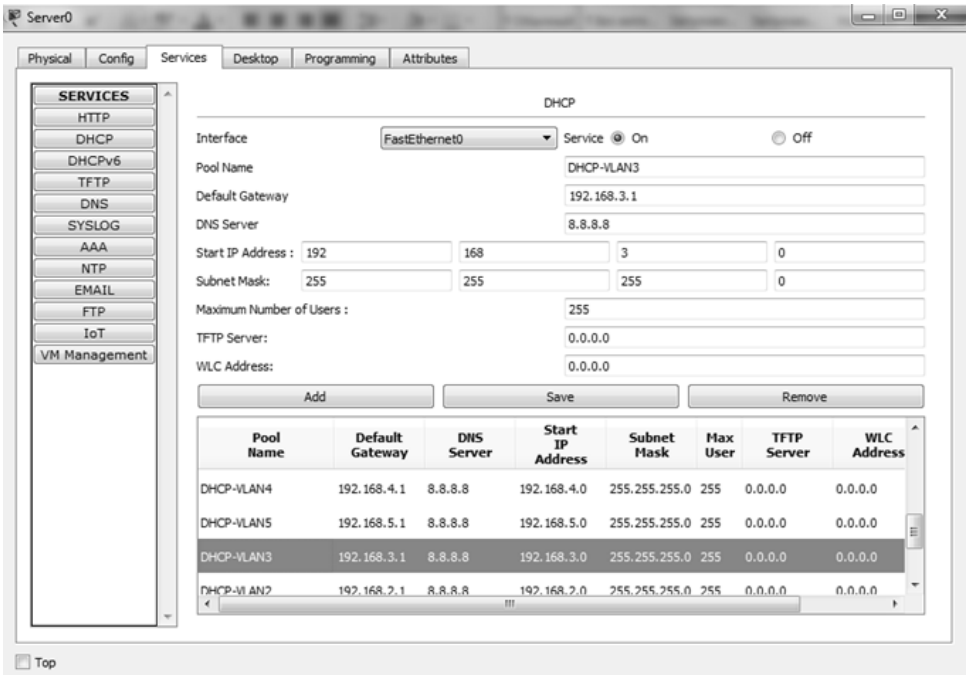


Рис. 4.20

Перенаправить DHCP запросы к серверу. Для этого на свитче 3560 открыть консоль и ввести команды:

en

conf t

int vlan (номер VLANa.) .

ip helper-address 192.168.8.2 (адрес сервера)

do wr mem

Проверить работу сервера с хоста открыв в настройках хоста Desktop-> ip Configuration (Рис. 4.21) и включить службу DHCP и проверить работоспособность сети.

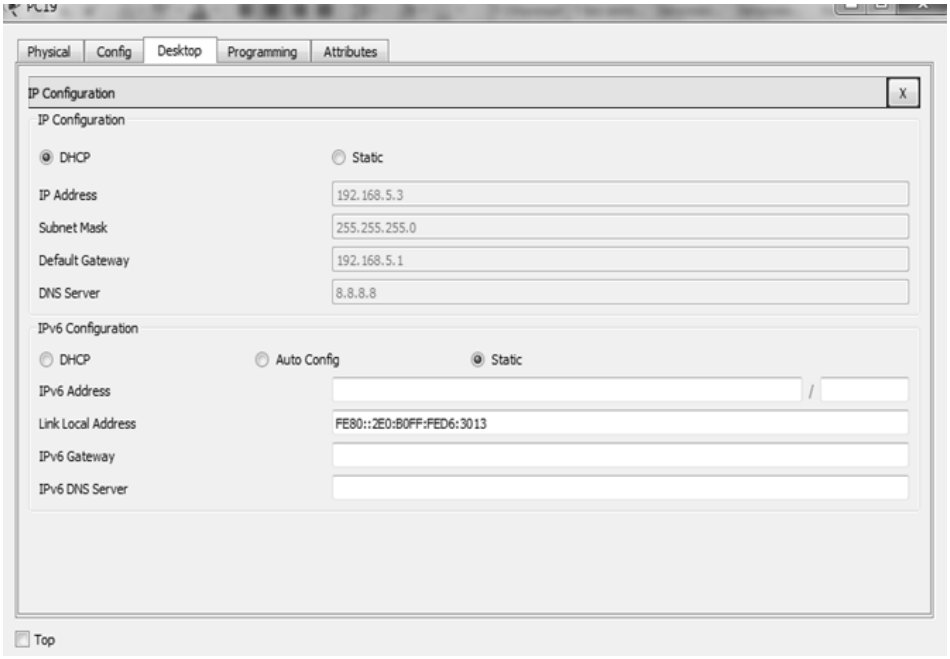


Рисунок 38 Узел получил IP адрес по DHCP

4.3.2 Механизмы идентификации, аутентификации и авторизации

Администрирование сетевых устройств осуществляется с использованием Telnet-сессии, SSH-сессии или другим способом. Однако для управления устройством необходимо осуществить аутентификацию, для которой используют три основных протокола AAA: RADIUS; TACACS; DIAMETER. При использовании протокола RADIUS пользователь не может определять команды, разрешенные или запрещенные для выполнения на коммутаторе. Поэтому протокол RADIUS не так полезен для управления маршрутизатором или не настолько приспосабливаемый для служб терминалов [2].

TACACS+ предоставляет два способа управления авторизацией команд маршрутизатора по каждому пользователю или по группам. Первый способ состоит в назначении уровней привилегий командам и проверке маршрутизатором с помощью сервера TACACS+ факта авторизации пользователя на указанном уровне привилегий. Для применения второго способа следует явно указать разрешенные команды на сервере TACACS+ для каждого пользователя или для каждой группы.

Выполнить настройки доступа к маршрутизатору по технологии AAA на основе протокола TACACS+ [3]

1. Подключиться к маршрутизатору router 2 через консольный порт с рабочей станции администратора сети, проверить имя маршрутизатора и домен (или задать их) и сгенерировать криптографические ключи, используемые в криптографическом протоколе SSH:

hostname router2
ip domain-name net.security2
crypto key generate rsa

2. Включить доступ к маршрутизатору по протоколу SSHv2, задать количество попыток аутентификации:

ip ssh version 2 ip ssh
time-out 60
ip ssh authentication-retries 3

3. Установить пароль на доступ пользователя к конфигурационному режиму:

*username noc secret 5 впарп№в**
enable secret LITI2022

4. Отключить службы DNS и CDP

no ip domain-lookup
no cdp run

5. Включить шифрование паролей в конфигурационном файле:

service password-encryption

6. Выполнить настройки доступа к маршрутизатору по технологии AAA на основе протокола TACACS+:

tacacs-server host 192.168.6.2 key dtryuyun56
tacacs-server host 192.168.6.3 key 67yjjukjuk
aaa new-model aaa authentication login default group tacacs+
local
aaa authentication enable default group tacacs+
enable
aaa authorization exec default group tacacs+

local

7. Настроить удаленный доступ к маршрутизатору с разрешенных IP-адресов рабочих станций отдела безопасности:

```
ip access-list extended sec-vty
permit tcp 192.168.6.0 0.0.0.8  any eq 22
deny ip any any
line con 0
exec-timeout 5 0
login authentication default
line vty 0 15
exec-timeout 10 0
transport input ssh
access-class sec-vty in
```

8. Выполнить настройку службы регистрации событий с отправкой их на сервер регистрации событий (IP-адрес 192.168.7.2) по протоколу SYSLOG:

```
service timestamps log datetime msec
service timestamps debug datetime msec
logging 192.168.7.2
logging trap debugging logging buffered 512000
```

9. Выполнить настройки протокола SNMP для доступа к маршрутизатору с сервера мониторинга:

```
snmp-server community Hn4bUn3ba ro
snmp-server community mf5FNOd2d rw
```

10. Проверить корректность функционирования сети управления, а также регистрацию событий на сервере SYSLOG.

11. Разработать политику безопасности при маршрутизации сетевого трафика, в соответствии со схемой, представленной в практической работе 1. Настроить правила маршрутизации сетевого трафика, а также доступом к серверам, расположенным в ЛВС.

3.4. Контрольные вопросы

1. Какое утверждение описывает результат ввода команды iproute 0.0.0.0 0.0.0.0 192.168.1.1 в маршрутизаторе?
2. Почему маршрутизаторы могут передавать данные только на сетевом уровне модели OSI?
3. Какой информацией должны обмениваться маршрутизаторы, чтобы достичь горизонта сходимости?
4. В чем отличие статической маршрутизации от динамической? Когда и в каких условиях ее целесообразно применять?
5. Каким образом маршрутизатор «узнает» о недоступности маршрута?
6. В каких случаях достаточно использовать аутентификацию маршрутизатора на самом устройстве, а в каких с использованием протоколов AAA?

СПИСОК ЛИТЕРАТУРЫ

1. Интуит. Лекция 8: Протоколы маршрутизации (RIP, OSPF и BGP). https://intuit.ru/studies/professional_retraining/943/courses/2/lecture/42?page=2.
2. Сравнение TACACS+ и RADIUS. Электронный ресурс https://www.cisco.com/c/ru_ru/support/docs/security-vpn/remote-authentication-dial-user-service-radius/13838-10.html#comp_auth.
3. Д.Н. Колегов. Лабораторный практикум по построению компьютерных сетей. Лабораторный практикум по основам построения защищенных компьютерных сетей. Томск: Томский государственный университет, 2013. – 140 с
4. Димарцио Д. Ф. Маршрутизаторы Cisco. Пособие для самостоятельного изучения. – Пер. с англ. – СПб: СимволПлюс, 2003. – 512 с., ил