# Лабораторная работа: доступ к сетевым устройствам по протоколу SSH

#### Топология



#### Таблица адресации

Устройство	Интерфейс	IP-адрес	Маска подсети	Шлюз по умолчанию
R1	G0/1	192.168.1.1	255.255.255.0	Недоступно
S1	VLAN 1	192.168.1.11	255.255.255.0	192.168.1.1
ПК-А	Сетевой адаптер	192.168.1.3	255.255.255.0	192.168.1.1

#### Задачи

- Часть 1. Настройка основных параметров устройства
- Часть 2. Настройка маршрутизатора для доступа по протоколу SSH
- Часть 3. Проверка сеанса связи по протоколу Telnet с помощью программы Wireshark
- Часть 4. Проверка сеанса связи по протоколу SSH с помощью программы Wireshark
- Часть 5. Настройка коммутатора для доступа по протоколу SSH
- Часть 6. Настройка протокола SSH в интерфейсе командной строки коммутатора

#### Исходные данные/сценарий

Раньше для удалённой настройки сетевых устройств в основном применялся протокол Telnet. При этом протоколы типа Telnet не включают проверку подлинности и шифрование информации, передаваемой между клиентом и сервером, что позволяет сетевым средствам слежения перехватывать пароли и данные конфигурации.

Secure Shell(SSH)— это сетевой протокол, устанавливающий безопасное подключение эмулятора терминала к маршрутизатору или иному сетевому устройству. Протокол SSH шифрует все сведения, которые поступают по сетевому каналу, и предусматривает аутентификацию удалённого компьютера. Протокол SSH всё больше заменяет Telnet — именно его выбирают сетевые специалисты в качестве средства удалённого входа в систему. Чаще всего протокол SSH применяется для входа на удалённое устройство и выполнения команд, но может также передавать файлы по связанным протоколам SFTP или SCP.

Чтобы протокол SSH работал, на взаимодействующих сетевых устройствах должна быть настроена его поддержка. В ходе лабораторной работы вы активируете на маршрутизаторе SSH-сервер и подключитесь к маршрутизатору, используя ПК с клиентом SSH. В локальной сети подключение обычно устанавливается с помощью Ethernet и IP-адреса. Кроме того, в ходе лабораторной работы вы настроите маршрутизатор для приёма подключений по протоколу SSH и воспользуетесь программой Wireshark для перехвата и просмотра сеансов Telnet и SSH. Это покажет, какую важную роль играет шифрование данных, осуществляемое протоколом SSH. И, наконец, вам придётся самостоятельно настроить коммутатор для подключения по протоколу SSH.

Примечание. Маршрутизаторы, используемые на практических занятиях ССNA: маршрутизаторы с интеграцией сервисов серии Cisco 1941 (ISR) установленной версии Cisco IOS 15.2(4) M3 (образ universalk9). Используемые коммутаторы: семейство коммутаторов Cisco Catalyst 2960 версии CISCO IOS 15.0(2) (образ lanbasek9). Можно использовать другие маршрутизаторы, коммутаторы и версии CISCO IOS. В зависимости от модели и версии Cisco IOS выполняемые доступные команды и выводы могут отличаться от данных, полученных в ходе лабораторных работ. Точные идентификаторы интерфейса см. в таблице сводной информации об интерфейсах маршрутизаторов в конце данной лабораторной работы.

**Примечание**. Убедитесь, что информация, имеющаяся на маршрутизаторе и коммутаторе, удалена и они не содержат файлов загрузочной конфигурации. Если вы не уверены, что сможете это сделать, обратитесь к инструктору.

#### Необходимые ресурсы

- 1 маршрутизатор (Cisco 1941 с универсальным образом МЗ версии CISCO IOS 15.2(4) или аналогичным)
- 1 коммутатор (серия Cisco 2960, с программным обеспечением Cisco IOS версии 15.0(2), образ lanbasek9 или аналогичный)
- Один ПК (Windows 7, Vista или XP с эмулятором терминала, например Tera Term, и установленной программой Wireshark)
- Консольные кабели для настройки устройств CISCO IOS через консольные порты
- Кабели Ethernet в соответствии с топологией

#### Часть 1: Основные настройки устройства

В части 1 потребуется настройка топологии сети и основных параметров, таких как IP-адреса интерфейсов, доступ к устройствам и пароли на маршрутизаторе.

#### Шаг 1: Создайте сеть в соответствии с изображенной на схеме топологией.

#### Шаг 2: Выполните инициализацию и перезагрузку маршрутизатора и коммутатора.

#### Шаг 3: Настройте маршрутизатор.

- а. Подключите консоль к маршрутизатору и активируйте привилегированный режим.
- b. Войдите в режим конфигурации.
- с. Отключите поиск в DNS, чтобы предотвратить попытки маршрутизатора преобразовывать неверно введённые команды таким образом, как будто они являются именами узлов.
- d. Назначьте class в качестве пароля привилегированного режима.
- e. Назначьте cisco в качестве пароля консоли и включите вход по паролю.
- f. Назначьте cisco в качестве пароля виртуального терминала и включите вход по паролю.
- g. Зашифруйте пароли.
- h. Создайте баннер, который предупреждает о запрете несанкционированного доступа.

- i. Настройте и активируйте интерфейс маршрутизатора G0/1 с помощью сведений, содержащихся в таблице адресации.
- ј. Сохраните текущую конфигурацию в файл загрузочной конфигурации.

#### Шаг 4: Настройте ПК-А.

- а. Настройте на ПК-А IP-адрес и маску подсети.
- b. Настройте на ПК-А шлюз по умолчанию.

#### Шаг 5: Проверьте подключение к сети.

Отправьте эхо-запрос с помощью команды ping с ПК-А на маршрутизатор R1. Если эхо-запрос с помощью команды ping не проходит, найдите и устраните неполадки подключения.

#### Часть 2: Настройка маршрутизатора для доступа по протоколу SSH

Подключение к сетевым устройствам по протоколу Telnet сопряжено с риском для безопасности, поскольку вся информация передаётся в виде открытого текста. Протокол SSH шифрует данные сессии и требует аутентификации устройств, поэтому для удалённых подключений рекомендуется использовать именно его. В части 2 вам нужно настроить маршрутизатор для приёма соединений по протоколу SSH по линиям VTY.

#### Шаг 1: Настройте аутентификацию устройств.

При генерации ключа шифрования используются имя устройства и домен. Это значит, что эти имена необходимо указать перед вводом команды **crypto key**.

а. Укажите имя устройства.

Router(config) # hostname R1

b. Укажите домен для устройства.

R1(config) # ip domain-name ccna-lab.com

#### Шаг 2: Создайте ключ шифрования с указанием его длины.

R1(config)# crypto key generate rsa modulus 1024 The name for the keys will be: R1.ccna-lab.com

% The key modulus size is 1024 bits % Generating 1024 bit RSA keys, keys will be non-exportable... [OK] (elapsed time was 1 seconds)

R1(config)# \*Jan 28 21:09:29.867: %SSH-5-ENABLED: SSH 1.99 has been enabled

#### Шаг 3: Создайте имя пользователя в локальной базе учётных записей.

R1(config)# username admin privilege 15 secret adminpass
R1(config)#
\*Feb 6 23:24:43.971: End->Password:QHjxdsVkjtoP7VxKIcPsLdTiMIvyLkyjT1HbmYxZigc
R1(config)#

Примечание. Пятнадцатый уровень привилегий предоставляет пользователю права администратора.

#### Шаг 4: Активируйте протокол SSH на линиях VTY.

a. Активируйте протоколы Telnet и SSH на входящих линиях VTY с помощью команды transport input.

R1(config) # line vty 0 4
R1(config-line) # transport input telnet ssh

Измените способ входа в систему — выберите проверку пользователей по локальной базе учётных записей.

```
R1(config-line)# login local
R1(config-line)# end
R1#
```

#### Шаг 5: Сохраните текущую конфигурацию в файл загрузочной конфигурации.

```
R1# copy running-config startup-config
Destination filename [startup-config]?
Building configuration...
[OK]
R1#
```

## Часть 3: Проверка сеанса связи по протоколу Telnet с помощью программы Wireshark

В части 3 вы воспользуетесь программой Wireshark для перехвата и просмотра данных, передаваемых во время сеанса связи маршрутизатора по протоколу Telnet. С помощью программы Tera Term вы подключитесь к маршрутизатору R1 по протоколу Telnet, войдёте в систему и запустите на маршрутизаторе команду show run.

**Примечание**. Если на вашем компьютере нет программного обеспечения клиента Telnet/SSH, его необходимо установить. Чаще всего для работы с протоколами Telnet и SSH используются программы Tera Term (http://download.cnet.com/Tera-Term/3000-20432 4-75766675.html) и PuTTy (www.putty.org).

Примечание. По умолчанию доступ к Telnet из командной строки вWindows 7 отключён. Чтобы активировать подключение по протоколу Telnet из окна командной строки, нажмите кнопку Пуск >Панель управления>Программы>Программы и компоненты>Включение или отключение компонентов Windows. Установите флажок рядом с компонентом Клиент Telnet и нажмите кнопку OK.

#### Шаг 1: Откройте Wireshark и начните сбор данных в интерфейсе локальной сети.

**Примечание**. Если перехват данных в интерфейсе локальной сети запустить не удаётся, попробуйте открыть программу Wireshark с помощью параметра **Запуск от имени администратора**.

#### Шаг 2: Начните сеанс подключения к маршрутизатору по протоколу Telnet.

a. Запустите программу Tera Term, установите переключатель сервиса **Telnet**, а в поле «Host» введите **192.168.1.1**.

Tera Term: Новое	соединение	×
ICP/ <u>I</u> P	Хост: 192.168.1.1	•
	© <u>S</u> SH <u>в</u> ерсия SSH: SSH2	
	© Другие <u>п</u> ротокол: UNSPEC	•
© <u>с</u> ом	Порт:	-
	ОК Выход <u>П</u> омощь	

Какой порт TCP используется для сеансов Telnet по умолчанию?

b. В окне командной строки после приглашения Username: (Имя пользователя) введите **admin**, а после Password: (Пароль) — **adminpass**. Эти запросы появляются потому, что командой **login local** вы настроили линии VTY на использование локальной базы учётных записей.

📜 192.168.1.1:23 - Tera Term VT	
File Edit Setup Control Window Help	
**************************************	<u> </u>
User Access Verification	
Username:	

с. Введите команду show run.

R1# show run

d. Введите команду **exit**, чтобы завершить сеанс работы с протоколом Telnet и выйти из программы Tera Term.

R1# exit

Шаг 3: Остановите сбор данных программой Wireshark.



Шаг 4: Примените один из фильтров Telnet для данных, собираемых программой Wireshark.

Filter: telnet  Expression Cl	<b>r</b> Apply
-------------------------------	----------------

© Корпорация Cisco и/или её дочерние компании, 2014. Все права защищены.

В данном документе содержится общедоступная информация корпорации Cisco.

#### Шаг 5: Используйте функцию TCP в Wireshark для просмотра сеанса Telnet.

а. Нажмите правой кнопкой мыши на одну из строк Telnet в разделе Packet list (Список пакетов) программы Wireshark и выберите в раскрывающемся списке пункт Follow TCP Stream (Следить за TCP-потоком).

🖉 Ir	itel(R	) PRO/:	1000	MT Netwo	ork Conn	ection [	[Wireshark	(1.6.1	(SVN Rev	/ 38096 fi	rom /tı	runk-	1.6)]										_	
Eile	<u>E</u> dit	<u>V</u> iew	Go	<u>C</u> apture	<u>A</u> nalyze	<u>S</u> tatisti	cs Telepho	on <u>y T</u> o	ools <u>I</u> nte	ernals <u>H</u> e	elp													
0	۲			(  🖻	550 🗴		୍ 🖕	ا	ə T	₽   [			€ (	20	**	×.	¥	<b>5</b>	*	Ø				
Filter	: tel	net								Expr	ression.	с	lear /	Apply										
No.		Time		Source			Destin	ation		Pro	otocol	Leng	ith In	fo										
	117	35.67	4982	2 192.	168.1.	3	192	169 1	1	TT (Income Section 1997)	INCT		55 T	elnet	Data	L								
	118	35.67	6097	7 192.3	168.1.	1	192.	Mai	rk Packet i	toggie			52 T	elnet	Data	· • • •								
	120	36.11	5021	L 192.	168.1.	3	192.	Ign	ore Packe	t (toggie)			55 T	eInet	Data	۰								
	121	36.11	6029	9 192.	168.1.	1	192.	() Set	Time Ref	erence (to	ggle)		49 T	einet	Data									
	124	3/./8	94180	5 192.	160.1.	5 1	192.	Mai	nually Res	olve Addre	ess		55 I	elnet	Data									
	122	20 17	2521	1 102	168 1	2	192.					_	55 T	alnat	Data									
	120	20 17	2351 7/21	2 102 .	168 1	5 1	102	App	oly as Filte	r			60 T	alnet	Data									
	130	39 36	281	9 192	168 1	3	192	Pre	pare a Filt	er			55 T	elnet	Data									
	131	39.36	5331	5 192.	168.1.	1	192.	Cor	nversation	Filter			60 T	elnet	Data									
	132	39.52	419	5 192.	168.1.	3	192.	Col	orize Conv	ersation/			55 T	elnet	Data									
	133	39.52	4827	7 192.3	168.1.	1	192.	SC	IP	_		1	60 T	elnet	Data									
	134	39.64	1074	4 192.3	168.1.	3	192.	Fol	ow TCP S	tream			55 T	elnet	Data	· • • •								
	135	39.64	1667	7 192.	168.1.	1	192.	Fol	ow UDP S	tream			60 T	elnet	Data									
	136	39.82	2087	7 192.	168.1.	3	192.	Fol	ow SSL St	ream			56 T	elnet	Data									
	137	39.82	2730	0 192.3	168.1.	1	192.	Cop	ру			•	60 T	elnet	Data	۱								~
+ F	rame	117:	55	bytes	on wir	e (440	) bits)	23 Day	rodo Ac				its)											
÷Ε	ther	net I	Ι, 5	Snc: Vm	ware_b	e:6c:8	39 (00:	us Dec					9:47	:75:c	3:e1	(fc:	99:4	7:7	5:c3:	e1)				
÷Ι	nter	net P	roto	ocol Ve	rsion	4, Sro	:: 192.:	🗎 Prir	nt				: 19	2.168	.1.1	(192	2.168	3.1.1	1)					
ΞT	rans	missi	on o	Control	Proto	ocol, s	Snc Port	Sho	w Packet	in New Wir	ndow		teln	et (2	3), s	eq:	55,	Ack	: 105	57, L	en: 1	_		
±Τ	elne	t					-																	
1																								

b. В окне Follow TCP Stream (Следить за TCP-потоком) отображаются данные о текущем сеансе подключения к маршрутизатору по протоколу Telnet. Весь сеанс связи (включая пароль) отображается открытым текстом. Обратите внимание на то, что введённые имя пользователя и команда **show run** отображаются с повторяющимися символами. Это связано с настройкой отображения в Telnet, которая позволяет выводить на экран символы, набираемые на клавиатуре.

Follow TCP Stream	<u>_     ×</u>
Stream Content	
Unauthorized Access is Prohibited!	<u>_</u>
User Access Verification Username:	
erassword: adminpass	
Building configuration Current configuration : 1644 bytes	
! Last configuration change at 23:26:03 UTC Wed Feb 6 2013 version 15.2 service timestamps debug datetime msec service timestamps log datetime msec service password-encryption	
hostname R1	
: boot-start-marker boot-end-marker !	
enable secret 4 06YFDUHH61wAE/kLkDq9BGho1QM5EnRtoyr8cHAUg.2	
Entire conversation (2266 bytes)	-
Eind Save As Print O ASCII O EBCDIC O Hex Dump O C Arrays O Ra	w
Help Filter Out This Stream	e

с. Закончив просмотр сеанса Telnet в окне Follow TCP Stream (Следить за TCP-потоком), нажмите кнопку Close (Закрыть).

### Часть 4: Проверка сеанса связи по протоколу SSH с помощью программы Wireshark

В части 4 вам нужно будет с помощью программы Tera Term установить сеанс подключения к маршрутизатору по протоколу SSH. Программа Wireshark будет использоваться для перехвата и просмотра данных этого сеанса.

#### Шаг 1: Откройте Wireshark и начните сбор данных в интерфейсе локальной сети.

#### Шаг 2: Запустите на маршрутизаторе сеанс связи по протоколу SSH.

а. Откройте программу Tera Term и введите в поле «Host» окна «Tera Term: Новое соединение» IPадрес интерфейса G0/1 маршрутизатора R1. Убедитесь в том, что переключатель SSH установлен, и нажмите кнопку OK для подключения к маршрутизатору.

Гега Term: Новое	соединение	×
	≚ост: 192.168.1.1	▼ <u>п</u> орт TCP#: 22 ерсия SSH: <u>SSH2</u> ▼
	О Другие	протокол: UNSPEC 🔽
© <u>с</u> ом	Порт: СОМ1: Последо	овательный порт (СОР 🔽
	ОК Выход	<u>П</u> омощь

Какой порт TCP используется для сеансов SSH по умолчанию? \_\_\_\_

b. После первой установки подключения к устройству по протоколу SSH откроется окно SECURITY WARNING (Предупреждение безопасности), которое означает, что вы ещё не подключались к этому устройству. Это сообщение является частью процесса аутентификации. Прочтите текст предупреждения безопасности и нажмите кнопку Continue (Продолжить).

SECURITY WARNING	×
There is no entry for the server "192.168.1.1" in your list of known hosts. The machine you have contacted may be a hostile machine pretending to be the server.	
If you choose to add this machine to the known hosts list and continue, then you will not receive this warning again.	
The server's host key fingerprint is: f5:b1:e7:f8:c6:74:89:88:79:1c:24:8f:2c:6e:6e:39	
,	
+[ RSA 1024]+	
. S + = o .	
E .o	
++	
Add this machine and its key to the known hosts list	
Continue Disconnect	

с. В окне SSH Authentication (Аутентификация SSH) в качестве имени пользователя укажите **admin**, а в качестве пароля — **adminpass**. Нажмите кнопку **OK**, чтобы войти в систему маршрутизатора.

SSH Authentication
Logging in to 192.168.1.1
Authentication required.
User name: admin
Passphrase:
Remember password in memory
Forward agent
• Use plain password to log in
C Use RSA/DSA/ECDSA key to log in Private key file:
C Use rhosts to log in (55H1) Local user name:
Host private key file:
O Use challenge/response to log in(keyboard-interactive)
O Use Pageant
OK Disconnect

d. Вы установили сеанс SSH на маршрутизаторе. Окно программы Tera Term очень похоже на окно командной строки. После приглашения введите команду **show run**.

達 192.168.1.1:22 - Tera Term VT	
File Edit Setup Control Window Help	
**************************************	

е. Чтобы завершить сеанс SSH и выйти из программы Tera Term, введите команду exit.

R1# **exit** 

#### Шаг 3: Остановите сбор данных программой Wireshark.



### Шаг 4: Примените один из фильтров SSH для данных, собираемых программой Wireshark.



#### Шаг 5: Используйте функцию TCP в Wireshark для просмотра ceaнса Telnet.

- а. Нажмите правой кнопкой мыши на одну из строк SSHv2 в разделе Packet list (Список пакетов) программы Wireshark и выберите в раскрывающемся списке пункт Follow TCP Stream (Следить за TCP-потоком).
- b. Изучите окно Follow TCP Stream (Следить за TCP-потоком) сеанса SSH. Данные зашифрованы и не доступны для прочтения. Сравните данные сеанса SSH с данными сеанса Telnet.

Follow TCP Stream
Stream Content SSH-1.99-Cisco-1.25 SSH-2.0_TISSH/2.62 win32
<pre>sh=2.0-115sh/2.02 whis2 T !M.^AA. k. ]Jydiffie-hellman-group-exchange-shal,diffie-hellman-group14-shal,diffie- hellman-group1-shalssh=rsa)aes128-cbc,3des-cbc,aes192-cbc,aes256-cbc)aes128- cbc,3des-cbc,aes192-cbc,aes256-cbc+hmac-shal,hmac-shal-96,hmac-md5.96 +hmac-shal,hmac-shal-96,hmac-md5,hmac- md5-96nonenone</pre>
Entire conversation (8602 bytes)
Eind Save As Print O ASCII O EBCDIC O Hex Dump O C Arrays O Raw
Help Filter Out This Stream

Почему для удалённых подключений протокол SSH является более предпочтительным, чем протокол Telnet?

- с. Завершив изучение сеанса SSH, нажмите кнопку Close (Закрыть).
- d. Закройте программу Wireshark.

#### Часть 5: Настройка коммутатора для доступа по протоколу SSH

В части 5 вы настроите коммутатор в топологии для приёма подключений по протоколу SSH, а затем установите сеанс SSH с помощью программы Tera Term.

#### Шаг 1: Настройте базовые параметры коммутатора.

#### Шаг 2: Настройте коммутатор для доступа по протоколу SSH.

Для настройки протокола SSH на коммутаторе используйте те же команды, которые применялись для аналогичной настройки маршрутизатора в части 2.

#### Шаг 3: Установите подключение к коммутатору по протоколу SSH.

Запустите программу Tera Term на ПК-А, а затем установите подключение по протоколу SSH к интерфейсу SVI коммутатора S1.

#### Шаг 4: При необходимости устраните неполадки.

Удалось ли вам установить ceaнс SSH с коммутатором?

### Часть 6: Настройка протокола SSH в интерфейсе командной строки коммутатора

Клиент SSH интегрирован в операционную систему Cisco IOS и может запускаться из интерфейса командной строки. В части 6 вы установите подключение к маршрутизатору по протоколу SSH из интерфейса командной строки коммутатора.

#### Шаг 1: Посмотрите, какие параметры доступны для клиента SSH в Cisco IOS.

Введите вопросительный знак (?), чтобы отобразить варианты параметров для команды ssh.

S1# ssh ?

- -c Select encryption algorithm
- -l Log in using this user name
- -m Select HMAC algorithm
- -o Specify options
- -p Connect to this port
- -v Specify SSH Protocol Version
- -vrf Specify vrf name

WORD IP address or hostname of a remote system

#### Шаг 2: Установите подключение коммутатора S1 к маршрутизатору R1 по протоколу SSH.

a. Чтобы подключиться к маршрутизатору R1 по протоколу SSH, введите команду –ladmin. Это позволит вам войти в систему под именем admin. При появлении запроса в качестве пароля введите adminpass.

R1#

b. Чтобы вернуться к коммутатору S1, не закрывая сеанс подключения к маршрутизатору R1 по протоколу SSH, нажмите клавиши Ctrl+Shift+6. Отпустите клавиши Ctrl+Shift+6 и нажмите х. Откроется окно командной строки коммутатора с привилегированным режимом.

R1#

S1#

с. Чтобы вернуться к сеансу SSH на маршрутизаторе R1, нажмите клавишу BBOД в пустом поле интерфейса командной строки. Чтобы открыть окно командной строки маршрутизатора, нажмите клавишу BBOД ещё раз.

S1# [Resuming connection 1 to 192.168.1.1 ... ]

R1#

d. Чтобы завершить сеанс SSH на маршрутизаторе R1, введите в окне командной строки команду exit.

R1# exit

[Connection to 192.168.1.1 closed by foreign host]

S1#

Какие версии протокола SSH поддерживаются интерфейсом командной строки?

#### Вопросы на закрепление

Как предоставить доступ к сетевому устройству нескольким пользователям, у каждого из которых есть собственное имя пользователя?

Общие сведения об интерфейсах маршрутизаторов										
Модель маршрутизатора	Интерфейс Ethernet #1	Интерфейс Ethernet #2	Последовательный интерфейс #1	Последовательный интерфейс #2						
1800	Fast Ethernet 0/0 (F0/0)	Fast Ethernet 0/1 (F0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)						
1900	Gigabit Ethernet 0/0 (G0/0)	Gigabit Ethernet 0/1 (G0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)						
2801	Fast Ethernet 0/0 (F0/0)	Fast Ethernet 0/1 (F0/1)	Serial 0/1/0 (S0/1/0)	Serial 0/1/1 (S0/1/1)						
2811	Fast Ethernet 0/0 (F0/0)	Fast Ethernet 0/1 (F0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)						
2900	Gigabit Ethernet 0/0 (G0/0)	Gigabit Ethernet 0/1 (G0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)						

#### Сводная таблица интерфейса маршрутизатора

**Примечание**. Чтобы узнать, каким образом настроен маршрутизатор, изучите интерфейсы для определения типа маршрутизатора и количества имеющихся на нём интерфейсов. Не существует эффективного способа перечислить все комбинации настроек для каждого класса маршрутизаторов. Эта таблица включает в себя идентификаторы возможных сочетаний Ethernet и последовательных интерфейсов в устройстве. В таблицу интерфейсов не включены иные типы интерфейсов, даже если они присутствуют на каком-либо определённом маршрутизаторе. В качестве примера можно привести интерфейс ISDN BRI. Строка в скобках — это принятое сокращение, которое может использоваться в командах IOS для представления интерфейса.