Тема 1 Организация защиты удаленного доступа

Лекция 5. Аутентификация, авторизация и аудит

Дисциплина: Анализ информационных потребностей подразделений информационно-аналитического мониторинга

Доцент: Кирьянов Александр Владимирович
email:kiryanov_a@mirea.ru

Учебные вопросы и цели занятия:

1. Назначение аутентификации.
2. Локальная аутентификация.
3. Серверное решение AAA.
4. Серверная авторизация и аудит AAA.

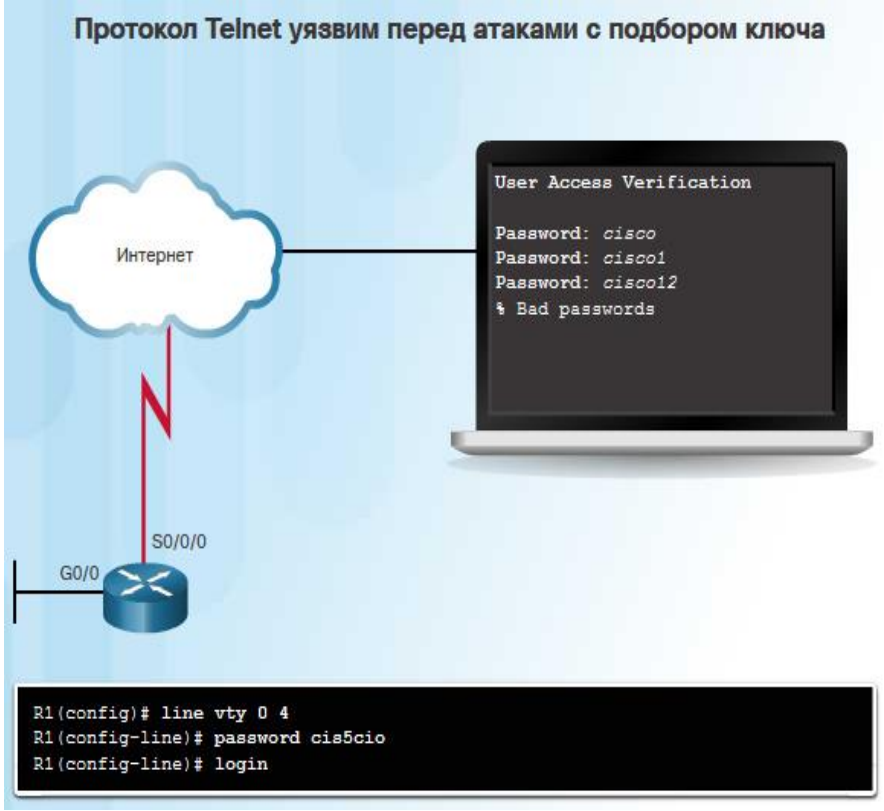
Сеть должна быть спроектирована так, чтобы была возможность контролировать, кому и когда разрешено к ней подключаться и что им разрешено в ней делать. Эти спецификации дизайна сети определены в политике сетевой безопасности. Политика определяет доступ к сетевым ресурсам сетевых администраторов, корпоративных пользователей, удаленных пользователей, деловых партнеров и клиентов. Политика сетевой безопасности также может определять систему отчетности, где регистрируется, кто и когда входил в сеть и что они в ней делали.

Система управления доступом к сети с использованием только пользовательского режима или только команд паролей привилегированного режима ограничена и не очень хорошо масштабируется. Использование протокола аутентификации, авторизации и учета (AAA) создает необходимую структуру для масштабируемой защиты доступа.

Маршрутизаторы и коммутаторы Cisco IOS можно настроить так, чтобы они использовали AAA для доступа к локальной базе данных имен пользователей и паролей. Использование локальной базы данных имен пользователей и паролей обеспечивает более высокий уровень защиты, чем простой пароль. Это экономичное и легко реализуемое решение безопасности для небольших организаций.

Доступ к LAN может быть защищен с использованием протокола IEEE 802.1X. Протокол 802.1X – это протокол аутентификации и контроля доступа на основе портов, который ограничивает для неавторизованных рабочих станций возможность подключаться к локальной сети через общедоступные порты коммутатора.

Первый учебный вопрос.
Назначение аутентификации

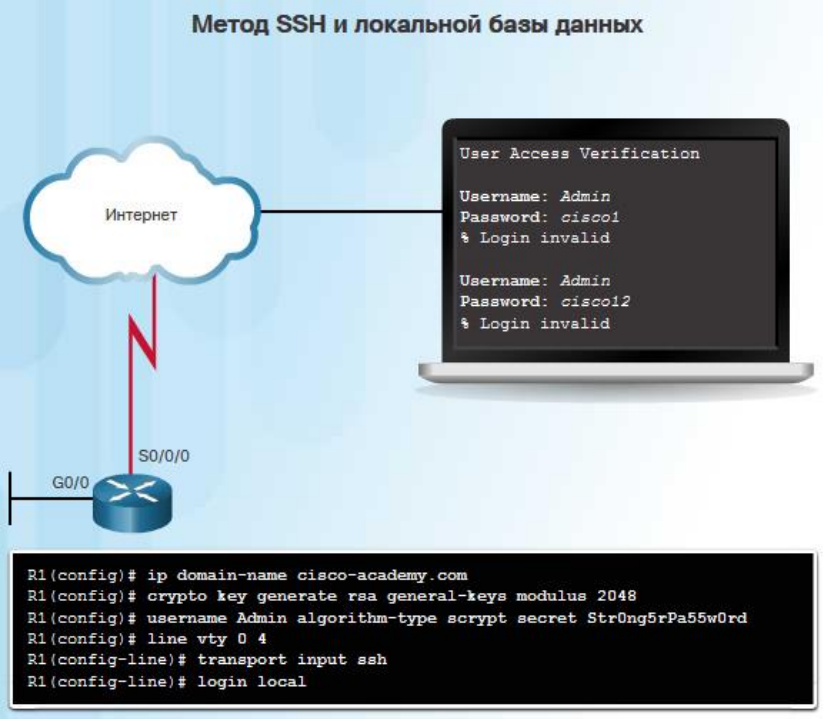


Аутентификация без AAA

Хакеры могут получить доступ к важному сетевому оборудованию и сетевым сервисам. Система контроля доступа ограничивает, кто или как может использовать определенные ресурсы. Она также ограничивает сервисы и опции, которые доступны после предоставления доступа. На устройствах Cisco может выполняться много видов аутентификации, и каждый такой метод дает свой уровень безопасности.

Самый простой метод аутентификации для удаленного доступа – настроить имя пользователя и пароль на консоли, линиях vty и вспомогательных портах, как показано на рисунке. Этот метод самый простой в реализации, но при этом также самый слабый и наименее безопасный. Этот метод не дает возможности учета. Любой пользователь с паролем может получить доступ к устройству и изменить конфигурацию.

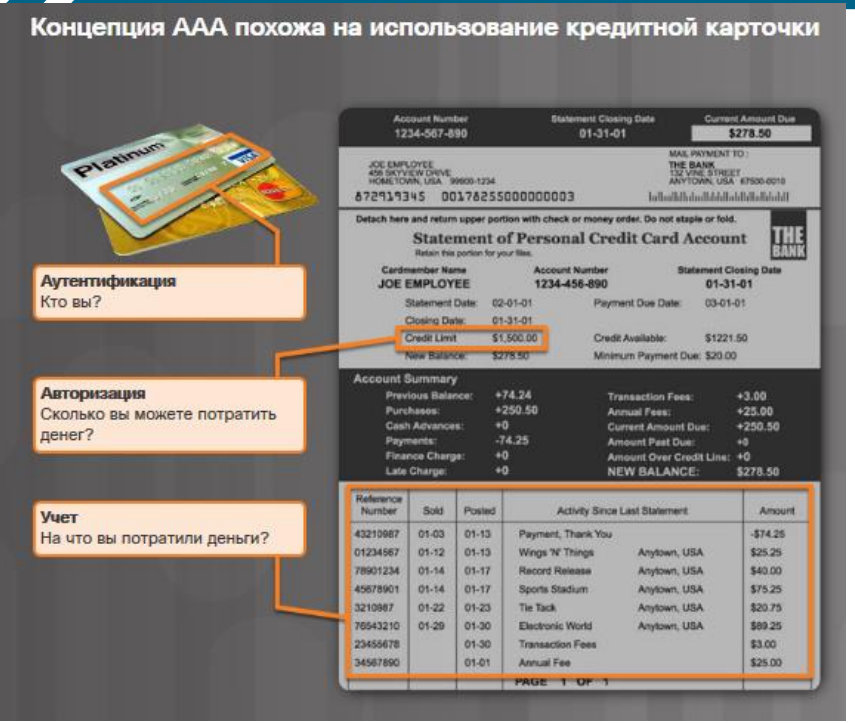
Первый учебный вопрос.
Назначение аутентификации



SSH – более безопасная форма удаленного доступа. Она требует ввода имени пользователя и пароля, которые передаются в зашифрованном виде. Метод локальной базы данных обеспечивает дополнительную безопасность, потому что атакующий должен знать имя пользователя и пароль. Также он обеспечивает дополнительные возможности учета, потому что имя пользователя регистрируется при входе пользователя в систему. Хотя Telnet можно настроить с использованием имени пользователя и пароля, они отправляются в формате обычного текста, т. е. могут быть перехвачены и использованы.

Метод локальной базы данных имеет определенные ограничения. Учетные записи пользователей необходимо локально настраивать на каждом устройстве, как показано в конфигурации SSH на рисунке. В крупной корпоративной инфраструктуре с большим числом маршрутизаторов и коммутаторов развертывание и изменение локальных баз данных на каждом устройстве может отнимать много времени. Кроме того, локальная конфигурация базы данных не поддерживает откат аутентификации. Что делать, если администратор забудет имя пользователя и пароль для устройства? Без резервного копирования данных аутентификации единственным вариантом становится восстановление пароля.

Первый учебный вопрос.
Назначение аутентификации



Компоненты AAA

Службы безопасности сети AAA обеспечивают базовую инфраструктуру настройки контроля доступа на сетевом устройстве. AAA позволяет контролировать, кому разрешен доступ к сети (аутентификация) и что им разрешено делать (авторизация), а также проверять выполненные действия при доступе к сети (учет).

Система сетевой и административной безопасности AAA в среде Cisco имеет три функциональных компонента:

Аутентификация – Пользователи и администраторы должны доказать, что они – именно те, за кого сами себя выдают. Аутентификация производится посредством проверки комбинаций имени пользователя и пароля, контрольных вопросов и ответов, токен-карт и других методов. Например: «Я пользователь student и я знаю пароль, который доказывает это».

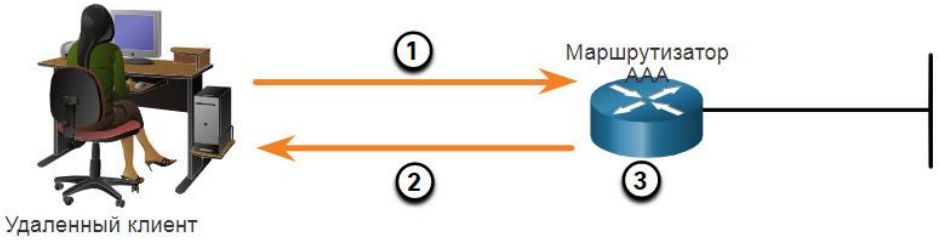
Авторизация – После аутентификации пользователя службы авторизации определяют, к каким ресурсам пользователь может получать доступ и какие операции он имеет право выполнять.

Пример: «Пользователь student может получать доступ к хост-серверу XYZ только с помощью SSH».

Учет и аудит – Система учета записывает действия пользователя, включая ресурсы, к которым он получил доступ, длительность доступа к конкретному ресурсу и любые внесенные им изменения. Система учета отслеживает способ использования сетевых ресурсов. Пример: «Пользователь student имел доступ к хост-серверу XYZ с помощью SSH в течение 15 минут».

Данная концепция аналогична использованию кредитной карты, как показано на рисунке. Кредитная карта определяет, кто может ее использовать, сколько этот пользователь может потратить, а также учитывает покупки товаров и услуг пользователем.

Первый учебный вопрос.
Назначение аутентификации



1. Клиент устанавливает соединение с маршрутизатором.
2. Маршрутизатор AAA запрашивает у пользователя имя пользователя и пароль.
3. Маршрутизатор аутентифицирует имя пользователя и пароль, используя локальную базу данных, и пользователю предоставляется доступ к сети на основе информации в локальной базе данных.

Локальная аутентификация AAA – Локальная система аутентификации AAA использует для аутентификации локальную базу данных. Этот метод иногда называется самодостаточной аутентификацией. В данном курсе он будет называться локальной аутентификацией AAA. Этот метод выполняет локальное сохранение имен пользователей и паролей маршрутизатора Cisco, а аутентификация пользователей производится по локальной базе данных в соответствии с рисунком. для небольших сетей.

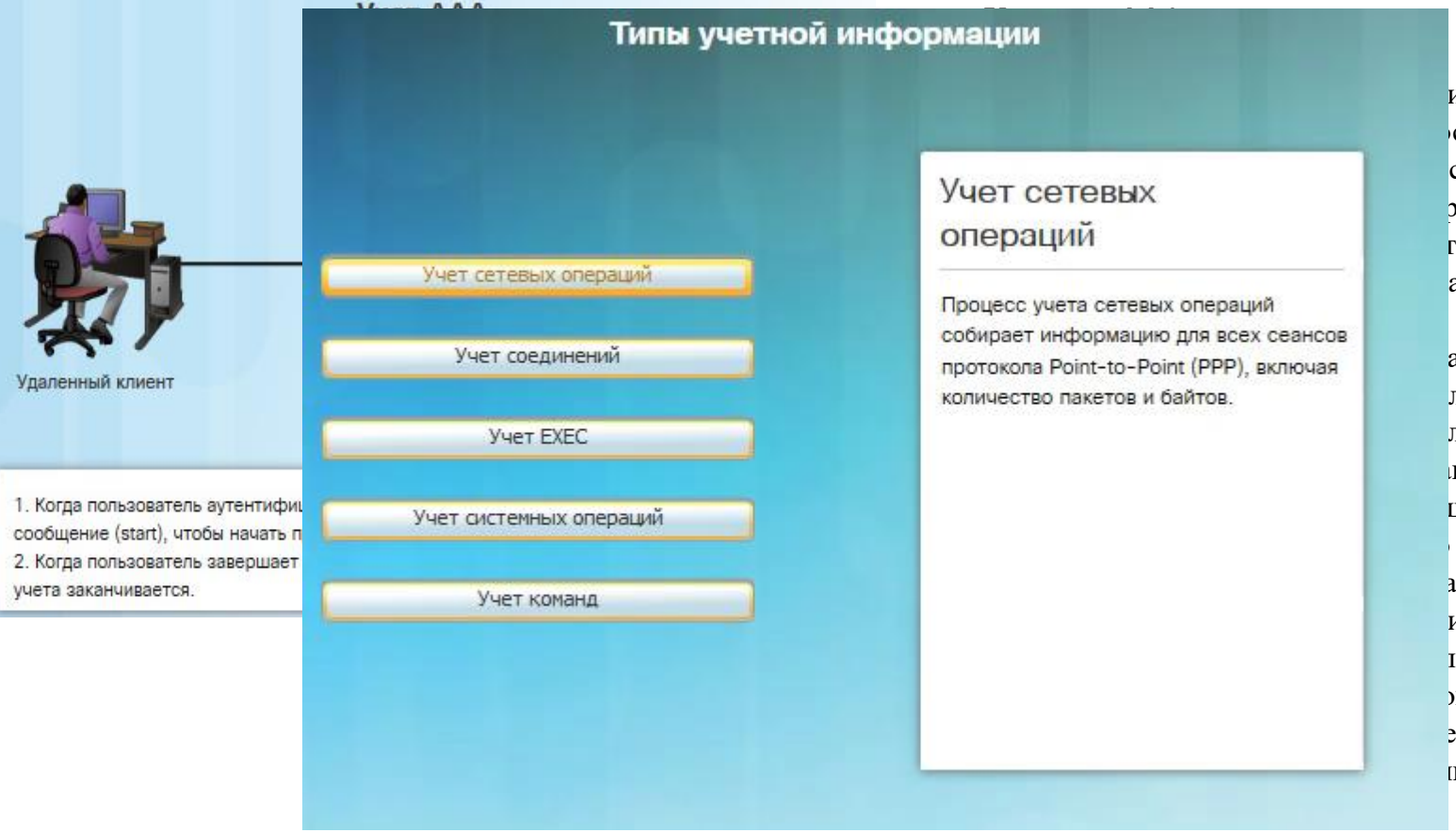
Серверная аутентификация AAA – В случае реализации на базе сервера маршрутизатор взаимодействует с сервером AAA, например Cisco Secure Access Control System (ACS) для Windows, как показано на рис. 2. Центральный сервер AAA содержит имена пользователя и пароли для всех пользователей. Маршрутизатор использует для связи с сервером AAA службу удаленной аутентификации пользователей с коммутируемым доступом (RADIUS, Remote Authentication Dial-In User) либо протокол управления доступом к контроллеру терминального доступа (TACACS+, Terminal Access Controller Access Control System). Серверный вариант AAA более подходит при наличии нескольких маршрутизаторов и коммутаторов.

1. Клиент устанавливает соединение с маршрутизатором.
2. Маршрутизатор AAA запрашивает у пользователя его имя и пароль.
3. Маршрутизатор аутентифицирует имя пользователя и пароль с помощью удаленного сервера AAA.
4. Пользователю предоставляется доступ к сети на основе информации на удаленном сервере AAA.

Авторизация

После успешной аутентификации пользователей с выбранным локальным или серверным источником данных AAA они авторизуются для доступа к определенным сетевым ресурсам, как показано на рисунке. Авторизация определяет, что пользователи могут и не могут делать в сети после аутентификации. Примерно так же уровни привилегий и CLI на основе ролей дают пользователям определенные права и привилегии при выполнении определенных команд на маршрутизаторе.

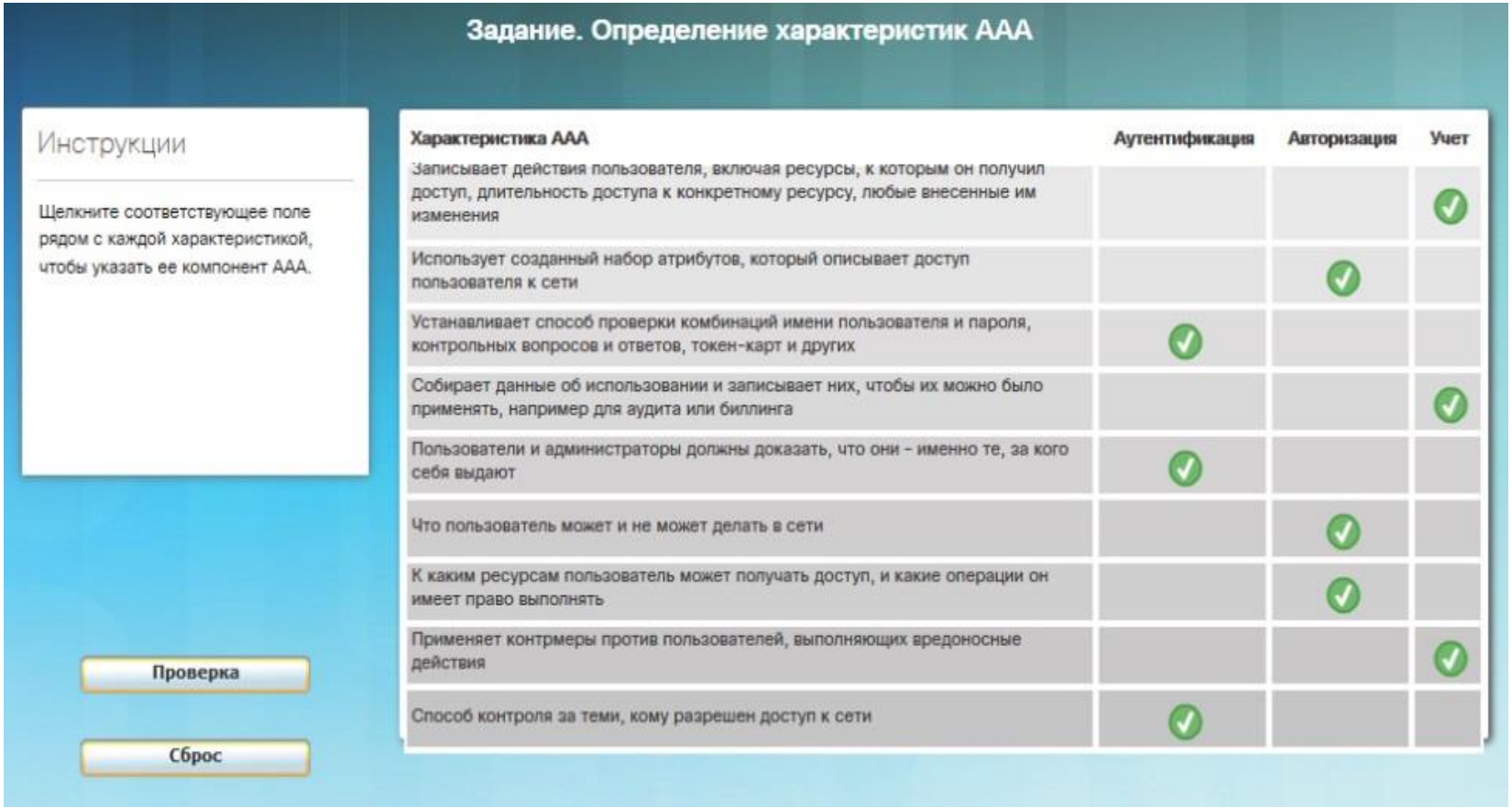
Первый учебный вопрос.
Назначение аутентификации



сбор информации
отчеты. Данные могут
инга. Собранные данные
становки подключения,
сло байт.
рверного решения AAA.
атистику использования.
ания подробных отчетов

ацией AAA. Это помогает
лять доступом к сетевым
лее высокий уровень
ция. На серверах AAA
шедших аутентификацию
на рисунке. В частности,
авленные пользователем
и. В журнале содержится
льзователя, дату и время и
манду. Эта информация
еисправностей устройств.
полняющих вредоносные

Выводы по первому вопросу. Назначение аутентификации



Характеристика AAA	Аутентификация	Авторизация	Учет
Записывает действия пользователя, включая ресурсы, к которым он получил доступ, длительность доступа к конкретному ресурсу, любые внесенные им изменения			✓
Использует созданный набор атрибутов, который описывает доступ пользователя к сети		✓	
Устанавливает способ проверки комбинаций имени пользователя и пароля, контрольных вопросов и ответов, токен-карт и других	✓		
Собирает данные об использовании и записывает них, чтобы их можно было применять, например для аудита или биллинга			✓
Пользователи и администраторы должны доказать, что они – именно те, за кого себя выдают	✓		
Что пользователь может и не может делать в сети		✓	
К каким ресурсам пользователь может получать доступ, и какие операции он имеет право выполнять		✓	
Применяет контрмеры против пользователей, выполняющих вредоносные действия			✓
Способ контроля за теми, кому разрешен доступ к сети	✓		

Второй учебный вопрос.
Локальная аутентификация

Аутентификация административного доступа

Локальную аутентификацию AAA следует настраивать для небольших сетей. Этот метод использует локальные имена пользователей и пароли, сохраненные на маршрутизаторе. Системный администратор должен заполнить локальную базу данных безопасности, введя профили с именами пользователей и паролями для каждого пользователя, который может войти в систему.

Метод локальной аутентификации AAA сходен с использованием команды **login local** , за одним исключением. AAA также дает возможность настроить резервные методы аутентификации.

Чтобы настроить локальные сервисы AAA для аутентификации доступа администратора, требуется ряд простых шагов:

Шаг 1. Добавьте имена пользователей и пароли в локальную базу данных маршрутизатора для пользователей, которым необходим административный доступ к этому маршрутизатору.

Шаг 2. Включите AAA в глобальном режиме на маршрутизаторе.

Шаг 3. Сконфигурируйте параметры AAA на маршрутизаторе.

Шаг 4. Подтвердите конфигурацию AAA и устраните неисправности.

Команда **aaa authentication login** на рисунке позволяет пользователям **ADMIN** и **JR-ADMIN** войти в маршрутизатор через консоль или линии терминала vty. Ключевое слово **default** означает, что метод аутентификации относится ко всем линиям, кроме тех, для которых задана отдельная конфигурация. Аутентификация производится с учетом регистра, что указывает ключевое слово **local-ca**se . Это означает, что имя пользователя и пароль проверяются с учетом регистра.

Второй учебный вопрос.
Локальная аутентификация

Синтаксис команды aaa authentication login

```
router(config-line)#
aaa authentication login {default | list-name} method1…[method4]
```

Команда	Описание
default	Использует перечисленные методы аутентификации, после ввода этого ключевого слова, в качестве заданного по умолчанию списка методов, когда пользователь выполняет вход в систему.
list-name	Строка символов, используемая для именования списка методов аутентификации, активируемых при входе пользователя в систему.
method1...[method4]	Определяет список методов, которые будет запрашивать процесс аутентификации AAA в заданной последовательности. Необходимо указать по крайней мере один метод. Можно указать максимум четыре метода.

Методы аутентификации

Чтобы включить AAA, нужно предварительно настроить команду глобальной конфигурации **aaa new-model**. Чтобы отключить AAA, нужно использовать форму **no** этой же команды.

Когда команда **aaa new-model** вводится в первый раз, «невидимая» аутентификация по умолчанию автоматически производится для всех линий, кроме консоли, с использованием локальной базы данных. По этой причине перед активацией AAA всегда необходимо настраивать запись в локальной базе данных.

Используйте команду **aaa authentication login** на рисунке, чтобы активировать аутентификацию консоли и линий aux и vty. Ключевое слово **default** позволяет выполнять аутентификацию на всех линиях. Также можно настроить пользовательский метод аутентификации с помощью команды ***list-name***.

Второй учебный вопрос.
Локальная аутентификация

Типы методов входа в систему

Ключевые слова для типа метода	Описание
`enable`	Использует enable password для аутентификации.
`local`	Использует локальную базу данных имен пользователей для аутентификации.
`local-case`	Использует чувствительную к регистру локальную аутентификацию по имени пользователя.
`none`	Не использует аутентификацию.
`group radius`	Использует список всех серверов RADIUS для аутентификации.
`group tacacs+`	Использует список всех серверов TACACS+ для аутентификации.
`group group-name`	Использует подмножество серверов RADIUS или TACACS+ для аутентификации, как определено командой `aaa group server radius` или `aaa group server tacacs+`.

В заключительной части команды определяется тип методов, которые будут запрашиваться для аутентификации пользователей. Можно определить до четырех методов, в том числе резервные методы на случай недоступности одного из методов.

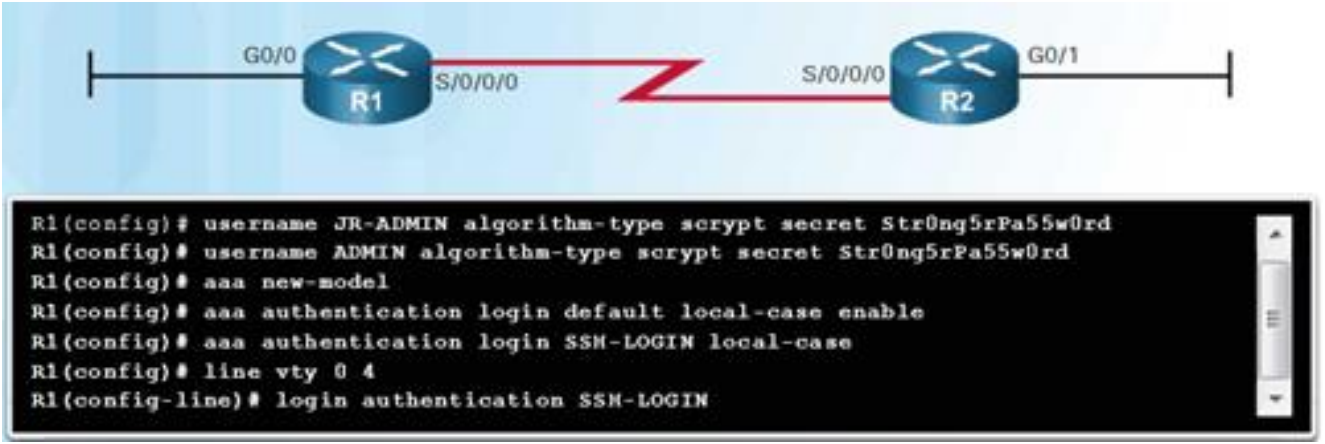
На рисунке показаны распространенные методы, которые можно указать. При попытке входа пользователя в систему используется первый метод из списка. Программное обеспечение Cisco IOS пытается использовать для аутентификации следующий метод из списка только при отсутствии ответа или ошибке предыдущего метода. Если выбранный метод аутентификации запрещает пользователю доступ, процедура аутентификации останавливается, и никакие другие методы аутентификации использовать нельзя.

Чтобы активировать локальную аутентификацию с использованием заранее сконфигурированной локальной базы данных, необходимо использовать ключевое слово **local** или **local-case**. Разница между этими двумя вариантами заключается в том, что local принимает имя пользователя без учета регистра, а local-case учитывает регистр. Например, если в локальной базе данных настроено имя пользователя ADMIN, метод **local** принимает варианты ADMIN, Admin и даже admin. Если же настроен метод **local-case**, допускается только вариант ADMIN.

Чтобы указать, что пользователь может пройти аутентификацию с паролем привилегированного доступа, нужно использовать ключевое слово **enable**. Чтобы обеспечить успешную аутентификацию даже в случае, когда все методы возвращают ошибку, нужно задать окончательный метод **none**.

В целях безопасности ключевое слово **none** следует использовать только при тестировании конфигурации AAA.

Второй учебный вопрос.
Локальная аутентификация



Стандартный и именованный методы

Для дополнительной гибкости с помощью команды **aaa authentication login *list-name*** можно применять разные списки методов к разным интерфейсам.

Например, администратор может использовать специальный вход для SSH и метод входа по умолчанию для консоли линии, как показано на рисунке. В этом примере линия **vty** будет использовать для аутентификации только локальную базу данных. Все другие линии (т. е. линия консоли и вспомогательные линии) будут использовать локальную базу данных и пароль привилегированного доступа в качестве резервного метода, если для устройства нет записей в базе данных.

Обратите внимание, что именованный список должен быть явно активирован на линии с использованием команды **login authentication** для конфигурации линии. Если для линии применяется пользовательский список методов аутентификации, он заменяет список методов по умолчанию для этого интерфейса.

Если для интерфейса применяется пользовательский метод аутентификации, можно вернуться к списку методов по умолчанию с помощью команды **no authentication login**.

Второй учебный вопрос.
Локальная аутентификация

```
Router(config)#
aaa local authentication attempts max-fail [number-of-unsuccessful-attempts]
```

Команда	Описание
number-of-unsuccessful-attempts	Количество неудачных попыток аутентификации, при достижении которого соединение сбрасывается, а учетная запись пользователя блокируется.

Точная настройка конфигурации аутентификации

Дополнительную безопасность линии можно обеспечить с помощью команды **aaa local authentication attempts max-fail** в режиме глобальной конфигурации, как показано на рисунке. Эта команда защищает учетную запись пользователя AAA, блокируя ее при чрезмерном количестве неудачных попыток входа.

В отличие от команды **login delay**, которая вводит задержку между неудачными попытками входа без блокировки учетной записи, команда **aaa local authentication attempts max-fail** блокирует учетную запись пользователя при неудачной аутентификации. Заблокированная учетная запись пользователя остается заблокированной, пока администратор не очистит ее вручную с помощью команды **clear aaa local user lockout** привилегированного режима EXEC.

Второй учебный вопрос.
Локальная аутентификация


```
R1# show aaa local user lockout
              Local-user          Lock time
              JR-ADMIN            04:28:49 UTC Sat Dec 27 2015
```

Чтобы отобразить список всех заблокированных пользователей, используйте команду **show aaa local user lockout** в привилегированном режиме EXEC, как показано на рисунке.

Когда пользователь входит на маршрутизатор Cisco, где используется AAA, сеансу этого пользователя присваивается уникальный идентификатор. В течение времени сеанса связанные с ним атрибуты собираются и сохраняются в базе данных AAA. В число этих атрибутов может входить IP-адрес пользователя, использованный для доступа к маршрутизатору протокол (например, PPP), данные по скорости соединения и данные по числу передаваемых или принимаемых пакетов или байтов.

Для отображения атрибутов, собранных для одного сеанса AAA, нужно использовать команду **show aaa user** в привилегированном режиме EXEC. Эта команда дает информацию не о всех пользователях, вошедших на устройство, а только о пользователях, которые прошли аутентификацию или авторизацию AAA, и о пользователях, сеансы которых учитываются модулем AAA.

Команда **show aaa sessions** может использоваться для отображения уникального идентификатора сеанса, как показано на рисунке.

```
R1# show aaa sessions
Total sessions since last reload: 4
Session Id: 1
    Unique Id: 175
    User Name: ADMIN
    IP Address: 192.168.1.10
    Idle Time: 0
    CT Call Handle: 0
```

Второй учебный вопрос.
Локальная аутентификация

Отладка локальной аутентификации AAA

```
R1# debug aaa ?
  accounting          Accounting
  administrative      Administrative
  api                 AAA api events
  attr                AAA Attr Manager
  authentication      Authentication
  authorization       Authorization
  cache               Cache activities
  coa                 AAA CoA processing
  db                  AAA DB Manager
  dead-criteria       AAA Dead-Criteria Info
  id                  AAA Unique Id
  ipc                 AAA IPC
  mlist-ref-count     Method list reference counts
  mlist-state         Information about AAA method
                      list state change and notification
  per-user            Per-user attributes
  pod                 AAA POD processing
  protocol            AAA protocol processing
  server-ref-count    Server handle reference counts
  sg-ref-count        Server group handle reference counts
  sg-server-selection Server Group Server Selection
  subsys              AAA Subsystem
  testing             Info. about AAA generated test packets
```

Варианты отладки

На маршрутизаторе Cisco имеются команды **debug**, полезные для диагностики и устранения проблем с аутентификацией. Как показано на рисунке, команда **debug aaa** содержит несколько ключевых слов, которые можно использовать для этой цели. Особый интерес представляет собой команда **debug aaa authentication**.

Она важна для анализа результатов отладки в случаях, когда все работает нормально. Результаты исполнения команды **debug** важны для идентификации проблем в случаях, когда что-то работает не так. При использовании любых команд **debug** в рабочей среде необходимо соблюдать осторожность, поскольку они интерпретируются на плоскости управления и, соответственно, создают значительную нагрузку на ресурсы маршрутизатора и могут отрицательно повлиять на производительность сети.

Второй учебный вопрос.
Локальная аутентификация

Основные сведения о результате отладки

```
R1# debug aaa authentication
113123: Feb 4 10:11:19.305 CST: AAA/MEMORY: create_user (0x619C4940) user=''ruser=''
        port='tty1' rem_addr='async/81560' authen_type=ASCII service=LOGIN priv=1
113124: Feb 4 10:11:19.305 CST: AAA/AUTHEN/START (2784097690): port='tty1' list=''
        action=LOGIN service=LOGIN
113125: Feb 4 10:11:19.305 CST: AAA/AUTHEN/START (2784097690): using "default" list
113126: Feb 4 10:11:19.305 CST: AAA/AUTHEN/START (2784097690): Method=LOCAL
113127: Feb 4 10:11:19.305 CST: AAA/AUTHEN (2784097690): status = GETUSER
113128: Feb 4 10:11:26.305 CST: AAA/AUTHEN/CONT (2784097690): continue_login
        (user='(undef)')
113129: Feb 4 10:11:26.305 CST: AAA/AUTHEN (2784097690): status = GETUSER
113130: Feb 4 10:11:26.305 CST: AAA/AUTHEN/CONT (2784097690): Method=LOCAL
113131: Feb 4 10:11:26.305 CST: AAA/AUTHEN (2784097690): status = GETPASS
113132: Feb 4 10:11:28.145 CST: AAA/AUTHEN/CONT (2784097690): continue_login
        (user='diallocal')
113133: Feb 4 10:11:28.145 CST: AAA/AUTHEN (2784097690): status = GETPASS
113134: Feb 4 10:11:28.145 CST: AAA/AUTHEN/CONT (2784097690): Method=LOCAL
113135: Feb 4 10:11:28.145 CST: AAA/AUTHEN (2784097690): status = PASS
```

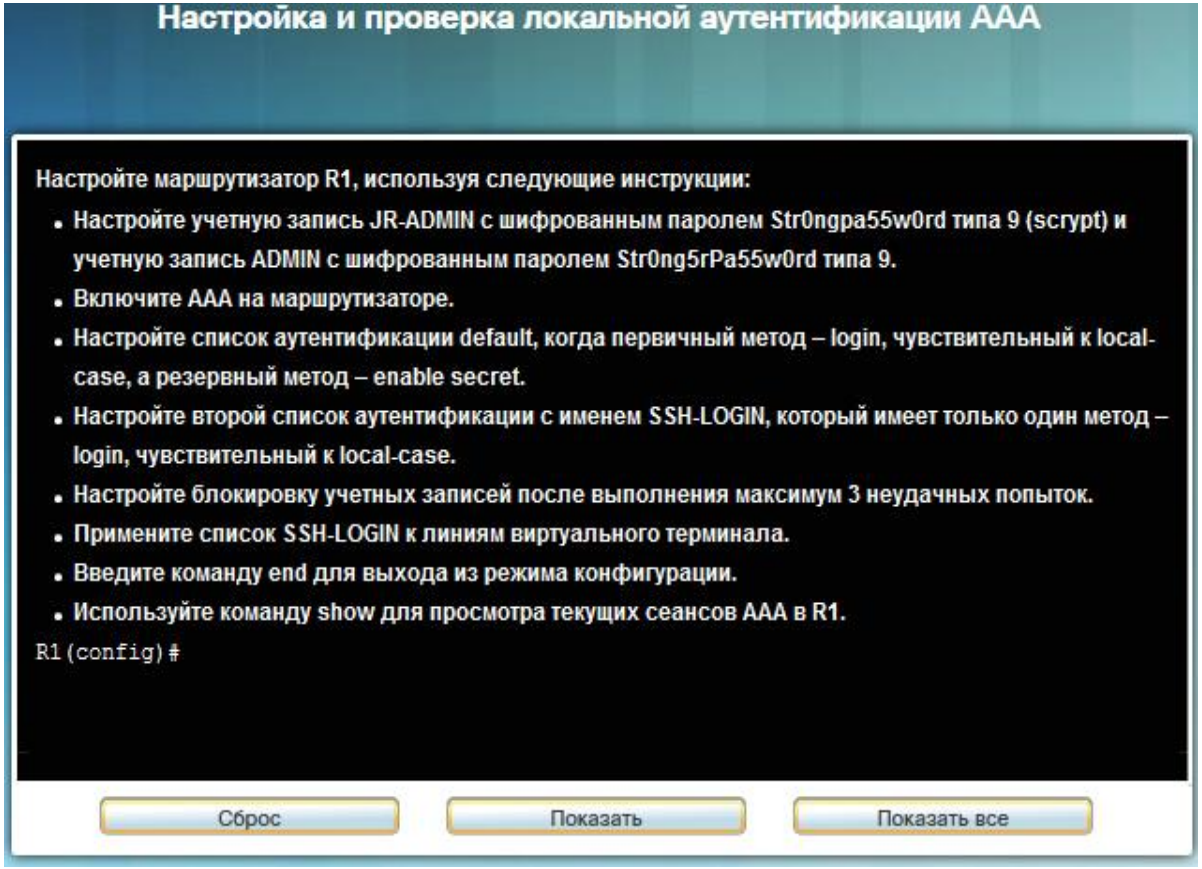
Отладка аутентификации AAA

Команда **debug aaa authentication** полезна для диагностики и устранения проблем AAA, как показано на рисунке.

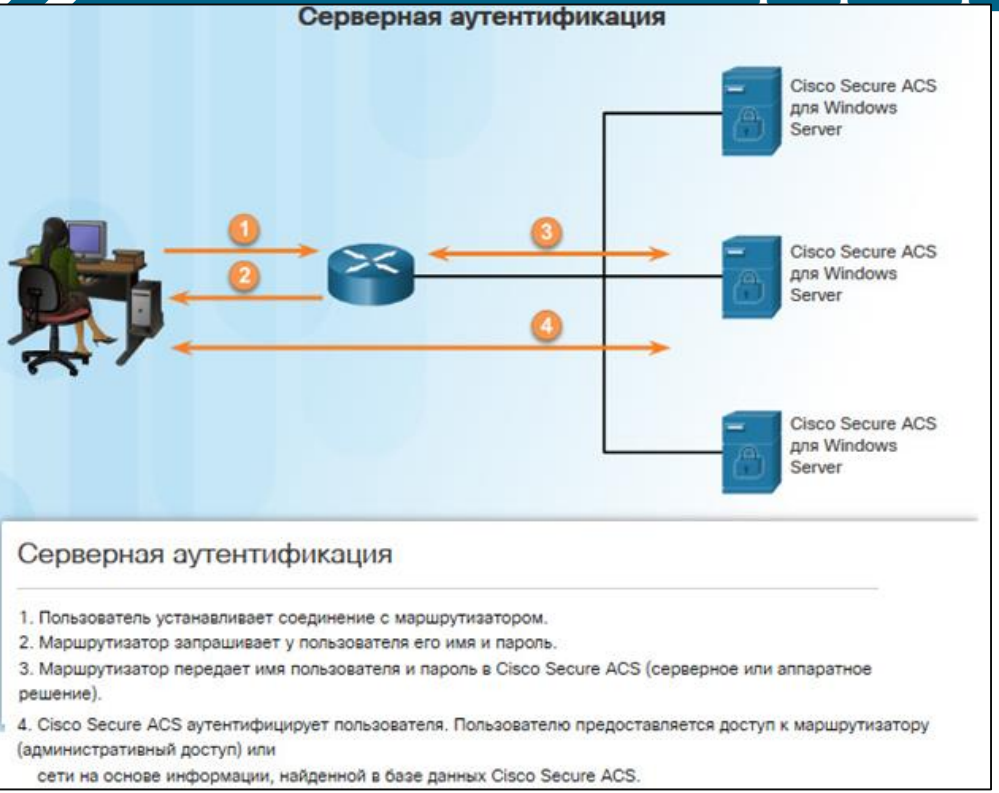
Необходимо специально следить за сообщениями о состоянии **GETUSER** и **GETPASS**. Также эти сообщения полезны для определения используемого списка методов. В данном примере был использован метод локальной базы данных. Статус входа в систему указывается сообщением **PASS**, которое означает, что вход произведен успешно.

Для отключения этой команды используйте команду **no debug aaa authentication** или полное отключение командой **undebug all**.

Выводы по второму вопросу
Локальная аутентификация



Третий учебный вопрос. Серверное решение AAA



Сравнение локальной и серверной аутентификации AAA

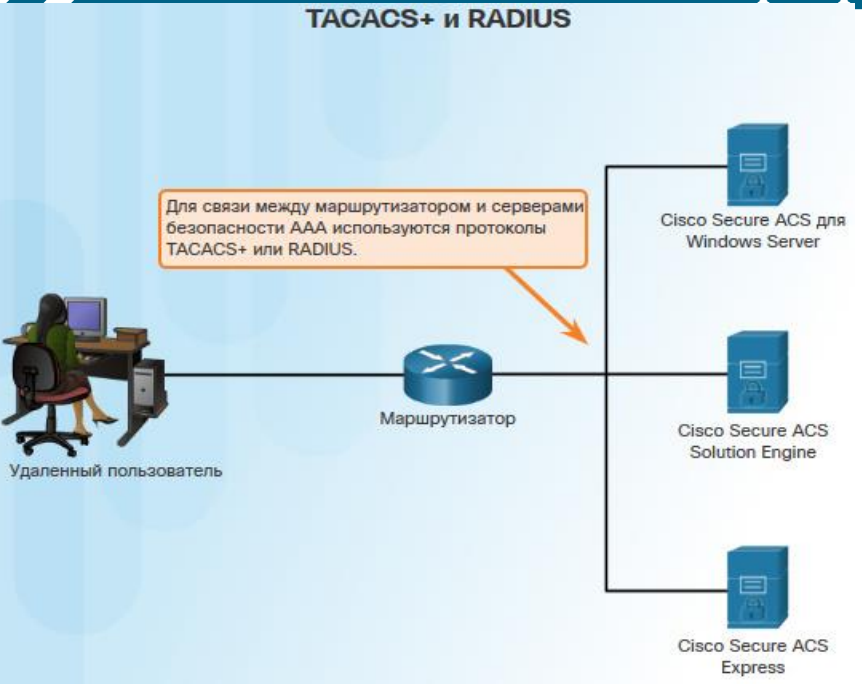
Локальная реализация AAA допускается в очень небольших сетях. Однако локальная аутентификация не очень хорошо масштабируется.

В большинстве корпоративных сред используется множество маршрутизаторов, коммутаторов и других инфраструктурных устройств Cisco, у маршрутизаторов есть множество администраторов, а доступ к корпоративной сети нужен сотням или тысячам пользователей. Обслуживание локальной базы данных для каждого устройства в сети такого масштаба нецелесообразно.

Чтобы решить эту проблему, можно использовать для управления доступом пользователей и администраторов ко всей корпоративной сети с помощью одного или нескольких серверов AAA, например Cisco Secure ACS. Cisco Secure ACS может создавать централизованную базу данных пользователей и административного доступа, которой смогут пользоваться все устройства сети. Также поддерживается работа с многими внешними базами данных, в том числе на базе Active Directory и Lightweight Directory Access Protocol (LDAP).

В этих базах данных хранятся данные учетных записей пользователей и пароли, что позволяет централизованно администрировать учетные записи пользователей. Для дополнительного резервирования можно использовать несколько серверов, как показано на рисунке.

Третий учебный вопрос.
Серверное решение AAA



Cisco Secure ACS поддерживает протоколы TACACS+ и RADIUS, как показано на рисунке.

TACACS+ и RADIUS – протоколы аутентификации, используемые для связи с серверами AAA. Как показано на рисунке, каждый из протоколов поддерживает разные функции и возможности. Выбор между TACACS+ и RADIUS зависит от потребностей организации.

Например, крупный интернет-провайдер может выбрать RADIUS, потому что он поддерживает детальный учет, необходимый для биллинга пользователей. Организация с разными группами пользователей может выбрать TACACS+, потому что он требует применения политик авторизации на уровне пользователей или групп.

Важно понимать многочисленные отличия между протоколами TACACS+ и RADIUS.

Три основных характеристики TACACS+:
- Разделяет аутентификацию и авторизацию
- Шифрует все данные
- Использует TCP-порт 49

Четыре основных характеристики RADIUS:
- Объединяет аутентификацию и авторизацию RADIUS в рамках одного процесса
- Шифрует только пароль
- Использует UDP
- Поддерживает технологии удаленного доступа 802.1X и протокол инициирования сеанса (SIP, Session Initiation Protocol)

Сравнение TACACS+ и RADIUS

	TACACS+	RADIUS
Функциональные возможности	Разделяет AAA в соответствии с архитектурой AAA, что обеспечивает модульный принцип реализации сервера безопасности	Объединяет аутентификацию и авторизацию, но отделяет учет, что обеспечивает меньшую гибкость реализации по сравнению с TACACS+
Стандарт	Обычно поддерживается компанией Cisco	Открытый стандарт/стандарт RFC
Транспортный протокол	TCP	UDP
CHAP	Двунаправленный запрос и ответ, используемые в протоколе Challenge Handshake Authentication Protocol (CHAP)	Однонаправленный запрос и ответ из сервера безопасности RADIUS в клиент RADIUS
Конфиденциальность	Шифруется весь пакет	Шифруется пароль
Индивидуальная настройка	Обеспечивает авторизацию команд маршрутизатора для каждого пользователя или для каждой группы	Не позволяет выполнять авторизацию команд маршрутизатора для каждого пользователя или для каждой группы
Учет	С ограничениями	Расширенный

Хотя для взаимодействия между маршрутизатором и серверами AAA может использоваться любой из протоколов, протокол TACACS+ считается более защищенным. Это связано с тем, что все передаваемые по протоколу TACACS+ данные шифруются, а при передаче по протоколу RADIUS шифруется только пароль пользователя. RADIUS не шифрует имена пользователей, учетную информацию и другую информацию, передаваемую в сообщениях RADIUS.

Третий учебный вопрос. Серверное решение AAA

Аутен

TACA на название,
TACACS+ п ими версиями
TACACS. TA

TACA реализации,
позволяя ис другой метод
аутентифика

Расши кодов ответов
по сравнени х протоколов,
включая IP и асности связи
шифруется в

Рассм

Третий учебный вопрос. Серверное решение AAA

Аутент

Протоко на открытом стандарте IE US работает в локальных кол RADIUS определяется

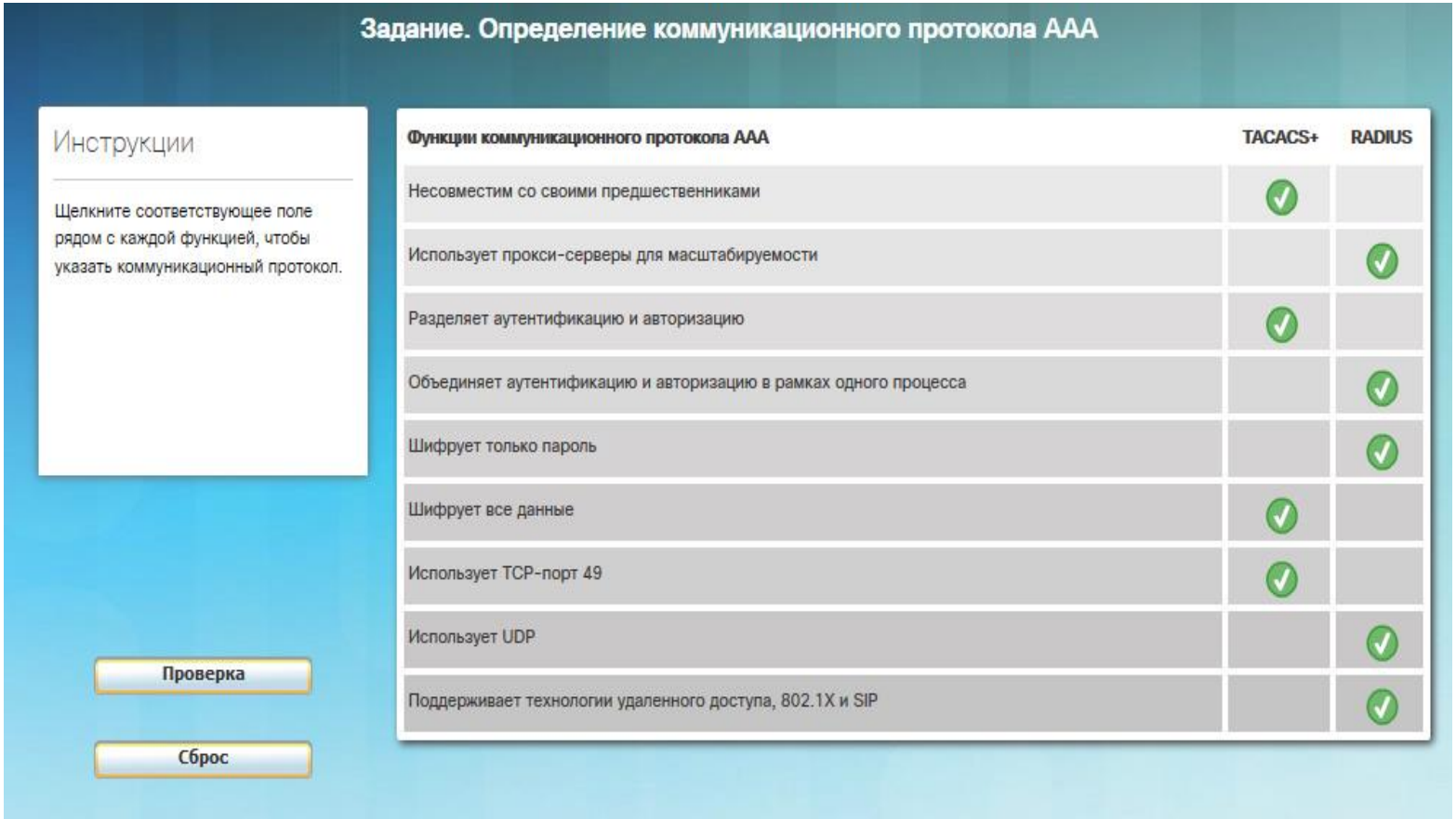
Протоко Р). Для этого используется бщий секрет. Однако остал

RADIU пользователя производится DP 1646 или 1813 для учет

RADIU стройств SIP, например шир вер RADIUS с помощью R 1X.

Рассмот

Выводы по третьему учебному вопросу. Серверное решение AAA



Четвертый учебный вопрос.
Серверная авторизация и аудит AAA

ойства или конечного пользователя, а
иям доступ к определенным зонам или

изации. Маршрутизатор можно настроить
лько определенные функции. Необходимо

ь доступ пользователя к определенным
дает защиту инфраструктуры в больших
ACS упрощают настройку конфигурации

В этом анимационном ролике показано, как JR-ADMIN успешно создал сеанс связи SSH с маршрутизатором и прошел аутентификацию на сервере TACACS+ AAA ACS.

В анимированном ролике у JR-ADMIN есть разрешение на доступ к команде **show version**, но нет команде **configure terminal**. Маршрутизатор запрашивает у ACS разрешение выполнить команду от имени пользователя. Когда пользователь отправляет команду **show version**, ACS отправляет ответ ACCEPT. Если пользователь отправляет команду **configure terminal**, ACS отправляет ответ REJECT.

По умолчанию TACACS+ разрешает установить новый сеанс TCP для каждого запроса авторизации, что может привести к задержке при вводе команд пользователями. Для повышения производительности Cisco Secure ACS поддерживает постоянные сеансы TCP, настраиваемые с помощью команды single-connection режима конфигурации сервера TACACS.

Синтаксис команды aaa authorization

```
R1(config)# aaa authorization {network | exec | commands level}
{default | list-name} method1...[method4]
```

```
R1(config)# aaa authorization exec ?
  WORD     Named authorization list.
  default  The default authorization list.
```

Списки методов авторизации

```
R1(config)# aaa authorization {network | exec | commands level}
{default | list-name} method1...[method4]
```

```
R1(config)# aaa authorization exec default ?
  cache              Use Cached-group
  group              Use server-group.
  if-authenticated   Succeed if user has authenticated.
  krb5-instance      Use Kerberos instance privilege maps.
  local              Use local database.
  none               No authorization (always succeeds).

R1(config)# aaa authorization exec default group ?
  WORD     Server-group name
  ldap     Use list of all LDAP hosts.
  radius   Use list of all Radius hosts.
  tacacs+  Use list of all Tacacs+ hosts.
```

Конфигурация авторизации AAA

Чтобы настроить авторизацию команд, следует использовать команду **aaa authorization**, как показано на рисунках 1 и 2. Тип службы может определить типы команд или служб:

network – Для сетевых служб, например PPP

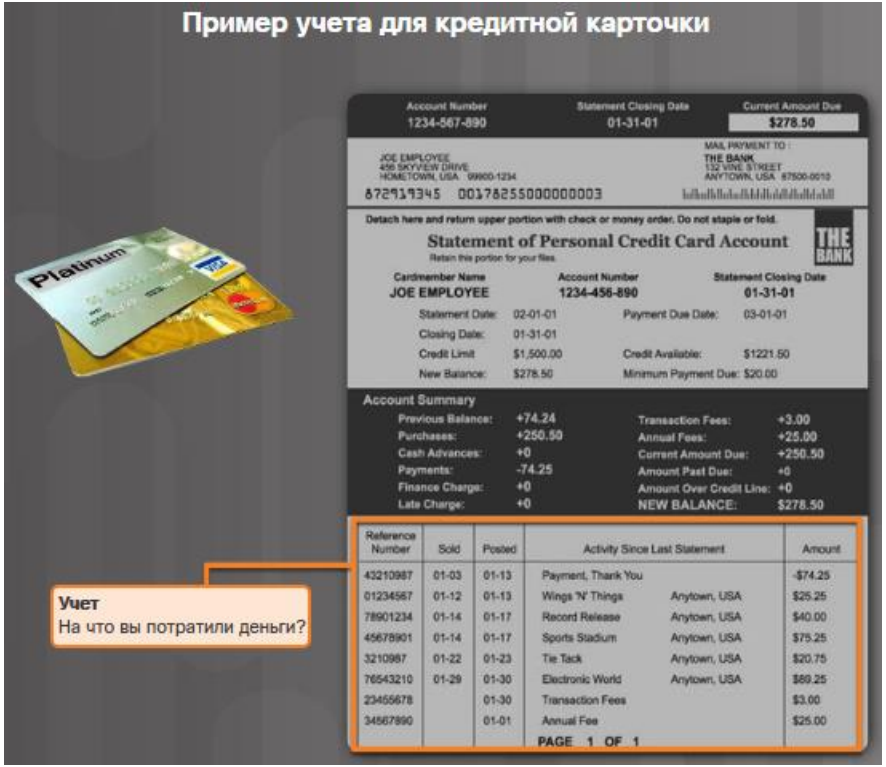
exec – Для запуска исполняемого кода (оболочки); см. рис. 2

commands *level* – Для исполняемых команд (оболочки)


```
R1(config)# username JR-ADMIN algorithm-type scrypt secret StrOng5rPa55wOrd
R1(config)# username ADMIN algorithm-type scrypt secret StrOng5rPa55wOrd
R1(config)# aaa new-model
R1(config)# aaa authorization exec default group tacacs+
R1(config)# aaa authorization network default group tacacs+
```

Когда авторизация AAA не включена, всем пользователям разрешен полный доступ. После запуска аутентификации изменения по умолчанию не разрешают доступ. Это означает, что администратор должен создать пользователя с полными правами доступа до активации авторизации, как показано на рисунке. Без этого администратор сразу же потеряет доступ к системе после ввода команды **aaa authorization**. Восстановить доступ можно будет только после перезагрузки маршрутизатора. Перезагрузка используемого в работе маршрутизатора может оказаться неприемлемой. Необходимо, чтобы хотя бы у одного пользователя всегда были полные права доступа.

Четвертый учебный вопрос.
Серверная авторизация и аудит AAA



Знакомство с серверным учетом AAA

Компаниям часто нужно следить за тем, какие ресурсы используют отдельные пользователи или группы. Учет AAA позволяет отслеживать использование ресурсов.

Хотя учет обычно считается задачей управления сетью или финансового управления, мы тоже немного расскажем о нем, потому что он тесно связан с безопасностью. В частности, система учета создает список пользователей с указанием времени их входа в систему. Например, если администратор узнает, что сотрудник вошел в систему посреди ночи, эта информация может стать поводом для дальнейшего расследования причин такого входа.

Еще одна причина внедрения учета – создание списка изменений в сети с указанием пользователя, который вносит изменения, и точного характера этих изменений. Эта информация помогает в диагностике и устранении неисправностей, если изменения влекут за собой непредвиденные результаты.

Как и в случае аутентификации и авторизации, списки методов учета определяют конкретные способы выполнения учета и последовательность их применения. После активации список методов учета по умолчанию автоматически применяется ко всем интерфейсам, кроме тех, для которых явным образом определен пользовательский список методов учета.

Конфигурация учета AAA

Для настройки учета AAA используйте команду **aaa accounting** (смотри рисунок 1) .

Обычно используются следующие три параметра **aaa accounting** ключевые слова:

network – Выполняет учет всех запросов сетевых услуг, включая PPP.

exec – Запускает учет сеанса оболочки EXEC.

connection – Запускает учет для всех исходящих соединений, например SSH и Telnet.

Как и при аутентификации AAA, можно использовать ключевое слово ***default*** или ***list-name***.

Затем настраивается тип записи (триггер). Триггер определяет, какие действия вызывают обновление записей учета. Возможные триггеры:

start-stop – Отправляет уведомление **start** о начале процесса и уведомление stop по окончании процесса.

stop-only – Отправляет запись учета **stop** для всех случаев, включая ошибки аутентификации.

none – Отключает учет на линии или интерфейсе.

На рис. 2 показаны доступные списки методов учета.

Синтаксис команды aaa accounting

```
R1(config)#
aaa accounting {network | exec | connection} {default | list-name}
{start-stop | stop-only | none } [broadcast] method1...[method4]
```

```
R1(config)# aaa accounting exec?
  WORD       Named Accounting list.
  default    The default accounting list.
```

Списки методов учета

```
R1(config)#
aaa accounting {network | exec | connection} {default | list-name}
{start-stop | stop-only | none } [broadcast] method1...[method4]
```

```
R1(config)# aaa accounting exec default start-stop?
  broadcast Use Broadcast for Accounting
  group     Use Server-group

R1(config)# aaa accounting exec default start-stop group?
  WORD      Server-group name
  radius    Use list of all Radius hosts.
  tacacs+   Use list of all Tacacs+ hosts.
```

Четвертый учебный вопрос. Серверная авторизация и аудит AAA

Пример учета AAA


```
R1(config)# username JR-ADMIN algorithm-type scrypt secret StrOng5rPa5wOrd
R1(config)# username ADMIN algorithm-type scrypt secret StrOng5rPa55wOrd
R1(config)# aaa new-model
R1(config)# aaa authentication login default group tacacs+
R1(config)# aaa authorization exec default group tacacs+
R1(config)# aaa authorization network default group tacacs+
R1(config)# aaa accounting exec default start-stop group tacacs+
R1(config)# aaa accounting network default start-stop group tacacs+
```

На рисунке приведен пример учета для регистрации использования команд EXEC и сетевых соединений.

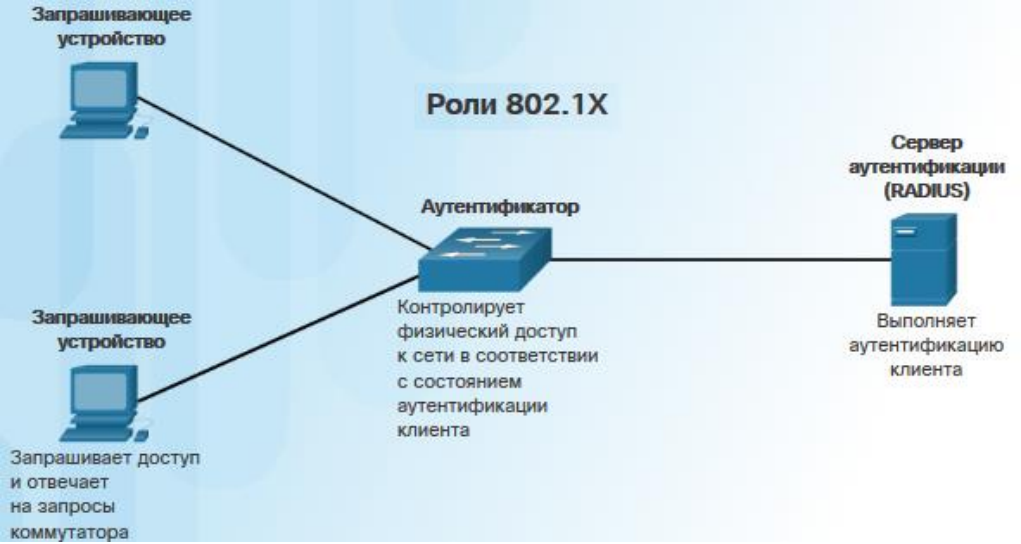
В маршрутизаторе R1 настроена локальная база данных имен пользователей, включен AAA и настроена аутентификация AAA. В сети реализованы серверы TACACS+ и RADIUS. Настройте маршрутизатор R1, используя следующие инструкции:

- Настройте список методов авторизации AAA по умолчанию для оболочек EXEC и сетевых сервисов, использующих TACACS+.
- Настройте список методов учета AAA по умолчанию для оболочек EXEC и сетевых сервисов TACACS+ с уведомлениями «старт» и «стоп», отправляемыми в начале и конце процесса.
- После настройки выйдите из режима конфигурации.

```
R1(config)#
```

С помощью средства проверки синтаксиса, приведенного на рисунке, настройте серверную авторизацию и учет AAA на маршрутизаторе R1. Локальная база данных пользователей настроена, AAA включено, аутентификация AAA настроена, в сети реализованы серверы TACACS+ и RADIUS.

Четвертый учебный вопрос.
Серверная авторизация и аудит AAA



Обеспечение безопасности с использованием аутентификации 802.1X на основе портов

Стандарт IEEE 802.1X определяет контроль доступа на основе портов и протокол аутентификации, который запрещает не прошедшим авторизацию рабочим станциям подключаться к LAN через общедоступные порты коммутатора. Сервер аутентификации проводит аутентификацию каждой рабочей станции, подключаемой к порту коммутатора, прежде чем предоставлять любые сервисы коммутатора или LAN.

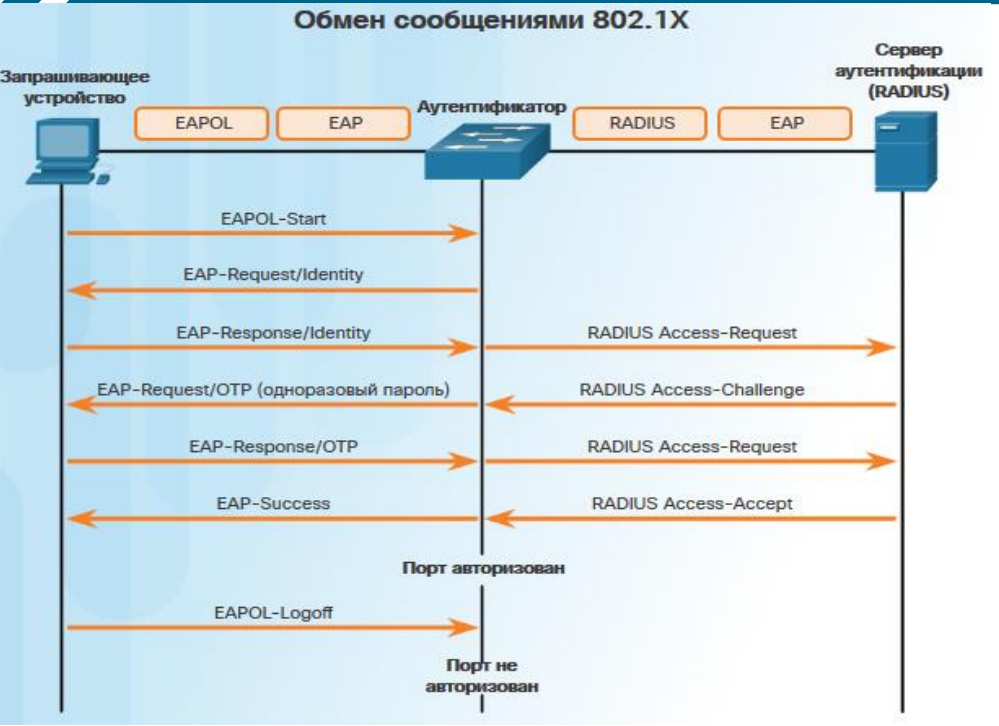
На рисунке показано, что с аутентификацией на базе портов 802.1X устройства в сети имеют определенные роли:

Запрашивающее устройство (клиент) - Устройство (рабочая станция), которое запрашивает доступ к сервисам LAN и коммутатора и отвечает на запросы коммутатора. На рабочей станции должно использоваться клиентское ПО, совместимое со стандартом 802.1X. (Порт, к которому подключается клиент, является запрашивающим устройством [клиентом] согласно спецификации IEEE 802.1X.)

Аутентификатор (коммутатор) – Контролирует физический доступ к сети, руководствуясь состоянием аутентификации узла сети. Он выступает в роли посредника (прокси-сервера) между клиентом (запрашивающим устройством) и сервером аутентификации. Он запрашивает у клиента идентификационные данные, проверяет их на сервере и ретранслирует клиенту отклик сервера. В составе коммутатора имеется программный агент RADIUS, который отвечает за инкапсуляцию и декапсуляцию кадров EAP (расширяемый протокол аутентификации), а также за взаимодействие с сервером аутентификации.

Сервер аутентификации - Непосредственно выполняет аутентификацию клиента. Сервер аутентификации проверяет подлинность клиента и сообщает коммутатору, есть ли у клиента полномочия на доступ к сервисам LAN и коммутатора. Поскольку коммутатор выступает в качестве прокси-сервера, служба аутентификации для клиента прозрачна. Система безопасности RADIUS с расширениями EAP – единственный поддерживаемый сервер аутентификации.

Четвертый учебный вопрос.
Серверная авторизация и аудит AAA



До прохождения аутентификации рабочей станции средства контроля доступа 802.1x пропускают через порт только трафик протокола расширяемой аутентификации по LAN (EAPOL). После успешной аутентификации разрешается пересылка через порт обычного трафика.

Состояние порта коммутатора определяет, предоставлен ли клиенту доступ в сеть. При настройке для аутентификации 802.1X на базе портов начальным состоянием порта является неавторизованное состояние. В этом состоянии порт запрещает весь входящий и исходящий трафик, кроме пакетов протокола 802.1x. После успешной аутентификации клиента порт переходит в авторизованное состояние, и весь трафик клиента может пересылаться обычным образом. Если коммутатор запрашивает идентификацию клиента (инициируется аутентификатором) и клиент не поддерживает 802.1X, порт остается в неавторизованном состоянии, и клиенту не предоставляется доступ к сети.

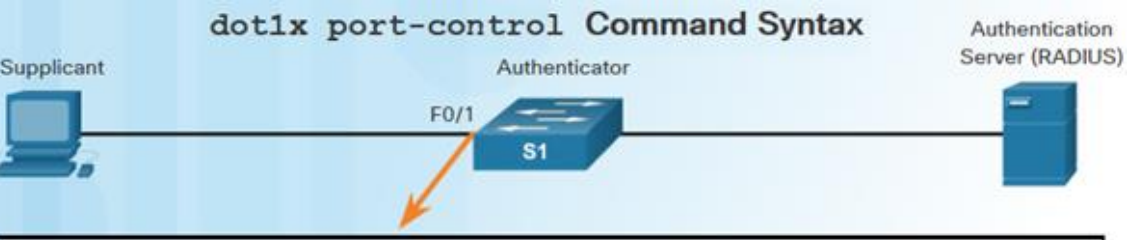
Если же клиент с поддержкой 802.1X подключается к порту и инициирует процесс аутентификации (инициируется запрашивающим устройством), отправляя кадр начального состояния EAPOL на коммутатор с протоколом 802.1X, никакой ответ не присылается, и клиент начинает отправлять кадры, как если бы порт находился в авторизованном состоянии.

На рисунке показан полный процесс обмена сообщениями между запрашивающим устройством, аутентификатором и сервером аутентификации. Инкапсуляция происходит следующим образом:

Между запрашивающим устройством и аутентификатором - Данные EAP инкапсулируются в кадры EAPOL.

Между аутентификатором и сервером аутентификации – Данные EAP инкапсулируются с использованием RADIUS.

Четвертый учебный вопрос.
Серверная авторизация и аудит AAA




```
S1(config-if)# authentication port-control {auto | force-authorized | force-unauthorized}
```

Parameter	Description
auto	Enables 802.1X port-based authentication and causes the port to begin in the unauthorized state, enabling only EAPOL, STP, and CDP frames to be sent and received through the port.
force-authorized	The port sends and receives normal traffic without 802.1x-based authentication of the client. This is the default setting.
force-unauthorized	Causes the port to remain in the unauthorized state, ignoring all attempts by the client to authenticate. The switch cannot provide authentication services to the client through the port.

Состояния авторизации портов 802.1X

При успешном прохождении аутентификации клиентом (получении кадра принятия от сервера аутентификации) состояние порта сменяется на авторизованное, и все кадры от клиента, прошедшего аутентификацию, активируются на порту.

При отказе в аутентификации порт остается в неавторизованном состоянии, но аутентификация может быть произведена повторно. В тех случаях, когда сервер аутентификации недоступен, коммутатор может повторить отправку запроса. Если к серверу не удалось обратиться после определенного числа повторов, аутентификация считается непройденной, и доступ к сети не предоставляется.

После завершения работы клиента он отправляет сообщение выхода EAPOL, в результате чего порт коммутатора возвращается в неавторизованное состояние.

Используйте команду **authentication port-control** для контроля состояния авторизации порта. На рисунке показаны синтаксис команды и описание параметров. По умолчанию порт находится в состоянии принудительной авторизации, т. е. может отправлять и принимать трафик без аутентификации 802.1x. Ключевое слово **auto** необходимо ввести для включения аутентификации 802.1X. При успешном прохождении аутентификации клиентом (получении кадра принятия от сервера аутентификации) состояние порта сменяется на авторизованное, и все кадры от клиента, прошедшего аутентификацию, активируются на порту. При отказе в аутентификации порт остается в неавторизованном состоянии, но аутентификация может быть произведена повторно. В тех случаях, когда сервер аутентификации недоступен, коммутатор может повторить отправку запроса. Если к серверу не удалось обратиться после определенного числа повторов, аутентификация считается непройденной, и доступ к сети не предоставляется.

После завершения работы клиента он отправляет сообщение выхода EAPOL, в результате чего порт коммутатора возвращается в неавторизованное состояние. Если состояние порта сменяется на отключенное или порт получает кадр выхода EAPOL, то порт возвращается в неавторизованное состояние.

Четвертый учебный вопрос.
Серверная авторизация и аудит AAA


```
S1(config)# aaa new-model
S1(config)# radius server CCNAS
S1(config-radius-server)# address ipv4 10.1.1.50 auth-port 1812 acct-port 1813
S1(config-radius-server)# key RADIUS-Pa55w0rd
S1(config-radius-server)# exit
S1(config)# aaa authentication dot1x default group radius
S1(config)# dot1x system-auth-control
S1(config)# interface F0/1
S1(config-if)# description Access Port
S1(config-if)# switchport mode access
S1(config-if)# authentication port-control auto
S1(config-if)# dot1x pae authenticator
```

Конфигурирование 802.1X

На рис. 1 показана ситуация, когда ПК подключен к порту коммутатора F0/1 и аутентификация устройства производится через 802.1X с сервером RADIUS. Для настройки 802.1X требуется простая процедура:

Шаг 1. Включите AAA с помощью команды aaa new-model и настройте сервер RADIUS.

Шаг 2. Создайте список методов аутентификации на базе портов 802.1X, используя команду aaa authentication dot1x .

Шаг 3. Глобально включите аутентификацию на основе порта 802.1x с помощью команды dot1x system-auth-control .

Шаг 4. Включите аутентификацию на основе порта в интерфейсе с помощью команды authentication port-control auto .

Шаг 5. Включите аутентификацию 802.1X в интерфейсе с помощью команды dot1x pae . Опция authenticator устанавливает тип Port Access Entity (PAE), чтобы интерфейс функционировал только как аутентификатор и не отвечал ни на какие сообщения запрашивающего устройства.

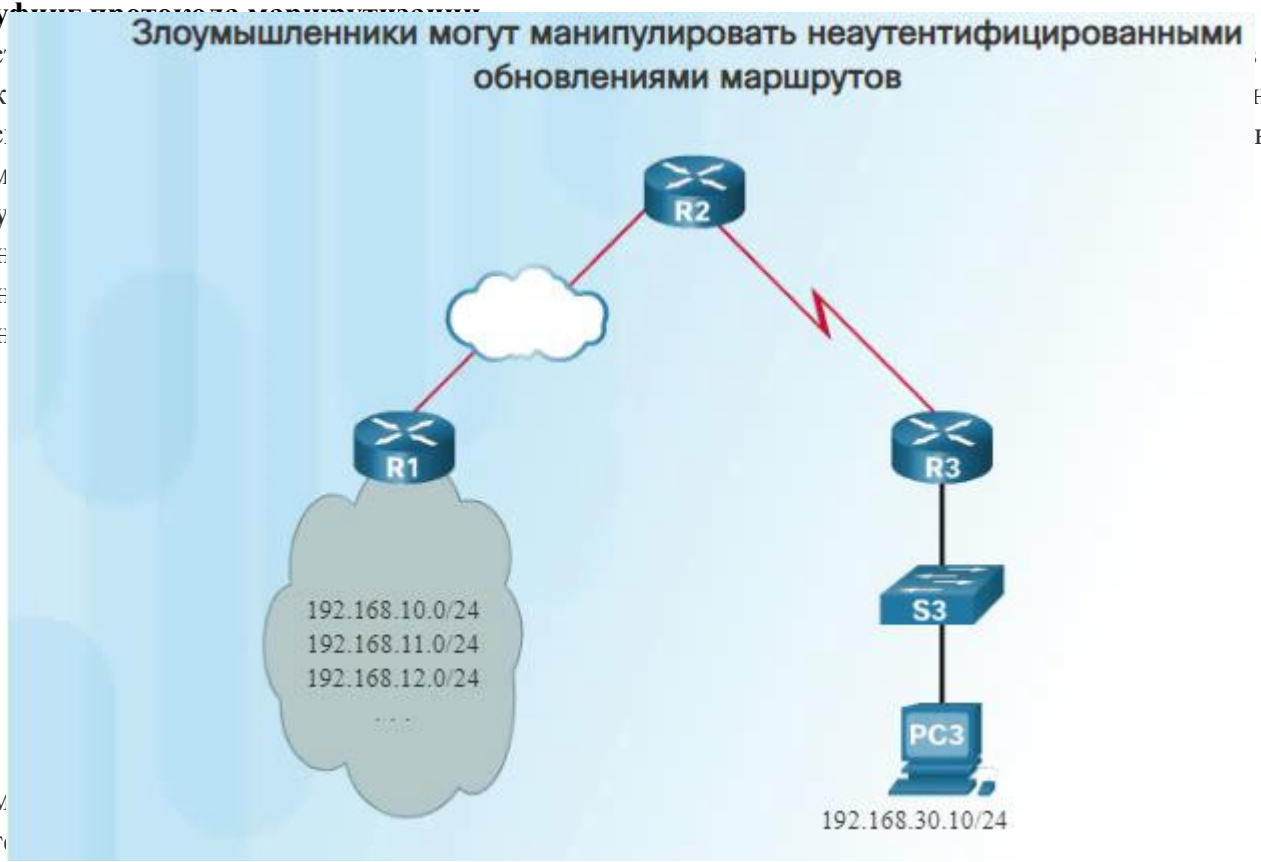
Четвертый учебный вопрос. Защита плоскости управления

Спуфинг протокола маршрутизации

Сист одноранговой сети или за счет
фальсифик нг информации о маршрутизации
обычно ис ку или заставить трафик идти по
необычном

Спу

– Перен
– Перен
– Перен



Для просм
ознакомьт

Далее для нейтрализации атак на протоколы маршрутизации сконфигурирем аутентификацию OSPF.

Рассмотрим пример того, как атака создает петлю маршрутизации.

Аутентификация протокола маршрутизации OSPF MD5

OSPF поддерживает аутентификацию протокола маршрутизации с использованием MD5. Аутентификацию MD5 можно включить глобально для всех интерфейсов или отдельно для каждого.

Включение аутентификации OSPF MD5 в глобальном режиме:

- команда **ip ospf message-digest-key** *key* **md5** *password* в режиме конфигурации интерфейса.
- команда **area** *area-id* **authentication message-digest** в режиме конфигурации маршрутизатора.

Таким образом аутентификация принудительно включается на всех интерфейсах с поддержкой OSPF. Если интерфейс не сконфигурирован с помощью команды **ip ospf message-digest-key,** он не сможет сформировать смежности с другими соседями OSPF.

Включение аутентификации MD5 отдельно для каждого интерфейса:

- **команда ip ospf message-digest-key** *key* **md5** *password* в режиме конфигурации интерфейса.
- **команда ip ospf authentication message-digest** в режиме конфигурации интерфейса.

Настройки интерфейса переписывают глобальные настройки. Пароли аутентификации MD5 не обязательно должны быть одинаковы для всей области. Однако они должны быть одинаковыми между соседями.

OSPF, сконфигурированная с аутентификацией MD5


```
R1# conf t
R1(config)# interface s0/0/0
R1(config-if)# ip ospf message-digest-key 1 md5 cisco12345
R1(config-if)# ip ospf authentication message-digest
R1(config-if)#
000209: Feb 20 13:59:35.091 UTC: %OSPF-5-ADJCHG: Process 1, Nbr 10.1.1.2 on
Serial0/0/0 from FULL to DOWN, Neighbor Down: Dead timer expired
R1(config-if)#
000210: Feb 20 14:01:09.975 UTC: %OSPF-5-ADJCHG: Process 1, Nbr 10.1.1.2 on
Serial0/0/0 from LOADING to FULL, Loading Done
---------------------------
R2# conf t
000137: Feb 20 13:59:35.091 UTC: %OSPF-5-ADJCHG: Process 1, Nbr 192.168.1.1 on
Serial0/0/0 from FULL to DOWN, Neighbor Down: Dead timer expired
R2(config)# interface s0/0/0
R2(config-if)# ip ospf message-digest-key 1 md5 cisco12345
R2(config-if)# ip ospf authentication message-digest
R2(config-if)#
000138: Feb 20 14:01:09.975 UTC: %OSPF-5-ADJCHG: Process 1, Nbr 192.168.1.1 on
Serial0/0/0 from LOADING to FULL, Loading Done
R2(config-if)#
```

На рис. 1 маршрутизаторы R1 и R2 сконфигурированы с аутентификацией OSPF и маршрутизация работает корректно. Однако OSPF-сообщения не аутентифицированы и не зашифрованы.

На рис. 2 маршрутизаторы R1 и R2 сконфигурированы с аутентификацией OSPF MD5. Аутентификация сконфигурирована отдельно для каждого интерфейса, так как оба маршрутизатора используют только один интерфейс для создания смежностей OSPF.

Обращаем внимание, что при конфигурировании маршрутизатора R1 смежность OSPF с R2 теряется до тех пор, пока R2 не будет сконфигурирован с соответствующей аутентификацией MD5.

Четвертый учебный вопрос. Защита плоскости управления

Процедура конфигурации аутентификации OSPF SHA

Шаг 1. Задайте цепочку ключей аутентификации SHA.

```
Router(config)# key chain name
Router(config-keychain)# key key-id
Router(config-keychain-key)# key-string string
Router(config-keychain-key)# cryptographic-algorithm hmac-sha-256
Router(config)# send-lifetime start-time {infinite | end-time | duration seconds}
```

Шаг 2. Присвойте цепочку ключей аутентификации требуемым интерфейсам.

```
Router(config)# interface type number
Router(config-if)# ip ospf authentication key-chain name
```

Аутентификация протокола ршрутизации OSPF SHA

Аутентификация MD5 в тоящее время считается уязвимой ед атаками и должна ользоваться только в случае, когда ее надежная аутентификация оступна. В версии Cisco IOS 4(1)T добавлена поддержка для ентификации OSPF SHA, как сано в документе RFC 5709. Таким разом, администратор должен использовать аутентификацию SHA, при условии что операционные системы всех маршрутизаторов поддерживают аутентификацию OSPF SHA.

Аутентификация OSPF SHA включает два важных шага. Синтаксис команд показан на рисунке.

Шаг 1. Укажите цепочку ключей аутентификации в режиме глобальной конфигурации.

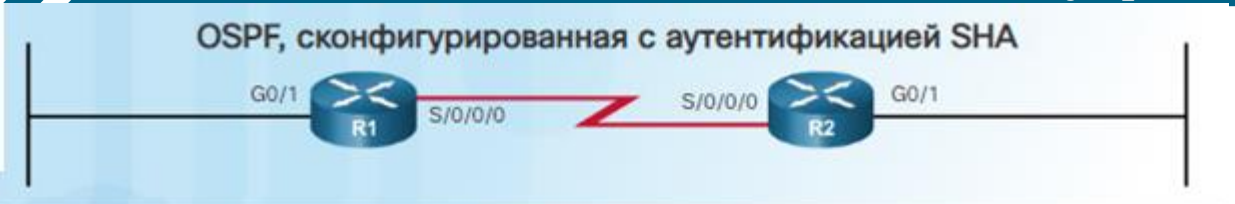
Присвойте имя цепочке ключей с помощью команды **key chain** .

Присвойте номер и пароль цепочке ключей с помощью команд **key** и **key-string** .

Укажите аутентификацию SHA с помощью команды **cryptographic-algorithm** .

(Необязательно) Укажите, когда истекает срок действия ключа, с помощью команды **send-lifetime** .

Шаг 2. Присвойте ключ аутентификации нужным интерфейсам с помощью команды **ip ospf authentication key-chain** .

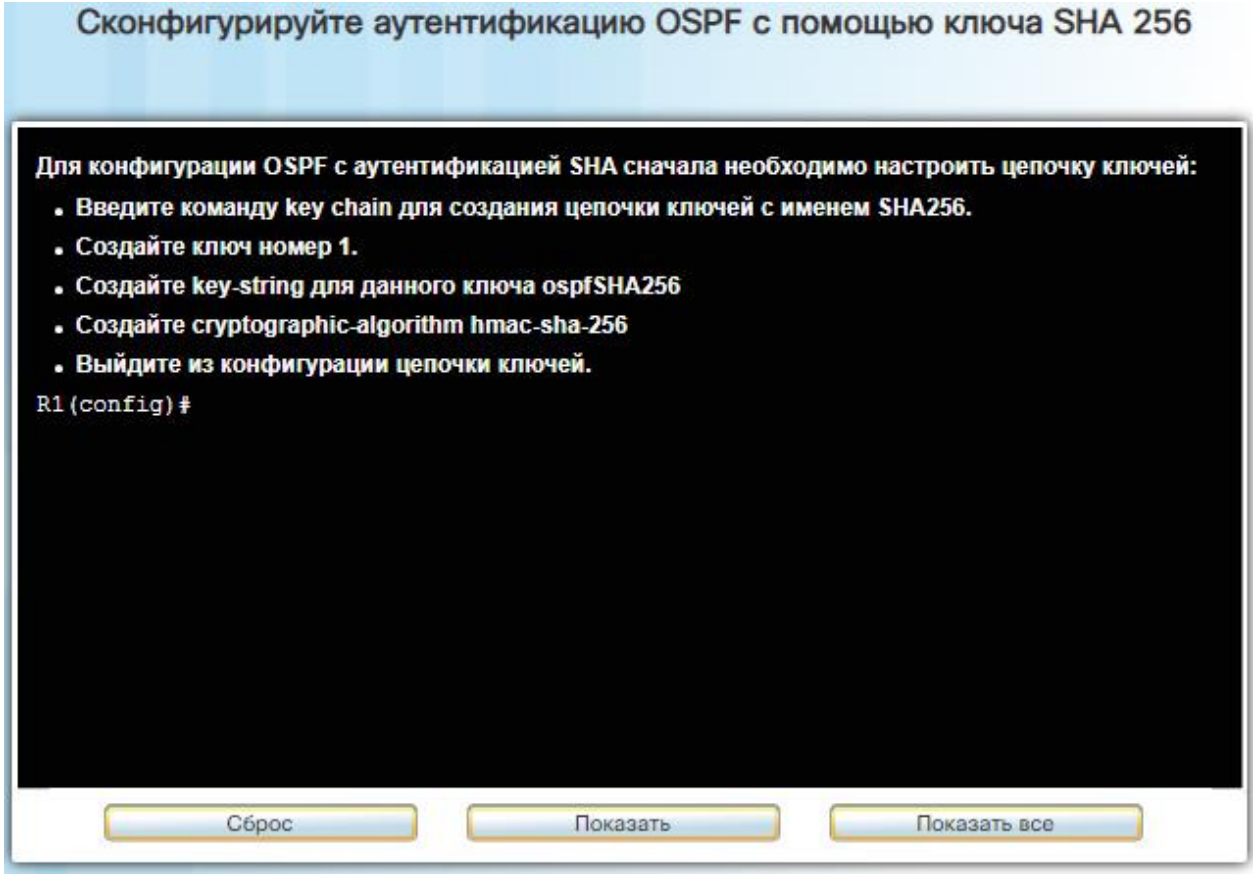



```
R1(config)# key chain SHA256
R1(config-keychain)# key 1
R1(config-keychain-key)# key-string ospfSHA256
R1(config-keychain-key)# cryptographic-algorithm hmac-sha-256
R1(config-keychain-key)# exit
R1(config-keychain)# exit
R1(config)# interface s0/0/0
R1(config-if)# ip ospf authentication key-chain SHA256
R1(config-if)#
000218: Feb 20 15:06:07.607 UTC: %OSPF-5-ADJCHG: Process 1, Nbr 10.1.1.2 on Serial0/0/0
from FULL to DOWN, Neighbor Down: Dead timer expired
R1(config-if)#
000219: Feb 20 15:07:22.635 UTC: %OSPF-5-ADJCHG: Process 1, Nbr 10.1.1.2 on Serial0/0/0
from LOADING to FULL, Loading Done
R1(config-if)#
-------------------------------------
R2(config)# key chain SHA256
R2(config-keychain)# key 1
R2(config-keychain-key)# key-string ospfSHA256
R2(config-keychain-key)# cryptographic-algorithm hmac-sha-256
R2(config-keychain-key)# exit
R2(config-keychain)# exit
```

На рис. 2 маршрутизаторы R1 и R2 конфигурируются с аутентификацией OSPF SHA с помощью ключа SHA256 и строки ключа ospfSHA256. Обращаем внимание, что при конфигурировании маршрутизатора R1 смежность OSPF с R2 теряется до тех пор, пока R2 не будет сконфигурирован с соответствующей аутентификацией SHA.

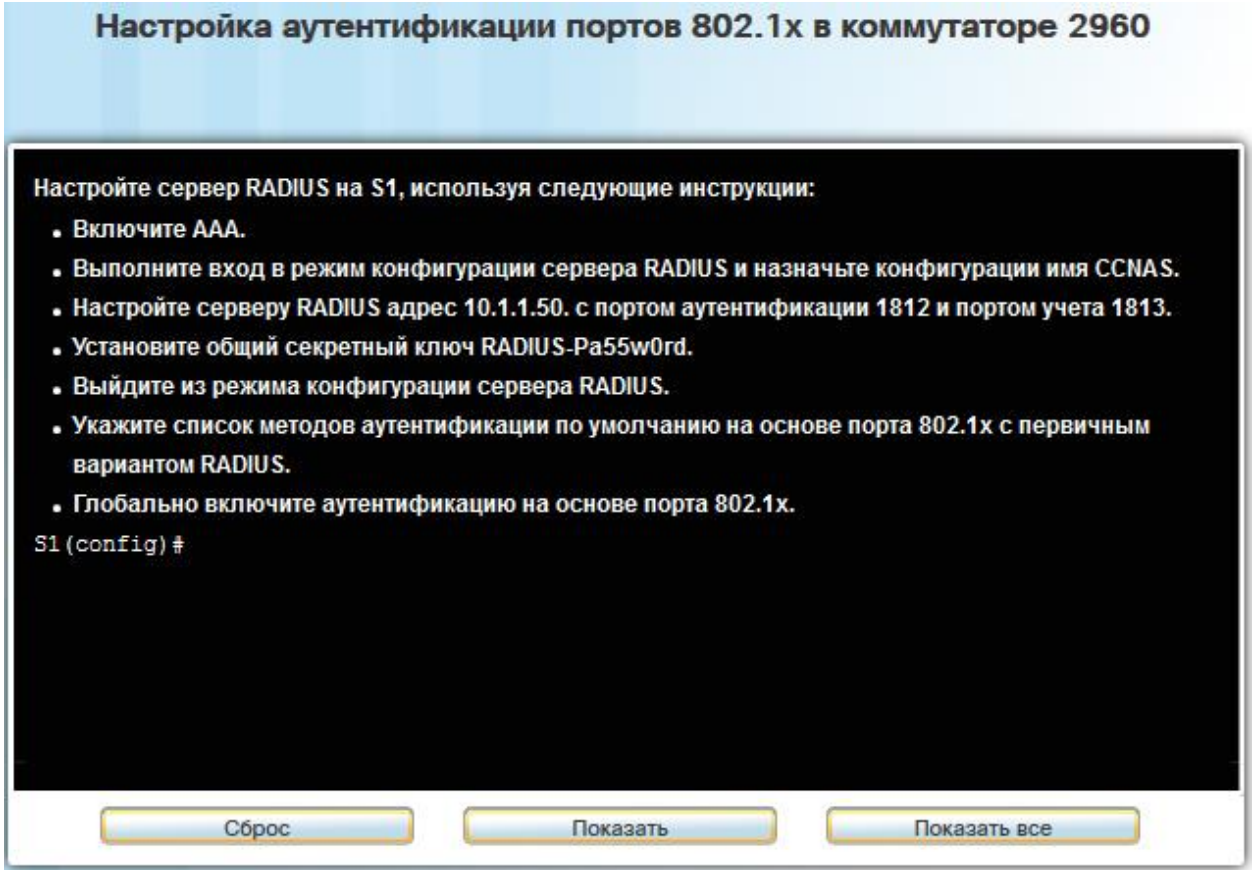
Выводы по четвертому учебному вопросу. Защита плоскости управления

Воспользуйтесь программой проверки синтаксиса (см. рис. 3), чтобы сконфигурировать аутентификацию OSPF с помощью ключа SHA 256.



Выводы по четвертому учебному вопросу. Серверная авторизация и аудит AAA

С помощью средства проверки синтаксиса, приведенного на рисунке, настройте аутентификацию порта 802.1X на коммутаторе 2960.



Учебные вопросы и цели занятия:

1. Назначение аутентификации.
2. Локальная аутентификация.
3. Серверное решение аутентификации.
4. Серверная авторизация и аудит AAA.

Заключение

Использование протокола аутентификации, авторизации и учета (AAA) создает масштабируемую структуру для администрирования доступа. AAA контролирует, кому и когда разрешено подключаться к сети, что им разрешено в ней делать, а также отслеживает записи выполненных действий.

В небольших или простых сетях аутентификация AAA реализуется с использованием локальной базы данных. Однако в больших и сложных сетях аутентификация AAA должна реализовываться с использованием серверного механизма AAA.

AAA могут использовать протоколы RADIUS и TACACS+ для взаимодействия с маршрутизаторами клиентов. Система Cisco Access Control System (ACS) может использоваться для предоставления доступа к серверам AAA или для расширения функций механизма Cisco Identity Services Engine (ISE).

Также для аутентификации на базе портов можно использовать протокол 802.1X.