Тема 1.1 Организация безопасного удаленного доступа

Лекция 3. Обеспечение безопасности сетевых устройств на основе ролей

Дисциплина: Анализ информационных потребностей подразделений информационно-аналитического мониторинга

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

Учебные вопросы и цели занятия:

1. Защита файлов конфигурации и образа ОС.
2. Назначение административных ролей.
3. Автоматические функции обеспечения безопасности.
4. Защита плоскости управления.

Вступительная часть

Обеспечение безопасности проходящего сетевого трафика и внимательное изучение входящего трафика являются критически важными аспектами сетевой безопасности. Защита граничного маршрутизатора, который подключается к внешней сети, – это важный первый шаг в обеспечении безопасности сети.

Защищая сеть, не менее важно защищать сами устройства. Это включает использование интерфейса командной строки Cisco IOS для внедрения проверенных способов физической защиты маршрутизатора и защиты административного доступа к маршрутизатору. Большинство сервисов маршрутизаторов включены по умолчанию. Некоторые из этих функций были включены изначально, но сейчас уже не нужны. На данном занятии рассматриваются несколько из этих сервисов, а также режим One-Step Lockdown команды auto secure, который может использоваться для автоматизации задач по защите устройств.

Аутентификация протокола маршрутизации – это обязательный лучший способ предотвращения спуфинга протокола маршрутизации. В этой главе мы также остановимся на аутентификации конфигурирования открытого протокола кратчайшего пути (Open Shortest Path First, OSPF) с шифрованием Message Digest 5 (MD5) и Secure Hash Algorithm (SHA). Плоскости управления, менеджмента и данных рассматриваются с точки зрения использования ограничения плоскости управления (Control Plane Policing, CoPP).

Функция устойчивой конфигурации Cisco IOS

Функция устойчивой конфигурации Cisco IOS обеспечивает быстрое восстановление в случае злоумышленного или ненамеренного переформатирования флеш-памяти или удаления файла загрузочной конфигурации из энергонезависимой переписываемой памяти (nonvolatile random-access memory, NVRAM). Эта функция обеспечивает сохранение защищенной рабочей копии файла образа IOS маршрутизатора и копии файла текущей конфигурации. Эти защищенные файлы не могут быть удалены пользователем и называются первичным загрузочным набором (bootset).

Включение функции отказоустойчивости образа IOS

Для защиты образа IOS и включения функции отказоустойчивости образа Cisco IOS используйте команду **secure boot-image** в режиме глобальной конфигурации. При первом включении сохраняется текущий защищенный образ Cisco IOS и создается запись в системном журнале. Отключить функцию отказоустойчивости образа Cisco IOS можно только через сеанс консоли с помощью команды **no** . Эта команда функционирует правильно, только если система сконфигурирована для запуска изображения с флеш-диска через интерфейс ATA. Кроме того, текущий образ может быть загружен с устройства постоянного хранения и сохранен (защищен) в качестве основного. Образы, загружаемые из удаленного местоположения, например TFTP-сервера, не могут быть защищены.

```
R1# conf t
R1(config)# secure boot-image
R1(config)#
*Feb 18 17:57:29.035: %IOS_RESILIENCE-5-IMAGE_RESIL_ACTIVE:
Successfully secured running image
R1(config)# secure boot-config
R1(config)#
*Feb 18 18:02:29.459: %IOS_RESILIENCE-5-CONFIG_RESIL_ACTIVE:
Successfully secured config archive [flash0:.runcfg-20150218-180228.ar]
R1(config)# exit
R1# show secure bootset
IOS resilience router id FTX1636848Z

IOS image resilience version 15.4 activated at 18:02:04 UTC Wed Feb
18 2015
Secure archive flash0:c1900-universalk9-mz.SPA.154-3.M2.bin type is
image (elf) []
  file size is 75551300 bytes, run size is 75730352 bytes
  Runnable image, entry point 0x81000000, run from ram

IOS configuration resilience version 15.4 activated at 18:02:29 UTC
Wed Feb 18 2015
Secure archive flash0:.runcfg-20150218-180228.ar type is config
configuration archive size 2182 bytes

R1#
```

Включение функции отказоустойчивости образа IOS

Чтобы получить мгновенный снимок текущей конфигурации маршрутизатора и надежно заархивировать его в устройстве постоянного хранения, используйте команду **secure boot-config** в режиме глобальной конфигурации, как показано на рисунке. На консоли отображается сообщение журнала, уведомляющее пользователя о том, что функция устойчивой конфигурации активирована. Архив конфигурации скрыт и не может просматриваться и удаляться непосредственно из запроса интерфейса CLI. Команду **secure boot-config** можно использовать повторно, чтобы обновлять архив конфигурации до новейшей версии после ввода команд новой конфигурации.

Защищенные файлы не появляются в результатах команды **dir,** которая вводится из интерфейса CLI. Это связано с тем, что файловая система Cisco IOS не дает показывать защищенные файлы. Архивы текущего образа и текущей конфигурации в результатах команды **dir** не видны. Используйте команду **show secure bootset,** чтобы проверить существование архива, как показано на рисунке.

Образ первичного загрузочного набора

Если маршрутизатор был взломан, восстановить первичный загрузочный набор можно из защищенного архива так, как показано на рисунке.

Шаг 1. Перезагрузите маршрутизатор, используя команду **reload** . При необходимости введите последовательность прерывания, чтобы войти в режим ROMmon.

Шаг 2. В режиме ROMmon введите команду **dir,** чтобы вывести содержимое устройства, содержащее защищенный файл загрузочного набора.

Шаг 3. Загрузите на маршрутизатор защищенный образ загрузочного набора с помощью команды **boot,** а затем укажите расположение флеш-памяти (например, flash0), двоеточие и имя файла из шага 2.

Образ первичного загрузочного набора

```
Router# reload
<Issue Break sequence, if necessary>
rommon 1 > dir flash0:
program load complete, entry point: 0x80803000, size: 0x1b340
Directory of flash0:

4       75551300  -rw-      c1900-universalk9-mz.SPA.154-3.M2.bin

<output omitted>

rommon 2 > boot flash0:c1900-universalk9-mz.SPA.154-3.M2.bin
<Router reboots with specified image>
Router> enable
Router# conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)# secure boot-config restore flash0:rescue-cfg
ios resilience:configuration successfully restored as flash0:rescue-cfg

Router(config)# end
Router# copy flash0:rescue-cfg running-config
Destination filename [running-config]?
%IOS image resilience is already active
%IOS configuration resilience is already active

2182 bytes copied in 0.248 secs (8798 bytes/sec)

R1#
```

Шаг 4. Войдите в режим глобальной конфигурации и восстановите защищенную конфигурацию в имени файла по вашему выбору с помощью команды **secure boot-config restore,** а затем укажите расположение флеш-памяти (например, flasho), двоеточие и выбранное вами имя файла.
На этом рисунке используется имя файла rescue-cfg.
Шаг 5. Выйдите из режима глобальной конфигурации и введите команду **copy,** чтобы скопировать восстановленный файл конфигурации в текущую конфигурацию.

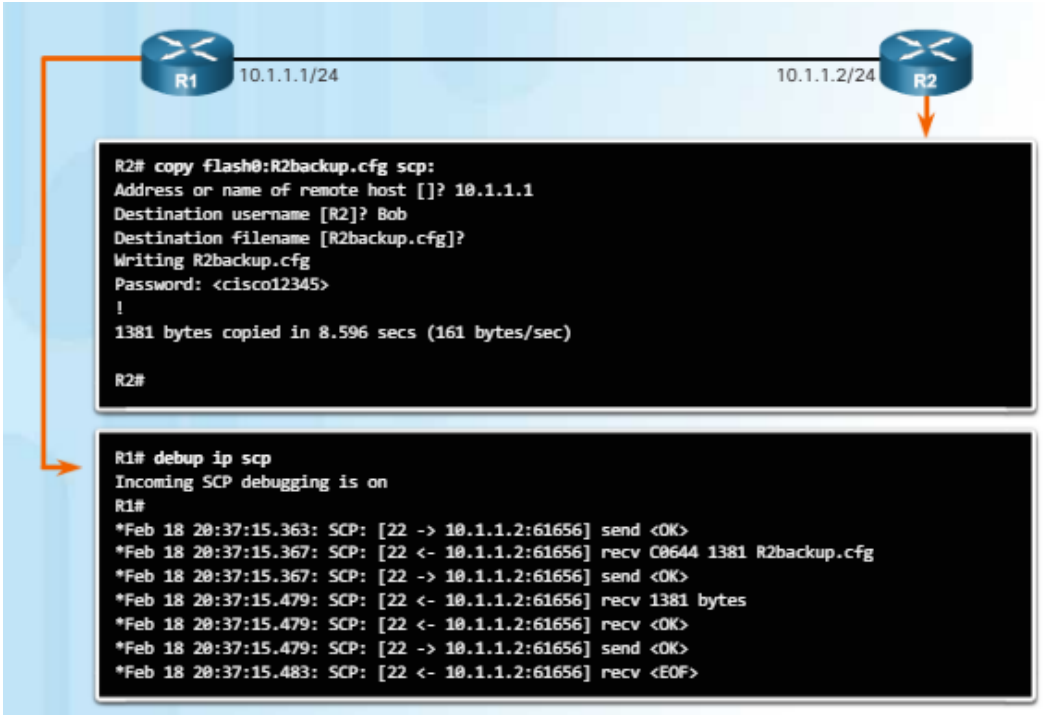
Настройка протокола безопасного копирования (Secure Copy)

Функция отказоустойчивости Cisco IOS обеспечивает способ защиты файлов конфигурации и образа IOS локально на устройстве. Используйте функцию защищенного протокола копирования (Secure Copy Protocol, SCP) для удаленного копирования этих файлов. SCP обеспечивает надежный и аутентифицированный способ копирования конфигурации маршрутизатора или файлов образа маршрутизатора в удаленное местоположение. SCP работает по протоколу SSH и требует, чтобы были сконфигурированы аутентификация и авторизация AAA, чтобы маршрутизатор смог определить, имеется ли у пользователя соответствующий уровень привилегий.

Настройка протокола безопасного копирования (Secure Copy)

Шаг 1. Сконфигурируйте доступ по SSH, если он еще не сконфигурирован.
Шаг 2. Для локальной аутентификации сконфигурируйте как минимум одного пользователя с уровнем привилегий 15.
Шаг 3. Включите AAA с помощью команды **aaa new-model** в режиме глобальной конфигурации.
Шаг 4. Используйте команду **aaa authentication login default local,** чтобы указать локальную базу данных, которая будет использоваться для аутентификации.
Шаг 5. Используйте команду **aaa authorization exec default local,** чтобы сконфигурировать авторизацию команды. В этом примере все локальные пользователи будут иметь доступ к командам ввода EXEC.
Шаг 6. Включите функциональность SCP со стороны сервера с помощью команды **ip scp server enable** .

Настройка протокола безопасного копирования (Secure Copy)



Маршрутизатор R1 теперь становится сервером SCP и будет использовать SSH-подключения, чтобы принимать защищенные копии, передаваемые от аутентифицированных и авторизированных пользователей. Передача может выполняться с любого клиента SCP, будь этот клиент другим маршрутизатором, коммутатором или рабочей станцией.
На рисунке показана передача по защищенному протоколу копирования (SCP) с маршрутизатора на маршрутизатор. На маршрутизаторе R2 используйте команду **copy** . Сначала укажите исходное местоположение файла (flasho:R2backup.cfg), а затем его место назначения (scp:). Ответьте на серию вопросов, чтобы установить подключение к серверу SCP на маршрутизаторе R1. На маршрутизаторе R1 можно ввести команду **debug ip scp,** чтобы посмотреть, как идет передача.

Основные сведения о системном журнале

Обеспечение возможности ведения журналов данных – это важная часть любой политики сетевой безопасности. Когда в сети происходят те или иные события, сетевые устройства задействуют доверенные механизмы для уведомления администратора и отправки ему подробных системных сообщений. Эти сообщения могут быть не очень важными или, наоборот, важными, а для их хранения, интерпретации и просмотра существует несколько способов. Администраторы могут получать уведомления обо всех сообщениях или только о сообщениях, которые могут оказать значительное влияние на сетевую инфраструктуру.

Наиболее распространенным способом доступа к системным сообщениям с сетевых устройств является использование протокола syslog, который описан в стандарте RFC 5424. Syslog использует порт 514 – Протокол пользовательских датаграмм (User Datagram Protocol, UDP) для отправки сообщений с уведомлениями о событиях по IP-сетям в коллекторы сообщений о событиях, как показано на рисунке. Протокол syslog поддерживают большинство сетевых устройств, включая маршрутизаторы, коммутаторы, серверы приложений, межсетевые экраны и другие сетевые устройства. Сервис ведения системного журнала (syslog) обеспечивает три основных функции:

- Возможность собирать информацию из системных журналов с целью мониторинга и устранения неисправностей
- Возможность выбирать тип информации из системных журналов, которую нужно собрать
- Возможность указывать место назначения для отправки захваченных syslog-сообщений

Использование системного журнала (Syslog)

На сетевых устройствах Cisco работа протокола syslog начинается с отправки системных сообщений и результатов отладки в локальный процесс ведения журналов, который является внутренним для этих устройств. То, каким образом в ходе процесса ведения журналов будет выполняться управление этими сообщениями и их вывод, зависит от конфигураций устройств. Например, syslog-сообщения могут отправляться по сети на внешний syslog-сервер. Эти сообщения могут быть получены и затем сформированы в разные отчеты для удобства восприятия.

Маршрутизаторы Cisco могут заносить в журнал информацию об изменениях конфигурации, нарушениях ACL, статусе интерфейса, использовании CPU и многих других типах событий. Например, команды **memory free low-watermark threshold io** и **memory free low-watermark processor** можно использовать для установки пороговых значений памяти. При уменьшении доступной свободной памяти ниже заданного порогового значения маршрутизатор будет отправлять уведомления (в килобайтах) на syslog-сервер. Когда размер доступной свободной памяти станет на 5% выше порогового значения, маршрутизатор снова отправит соответствующие уведомления.

Использование системного журнала (Syslog)

Маршрутизаторы Cisco могут заносить в журнал информацию об изменениях конфигурации, нарушениях ACL, статусе интерфейса и многих других типах событий. Маршрутизаторы Cisco можно сконфигурировать таким образом, чтобы они отправляли syslog-сообщения на несколько разных устройств:

Буфер журнала. Сообщения сохраняются в памяти маршрутизатора в течение какого-либо периода времени. Однако при перезагрузке маршрутизатора события стираются.
Консоль. Ведение журнала консоли включено по умолчанию. Syslog-сообщения отправляются на линию консоли, когда администратор активирует интерфейс.
Линии терминала. Активные сеансы ввода EXEC можно сконфигурировать так, чтобы получать сообщения журнала по любым линиям терминалов.
Сервер Syslog. Маршрутизаторы Cisco можно сконфигурировать таким образом, чтобы сообщения журнала пересылались во внешний syslog-сервис.

Syslog-сообщение

	Уровень	Ключевое слово	Описание	Определение
Самый высокий уровень	0	emergencies	Система неработоспособна	LOG_EMERG
	1	alerts	Требуется незамедлительное принятие мер	LOG_ALERT
	2	critical	Созданы критические условия	LOG_CRIT
	3	errors	Созданы условия для ошибки	LOG_ERR
	4	warnings	Созданы условия для предупреждения	LOG_WARNING
	5	notifications	Нормальное, но значащее состояние	LOG_NOTICE
	6	informational	Только информационные сообщения	LOG_INFO
Самый низкий уровень	7	debugging	Сообщения об отладке	LOG_DEBUG

Устройства Cisco выдают syslog-сообщения в ответ на события, которые происходят в сети. Каждое syslog-сообщение содержит информацию об уровне критичности и объекте.
Чем меньше числовое значение уровня, тем критичнее syslog-предупреждение.
Для уровней критичности сообщений можно указать, где должен отображаться каждый тип сообщений (например, на консоли или в других местах назначений). Полный список уровней syslog представлен на рисунке.

Syslog-сообщение

Уровень и имя Syslog	Определение	Пример
0 LOG_EMERG	Аварийное состояние – как правило, рассылается в широковещательном режиме всем пользователям.	Загрузка программного обеспечения Cisco IOS завершилась сбоем
1 LOG_ALERT	Состояние, которое необходимо немедленно устранить.	Слишком высокая температура
2 LOG_CRIT	Произошло критически важное событие, на которое необходимо обратить внимание.	Не удалось выделить память
3 LOG_ERR	Внутри устройства произошла ошибка.	Недопустимый размер памяти
4 LOG_WARNING	Создано условие, которое, возможно, необходимо проанализировать.	Сбой криптографической операции
5 LOG_NOTICE	Состояния, не являющиеся ошибкой, при которых может потребоваться выполнение специальных операций.	Изменение состояния интерфейса (работоспособен или неработоспособен)
6 LOG_INFO	Произошло обычное событие.	Пакет отклонен списком ACL
7 LOG_DEBUG	Сообщения, содержащие информацию, которая обычно используется только при отладке программы.	Недействительный тип пакета

Каждый уровень syslog имеет собственное значение, их описания приводятся на рисунке.
Уровни Syslog от ноля до четырех – это сообщения о программной и аппаратной функциональности. Критичность проблемы определяет фактически применяемый уровень syslog. Уровни Syslog 5 и 6 предназначены для уведомлений и информационных сообщений. Уровень Syslog 7 показывает, что сообщения генерируются в результате работы разных команд отладки.

Помимо информации об уровне критичности, syslog-сообщения также содержат информацию об объекте. Объекты Syslog – это сервисные идентификаторы, которые идентифицируют и категоризируют данные состояния системы с целью составления отчетов об ошибках и предоставления сообщений о событиях. Доступные возможности для объектов ведения журналов зависят от сетевого устройства.

Формат syslog-сообщений Cisco IOS

	Столбец 1	Столбец 2
1	`seq no`	отмечает сообщения в журнале порядковым номером, если задан параметр `service sequence-numbers`
2	`timestamp`	отображается, если настроен журнал `service timestamps`
3	`facility`	обозначает источник системного сообщения или его причину
4	`severity`	уровни 0–7
5	`MNEMONIC`	текстовая строка, которая уникально описывает сообщение
6	`description`	текстовая строка, содержащая подробную информацию о сообщаемом событии

Формат syslog-сообщений Cisco IOS

	Столбец 1	Столбец 2
1	`seq no`	отмечает сообщения в журнале порядковым номером, если задан параметр `service sequence-numbers`
2	`timestamp`	отображается, если настроен журнал `service timestamps`
3	`facility`	обозначает источник системного сообщения или его причину
4	`severity`	уровни 0–7
5	`MNEMONIC`	текстовая строка, которая уникально описывает сообщение
6	`description`	текстовая строка, содержащая подробную информацию о сообщаемом событии

Конфигурирование ведения системных журналов

```
Router(config)#
logging host [hostname | ip-address]
```

Параметр	Описание
hostname	Указывает имя хоста, который вы хотите использовать в качестве сервера syslog.
ip-address	Указывает IP-адрес узла, который вы хотите использовать в качестве сервера syslog.

Шаг 1. Настройте хост назначения для ведения журналов с помощью команды **logging host,**

Конфигурирование ведения системных журналов

```
Router(config)#
logging trap level
```

Параметр	Описание
level	Ограничивает ведение журналов сообщений на серверах syslog в соответствии с заданным уровнем и ниже. Можно ввести номер уровня (0–7) или имя уровня.

Шаг 2. (Необязательно) Установите уровень критичности ведения журналов (прерывание) с помощью команды **logging trap**

Конфигурирование ведения системных журналов

```
Router(config)#
logging source-interface interface-type interface-number
```

Параметр	Описание
interface-type	Указывает тип интерфейса.
interface-number	Указывает номер интерфейса (например, 0/1).

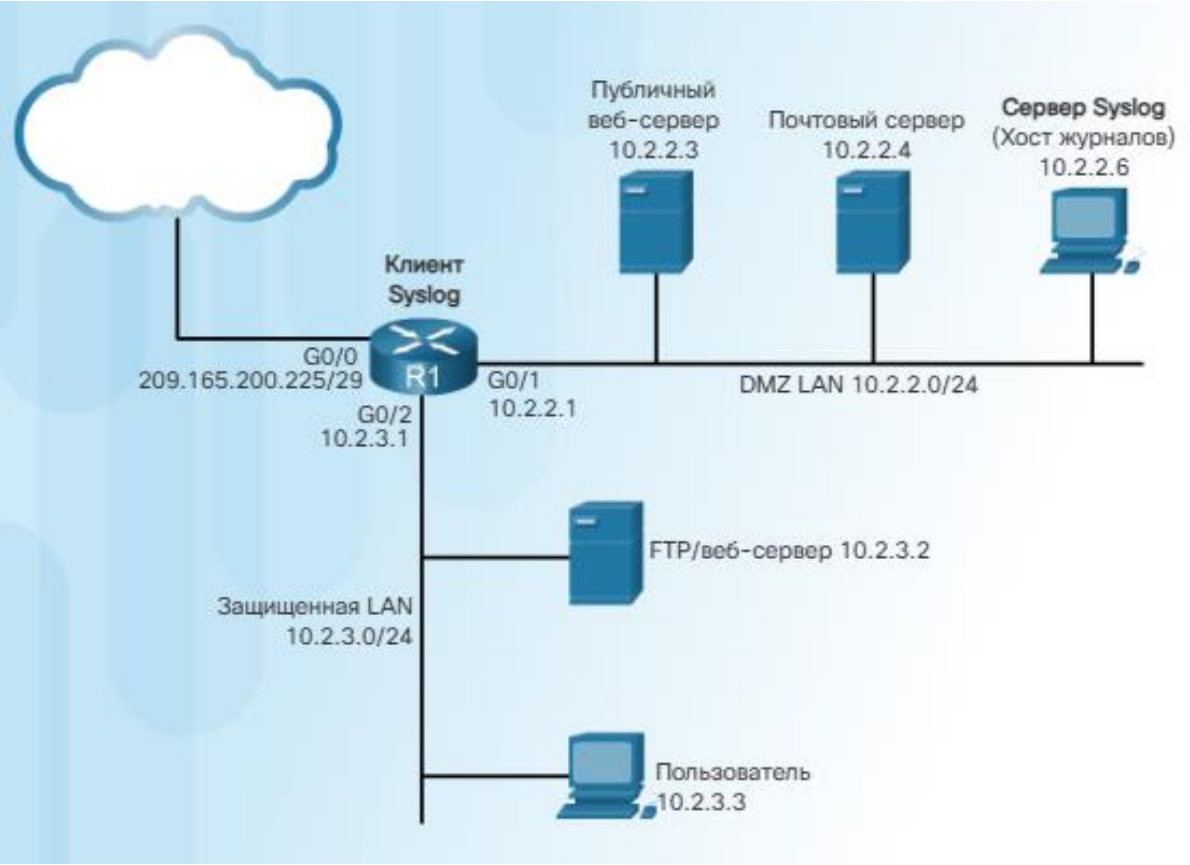
Шаг 3. Установите интерфейс источника с помощью команды **logging source-interface.** Эта команда показывает, что пакеты syslog содержат IPv4- или IPv6-адреса определенного интерфейса, независимо от того, через какой интерфейс выходит пакет из маршрутизатора.

Конфигурирование ведения системных журналов

```
Router(config)#
logging on
```

Шаг 4. Включите ведение журналов на всех активных адресах назначения с помощью команды **logging on**

Эталонная топология syslog



Эталонная топология syslog

```
R1(config)# logging host 10.2.2.6
000051: *Feb 19 12:45:32.491: %SYS-6-LOGGINGHOST_STARTSTOP:
Logging to host 10.2.2.6 port 514 started - CLI initiated
R1(config)# logging trap informational
R1(config)# logging source-interface gigabitethernet0/1
R1(config)# logging on
R1(config)# exit
000052: *Feb 19 12:46:07.151: %SYS-5-CONFIG_I: Configured from console by console
R1# show logging
Syslog logging: enabled (0 messages dropped, 2 messages rate-limited, 0 flushes,
0 overruns, xml disabled, filtering disabled)
utput omitted>

     Trap logging: level informational, 55 message lines logged
        Logging to 10.2.2.6  (udp port 514, audit disabled,
              link up),
              2 message lines logged,
              0 message lines rate-limited,
              0 message lines dropped-by-MD,
              xml disabled, sequence number disabled
              filtering disabled
        Logging Source-Interface:       VRF Name:
        GigabitEthernet0/1

Log Buffer (8192 bytes):
utput omitted>
```

Пример конфигурации syslog для маршрутизатора R1. Используйте команду **show logging,** чтобы посмотреть конфигурацию ведения журналов и буферные syslog-сообщения.

Второй учебный вопрос.
Назначение административных ролей

Специалисты ИТ-отдела в крупных организациях выполняют самые разные должностные обязанности. Уровень доступа для выполнения разных должностных обязанностей тоже должен быть разным (см. рисунки 1 и 2).

Настройка синтаксиса уровня привилегий

Настройка синтаксиса уровня привилегий

- Конфигурирование AAA
- Ввод команд **show**
- Настройка межсетевого экрана
- Настройка IDS/IPS
- Настройка NetFlow

Привилегии инженера сети WAN

Привилегии инженера сети WAN

- Настройка маршрутизации
- Настройка интерфейсов
- Ввод команд **show**

Второй учебный вопрос.
Назначение административных ролей

16 уровней привилегий

- Уровень 0: предопределен для доступа на уровне пользователя. Применяется редко, но содержит пять команд: **disable**, **enable**, **exit**, **help**, и **logout**.
- Уровень 1: уровень по умолчанию для входа в систему из командной строки маршрутизатора **Router>**. Пользователь не может вносить изменения и просматривать текущий файл конфигурации.
- Уровни 2–14: можно настраивать для привилегий на уровне пользователя. Команды с нижних уровней можно перемещать вверх на более высокий уровень, либо команды с верхних уровней можно перемещать вниз на более низкий уровень.
- Уровень 15: зарезервирован для привилегий в режиме enable (команда **enable**). Пользователи могут изменять конфигурации и просматривать файлы конфигурации.

Синтаксис уровня привилегий

Router(config)#

privilege *mode* [**level** *level* | **reset**] *command*

Команда	Описание
mode	Задает режим конфигурации. С помощью команды **privilege?** можно получить полный список режимов конфигурации маршрутизатора, доступных в маршрутизаторе.
level	(Необязательная) Позволяет установить уровень привилегий с помощью заданной команды.
level	(Необязательная) Уровень привилегий, связанный с командой. Можно указать до 16 уровней привилегий, используя числа от 0 до 15.
reset	(Необязательная) Сбрасывает уровень привилегий команды.
command	(Необязательная) Аргумент, который следует использовать, если нужно сбросить уровень привилегий.

ПО Cisco IOS предусматривает два способа предоставления доступа к инфраструктуре:

- уровень привилегий
- интерфейс командной строки (CLI) на основе ролей.

Оба способа позволяют определить, кому разрешается подключаться к устройству и что этот специалист может делать на этом устройстве. Доступ с использованием CLI на основе ролей обеспечивает большую точность и контроль.

По умолчанию интерфейс CLI программного обеспечения Cisco IOS имеет два уровня доступа к командам:

- **Пользовательский режим (уровень привилегий 1).** Обеспечивает самые низкие привилегии режима ввода и позволяет использовать только команды пользовательского уровня в командной строке маршрутизатора **router>**.
- **Привилегированный режим (уровень привилегий 15).** Включает все команды уровня **enable** в командной строке маршрутизатора **router#**.

Всего, как показано на рисунке 1, имеется 16 уровней привилегий. Чем выше уровень привилегий, тем больше прав доступа к маршрутизатору есть у пользователя. Команды, доступные на нижних уровнях привилегий, также выполняются на более высоких уровнях. Чтобы присвоить команды индивидуальному уровню привилегий, воспользуйтесь командой **privilege** в режиме глобальной конфигурации (рис. 2).

Второй учебный вопрос.
Назначение административных ролей


```
R1# conf t
R1(config)# !Level 5 and SUPPORT user configuration
R1(config)# privilege exec level 5 ping
R1(config)# enable algorithm-type scrypt secret level 5 cisco5
R1(config)# username SUPPORT privilege 5 algorithm-type scrypt secret cisco5
R1(config)# !Level 10 and JR-ADMIN user configuration
R1(config)# privilege exec level 10 reload
R1(config)# enable algorithm-type scrypt secret level 10 cisco10
R1(config)# username JR-ADMIN privilege 10 algorithm-type scrypt secret cisco10
R1(config)# !Level 15 and ADMIN user configuration
R1(config)# enable algorithm-type scrypt secret level 15 cisco123
R1(config)# username ADMIN privilege 15 algorithm-type scrypt secret cisco123
```

```
R1> enable 5
Password: <cisco5>
R1# show privilege
Current privilege level is 5
R1# ping 10.1.1.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.1.1.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/4 ms
R1# reload
Translating "reload"

% Bad IP address or host name
Translating "reload"

% Unknown command or computer name, or unable to find computer address
R1#
```

Чтобы сконфигурировать уровень привилегий с помощью определенных команд, используйте команду **privilege exec level** *level* **[***command***]**.

На рисунке показаны примеры трех разных уровней привилегий.

Уровень привилегий 5 разрешает доступ ко всем командам, доступным для предварительно заданного уровня 1, и команде **ping**.

Уровень привилегий 10 разрешает доступ ко всем командам, доступным для уровня 5, а также команде **reload**.

Уровень привилегий 15 предварительно задан, и его нет необходимости конфигурировать в явной форме. Этот уровень привилегий разрешает доступ ко всем командам, включая команды просмотра и изменения конфигурации.

Для присвоения паролей разным уровням привилегий используется два способа:

- Для пользователя, которому предоставлен специальный уровень привилегий, воспользуйтесь командой **username** *name* **privilege level secret** *password,* в режиме глобальной конфигурации.
- Для уровня привилегий используйте команду **enable secret level** *level password* в режиме глобальной конфигурации.

Обе команды, **username secret** и **enable secret,** сконфигурированы для шифрования типа 9. Используйте команду **username,** чтобы присвоить уровень привилегий определенному пользователю. Используйте команду **enable secret,** чтобы присвоить уровень привилегий определенному паролю в режиме ввода. Например, пользователю SUPPORT присвоен уровень привилегий 5 с паролем cisco5. Однако, как показано на рисунке 2, любой пользователь имеет доступ к уровню привилегий 5, если он знает, что пароль **enable secret** – это cisco5, а также с уровнем привилегий 5 нельзя перезагрузить маршрутизатор.

Второй учебный вопрос.
Назначение административных ролей


```
R1# enable 10
Password: <cisco10>
R1# show privilege
Current privilege level is 10
R1# ping 10.1.1.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.1.1.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/4 ms
R1# reload

System configuration has been modified. Save? [yes/no]: ^C

R1# show running-config
          ^
% Invalid input detected at '^' marker.
R1#
```

На рисунке пользователь активирует уровень привилегий 10, который предоставляет доступ к команде **reload** . Однако пользователи с уровнем привилегий 10 не могут просматривать текущую конфигурацию.

На рисунке пользователь активирует уровень привилегий 15, на котором предоставляется полный доступ для просмотра и изменения конфигурации, включая текущую конфигурацию.

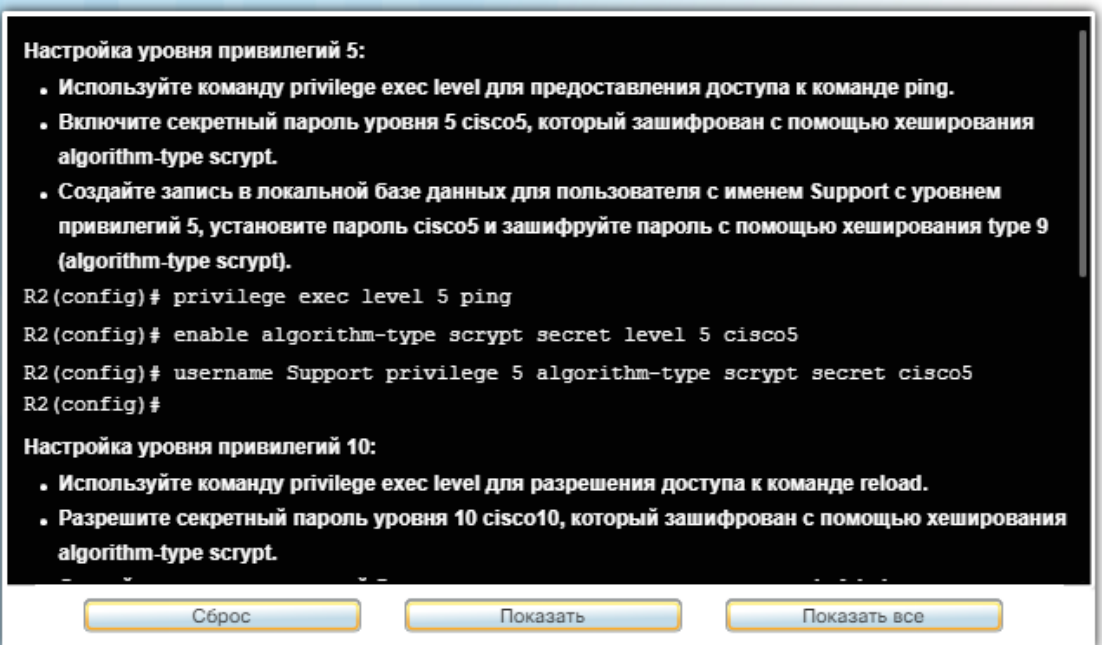
```
R1# enable 15
Password:
R1# show privilege
Current privilege level is 15
R1# show running-config
Building configuration...

Current configuration : 1979 bytes
!
! Last configuration change at 15:30:07 UTC Tue Feb 17 2015
!
version 15.4
<output omitted>
R1#
```

Второй учебный вопрос.
Назначение административных ролей

Использование уровней привилегий имеет свои ограничения:

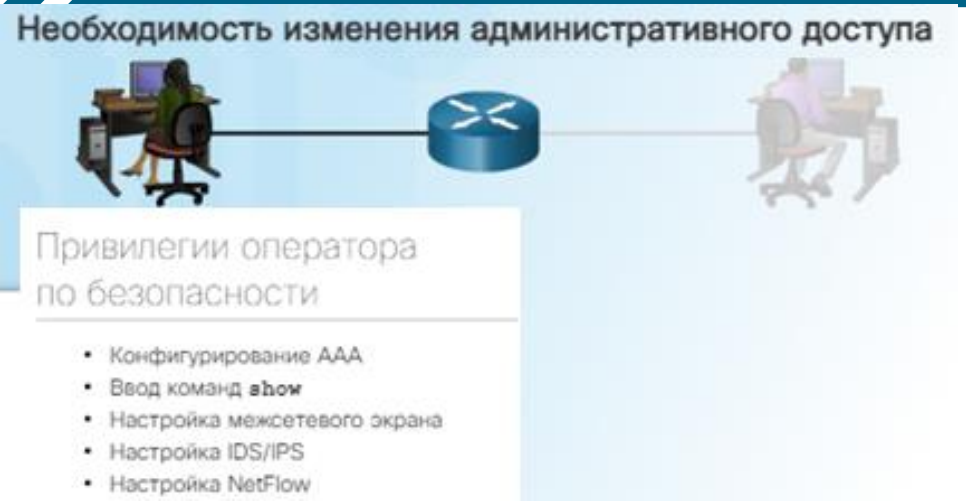
- Не обеспечивается управление доступом к определенным интерфейсам, портам, логическим интерфейсам и слотам на маршрутизаторе.
- Команды, доступные на нижних уровнях привилегий, всегда выполняются на более высоких уровнях.
- Команды, для которых специально задан более высокий уровень привилегий, недоступны для пользователей с более низкими привилегиями.
- Присвоение команды с несколькими ключевыми словами открывает доступ ко всем командам, использующим эти ключевые слова. Например, разрешив доступ к команде **show ip route,** вы открываете доступ пользователю ко всем командам **show** и **show ip**.



Если администратор должен создать учетную запись пользователя, который имеет доступ к большинству, но не всем командам, операторы привилегированного режима должны быть сконфигурированы для каждой команды, которая должна выполняться на уровне привилегий ниже 15-го.

Воспользуйтесь программой проверки синтаксиса (см. рисунок), чтобы сконфигурировать уровни привилегий на маршрутизаторе R2.

Второй учебный вопрос.
Назначение административных ролей



Доступ к CLI на основе ролей

Чтобы обеспечить больше гибкости, чем это позволяют уровни привилегий, в версии Cisco IOS 12.3(11)T компания Cisco внедрила функцию доступа CLI. Эта функция обеспечивает более точный, детальный доступ за счет контроля того, какие команды доступны определенным ролям, как показано на рисунках 1 и 2.

Доступ к CLI на основе ролей позволяет сетевому администратору создавать разные представления конфигураций маршрутизатора для разных пользователей. Каждое представление определяет те команды CLI, которые доступны для конкретного пользователя.

Второй учебный вопрос.
Назначение административных ролей

Интерфейс CLI на основе ролей представляет три типа представлений, определяющих доступность команд:

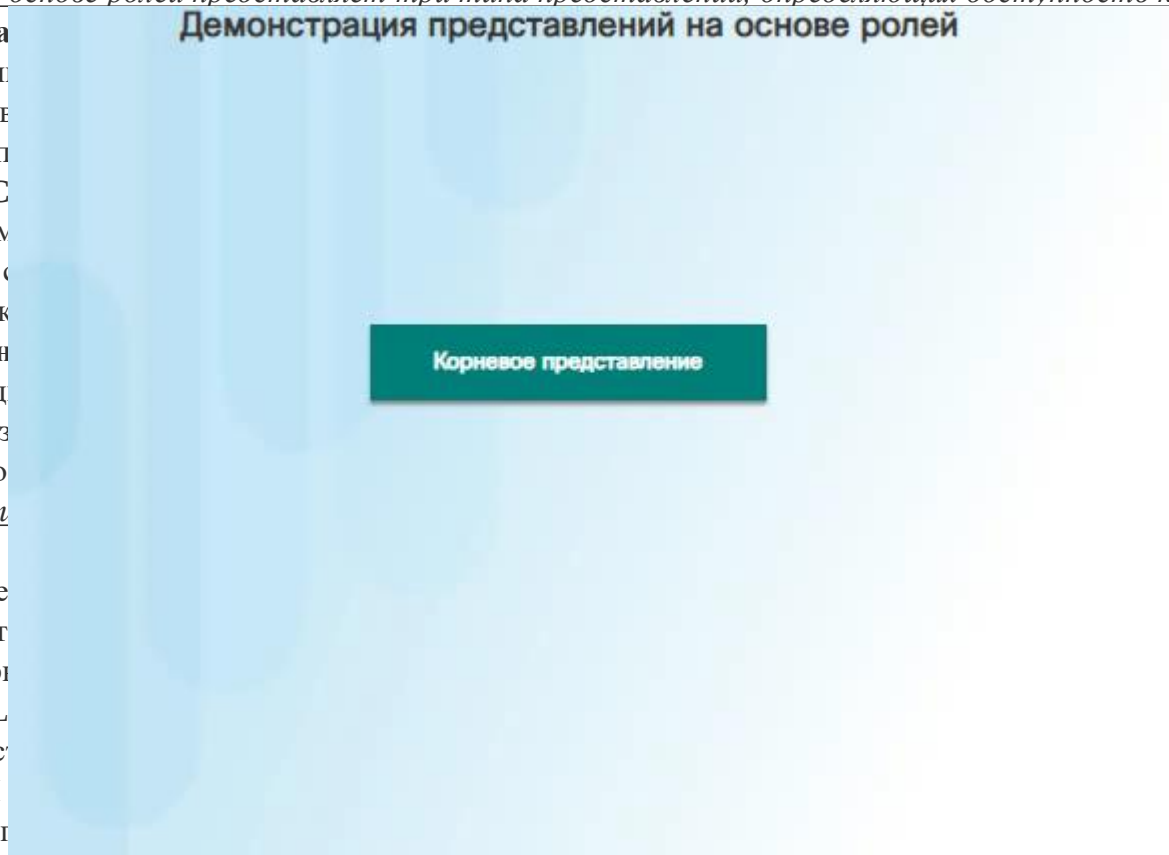
Корневое предстаатор должен находиться в корневом представлени уровнем привилегий 15. Однако корневое представ ого представления может сконфигурировать новое п

Представление Сот уровней привилегий, представление CLI не им ставлению должны быть присвоены все команды, о другого представления. Кроме того, одни и те же к

Суперпредставлен Администраторы могут определять, какие команд х сетевой администратор может присваивать польз того чтобы присваивать по одному представлению ением CLI.

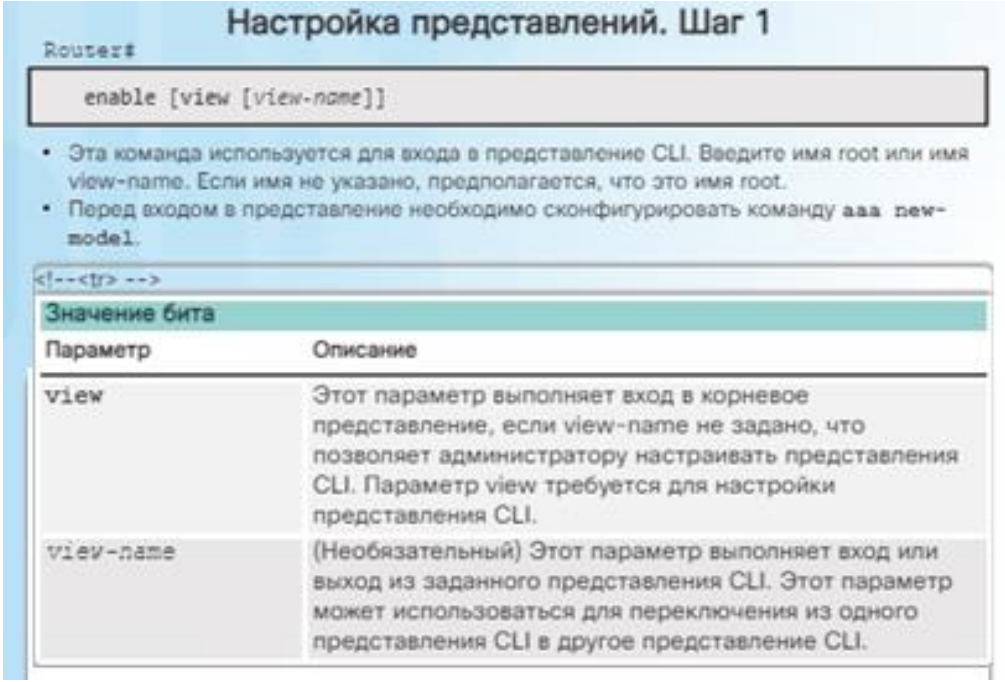
Суперпредставлени

- Одно представление
- Для суперпредставле редставление CLI, а затем добавлять это предст
- Пользователи, которы игурированы для любого из представлений CL
- Каждое суперпредс ерпредставлениями или с представления CLI
- При удалении суперп CLI по-прежнему можно присваивать другому суперпредставлению.



Конфигурирование представлений команд на основе ролей

Прежде чем администратор сможет создать представление, необходимо активировать AAA с помощью команды **aaa new-model** . Чтобы сконфигурировать и отредактировать представления, администратор должен войти в корневое представление с помощью команды **enable view** в привилегированном режиме. Синтаксис команды **enable view** показан на рисунке. Можно также использовать команду **enable view root** . При появлении приглашения введите пароль **enable secret** .



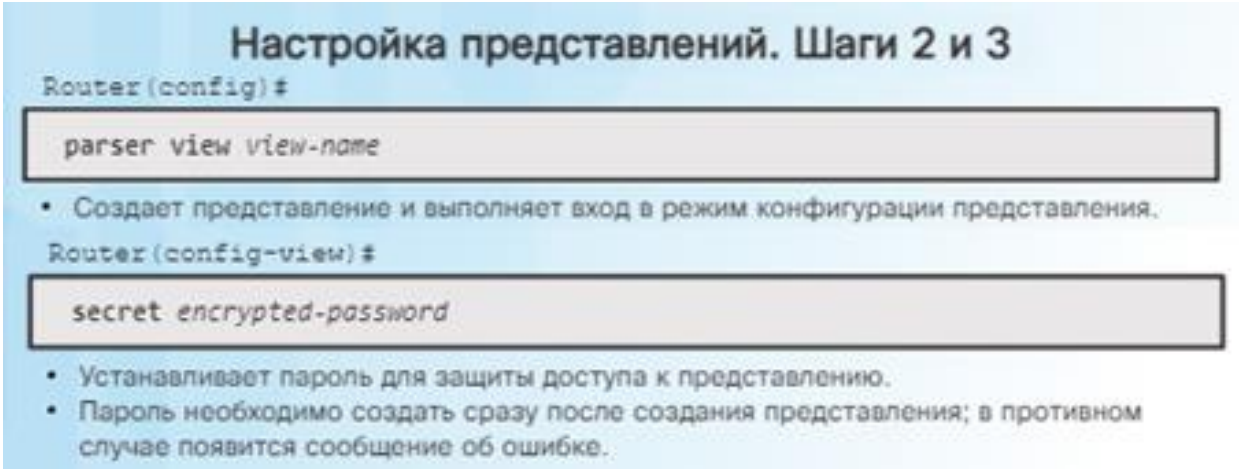
Второй учебный вопрос.
Назначение административных ролей

Для создания и управления представлением необходимо выполнить пять шагов.

Шаг 1. Включите AAA с помощью команды **aaa new-model** в режиме глобальной конфигурации. Выйдите из корневого представления и войдите в него с помощью команды **enable view** .

Шаг 2. Создайте представление с помощью команды **parser view** *view-name* в режиме глобальной конфигурации. Таким образом включится режим конфигурации представлений. Исключая корневое представление, действует максимальное ограничение – всего 15 представлений.

Шаг 3. Присвойте представлению секретный пароль с помощью команды **secret** *encrypted-password* в режиме конфигурации представлений. На рисунке показан синтаксис для команд **parser view** и **secret** .



Второй учебный вопрос.
Назначение административных ролей

Настройка представлений. Шаг 4

```
Router(config-view)#
commands parser mode {include | include-exclusive | exclude} [all]
[interface interface-name | command]
```

- Добавляет в представление команды или интерфейсы.

<!--<tr> -->

Значение бита	
Команда	**Описание**
commands	Добавляет в представление команды или интерфейсы.
parser-mode	Режим, в котором существует указанная команда; например, режим ввода EXEC.
include	Добавляет в представление команду или интерфейс и позволяет добавлять в другие представления ту же команду или интерфейс.
include-exclusive	Добавляет в представление команду или интерфейс и исключает эту же команду или интерфейс из добавления во все другие представления.
exclude	Исключает команду или интерфейс из представления.
all	«Подстановочный знак», который обеспечивает подстановку в представление каждой команды в заданном режиме конфигурации, которая начинается с того же самого ключевого слова, или

Шаг 4. Присвойте команды выбранному представлению с помощью команды **commands** *parser-mode* в режиме конфигурации представлений. На рисунке показан синтаксис для команд **command**.

Шаг 5. Выйдите из режима конфигурации представления, введя команду **exit**

Второй учебный вопрос.
Назначение административных ролей

Настройка представлений

```
R1(config)# aaa new-model
R1(config)# parser view SHOWVIEW
R1(config-view)# secret ?
  0     Specifies an UNENCRYPTED password will follow
  5     Specifies an ENCRYPTED secret will follow
  LINE  The UNENCRYPTED (cleartext) view secret string
R1(config-view)# secret cisco
R1(config-view)# commands exec include show
R1(config-view)# exit
R1(config)# parser view VERIFYVIEW
R1(config-view)# commands exec include ping
% Password not set for the view VERIFYVIEW

R1(config-view)# secret cisco5
R1(config-view)# commands exec include ping
R1(config-view)# exit
R1(config)# parser view REBOOTVIEW
R1(config-view)# secret cisco10
R1(config-view)# commands exec include reload
R1(config-view)# exit
R1(config)#
```

На рисунке представлен пример конфигурирования трех представлений. Обращаем внимание, что в примере команда **secret** поддерживает только шифрование MD5 (тип 5). Кроме того, заметьте, что когда команда добавлялась в представление до присвоения пароля, возникала ошибка.

На следующем рисунке показаны сконфигурированные представления в текущей конфигурации.

Проверка представлений в текущей конфигурации

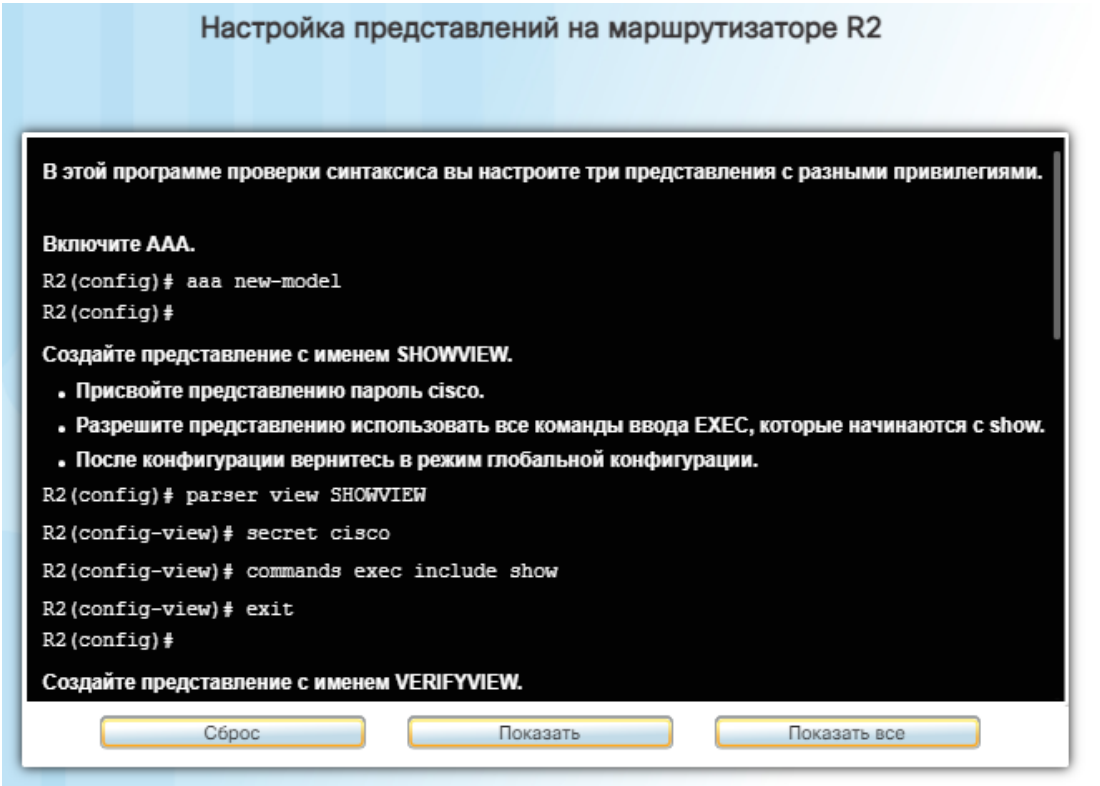
```
R1# show running-config

<output omitted>


parser view SHOWVIEW
 secret 5 $1$GL2J$8njLecwTaLAc0UuWo1/Fv0
 commands exec include show
!
parser view VERIFYVIEW
 secret 5 $1$d08J$1zOYSI4WainGxkn0Hu7lP1
 commands exec include ping
!
parser view REBOOTVIEW
 secret 5 $1$L7lZ$1Jtn5IhP43fVE7SVoF1pt.
 commands exec include reload
!
```

Второй учебный вопрос.
Назначение административных ролей

Воспользуйтесь программой проверки синтаксиса, чтобы сконфигурировать представления на маршрутизаторе R2.



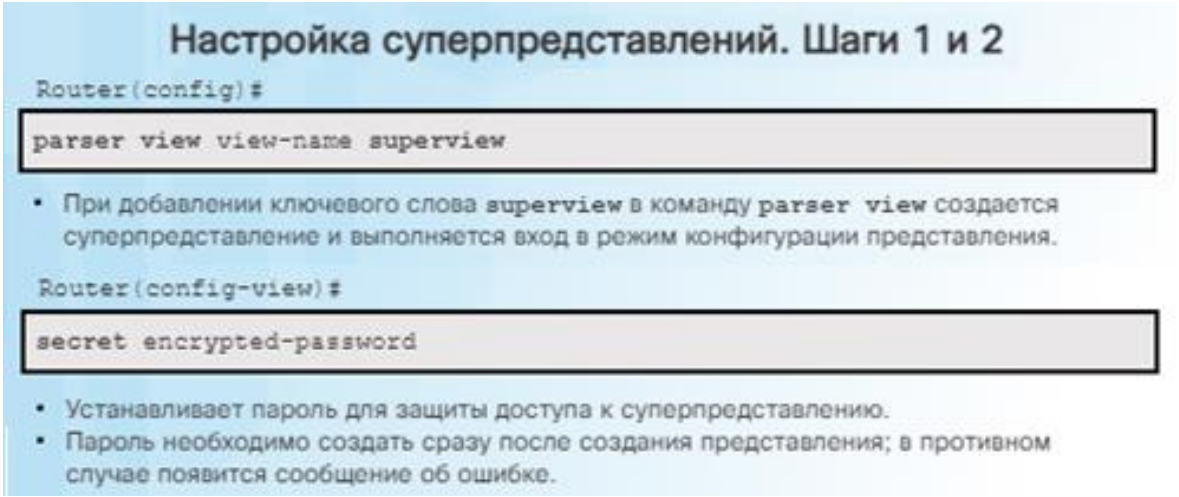
Конфигурирование суперпредставлений команд CLI на основе ролей

Шаги по конфигурированию суперпредставления в целом практически не отличаются от шагов для конфигурирования представления CLI, за исключением того, что команда **view** *view-name* используется для присвоения команд суперпредставлению. Чтобы сконфигурировать суперпредставление, администратор должен находиться в корневом представлении. Чтобы подтвердить, что используется корневое представление, воспользуйтесь или командой **enable view,** или командой **enable view root** . При появлении приглашения введите пароль **secret** .

Для создания и управления суперпредставлением необходимо выполнить четыре шага.

Шаг 1. Создайте представление с помощью команды **parser view** *view-name* **superview** и войдите в режим конфигурации суперпредставления.

Шаг 2. Присвойте представлению секретный пароль с помощью команды **secret** *encrypted-password* . На рисунке показан синтаксис для команд **parser view superview** и **secret** .



Конфигурирование суперпредставлений. Шаг 3

```
Router(config-view)#
view view-name
```

- Добавляет представление CLI в суперпредставление.
- Можно добавить несколько представлений.
- Представления могут использоваться суперпредставлениями совместно.

Шаг 3. Присвойте существующее представление помощью команды **view** *view-name* в режиме онфигурации представлений. На рисунке показан интаксис для команды view.

Шаг 4. Выйдите из режима конфигурации суперпредставления, введя команду **exit** . Суперпредставлению можно присваивать несколько представлений, и эти представления могут совместно использоваться суперпредставлениями.

На следующем рисунке представлен пример конфигурирования трех суперпредставлений: USER, SUPPORT и JR-ADMIN.

Пример настройки суперпредставлений

```
R1(config)# parser view USER superview
R1(config-view)# secret cisco
R1(config-view)# view SHOWVIEW
R1(config-view)# exit
R1(config)#
R1(config)# parser view SUPPORT superview
R1(config-view)# secret cisco1
R1(config-view)# view SHOWVIE
% Invalid view name SHOWVIE

R1(config-view)# view SHOWVIEW
R1(config-view)# view VERIFYVIEW
R1(config-view)# exit
R1(config)#
R1(config)# parser view JR-ADMIN superview
R1(config-view)# secret cisco2
R1(config-view)# view SHOWVIEW
R1(config-view)# view VERIFYVIEW
R1(config-view)# view REBOOTVIEW
R1(config-view)# exit
R1(config)#
```

Второй учебный вопрос.
Назначение административных ролей

Проверка суперпредставлений в текущей конфигурации

```
R1# show running-config

<output omitted>
!
parser view SUPPORT superview
 secret 5 $1$Vp1O$BBB1N68Z2ekr/aLH1edts.
 view SHOWVIEW
 view VERIFYVIEW
!
parser view USER superview
 secret 5 $1$E4k5$ukHyfYP7dHOC48N8pxm4s/
 view SHOWVIEW
!
parser view JR-ADMIN superview
 secret 5 $1$8kx2$rbAe/ji220OmQ1yw.568g0
 view SHOWVIEW
 view VERIFYVIEW
 view REBOOTVIEW
!
```

На рисунке показаны сконфигурированные суперпредставления в текущей конфигурации.

Для доступа к существующим представлениям введите команду **enable view** *view-name* в пользовательском режиме и

Настройка суперпредставлений на маршрутизаторе R2

Создайте суперпредставление с именем USER.

- **Присвойте суперпредставлению пароль cisco.**
- **Присвойте ему представление SHOWVIEW.**
- **После конфигурации вернитесь в режим глобальной конфигурации.**

```
R2(config)# parser view USER superview
R2(config-view)# secret cisco
R2(config-view)# view SHOWVIEW
R2(config-view)# exit
R2(config)#
```

Создайте суперпредставление с именем SUPPORT.

- **Присвойте суперпредставлению пароль cisco1.**
- **Присвойте ему представление SHOWVIEW.**
- **Присвойте ему представление VERIFYVIEW.**
- **После конфигурации вернитесь в режим глобальной конфигурации.**

```
R2(config)# parser view SUPPORT superview
```

Сброс | Показать | Показать все

Воспользуйтесь программой проверки синтаксиса, чтобы сконфигурировать суперпредставления на маршрутизаторе R2.

Второй учебный вопрос.
Назначение административных ролей

```
R1# enable view USER
Password: <cisco1>

R1# ?
Exec commands:
  <0-0>/<0-4>  Enter card slot/sublot number
  do-exec      Mode-independent "do-exec" prefix support
  enable       Turn on privileged commands
  exit         Exit from the EXEC
  show         Show running system information

R1# show ?
  banner      Display banner information
  flash0:     display information about flash0: file system
  flash1:     display information about flash1: file system
  flash:      display information about flash: file system
  parser      Display parser information
  usbflash0:  display information about usbflash0: file system

R1# show
```

Проверка представлений команд CLI на основе ролей

Для проверки представления используйте команду **enable view** . Введите имя представления для проверки и укажите пароль для входа в это представление. Используйте команду вопросительный знак (**?**), чтобы проверить, что доступные в этом представлении команды – правильные.

На рисунке представлено суперпредставление **USER** и перечислены команды, доступные в этом представлении.

```
R1# enable view SUPPORT
Password: <cisco1>

R1# ?
Exec commands:
  <0-0>/<0-4>  Enter card slot/sublot number
  do-exec      Mode-independent "do-exec" prefix support
  enable       Turn on privileged commands
  exit         Exit from the EXEC
  ping         Send echo messages
  show         Show running system information

R1#
```

На рисунке представлено суперпредставление **SUPPORT** и перечислены команды, доступные в этом представлении.

```
R1# enable view JR-ADMIN
Password:

R1# ?
Exec commands:
  <0-0>/<0-4>  Enter card slot/sublot number
  do-exec      Mode-independent "do-exec" prefix support
  enable       Turn on privileged commands
  exit         Exit from the EXEC
  ping         Send echo messages
  reload       Halt and perform a cold restart
  show         Show running system information

R1#
```

На рисунке представлено суперпредставление **JR-ADMIN** и перечислены команды, доступные в этом представлении.

Если не указать представление для команды **enable view**, как показано на рисунке, можно войти из корневого представления. В корневом представлении воспользуйтесь командой **show parser view all,** чтобы посмотреть сводку по всем представлениям. Обращаем внимание, что звездочкой обозначены суперпредставления.

```
R1# show parser view
Current view is 'JR-ADMIN'

R1# enable view
Password:

R1# show parser view
Current view is 'root'

R1# show parser view all
Views/SuperViews Present in System:
 SHOWVIEW
 VERIFYVIEW
 REBOOTVIEW
 USER *

 SUPPORT *

 JR-ADMIN *

-------(*) represent superview-------
R1#
```

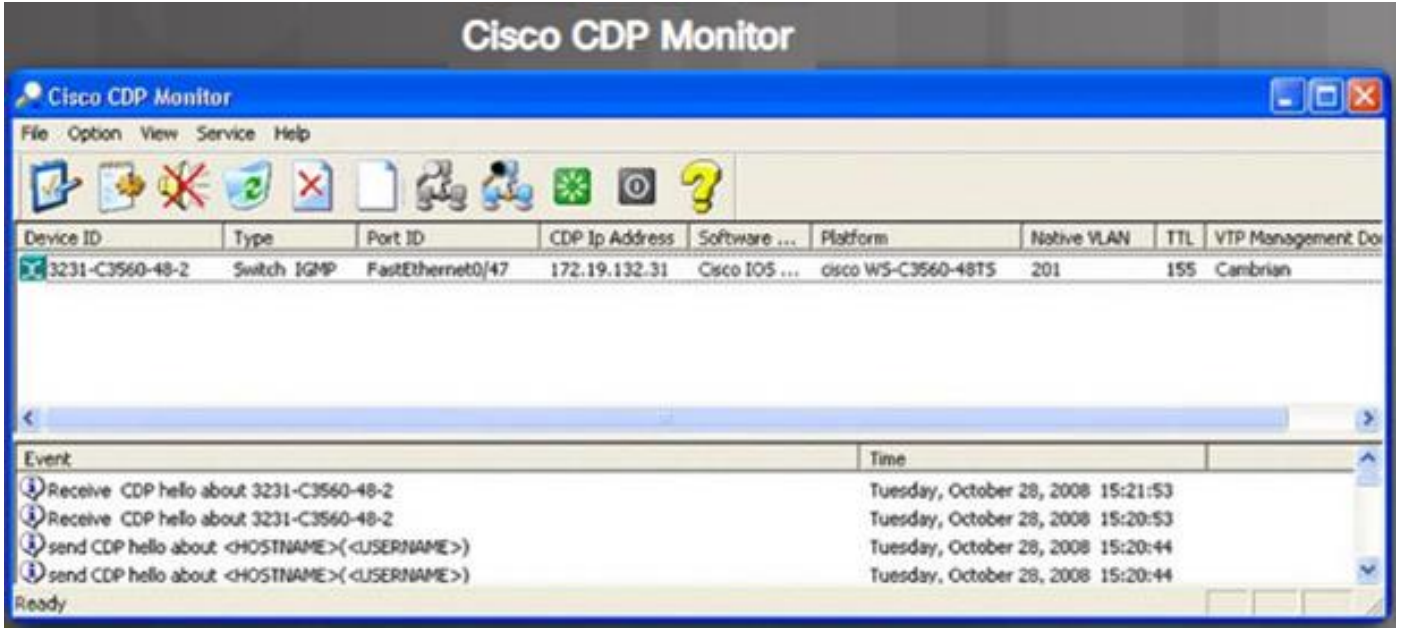
Сравнение информации CDP и LLDP

Маршрутизатор R1 и коммутатор S1 настроены с помощью команды режима глобальной конфигурации `lldp run`. CDP включен по умолчанию.

```
R1(config)# lldp run
R1(config)# end
R1# show cdp neighbors detail
-------------------------
Device ID: S1
Entry address(es):
  IP address: 192.168.1.254
Platform: cisco WS-C2960-24TT-L,  Capabilities: Switch IGMP
Interface: GigabitEthernet0/1,  Port ID (outgoing port): FastEthernet0/5
Holdtime : 164 sec

Version :
Cisco IOS Software, C2960 Software (C2960-LANBASEK9-M), Version 15.0(2)SE7,
RELEASE SOFTWARE (fc1)
        <output omitted>
R1# show lldp neighbors detail
------------------------------------------------
Local Intf: Gi0/1
```

На рисунке маршрутизатор R1 и коммутатор S1 оба сконфигурированы по протоколу LLDP с помощью команды **lldp run** режима глобальной конфигурации. На обоих устройствах по умолчанию запущен протокол CDP. Результат команд **show cdp neighbors detail** и **show lldp neighbors detail** показывает сведения об адресе устройства, его платформе и операционной системе.



К сожалению, злоумышленникам не нужно иметь устройства со включенными протоколами CDP или LLDP, чтобы получить эту конфиденциальную информацию. Для получения такой информации можно воспользоваться общедоступным ПО, например программой Cisco CDP Monitor, показанной на рисунке.

Задача протоколов CDP и LLDP – облегчить администраторам процесс обнаружения других устройств в сети и устранения их неисправностей. Однако из-за ограничений, связанных с безопасностью, такими протоколами обнаружения следует пользоваться очень осторожно. Несмотря на то что это очень полезный инструмент, он не должен использоваться в любом месте сети. Так, например, эту функцию рекомендуется отключать на устройствах периметра.

Состояние сервисов по умолчанию

Функция	Значение по умолчанию
Cisco Discovery Protocol (CDP)	Enabled
Link Layer Discovery Protocol (LLDP)	Disabled
Configuration autoloading	Disabled
FTP-сервер	Disabled
TFTP-сервер	Disabled
Сервис Network Time Protocol (NTP)	Disabled
Сервис Packet assembler/disassembler (PAD)	Enabled
Второстепенные сервисы TCP и User Datagram Protocol (UDP)	Enabled в версии 11.3 и более поздних версиях
Сервис Maintenance Operation Protocol (MOP)	Enabled в большинстве интерфейсов Ethernet
Simple Network Management Protocol (SNMP)	Enabled
Конфигурация или мониторинг HTTP или HTTPS	Настройка зависит от устройства Cisco.
Domain Name System (DNS)	Enabled
Internet Control Message Protocol (ICMP) redirects	Enabled
IP source routing	Enabled
Служба Finger	Enabled
ICMP unreachable notifications	Enabled
ICMP mask reply	Disabled

Настройки для протоколов и сервисов

Злоумышленники выбирают сервисы и протоколы, которые делают сеть более уязвимой перед вредоносным воздействием.

В зависимости от требований организации к безопасности многие из этих функций следует отключить или ограничить их возможности. Эти функции включают в себя целый ряд возможностей – от протоколов CDP и LLDP до глобально доступных протоколов, например ICMP, и других инструментов сканирования.

На рисунке представлены функции и настройки по умолчанию для протоколов и сервисов.

Третий учебный вопрос.
Автоматические функции обеспечения безопасности

Рекомендуемые настройки безопасности для протоколов и сервисов

Domain Name System (DNS)	Отключите, когда функция не нужна. Если сервис DNS-поиска нужен, убедитесь, что вы устанавливаете адрес DNS-сервера явным образом.
Internet Control Message Protocol (ICMP) redirects	Отключите, когда функция не нужна.
IP source routing	Выключите этот сервис, когда он не нужен.
Служба Finger	Выключите этот сервис, когда он не нужен.
ICMP unreachable notifications	Выключите на интерфейсах с недоверенными сетями.
ICMP mask reply	Выключите на интерфейсах с недоверенными сетями.
Сервис IP identification	Сервис нужно явно выключить.
TCP keepalives	Необходимо включить глобально, чтобы управлять TCP-соединениями и предотвращать атаки «отказ в обслуживании» (DoS) определенного вида. Сервис включен в выпусках ПО Cisco IOS до выпуска Cisco IOS 12.0 и выключен в выпуске Cisco IOS 12.0 и выше. Выключите этот сервис, когда он не нужен.
Gratuitous ARP (GARP)	Выключите протокол Gratuitous ARP на каждом интерфейсе маршрутизатора, если этот сервис не нужен.
Proxy ARP	Выключите этот сервис в каждом интерфейсе, если маршрутизатор не используется как мост

На рисунке представлены рекомендуемые настройки безопасности для протоколов и сервисов.

Для обеспечения безопасности устройств необходимо соблюдать несколько важных рекомендаций:

- Отключайте ненужные порты и интерфейсы.
- Отключайте и ограничивайте общедоступные конфигурируемые сервисы управления, например протокол SNMP.
- Отключайте протоколы сканирования сети, например ICMP. Обеспечьте защиту терминального доступа.
- Отключайте самообращенные (gratuitous) и прокси-запросы протоколов разрешения адресов (Address Resolution Protocol, ARP).
- Отключайте команду **IP-directed broadcast.**

Третий учебный вопрос.
Автоматические функции обеспечения безопасности

Ввод функции Cisco AutoSecure

```
R1# auto secure
  --- AutoSecure Configuration ---

*** AutoSecure configuration enhances the security
 of the router but it will not make router
 absolutely secure from all security attacks ***

All the configuration done as part of AutoSecure
will be shown here. For more details of why and
how this configuration is useful, and any possible
side effects, please refer to Cisco documentation of
AutoSecure.

At any prompt you may enter '?' for help.
Use ctrl-c to abort this session at any prompt.

Gathering information about the router for
AutoSecure

Is this router connected to internet? [no]:yes
```

Cisco AutoSecure – функция, впервые представленная в версии IOS12.3, связана с интерфейсом CLI и выполняет скрипт. AutoSecure сначала представляет рекомендации для устранения уязвимостей безопасности, а затем модифицирует конфигурацию защиты маршрутизатора, как показано на рисунке.

Функция AutoSecure может блокировать функции плоскости менеджмента и сервисы плоскости передачи данных, а также функции маршрутизатора. Существует несколько сервисов и функций плоскости менеджмента:

- Защита небольших серверов BOOTP, CDP, FTP, TFTP, PAD, UDP и TCP; MOP, ICMP (redirects, mask-replies), маршрутизация по IP-источнику, Finger, шифрование паролей, TCP keepalives, самообращенные запросы (gratuitous ARP), прокси-ARP и directed broadcast
- Официальное уведомление с использованием баннера
- Функции защиты пароля и входа в систему
- Защита NTP
- Защита доступа SSH
- Сервисы перехвата TCP.

Функция AutoSecure обеспечивает возможность использования следующих трех сервисов и функций плоскости передачи данных:

- Cisco Express Forwarding (CEF)
- Фильтрация трафика с помощью ACL-списков
- Проверка межсетевого экрана Cisco IOS на наличие общих протоколов

AutoSecure часто используется на местах для формирования базовой политики безопасности на новом маршрутизаторе. Функции затем можно изменять в соответствии с требованиями политики безопасности организации.

Использование функции Cisco AutoSecure

Используйте команду **auto secure,** чтобы включить настройку функции Cisco AutoSecure. Эта настройка может быть как интерактивной, так и не интерактивной.

На рис. 1 показан синтаксис для команды **auto secure**.

На рис. 2 показаны параметры команды.

На рис. 3 приведено описание параметров команды.

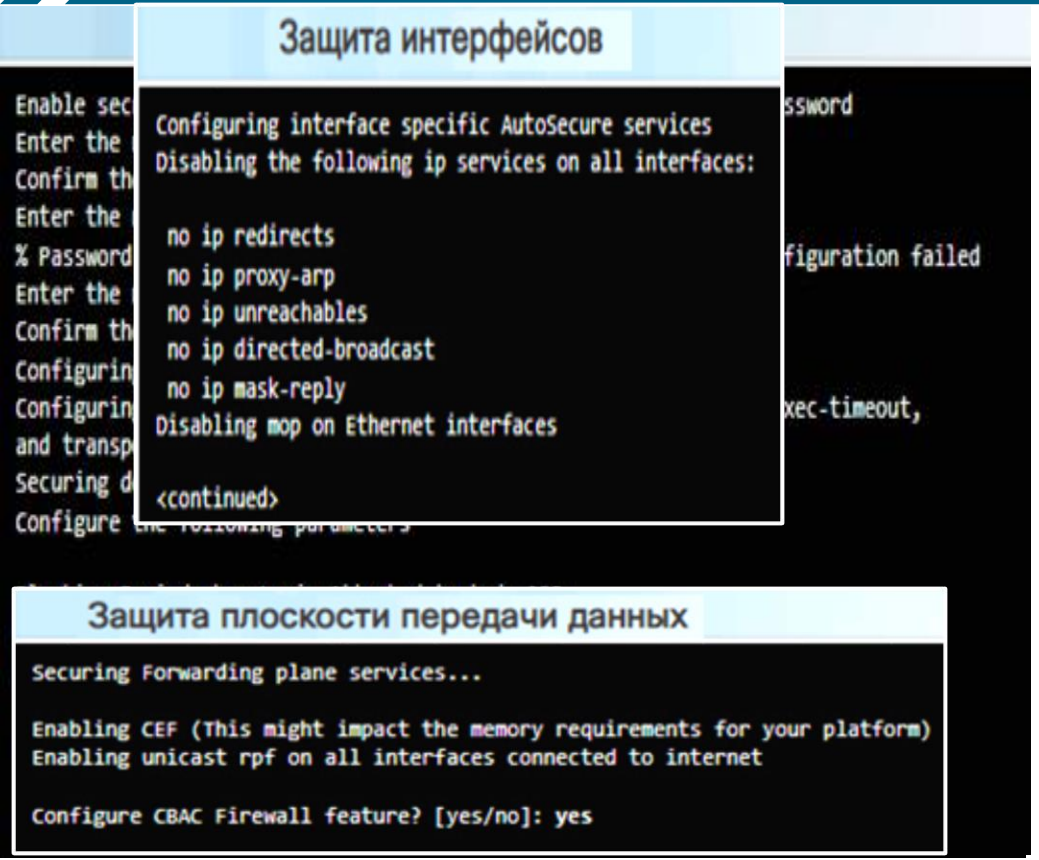
Описание параметров `auto secure`

Параметр	Описание
`no-interact`	(Необязательный) Пользователю не будет предлагаться конфигурация в интерактивном режиме. Никакие параметры интерактивного диалога настраиваться не будут, включая имена пользователей или пароли.
`full`	(Необязательный) Пользователю будет предложено ответить на все интерактивные вопросы. Такая настройка действует по умолчанию.
`forwarding`	(Необязательный) Будет защищена только плоскость передачи данных.
`management`	(Необязательный) Будет защищена только плоскость менеджмента.
`ntp`	(Необязательный) Указывает конфигурацию функции NTP в AutoSecure CLI.
`login`	(Необязательный) Указывает конфигурацию функции Login в AutoSecure CLI.
`ssh`	(Необязательный) Указывает конфигурацию функции SSH в AutoSecure CLI.
`firewall`	(Необязательный) Указывает конфигурацию функции Firewall в AutoSecure CLI.
`tcp-intercept`	(Необязательный) Указывает конфигурацию функции TCP-Intercept в AutoSecure CLI.

В интерактивном режиме маршрутизатор запрашивает варианты для включения и отключения сервисов и других функций безопасности. Это режим по умолчанию, но он также может быть сконфигурирован с использованием команды **auto secure full**.

Неинтерактивный режим конфигурируется с помощью команды **auto secure no-interact**. Функция Cisco AutoSecure при этом выполняется автоматически с рекомендуемыми Cisco настройками по умолчанию. Можно также вводить команду **auto secure** с ключевыми словами, чтобы сконфигурировать отдельные компоненты, например плоскости менеджмента (ключевое слово **management**) и плоскость передачи данных (ключевое слово **forwarding**).

Третий учебный вопрос.
Автоматические функции обеспечения безопасности



При вводе команды **auto secure** мастер интерфейса командной строки CLI проводит администратора по пути конфигурации устройства. Необходимы входные данные от пользователя.

1. Введена команда **auto secure** . На маршрутизаторе отображается приветственное сообщение мастера конфигурации **AutoSecure**, как показано на рис. 1.

2. Мастер собирает информацию о внешних интерфейсах, как показано на рис. 2.

3. Функция **AutoSecure** обеспечивает безопасность плоскости менеджмента за счет отключения ненужных сервисов, как показано на рис. 3.

4. AutoSecure запрашивает баннер, как показано на рис. 4.

5. AutoSecure запрашивает пароли и включает функции пароля и входа в систему, как показано на рис. 5.

6. Интерфейсы защищены, как показано на рис. 6.

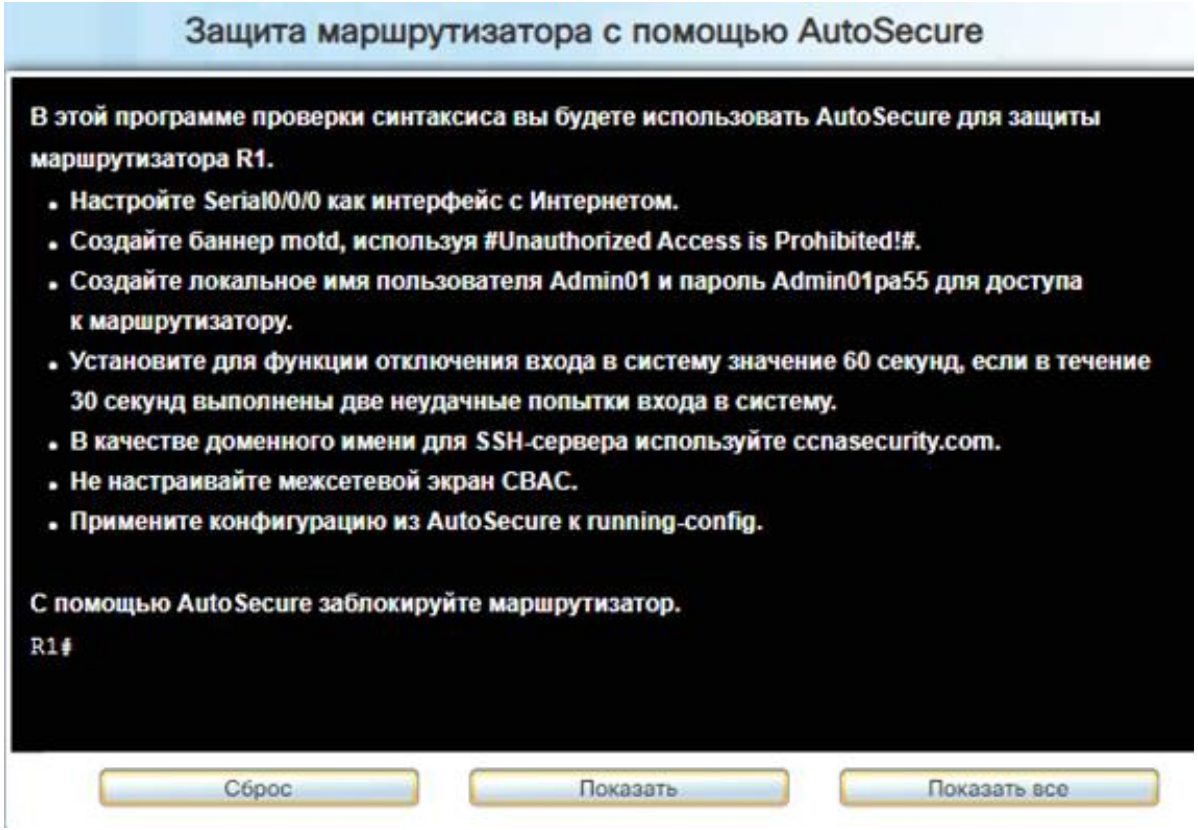
7. Плоскость передачи данных защищена, как показано на рис. 7.

По завершению работы мастера текущая конфигурация отображает все настройки и изменения конфигурации.

Выводы по третьему учебному вопросу. Автоматические функции обеспечения безопасности

Функция AutoSecure должна использоваться при первом конфигурировании маршрутизатора. Для производственных маршрутизаторов пользоваться ей не рекомендуется.

Для закрепления материала воспользуйтесь программой проверки синтаксиса, чтобы защитить маршрутизатор R1 с помощью функции AutoSecure.



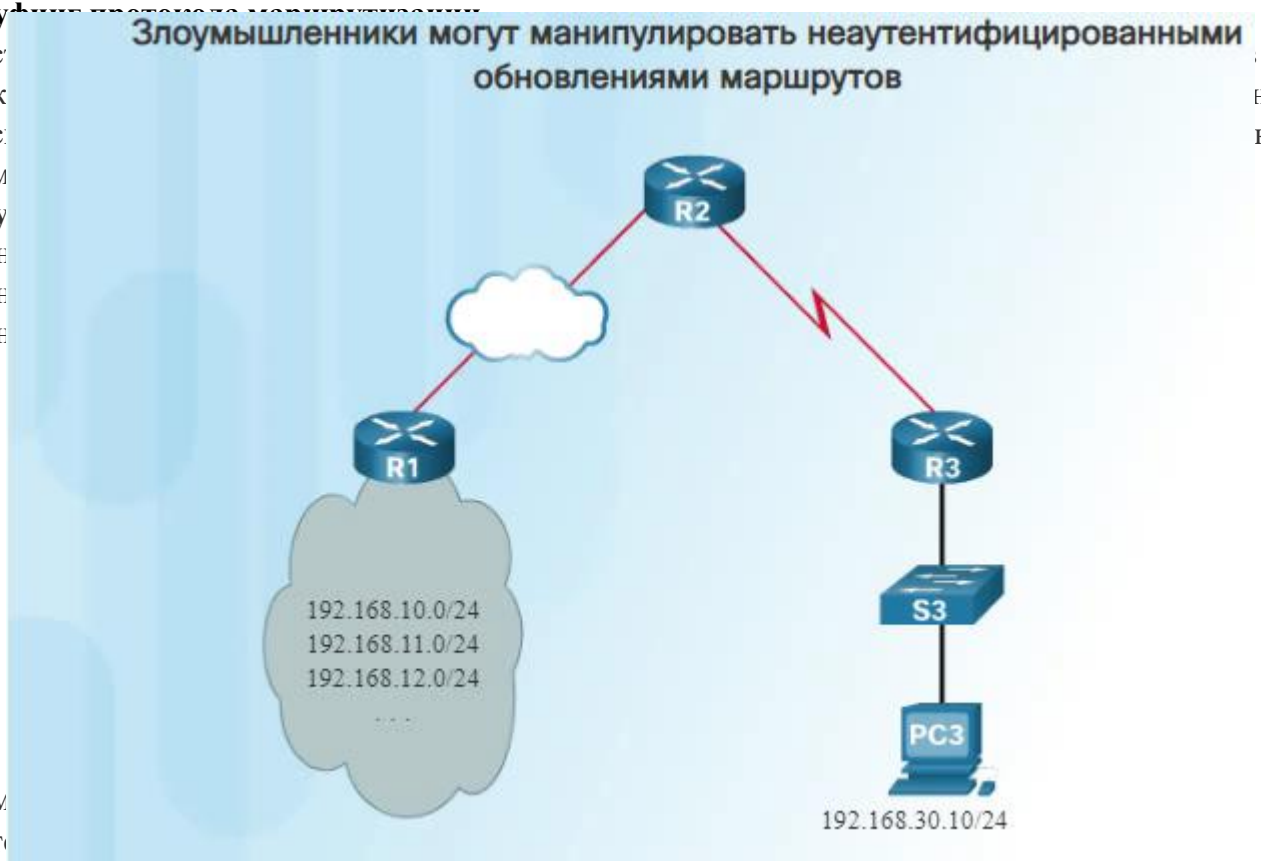
Четвертый учебный вопрос. Защита плоскости управления

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.

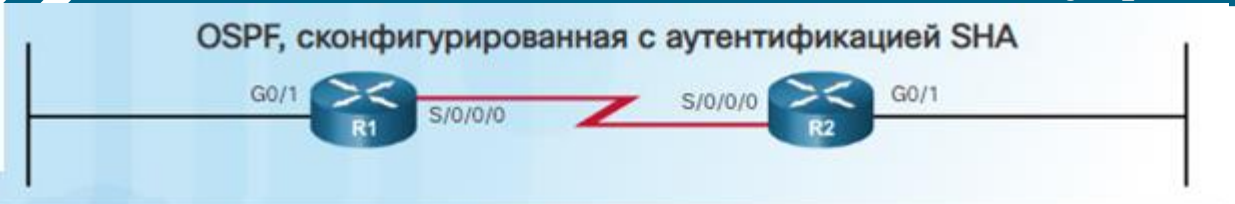
Присвойте имя цепочке ключей с помощью команды **key chain** .

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** .

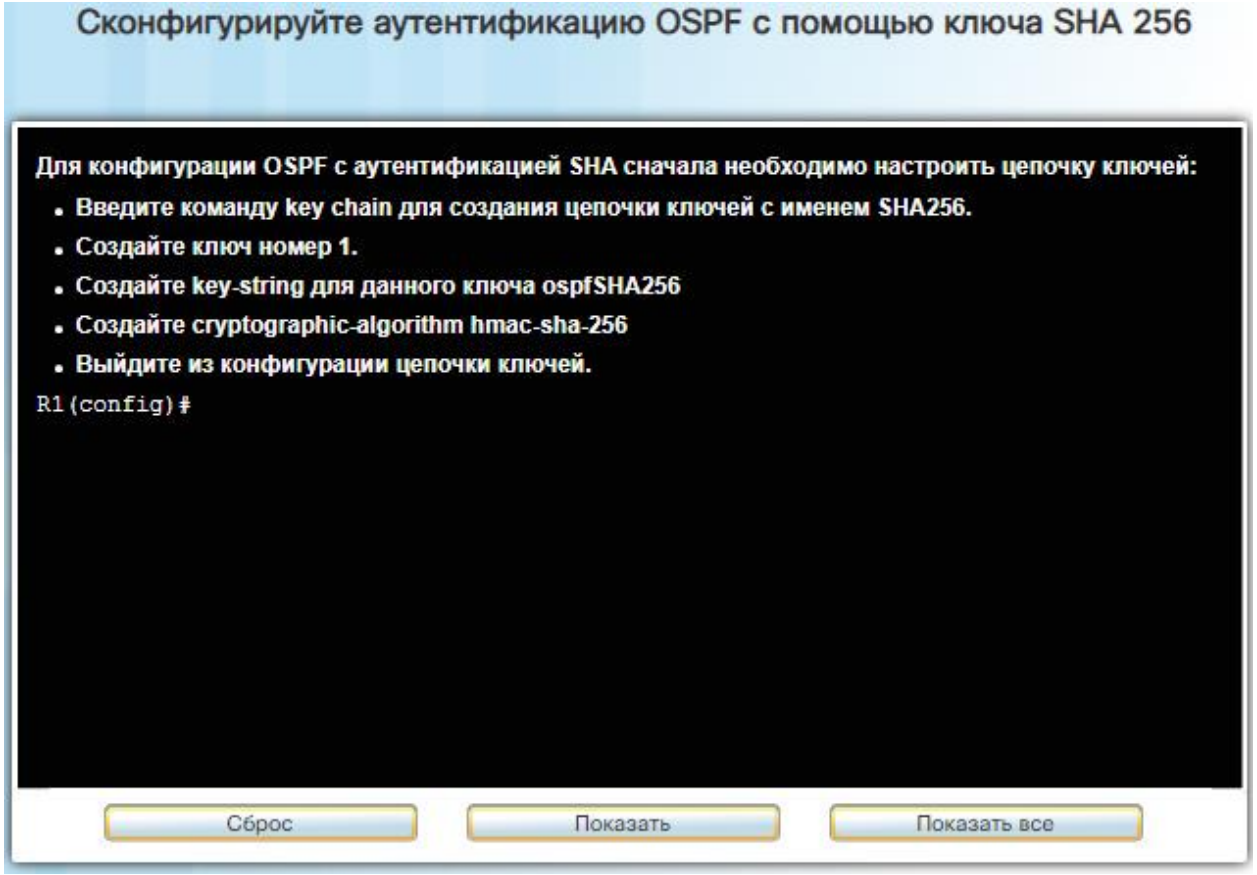



```
R1(config)# key chain SHA256
R1(config-keychain)# key 1
R1(config-keychain-key)# key-string ospfSHA256
R1(config-keychain-key)# cryptographic-algorithm hmac-sha-256
R1(config-keychain-key)# exit
R1(config-keychain)# exit
R1(config)# interface s0/0/0
R1(config-if)# ip ospf authentication key-chain 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.



Заключительная часть

Защиту сети необходимо начинать с защиты ее устройств. Под этим понимается защита периметра сети, обеспечение безопасности административного доступа к инфраструктурным устройствам, повышение безопасности виртуального входа в систему и использование защищенных протоколов вместо незащищенных.

Также важно ограничивать административный доступ. Администраторы должны предоставлять доступ к инфраструктурным устройствам в зависимости от уровней привилегий и внедрять интерфейс CLI на основе ролей для обеспечения иерархического административного доступа.

Образы IOS и файлы конфигурации должны быть защищены с использованием функции устойчивой конфигурации Cisco IOS. С данным направлением мы с вами познакомимся на следующем занятии.