Федеральное агентство по образованию Российской Федерации
Государственное образовательное учреждение высшего профессионального образования
Томский политехнический университет

А.С. Томашевский

АДМИНИСТРИРОВАНИЕ В ТЕЛЕКОММУНИКАЦИОННЫХ СИСТЕМАХ

Учебное пособие

Издательство
Томского политехнического университета
2008

Учебное издание

ТОМАШЕВСКИЙ Алексей Сергеевич

АДМИНИСТРИРОВАНИЕ В ТЕЛЕКОММУНИКАЦИОННЫХ СИСТЕМАХ

Учебное пособие

Ассистент каф. ОСУ А.С. Томашевский

ОГЛАВЛЕНИЕ

ВВЕДЕНИЕ В АДМИНИСТРИРОВАНИЕ ТЕЛЕКОММУНИКАЦИОННЫХ СИСТЕМ 4

1. ОСНОВЫ КОНФИГУРИРОВАНИЯ УСТРОЙСТВ CISCO 5

1.1. Предварительное конфигурирование 5
1.2. Система помощи 10
1.3. Режимы конфигурирования 12
1.4. Конфигурирование памяти 13
1.5. Пользовательский режим 18
1.6. Команды конфигурирования 20

2. ОСНОВЫ АДМИНИСТРИРОВАНИЯ И УПРАВЛЕНИЯ СЕТЕВЫМИ УСТРОЙСТВАМИ CISCO 28

2.1. Основы управления доступом 28
2.2. Основы предотвращения атак 38
2.3. Основы управления сетью 44
2.4. Основы управления временем 50

3. ОСНОВНЫЕ ПРИНЦИПЫ ПОИСКА НЕИСПРАВНОСТЕЙ В СЕТЯХ CISCO 57

3.1. Общее описание процесса поиска 57
3.2. Инструментальные средства поиска 63

4. УСТРАНЕНИЕ НАРУШЕНИЙ В РАБОТЕ АППАРАТНЫХ СРЕДСТВ, СРЕДСТВ ЗАГРУЗКИ И ПЕРЕДАЮЩЕЙ СРЕДЫ 76

4.1. Нарушения в работе аппаратных средств и средств загрузки 76
4.2. Устранение нарушений в работе передающей среды 81

5. РЕВИЗИИ РАЗЛИЧНЫХ ТИПОВ И СОЗДАНИЕ КАРТ СЕТИ 91

ТЕРМИНОЛОГИЧЕСКИЙ СЛОВАРЬ 95

СПИСОК ЛИТЕРАТУРЫ 100

ВВЕДЕНИЕ В АДМИНИСТРИРОВАНИЕ ТЕЛЕКОММУНИКАЦИОННЫХ СИСТЕМ

Компания Cisco Systems, Inc. является ведущим в мире поставщиком аппаратного и программного обеспечения для межсетевого взаимодействия. Cisco ежегодно устанавливает более 100 000 устройств, которые работают как в частных сетях, так и в сетях общего пользования. Это учебное пособие призвано помочь новым пользователям продуктов компании Cisco освоить основы администрирования своих устройств межсетевого взаимодействия.

В состав этих устройств входит разработанная компанией специальная операционная система – межсетевая операционная система Cisco (Cisco Internetwork Operating System – IOS). ОС IOS представляет собой сложную операционную систему реального времени, состоящую из нескольких подсистем и имеющую десятки тысяч возможных параметров конфигурирования. Используя приводимые в хронологическом порядке простые описания и практические примеры, авторы основное внимание уделяют ОС IOS с точки зрения конфигурирования, эксплуатации и сопровождения устройств межсетевого взаимодействия.

Основные концептуальные положения:

- Операционная система Cisco IOS – это программное обеспечение, под управлением которого работают устройства Cisco.
- Устройства Cisco работают на трех уровнях модели OSI – физическом, канальном и сетевом.
- ОС IOS использует информацию протоколов каждого уровня модели OSI.
- Мосты и коммутаторы работают на канальном уровне и соединяют несколько сетевых
- сегментов на основе различных канальных уровней в один логический сетевой сегмент.
- Маршрутизаторы работают на сетевом уровне и управляют передачей пакетов через сеть на основе информации сетевого уровня.
- Серверы доступа связывают асинхронные устройства с сетью, позволяя им работать в сети.

1. ОСНОВЫ КОНФИГУРИРОВАНИЯ УСТРОЙСТВ CISCO

1.1. Предварительное конфигурирование

Все устройства, работающие под управлением IOS, поставляются с завода сконфигурированными в минимально возможном объеме. В маршрутизаторах и серверах доступа компания Cisco производит установку лишь минимального количества параметров конфигурирования. Это влечет за собой необходимость ввода в устройства информации, только посте осуществления которого они смогут выполнять свои функции. Когда маршрутизатор (или сервер доступа) присылается с завода, все его интерфейсы или выключены или административно заблокированы. Чтобы начать установку конфигурации устройства Cisco, вставьте вилку устройства в розетку сети питания и найдите тумблер включения, располагающийся на задней стенке. Если включить тумблер питания (иногда он обозначается цифрой 1), то на устройство подастся напряжение, и на передней панели загорятся светодиодные индикаторы статуса.

Рис. 1. Внутренние компоненты, участвующие в процессе маршрутизации

На следующем этапе конфигурирования работающего под управлением ОС IOS устройства необходимо найти **порт консоли**. Каждое устройство Cisco имеет порт консоли, который используется для обращения к нему с помощью непосредственно подключаемого терминала. Порт консоли часто представляет собой порт интерфейса RS-232C или RJ-45 и обозначается надписью Console (Консоль).

Обнаружив порт консоли, необходимо подключить выделенный для этой цели терминал или ПК с эмулятором терминала. Компанией Cisco с каждым устройством поставляются необходимые для этого кабели. Если к устройству подключается терминал, следует воспользоваться разъемом RS-323C на терминале, подключить к нему кабель RJ-45 и затем подсоединить всю эту сборку непосредственно к устройству.

Установив физическое соединение между терминалом или ПК и устройством, необходимо произвести конфигурирование терминала для его соответствующего взаимодействия с устройством. Для этого следует настроить параметры терминала (или программы эмуляции терминала на ПК) таким образом, чтобы поддерживались следующие установки:

- тип эмулируемого терминала – VT100;
- скорость передачи данных – 9600 бод;
- запрет контроля четности;
- 8 бит данных;
- 1 стоп-бит.

После проверки правильности этих установок следует подать на устройство питание. На экране терминала появится сообщение.

Мосты и коммутаторы, которые функционируют под управлением IOS, могут выводить или не выводить подобное сообщение. Это зависит от модели устройства и выполняемых им функций. Вне зависимости от вида выводимого сообщения после подачи на устройство питания на экране терминала или устройства, эмулирующего терминал, должен высветиться какой-то результат. В некоторых случаях в зависимости от программы эмуляции терминала и установок для того, чтобы увидеть какую-нибудь реакцию, необходимо нажать на клавиатуре терминала клавишу <Enter> или <Return>.

Если сообщения на экране терминала или устройства, его эмулирующего, нет, проверьте соединения и удостоверьтесь в правильности установок терминала. Возможно, надо будет заглянуть в руководство *Getting Started Guide (С чего начать),* которое поставляется с каждым устройством Cisco.

При первом включении питания все маршрутизаторы и серверы доступа входят в **режим диалога конфигурирования системы**. Этот интерактивный режим отображается на экране консоли и, задавая вопросы, помогает сконфигурировать основные элементы ОС IOS. В режиме диалога конфигурирования системы сначала запрашиваются глобальные параметры системы, а затем параметры интерфейсов.

При входе в режим диалога конфигурирования системы на экране терминала должно появиться сообщение (System Configuration Dialog). После этого для начала работы в режиме диалога конфигурирования системы можно нажать клавишу <Return> или <Enter>. Приведенный ниже список интерфейсов соответствует состоянию устройства при его непосредственной поставке с завода: устройство еще не сконфигурировано. Поэтому все его интерфейсы показаны как не прошедшие конфигурирование (об этом говорит слово NO в столбце Ok?). Поскольку для интерфейсов IP-адреса не определены, в столбце IP Address для всех ин-

терфейсов стоит значение unassigned (не присвоен). В столбце Method стоит значение not set (нет установок). Значение этого столбца показывает, как конфигурировался интерфейс: вручную или автоматически через сеть. На данный момент установки для интерфейсов еще не производились. Последние два столбца называются Status (Состояние) и Protocol (Протокол). Столбец status показывает статус интерфейса, а столбец Protocol – тип запущенного на данном интерфейсе протокола канального уровня. По умолчанию на новом устройстве все интерфейсы и протоколы канального уровня имеют статус down («выключен»).

Нужно отметить, что интерфейс Ethernet является интерфейсом локальной сети, а последовательный интерфейс Serial – интерфейсом глобальной сети. Имя интерфейса Ethernet0 обозначает первую подключаемую к данному устройству локальную сеть Ethernet, а имя интерфейса Serial0 – первую подключаемую глобальную сеть с последовательной передачей. Физические порты на задней стенке корпуса устройства имеют точно такие же названия.

Следующими этапами конфигурирования устройства являются присвоение имени устройству, т. е. логического названия, которое будет ассоциироваться с данным физическим устройством, и задание пароля доступа.

```
Configuring global parameters:
Enter host name [Router]: Singapore
```

В ОС IOS существуют два уровня команд: привилегированный и непривилегированный. Для каждого устройства следует задать пароль. Этот пароль является ключом для входа в привилегированный режим. Пароли для входа в привилегированный режим должны содержаться в секрете и требуют такого же обращения, как пароли суперпользователя или системного администратора.

```
Enter enable secret: \zippy2u
```

Термин «виртуальный терминал» обозначает одно логическое соединение терминала с устройством, работающим под управлением ОС IOS. Например, можно использовать виртуальный терминал, чтобы подключиться к маршрутизатору и затем с помощью пароля режима enable secret войти в режим исполнения привилегированных команд. В данном примере устанавливается один пароль виртуального терминала Zipmein для всех пяти сеансов:

```
Enter virtual terminal password: Zipmein
```

Следующий шаг в диалоге конфигурирования системы связан с заданием желаемых типов протоколов. На этом этапе необходимо разрешить использование устройством протокола простого управления сетью (Simple Network Management Protocol – SNMP).

```
Configure SNMP Network Management? [yes]: yes
Community string [public]: public
```

Теперь диалог конфигурирования системы задаст вопрос относительно необходимости конфигурирования протоколов:

```
Configure DECnet? [no]: no
Configure AppleTalk? [no]: yes Multizone networks?
[no]: yes
Configure IPX? [no]: yes
Configure IP? [yes]:
Configure IGRP routing? [yes]: no
```

После выбора протоколов диалог настройки ОС IOS потребует ввода информации по каждому интерфейсу, установленному на маршрутизаторе. Для каждого интерфейса локальной или глобальной сети требуется ввести информацию об используемом протоколе. Конфигурирование протоколов IP, IPX и AppleTalk для каждого интерфейса осуществляется таким образом:

```
Configuring interface parameters:
Configuring interface Ethernet0:
```

Следующий вопрос запрашивает данные о том, используется ли конфигурируемый интерфейс, т. е. необходимо ли, чтобы этот интерфейс был включен и не был административно заблокированным.

```
Is this interface in use? [no]: yes
```

Теперь необходимо сообщить маршрутизатору, чтобы на этом интерфейсе применялся протокол IP, а для него использовался IP-адрес 131.108.1.1 и маска подсети 255.255.255.128.

```
Configure IP on this interface? [no]: yes
IP address for this interface: 131.108.1.1
Number of bits in subnet field [0]: 9
Class B network is 131.108.0.0, 9 subnet bits, mask is /25
```

Для включения данных протоколов необходимо ввести информацию о номере IPX-сети и о значении кабельного диапазона сети AppleTalk.

```
Configure IPX on this interface? [no]: yes
IPX network number [1]: 4010
Configure AppleTalk on this interface? [no]: yes
Extended AppleTalk network? [no]: yes
AppleTalk starting cable range [0]: 4001
```

На этом маршрутизаторе также необходимо сконфигурировать интерфейс Serial0 с теми же протоколами сетевого уровня, что делается следующим образом:

```
Configuring interface Serial0:
Is this interface in use? [no]: yes
Configure IP unnumbered on this interface? no]: no
IP address for this interface: 131.108.242.6
Number of bits in subnet field [0]: 14
Class B network is 131.108.0.0, 8 subnet bits; mask is /30
Configure IPX on this interface? [no]: yes
IPX network number [2]: 2902
Configure AppleTalk on this interface? [no]: yes
Extended AppleTalk network? [no]: yes
AppleTalk network number [1]: 2902
```

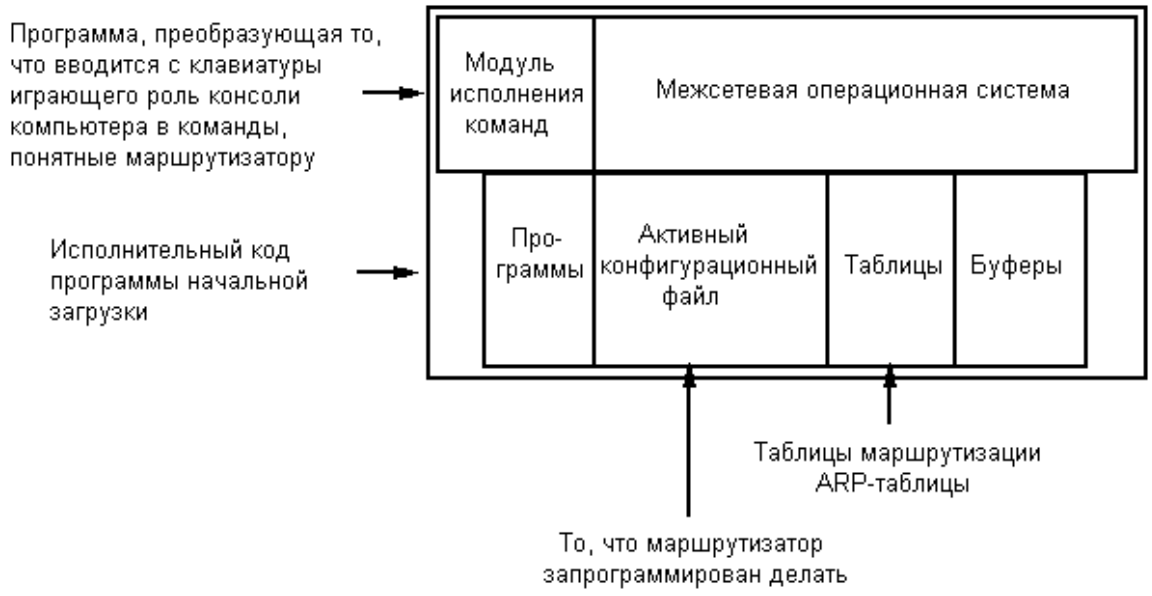


Рис. 2. В маршрутизаторе хранится активный конфигурационный файл

Результатом работы диалога конфигурирования системы является скрипт команд конфигурирования, который интерпретируется устройством. Сам по себе диалог конфигурирования системы не выполняет собственно конфигурирование устройства, а создает скрипт команд конфигурирования, который затем интерпретируется устройством и используется для конфигурирования. Скрипт написан на языке, который необходимо знать для того, чтобы настраивать изделия компании Cisco, работающие под управлением ОС IOS.

После нажатия клавиши <Return> маршрутизатор должен вывести командную строку следующего вида:

```
Singapore>
```

Начиная с этого момента, пользователь попадает в режим EXEC, который используется для исполнения команд ОС IOS.

1.2. Система помощи

В ОС IOS встроена система помощи, обратиться к которой можно из режима исполнения команд EXEC. Система помощи является контекстной, что означает, что оказываемая помощь зависит от того, что пользователь пытается сделать в ОС IOS на данный момент. Например, введя в командной строке знак ?, пользователь получит экран с информацией: в левой части выводимого текста содержатся сами команды, а в правой – короткие пояснения к каждой из них. Некоторые команды состоят из одного слова; система помощи ставит пользователя в известность об этом, показывая, что единственным выбором у него является нажатие после этой команды клавиши возврата каретки обозначая это действие, выводя на экран символы <cr>.

Систему помощи также можно использовать для определения возможных опций команд режима EXEC. ОС IOS содержит множество команд для получения информации о текущем состоянии устройства. Многие из этих команд начинаются со слова show.

Отметим, что ОС IOS повторяет начальную часть введенной с клавиатуры команды, так что необходимость в ее повторении отсутствует. Также встроенная в ОС IOS система помощи позволяет вводить команды не полностью, автоматически дополняя команду до конца при нажатии клавиши <Tab>. Если ввести часть команды, которая не имеет нескольких значений, и нажать клавишу <Tab>, то ОС IOS сама дополнит команду до конца. В качестве примера рассмотрим команду show sessions, которая позволяет увидеть все текущие Telnet-сеансы управления устройством через его каналы виртуального терминала.

Если ввести

```
Singapore>show sess
```

и затем нажать клавишу <Tab>, то ОС IOS автоматически дополнит команду:

```
Singapore>show sessions
```

При вводе неоднозначной команды, например,

```
Singapore>show s
```

ОС IOS не сможет ее дополнить, потому что данная команда может быть интерпретирована как show sessions и как show snmp. В этом случае нажатие на клавишу <Tab> для большинства систем приведет к срабатыванию встроенного в терминал зуммера.

Команда show sessions отличается от команды sessions. Команда sessions разрешает пользователю подключение к аппаратному модулю устройства с помощью сеанса виртуального терминала. Некоторые устройства Cisco имеют несколько аппаратных модулей, для обращения к каждому из которых нужен свой собственный виртуальный терминал. Примером этого являются модули маршрутизирующего коммутатора (Route Switch Module – RSM) и асинхронного интерфейса передачи данных (Asynchronous Transfer Mode – ATM) в коммутаторах типа Catalyst. Пользователь может обозначить, к какому из нескольких установленных модулей он хочет подключиться, с помощью команды session, введя после нее номер модуля. Например, если в коммутаторе Catalyst имеется модуль ATM, и он считается модулем номер 3 (обычно, это означает, что он стоит в третьем слоте расширения устройства), то для получения доступа к модулю можно сделать следующее:

```
Router>session 3
Trying ATM-3. . .
Connected to ATM-3.
Escape character is '^]'.
ATM>
```

Выполнив эту команду, система устанавливает сеанс с ATM-модулем. Этот сеанс отличается по функциям от Telnet-сеанса с самим маршрутизатором или коммутатором: теперь все исполняемые команды будут выполняться ATM-модулем.

1.3. Режимы конфигурирования

В режиме EXEC возможно исполнение команд двух основных уровней. Команда первого уровня исполняются в непривилегированном режиме. Непривилегированный режим обозначается символом «больше, чем» (>), размещаемым в командной строке после имени устройства, как показано ниже:

```
Singapore>
```

В этом режиме пользователю разрешено получать информацию о состоянии устройства, работающего под управлением IOS, но у него нет возможности изменять какие-либо параметры устройства.

Второй уровень включает команды привилегированного режима, который также известен под именем *разрешенный режим* (enable mode). Для того чтобы войти в этот режим, необходимо знать системный пароль, заданный в режиме enable secret. Чтобы переключиться из непривилегированного режима в привилегированный, нужно ввести команду enable:

```
Singapore>enable
Password:
Singapore#
```

В приведенном выше примере после выдачи запроса пароля в соответствующей командной строке вводится пароль режима enable secret (в нашем случае это!zippy2u), который не повторяется на экране терминала. При смене режима на привилегированный система обозначает это заменой в командной строке символа «>» символом «#» (так называемая «решетка»). Для того чтобы перейти из привилегированного режима в непривилегированный, следует ввести команду режима EXEC disable:

```
Singapore #disable
Singapore>
```

Следует отметить, что в привилегированном режиме пользователю доступно большее количество команд, нежели в непривилегированном, что и показывает система помощи:

```
Singapore#?
Exec commands:
<1-99> Session number to resume
access-enable Create a temporary Access-List entry
```

```
access-profile Apply user-profile to interface
access-template Create a temporary Access-List en-
try
attach Attach to system component
bfe For manual emergency modes setting
calendar Manage the hardware calendar
cd Change current directory
clear Reset functions
clock Manage the system clock
configure Enter configuration mode
connect Open a terminal connection
copy Copy from one file to another
debug Debugging functions (see also 'undebug')
delete Delete a file
dir List files on a filesystem
disable Turn off privileged commands
disconnect Disconnect an existing network connection
enable Turn on privileged commands
erase Erase a filesystem
exit Exit from the EXEC
format Format a filesystem
help Description of the interactive help system
lock Lock the terminal
login Log in as a particular user
logout Exit from the EXEC
microcode Microcode commands
mkdir Create new directory
mls Exec mis router commands
more Display the contents of a file
mpoa MPOA exec commands
mrinfo Request neighbor and version information
from a multicast router

–More–
```

Приведенный выше результат работы системы помощи для краткости усечен.

1.4. Конфигурирование памяти

Устройства Cisco имеют три блока памяти: оперативная, энергонезависимая память и флэш-память. Два из них отводятся под хранение конфигурации устройства, а третий – под хранение операционной си-

стемы IOS. Различие между командами конфигурирования и операционной системой заключается в том, что команды используются для формирования конфигурации устройства, а операционная система – это программное обеспечение, которое исполняется на этом устройстве. Для того чтобы выполнять связанные с памятью команды, необходимо находиться в привилегированном режиме (как показано в приводимых ниже примерах).

Текущую, или используемую, конфигурацию устройства, работающего под управлением ОС IOS, можно посмотреть с помощью команды show runing-config. Результатом работы данной команды является список команд конфигурирования ОС IOS, исполняемых устройством.

```
Singapore#show running-config
Current configuration:
hostname Singapore
enable secret 5 $2zu6m7$RMMZ8em/.8hksdkkh78p/TO
enable password !zippy4me
line vty 0 4
password Zipmein
snmp-server community public
ip routing
ipx routing
appletalk routing
no decnet routing
!
interface Ethernet0
ip address 131.108.1.1 255.255.255.128
ipx network 4010
appletalk cable-range 4001-4001
appletalk discovery
no mop enabled
!
–More–
```

Текущая конфигурация устройства хранится в оперативной памяти. При отключении питания устройства информация, содержащаяся в этом типе памяти, теряется. Если необходимо, чтобы после цикла отключения-включения питания устройстве восстанавливало текущую конфигурацию, ее следует записать в энергонезави-симую память, называемую памятью стартовой конфигурации. Для копирования конфигурации в энергонезависимую память используется команда режима EXEC copy, которая производит запись из первой указываемой памяти во вторую:

```
Singapore#copy running-config startup-config
[OK]
Singapore#
```

После ввода данной команды текущая конфигурация устройства, находящаяся в ОЗУ, копируется в качестве стартовой в энергонезависимую память. Также возможен обратный вариант, когда команда copy используется для копирования стартовой настройки в качестве текущей, как показано ниже:

```
Singapore#copy startup-config running-config
[OK]
Singapore#
```

Такое копирование может понадобиться, чтобы вернуться к стартовой конфигурации устройства после изменения текущей. Предположим, что в конфигурацию устройства внесено несколько изменений. После оценки поведения устройства оказывается, что изменения были неправильными. Если текущая конфигурация еще не была скопирована в качестве стартовой, то старую стартовую конфигурацию можно скопировать в качестве текущей. При копировании стартовой конфигурации из энергонезависимой памяти в ОЗУ в качестве текущей конфигурации следует помнить, что возможно слияние команд конфигурирования.

Для просмотра стартовой конфигурации следует ввести команду режима EXEC show startup-config:

```
Singapore#show startup-config
Using 1240 out of 7506 bytes
!hostname Singapore
enable secret 5 $2zu6m7$RMMZ8em/.8hksdkkh78p/TO
enable password !zippy4me
line vty 0 4
password Zipmein
snmp-server community public
ip routing
ipx routing
appletalk routing
no decnet routing
!interface Ethernet0
ip address 131.108.1.1 255.255.255.128
ipx network 4010
appletalk cable-range 4001-4001
```

```
appletalk discovery
no mop enabled
!-More-
```

Заметьте, что в первой строке указывается объем энергонезависимой памяти, использованный под стартовую конфигурацию, и общий ее объем. Стартовая и текущая конфигурации совпадают после выдачи команды copy running-config startup-config. Однако, если производится переконфигурирование устройства (как будет показано далее), и измененная текущая конфигурация не сохраняется в качестве стартовой, то в следующий раз при отключении и включении питания устройство вернется к последней конфигурации, сохраненной в энергонезависимой памяти. Стартовая конфигурация может быть полностью удалена из энергонезависимой памяти с помощью команды erase startup-config:

```
Singapore#erase startup-config
Erasing the nvram filesystem will remove all files!
Continue? [confirm]
[OK]
Singapore#
```

Если после этого перезагрузить маршрутизатор, отключив электропитание или используя привилегированную команду режима EXEC reload, то стартовая конфигурация будет пустой. Такая последовательность действий (стирание энергонезависимой памяти и перезагрузка устройства) приведет к тому, что вновь будет запущен описанный ранее в этой главе режим диалога конфигурирования системы.

Флэш-память – это то место, где устройства Cisco хранят двоичные исполняемые образы ОС IOS, которые и представляют собой операционную систему устройства. Не следует путать образы ОС IOS с ее конфигурациями: конфигурация ОС IOS говорит устройству о его текущей конфигурации, тогда как образ ОС IOS является той самой двоичной программой, которая выполняет синтаксический анализ и собственно конфигурацию.

Устройство может хранить несколько образов ОС IOS. Это зависит от объема установленной флэш-памяти и размера образов операционной системы. Если в данном устройстве хранится несколько образов ОС IOS, то пользователь может указать, какой именно образ ОС IOS следует исполнять устройству после перезагрузки. Получаемые от компании Cisco образы ОС IOS могут быть скопированы в устройство с использованием нескольких различных протоколов передачи файлов, имеющих в

основе протокол TCP/IP, включая простой протокол передачи файлов (Trivial File Transfer Protocol – TFTP), протокол передачи файлов (File Transfer Protocol – FTP), а также протокол удаленного копирования для платформы UNIX – UNIX remote copy protocol (rep).

Решение об использовании протокола FTP или TFTP зависит от нескольких факторов.

- Наличие данных протоколов на сервере или рабочей станции (зависит от системного администратора). Например, если на сервере или рабочей станции протокол TFTP не установлен, то для передачи придется воспользоваться протоколом FTP.
- Тип сетевого соединения между сервером (рабочей станцией) и устройством под управлением IOS. Например, если сервер или рабочая станция включены непосредственно в сеть, в которую подключен и маршрутизатор, то протокол TFTP будет функционировать нормально, и время передачи данных не будет слишком велико. Если же между сервером или рабочей станцией расположено одно или несколько устройств, то протокол FTP будет работать лучше, сокращая время передачи образов ОС IOS из сервера в устройство.
- Уровень безопасности, который необходимо сохранять при передаче образов ОС IOS из сервера. Протокол TFTP не требует для передачи никакой идентификации или аутентификации. В протоколе FTP для начала передачи информации достаточно ввести имя пользователя и пароль.

Все команды, используемые для перезаписи во флэш-память образов ОС IOS, выполняют оценку свободного пространства в памяти и, если это необходимо для высвобождения дополнительного объема памяти, предлагают стереть или сжать предыдущее содержимое флэш-памяти. С другой стороны, возможны ситуации, при которых надо стереть все содержимое флэш-памяти или его часть вне зависимости от процесса передачи. Все содержимое флэш-памяти можно стереть с помощью привилегированной команды режима EXEC erase flash. Чтобы из флэш-памяти стереть конкретный файл, нужно использовать команду delete. Например, для удаления из флэш-памяти файла образа ОС IOS c2500-i-1.120.P.bin вводится привилегированная команда режима EXEC delete c2500-i-1.120.P.bin. В устройствах Cisco, оснащенных внешними картами флэш-памяти (обычно устанавливаемыми в слот, который называется slot0), команда delete не стирает файл, а только помечает его как файл, доступный для удаления, и соответственно не высвобождает пространство флэш-памяти. Для завершения процесса удаления файла необходимо исполнить команду squeeze.

1.5. Пользовательский режим

Для конфигурирования устройства, работающего под управлением IOS, следует использовать привилегированную команду режима EXEC configure. Эта команда имеет три варианта:

- конфигурирование с терминала;
- конфигурирование из памяти;
- конфигурирование через сеть.

При вводе команды configure ОС IOS просит указать тот ее вариант, который будет использоваться:

```
Singapore#configure
Configuring from terminal, memory, or network [ter-
minal]?
```

Вариант по умолчанию, который стоит первым в перечне, позволяет осуществлять конфигурирование устройства в реальном времени с использованием терминала. Команды выполняются ОС IOS сразу после их введения:

```
Singapore#configure
Configuring from terminal, memory, or network [ter-
minal]?
Enter configuration commands, one per line. End
with CTRL+Z.
Singapore(config)#
```

После выполнения команды система изменяет вид командной строки, показывая, что она находится в режиме конфигурирования и позволяет вводить команды конфигурирования. По окончанию набора команды вводится комбинация клавиш <Ctrl+Z> (AZ). В приведенном ниже примере с помощью команды глобального конфигурирования hostname имя Singapore изменяется на Seoul:

```
Singapore #configure
Configuring from terminal, memory, or network [ter-
minal]?
Enter configuration commands, one per line. End
with CTRL+Z.
Singapore(config)#hostname Seoul
Seoul(config)#^Z
Seoul!
```

В данном примере команда исполняется немедленно, и имя устройства изменяется. Таким образом, для активации команд не нужно текущую конфигурацию переносить в стартовую.

Второй вариант команды – настройка из памяти – позволяет копировать хранящуюся в энергонезависимой памяти стартовую конфигурацию устройства в ОЗУ, где находится текущая конфигурация. Этот вариант полезен в тех случаях, когда после изменения в реальном времени какого-либо конфигурационного параметра необходимо вернуться к стартовой конфигурации. В данном случае команда configure выполняет те же самые функции, что и команда copy startup-config running-config, которая была описана в предыдущем разделе:

```
Seoul#configure
Configuring from terminal, memory, or network [ter-
minal]? memory
Singapore#
```

Третий вариант – настройка по сети – позволяет загружать файл конфигурации с TFTP-сервера:

```
Singapore#configure
Configuring from terminal, memory, or network [ter-
minal]? network
Host or network configuration file [host]?
Address of remote host [255.255.255.255]?
131.108.20.45
Name of configuration file [singapore-confg]?
Configure using singapore-confg from 131.108.20.45?
[confirm]
Loading singapore-confg !![OK]
Singapore#
```

Во всех приведенных выше примерах команды configure предлагаемые ОС IOS значения по умолчанию (показаны в квадратных скобках) принимались нажатием клавиши возврата каретки в ответ на вопрос.

TFTP представляет собой протокол, который позволяет ОС IOS запрашивать конкретный файл с TFTP-сервера. Протокол TFTP использует IP-протокол, и поэтому для нормальной работы этого варианта команды необходимо иметь настроенную и работающую IP-маршрутизацию между устройством и TFTP-сервером. Когда конфигурирование устройства с ОС IOS производится с TFTP-сервера, оно по умолчанию пытается загрузить файл, название которого состоит из имени устройства, за кото-

рым следует цепочка символов -confg. В примере ниже устройство с именем Singapore безуспешно пытается загрузить по умолчанию файл singapore-confg:

```
Singapore#configure
Configuring from terminal, memory, or network [ter-
minal]? network
Host or network configuration file [host]?
Address of remote host [255.255.255.255]?
131.108.20.45
Name of configuration file [singapore-confg]?
Configure using singapore-confg from 131.108.20.45?
[confirm]
Loading singapore-confg ... [timed out]
Singapore#
```

Устройство может потерпеть неудачу при загрузке файла конфигурации из-за проблем со взаимодействием в IP-сети или из-за нарушений правил протокола TFTP.

1.6. Команды конфигурирования

Команды конфигурирования используются для формирования конфигурации устройства.

Как было показано в предыдущем разделе, эти команды могут вводиться с терминала, загружаться из стартовой конфигурации или сгружаться в виде файла с использованием протокола TFTP и команды configure. Все команды конфигурирования должны вводиться в устройство, которое находится в режиме конфигурирования, а не в режиме исполнения команд EXEC. Команда конфигурирования, введенная в командной строке с именем устройства, считается неправильной и не воспринимается:

```
Singapore#hostaame ^ Seoul
% Invalid input detected at '^' marker
```

Команда, введенная в режиме конфигурирования, – верна.

```
Singapore#configure
Configuring from terminal, memory, or network [ter-
minal]?
Enter configuration commands, one per line. End
with CTRL+Z.
```

```
Singapore(config)# hostname Seoul
Seoul(config)#AZ
Seoul!
```

Все команды ОС IOS делятся на три категории:

- глобальные команды;
- основные команды;
- подкоманды.

Глобальными называются команды, действие которых распространяется на всю ОС IOS. Примером таких команд являются рассмотренные в этой главе команды hostname, enable secret и ip routing. Эти команды были использованы в скрипте команд конфигурирования, созданном диалогом конфигурирования системы. Применение любой из этих команд вносит изменения в конфигурацию ОС IOS, не требуя при этом использования дополнительных команд. Например, команда hostname задает имя устройства, команда enable secret определяет пароль, который будет использоваться при входе в привилегированный режим, а команда ip routing включает IP-маршрутизацию.

Основные команды позволяют подкомандам конфигурировать устройство. Сами эти команды не вносят изменений в конфигурацию устройства. В приведенном ниже примере основная команда interface Ethernet0 сообщает ОС IOS о том, что последующие подкоманды будут относиться непосредственно к интерфейсу локальной сети с именем Ethernet0. В этом примере подкоманда ip address назначает IP-адрес интерфейсу Ethernet0:

```
Singapore#configure
Configuring from terminal, memory, or network [ter-
minal]?
Enter configuration commands, one per line. End
with CTRL+Z.
Singapore(config)#interface EthernetO
Singapore(config-if)#ip address 131.108.1.1
255.255.255.128
Singapore(config-if)#^Z
Singapore#
```

Как уже было сказано, в данном примере ОС IOS восприняла команду interface Ethernet0 как основную. ОС сообщает об этом, изменяя заголовок командной строки с Singapore (config) на Singapore (config-if). Тем самым она указывает на то, что последующие команды являются подкомандами и будут относиться к интерфейсу. Сама команда interface

Ethernet0 не конфигурирует устройство – для этого она должна быть дополнена подкомандами.

Основные команды требуют четкого соответствия с контекстом подкоманд. Например, основная команда ip address 131.108.1.1 255.255.255.128 для правильной интерпретации требует указания конкретного интерфейса. Комбинация основной команды с подкомандой позволяет конфигурировать устройство.

Что касается ОС IOS версии 12.0, то в ней для некоторых основных команд существует дополнительный уровень подкоманд конфигурирования. Например, при конфигурировании ATM-интерфейса, который будет рассматриваться в главе 3, с помощью основной команды interface atm0 задается интерфейс для настройки. Затем с помощью подкоманды pvc [name] vpi/vci для этого интерфейса может указываться идентификатор виртуального пути (vpi) и идентификатор виртуального канала (vci). Эта подкоманда имеет свою подкоманду дополнительного уровня, которая позволяет указать качество ATM-сервиса, ассоциируемого со значением VPI/VCI. Скажем, в примере ниже для ATM-интерфейса значение VPI/VCI устанавливается равным 5/42 при передаче с заранее не заданной скоростью (unspecified bit rate – UBR) в 384 Кбит/с:

```
Router#configure
Configuring from terminal, memory, or network [ter-
minal]?
Enter configuration commands, one per line. End
with CTRL+Z.
Router(config)#interface atmO
Router(config-if)#pvc 5/42
Router(config-if)#ubr 384
Router(config-if)#^Z
Router#
```

Эта конфигурация в маршрутизаторе будет иметь следующий вид (показана лишь та часть экрана конфигурации, которая имеет отношение к рассматриваемому вопросу):

```
Router#show running-config
!
Current configuration:
interface ATMO
pvc 5/42
ubr 384
```

Как было показано в предыдущем разделе, конфигурирование устройства, работающего под управлением ОС IOS, может осуществляться с использованием файла конфигурации, загружаемого по протоколу TFTP с помощью команды configure с опцией network. Этот файл должен быть текстовым и содержать требуемые для конфигурирования устройства глобальные и основные команды с подкомандами. В процессе загрузки файла конфигурации устройство сразу же интерпретирует команды конфигурирования и исполняет их. Все происходит точно так же, как если бы эти команды вводились с помощью команды configure с опцией terminal.

Встроенная в ОС IOS **система помощи** доступна и при конфигурировании устройства. Для получения списка имеющихся опций конфигурирования достаточно в любое время в процессе конфигурирования ввести команду в виде знака вопроса (?). В представленном ниже примере эта функция осуществляет поиск глобальных команд, доступных в режиме конфигурирования:

```
Singapore(config)#?
Configure commands:
aaa Authentication, Authorization and Accounting
access-list Add an access list entry
alias Create command alias
arp Set a static ARP entry
async-bootp Modify system bootp parameters
banner Define a login banner
boot Modify system boot parameters
bridge Bridging Group
buffers Adjust system buffer pool parameters
busy-message Display message when connection to
host fails
cdp Global CDP configuration subcommands
chat-script Define a modem chat -script
clock Configure time-of-day clock
config-register Define the configuration register
default-value Default character-bits values
dialer-list Create a dialer list entry
dnsix-dmdp Provide DMDP service for DNSIX
dnsix-nat Provide DNSIX service for audit trails
–More–
```

Встроенная система помощи может также использоваться для получения списка подкоманд, которые можно вводить при вводе той или

иной команды. В следующем примере осуществляется поиск подкоманд, доступных при конфигурировании интерфейса Ethernet0 на использование протокола IP:

```
Singapore#configure
Configuring from terminal, memory, or network [ter-
minal]?
Enter configuration commands, one per line. End
with CTRL+Z.
Singapore(config)#interface EthernetO
Singapore(config-if)#ip ?
Interface IP configuration subcommands:
access-group Specify access control for packets
accounting Enable IP accounting on this interface
address Set the IP address of an interface
bandwidth-percent Set EIGRP bandwidth limit
broadcast-address Set the broadcast address of an
interface
directed-broadcast Enable forwarding of directed
broadcasts
gdp Gateway Discovery Protocol
hello-interval Configures IP-EIGRP hello interval
helper-address Specify a destination address for
UDP broadcasts
hold-time Configures IP-EIGRP hold time
irdp ICMP Router Discovery Protocol
mask-reply Enable sending ICMP Mask Reply messages
mobile Mobile Host Protocol
mtu Set IP Maximum Transmission Unit
policy Enable policy routing
-More-
```

Для **удаления команды конфигурирования** из устройства в начало команды конфигурирования добавляется ключевое слово no. В примере ниже показано удаление IP-адреса, присвоенного интерфейсу Ethernet0:

```
Singapore#configure
Configuring from terminal, memory, or network [ter-
minal]?
Enter configuration commands, one per line. End
with CTRL+Z.
```

```
Singapore(config)#interface EthernetO
Singapore(config-if)#no ip address 131.108.1.1 255.255.255.0
Singapore(config-if)#^Z
Singapore#
```

Для удаления любой команды (глобальной, основной или подкоманды) необходимо следовать этой же процедуре.

Команды конфигурирования, используемые ОС IOS **по умолчанию**, не показываются в результатах исполнения команд show running-config или show startup-config. Если ввести такую команду, то устройство воспримет ее и не выдаст сообщения об ошибке. Например, как будет показано в следующей главе, все интерфейсы последовательной передачи данных в маршрутизаторах Cisco по умолчанию используют инкапсуляцию по высокоуровневому протоколу управления каналом передачи данных (High-Level Data Link Control – HDLC). Соответственно, ввод подкоманды конфигурирования интерфейса encapsulation hdlc при конфигурировании последовательного интерфейса не приведет к появлению новой строки в конфигурации маршрутизатора.

Все команды ОС IOS также имеют значение по умолчанию. Для возврата значения любой глобальной, основной команды или подкоманды в значение, принимаемое ею по умолчанию, эта команда предваряется командой конфигурирования default. Многие команды ОС IOS по умолчанию действуют противоположно их прямому действию, и поэтому использование этих команд со значением по умолчанию равносильно их использованию в форме с ключевым словом **no** впереди, которая была показана в предыдущем разделе. Например, представленная ниже конфигурация приведет к удалению IP-адреса, присвоенного интерфейсу EtehernetO маршрутизатора в Сингапуре:

```
Singapore#configure
Configuring from terminal, memory, or network [ter-
minal]?
Enter configuration commands, one per line. End
with CTRL+Z.
Singapore(config)#interfaoe Ethernet0
Singapore(config-if)#default ip address
Singapore(config-if)#*Z
Singapore#
```

Однако некоторые команды по умолчанию имеют конкретную конфигурацию. В таких случаях команда default приводит к принятию командой конфигурирования ее значения по умолчанию.

```
Singapore#configure
Configuring from terminal, memory, or network [terminal]?
Enter configuration commands, one per line. End
with CTRL+Z.
Singapore(config)#default hostname
Singapore(config-if}#AZ
Router!
```

В этом примере команде hostname разрешается присвоить устройству имя по умолчанию, каковым является имя Router.

Новая команда конфигурирования может **замещать старую**. В этом случае ОС IOS автоматически удаляет старую команду. С другой стороны, новая команда может не замещать, а **сливаться с уже существующей командой**. В качестве примера слияния команд можно привести случай использования двух команд snmp-server. Представим, что создается следующая конфигурация:

```
Singapore#configure
Configuring from terminal, memory, or network [ter-
minal]?
Enter configuration commands, one per line. End
with CTRL+Z.
Singapore(config)#snmp-server community public
Singapore(config)#^Z
Singapore#
```

После этого принимается решение о замене конфигурации команды snmp-server следующей:

```
Singapore#configure
Enter configuration commands, one per line. End
with CTRL+Z.
Configuring from terminal, memory, or network [ter-
minal]?
Singapore(config)#snmp-server community zipnet
Singapore(config)#^Z
Singapore#
```

Поскольку возможно использование нескольких команд snmp-server, вторая команда snmpserver сливается с существующей конфигурацией, и обе команды являются активными, что и показывает соответствующая часть результата исполнения команды show running-config:

```
!
snmp-server community public
snmp-server community zipnet
!
```

Для того чтобы заменить первую команду конфигурирования snmp-server второй, необходимо выполнить следующие действия:

```
Singapore#configure
Configuring from terminal, memory, or network [ter-
minal]?
Enter configuration commands, one per line. End
with CTRL+Z.
Singapore(config)#no snmp-server community public
Singapore(config)#snmp-server community zipnet
Singapore(config)#^Z
Singapore#
```

Примером несливающейся команды является команда hostname, которая устанавливает имя устройства. В примере ниже маршрутизатору в Сингапуре присваивается новое имя:

```
Singapore#configure
Configuring from terminal, memory, or network [ter-
minal]?
Enter configuration commands, one per line. End
with CTRL+Z.
Singapore(config)#hostname Sing-router
Sing-router(config)#^Z
Sing-router#
```

Команда hostname сразу после введения меняет предыдущую конфигурацию. Результат исполнения команды show running-config показывает наличие в конфигурации только одной команды hostname:

```
!
hostname Sing-router
!
```

Следует помнить об этой особенности ОС IOS при добавлении новых команд в существующую конфигурацию.

2. ОСНОВЫ АДМИНИСТРИРОВАНИЯ И УПРАВЛЕНИЯ СЕТЕВЫМИ УСТРОЙСТВАМИ CISCO

2.1. Основы управления доступом

ОС IOS компании Cisco предлагает ряд механизмов и протоколов, которые помогают в управлении доступностью устройств. Эти базовые механизмы управления доступом могут оказать помощь в ограничении круга тех, кто обращается к устройствам сети, а также того, что они делают на каждом из устройств. Таким образом обеспечивается безопасность сети и создается протокол любых изменений в сети.

Подключение к виртуальному терминалу с использованием протокола Telnet и оболочки. Общими методами доступа к устройству, работающему под управлением ОС IOS, являются подключение через порт консоли или подключение по каналам виртуального терминала (vty). Каналы виртуального терминала представляют собой программное обеспечение, которое дает возможность подключаться к маршрутизатору по сети данных. Работающее под управлением устройство также поддерживает пять одновременных сеансов через каналы виртуального терминала.

Использование клиента протокола Telnet и клиента защищенной оболочки Shell (SSH) – вот два наиболее общеупотребительных метода подключения виртуального терминала. Для создания незащищенного соединения с серверным программным обеспечением, работающим на канале виртуального терминал клиент использует стандартный протокол. По умолчанию все основанные на ОС IOS устройства имеют Telnet-сервер активированным на всех каналах виртуального терминала.

SSH представляет собой протокол, который обеспечивает защищенное и шифрованное соединение между SSH-клиентом и сервером, работающим на канале виртуального терминала. Это соединение по своим функциональным характеристикам подобно соединению протокола Telnet. В отличие от Telnet-сервера, SSH-сервер не является активированным по умолчанию на каналах виртуального терминала.

Чтобы выбрать, Telnet- или SSH-клиент использовать в конкретной локальной системе, обратитесь за помощью к системному администратору. Исполняющее ОС IOS устройство может играть роль либо Telnet-клиента, либо SSH-клиента, для этого в строке приглашения режима EXEC вводится команда telnet или ssh.

SSH-клиенты и серверы могут обеспечить аутентификацию пользователя с помощью системы шифрования по открытому ключу, изоб-

ретенной Ривестом (Rivest), Шамиром (Shamir) и Аделманом (Adelman) (система RSA). Однако реализованная в SSH-клиенте RSA-аутентификация пользователя не поддерживается в SSH-сервере для ОС IOS компании Cisco. ОС IOS осуществляет аутентификацию пользователей только с применением комбинации из идентификатора пользователя и пароля. Хотя SSH-сервер ОС IOS использует метод RSA для генерации пары ключей, которые затем применяются при установке шифрованного сеанса с клиентом.

Протокол SSH обеспечивает защиту соединения между клиентом и сервером за счет применения алгоритмов шифрования стандарта DES (56-разрядная длина ключа) или Triple DES (168-разрядная длина ключа). Следует помнить, что не все версии ОС IOS поддерживают стандарты DES или Triple DES. Поэтому необходимо воспользоваться командой show version и проверить, поддерживает ли версия, исполняемая на устройстве, эти алгоритмы шифрования.

Активация SSH-сервера. Чтобы активировать SSH-сервер и позволить SSH-клиентам подключаться к каналам виртуального терминала, работающее с ОС IOS устройство должно иметь соответствующим образом сконфигурированные имя хост-машины и имя домена. Как обсуждалось ранее, эти параметры конфигурируются *с* помощью команд глобального конфигурирования hostname и ip domain-name.

Для конфигурирования SSH-сервера необходимо сгенерировать пару RSA-ключей используемых для шифрования сеанса между клиентом и сервером. Генерация пары ключей на устройстве, работающем с ОС IOS, осуществляется с помощью команды глобального конфигурирования crypto key generate rsa. После генерации пары RSA-ключей для устройства активация SSH-сервера на каналах виртуального терминала происходит автоматически. Удаление RSA-ключа выполняется с помощью команды глобального конфигурирования crypto key zeroize rsa, при этом автоматически деактивируется и SSH-сервер.

Активирует SSH-сервер на всех каналах виртуального терминала команда глобального конфигурирования ip ssh**:**

```
SF-1#configure
Configuring from terminal memory or network [termi-
nal]?
Enter configuration commands one per line. End with
CNTL/Z.
SF-1(config)#crypto key generate rsa
SF-1(config)#ip hss
SF-1(config)#^Z
```

Проверка конфигурации протокола SSH. Для просмотра открытого RSA-ключа, используемого протоколом SSH, применяется команда режима EXEC show crypto key mypubkey rsa:

```
SF-l>show crypto key mypubkey rsa
% Key pair was generated at: 19:01:46 EOT Aug 7
2000 Key name: SF-l.zipnet. om
Usage: General Purpose Key Key Data:
305C300D 06092A86 4886F70D 01010105 00034BOO
30480241 OOC6F6D1 CCBF8B9A
6D3E451F C362DD75 866F084B 04F43C95 OB68BA44
OB8D5B8C 35264CFA 04B8B532
OFF6473C 4768C46F CD820DAF B7CA8C75 4977CF6E
7ED1ACE3 FF020301 0001
% Key pair was generated at: 23:14:52 EOT Aug 29
2000
Key name: SF-l.zipnet. om.server
Usage: Encryption Key
Key Data:
307C300D 06092A86 4886F70D 01010105 00036BOO
30680261 OOC5D98C E628790E
17BOBA2B C31C9521 8543AE24 F19E0988 BF2901DC
11D723EF 3512DD29 C28DBC53
8112755C 307AC527 14B955FO AODD29AD AE53BAOO
4D84657B 4C605E8E 6EBDDB6E
4FB98167 8616F964 E067604A F852A27D 1F9B7AFF
3EC73F5C 75020301 0001
```

Более того, на устройстве, которое работает под управлением ОС IOS, можно с помощью команды show ip ssh посмотреть активные SSH-сеансы:

```
SF-l#show ip ssh
Connection Version Encryption State Username
0 1.5 3DES 6 admin
```

Защита порта консоли и виртуальных терминалов. На уровне отдельных устройств, работающих с ОС IOS, можно устанавливать пароль для доступа к порту консоли, для чего следует воспользоваться основной командой ОС IOS line console 0 и субкомандой password. Для каналов виртуального терминала добавить пароли можно с помощью основной команды line vty о 4 и субкоманды password. Используя суб-

команду access-class команды line, можно задавать список IP-адресов, которые будут иметь возможность подключаться или быть достижимыми через терминальные каналы устройства, работающего с ОС 1OS. Далее, с помощью ключевого слова in или out можно задавать наложение класса доступа в отношении входящих или исходящих сеансов. Эта субкоманда использует список доступа, квалифицирующий IP-адреса до начала каких-либо входящих или исходящих сеансов. Субкоманда access-class может быть применена для разрешения выхода в каналы виртуального терминала исполняющего ОС IOS устройства только с рабочих станций администратора сети, что является дополнительным методом защиты доступа к устройству.

В примере ниже маршрутизатор SF-1 конфигурируется паролем Zipmein для консоли и виртуального терминала:

```
SF-1#configure
Configuring from terminal memory or network [terminal]?
Enter configuration commands one per line. End with
CNTL/Z.
SF-1(config)#line console 0
SF-1(config)#password Zipmein
SF-1(config)#line vty 0 4
SF-1 (config)#password Zipmein
SF-1(config)#^Z
```

В рабочей конфигурации и конфигурации запуска пароли консоли и виртуального терминала хранятся в виде открытого текста. Если нужно зашифровать все пароли, выводимые на экран какой бы то ни было командой режима EXEC (например, show running-config или show startup-config), воспользуйтесь командой глобального конфигурирования service password-encryption. В результате исполнения этой команды пароли в незашифрованном виде нельзя будет увидеть ни через одну команду режима EXEC. Забытый пароль можно восстановить с помощью задокументированной для каждого типа устройств процедуры компании Cisco.

Альтернативой конфигурированию паролей на каждом устройстве с целью контроля за доступом является использование в сети протокола управления доступом. Такие протоколы управления доступом выполняют три функции: аутентификацию, авторизацию и учет, которые известны под коллективным названием AAA. (от англ, authentication, authorization, accounting)

Аутентификация – это процесс идентификации и проверки личности пользователя. В рамках ОС IOS возможны несколько методов

аутентификации пользователя, включая использование комбинации имени пользователя и пароля или передачу уникального ключа. Процесс *авторизации* определяет то, что пользователь может делать после успешной аутентификации, например, он может получить доступ к определенным сетевым устройствам и хост-машинам. Функция *учета* представляет собой метод регистрации того, что пользователь делает или сделал.

AAA-функции требуют наличия двух составляющих: клиента, который функционирует на устройстве, работающем под ОС IOS компании Cisco, и серверного программного обеспечения для управления доступом, которое обычно исполняется на сетевой рабочей станции. Наиболее общеупотребительными протоколами, используемыми для обеспечения связи между AAA-клиентом на устройстве компании Cisco серверным программным обеспечением для управления доступом, являются служба удаленной аутентификации пользователей, устанавливающих соединение по телефонным линиям (The Remote Authentication Dial-In User Service – RADIUS) и система управления доступом на основе применения контроллера управления доступом к терминалу (Terminal Access Controller Access Control System – TACACS+).

Предположим, что пользователь с помощью Telnet-приложения подключается маршрутизатору, в конфигурации которого отсутствует протокол управления доступом. Пользователь немедленно получает приглашение ввести пароль канала виртуального терминала в следующем виде:

```
% telnet Singapore
Trying...
Password:
```

Введя правильный пароль, пользователь получает доступ к режиму EXEC маршрутизатора. Такой пользователь не является предметом аутентификации или авторизации и может выполнять любую задачу (включая вход в привилегированный режим если известен пароль). Более того, пользователь, выполняющий такое действие, регистрируется в журнале. Очевидно, что такая открытая политика неприемлема почти во всех сетях. Единственным исключением могут быть лаборатории или испытательные полигоны, когда неконтролируемый доступ к устройству многих пользователей не оказывает существенного влияния на степень защиты, конфигурацию и производительность сети.

Если устройство, работающее под управлением ОС IOS, имеет настройки на использование протокола управления доступом, то оно приглашает пользователя ввести имя и пароль:

```
% telnet Singapore
Trying...
Username: allan
Password:
```

При использовании протокола управления доступом устройство, работающее с ОС IOS, выполняет следующие действия.

1. Получая внешний запрос на установление соединения по протоколу Telnet, клиент управления доступом в устройстве предлагает ввести имя пользователя и пароль.

2. Клиент управления доступом опрашивает пользователя и затем в виде запроса на аутентификацию посылает комбинацию из имени пользователя и пароля сервер управления доступом.

3. Сервер управления доступом выполняет аутентификацию комбинации имени пользователя и пароля. Эта комбинация либо проходит аутентификацию, либо нет, при этом клиенту отсылается назад соответствующее сообщение. Сервер может также дать клиенту информацию о степени авторизации пользовать Сервер открывает транзакцию.

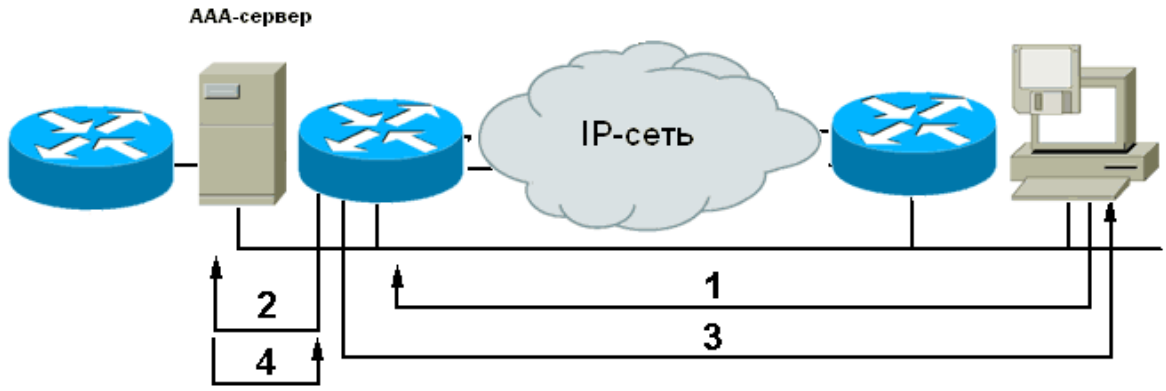
4. Клиент управления доступом принимает или отвергает комбинацию имени пользователя и пароля. Если комбинация принимается, то пользователь получает право доступа к системе и авторизуется на выполнение действий, определенных в авторизационной информации, переданной сервером.

Эта последовательность взаимодействий между клиентом и сервером управления доступом показана на рис. 3.

Активация ААА-служб. Чтобы активировать все ААА-службы в ОС IOS, необходимо воспользоваться командой глобального конфигурирования aaa new-model.

Затем, используя команды глобального конфигурирования aaa authentication, aaa authorization и aaa accounting, можно активировать ААА-клиент с конкретной конфигурацией аутентификации, авторизации и учета. Каждая из ААА-команд конфигурируется с помощью списков методов. Список методов представляет собой сконфигурированный список, описывающий ААА-методы, которые будет пытаться в порядке следования применить клиент для аутентификации пользователя, авторизации его деятельности и учета действий. Например, с помощью списков методов можно задать несколько механизмов аутентификации в попытке все-таки аутентифицировать пользователя, если начальный метод потерпит неудачу. Устройство с ОС IOS пытается использовать для аутентификации пользователя первый метод из перечисленных в списке. Если этот метод не дает отклика, устройство пробует

применить следующий метод аутентификации из приведенных в списке. Это продолжается до тех пор, пока не произойдет успешного завершения общения по одному из методов аутентификации, указанному в списке, или пока не будут использованы все заданные методы. Списки методов авторизации и учета работают аналогично тому, как было описано выше для списка методов аутентификации.



1. Запрос Telnet-соединения, приглашение ввести имя пользователя и пароль
2. Отправка имени пользователя/пароля
3. Аутентификация (да/нет)
3. Аутентификация (да/нет)

Рис. 3. В роли AAA-клиента устройство, работающее под управлением ОС IOS, обменивается информацией с AAA-сервером для решения задачи управления доступом

Двумя наиболее употребительными AAA-протоколами являются RADIUS и TACACS+. С помощью команд глобального конфигурирования aaa authentication, aaa authorization и aaa accounting использование в качестве метода протокола RADIUS можно задать, применив о group radius, а протокола TACACS+ – опцию group tacacs+.

Команда aaa authentication задает протоколы аутентификации с помощью упорядоченного списка методов, которые устройство может пытаться использовать для верификации доступа. Команда aaa authorization позволяет задавать выполнение авторизации по каждой команде режима EXEC или только в начале сеансов режима EXEC или сетевых сеансов (например сеансов протокола PPP). Она также позволяет задавать протокол, используемый при выполнении этих задач. В свою очередь, команда aaa accounting определяет события, после которых производится отправка серверу отчетных сообщений, например, в начале или конце каждого (пользователя либо после каждой команды. Эта команда также задает тип учета, выполняемого AAA-клиентом. Можно вести учет деятельности системы IOS, связанных с сетью служб

(например, PPP или ARAP) и EXEC-сеансов. Для пересылки учетной информации от AAA-клиенту к AAA-серверу можно использовать как протокол TACACS+, так и протокол RADIUS.

В примере ниже выполняется конфигурирование AAA-процессов на маршрутизаторе в Сингапуре. С помощью команды глобального конфигурирования aaa authentic login осуществляется активация AAA-аутентификации сеансов регистрации в системе. Первым протоколом аутентификации в списке методов стоит TACACS+. Если протокола TACACS+ не способен установить контакт с сервером для выполнения аутентификации, устройство будет выполнять ее с помощью второго метода – команд глобального конфигурирования enable secret или enable password. Этот список методов виден в команде aaa authentication login как опция group tacacs+, за корой следует опция enable.

При конфигурировании команд aaa authorization и aaa accounting и используется та же логика, которая применялась для команды aaa authenticate. Используя в команде глобального конфигурирования aaa authorization опции exec и network, можно задать различные методы авторизации для сеансов режима Exec и сетевых сеансов (например сеансов протокола PPP). Обозначающее метод ключевое слово if-authenticated говорит AAA-клиенту, чтобы тот в случае успешной аутентификации сеанса выдавал авторизацию.

Наконец, учетные сообщения по всем EXEC-сеансам выдаются только после окончания использования ими протокола TACACS+, в свою очередь, используемого командой глобального конфигурирования aaa accounting.

```
Singapore#configure
Configuring from terminal memory or network [termi-
nal]?
Enter configuration commands one per line. End with
CNTL/Z.
Singapore(config)#aaa new-model
Singapore(config)#aaa authentication login default
group tacacs+ enable
Singapore(config)#aaa authorization exec group tac-
acs+ if-authenticated
Singapore(config)#aaa authorization network group
radius if-authenticated
Singapore(config)#aaa accounting exec stop-only
group tacacs+
Singapore(config)#^Z
```

В этом примере опция group tacacs+ инструктирует устройство с ОС IOS связываться с TACACS+-сервером, задаваемым командой глобального конфигурирования tacacs-server host, что обсуждается в разделе «Протокол TACACS+». Используя команду глобального конфигурирования aaa server group и субкоманду server, можно вводить определения своих собственных групп AAA-серверов с задаваемым пользователем именем группы. Задаваемая пользователем группа AAA-серверов полезна в тех случаях, когда есть группа пользователей, работающих с одним AAA-сервером, и другая группа пользователей, которые работают с другим AAA-сервером. Эти две группы могут использовать или не использовать один и тот же AAA-протокол (скажем, RADIUS). До изобретения групп AAA-серверов все пользователи для каждого метода могли использовать только один набор AAA-серверов. Чаще всего группы AAA-серверов применяются для аутентификации удаленных, устанавливающих соединение по коммутируемым каналам пользователей с помощью одного RADIUS-сервера и аутентификации сетевых администраторов – с помощью другого.

Протокол RADIUS. Впервые спецификация протокола RADIUS была опубликована компанией Liingston nterprises, Inc., где он был определен в качестве протокола обмена AAA-информацией между RADIUS-клиентом и сервером. Протокол RADIUS является открытым протоколом; множество разнообразных сетевых устройств имеют клиентскую часть протокола RADIUS. RADIUS-сервер представляет собой рабочую станцию, на которой исполняется программное обеспечение серверной части протокола RADIUS от поставщика или какой-либо компании, например, Livingston, Merit или Microsoft. Задать IP-адрес RADIUS-сервера, с которым будет общаться клиент из ОС IOS, можно с помощью команды глобального конфигурирования radius-server host.

При аутентификации протокол RADIUS шифрует пароли, посылаемые между клиентом и сервером. Для такого шифрования необходимо сконфигурировать на RADIUS-сервере и в ОС IOS секретную цепочку. Чтобы сконфигурировать эту цепочку в клиенте ОС IOS, следует воспользоваться командой глобального конфигурирования radius-server key.

Маршрутизатор сети компании ZIP в Сан-Хосе конфигурируется адресом RADIUS-сервера и ключом шифрования следующим образом:

```
San Jose#configure
Configuring from terminal memory or network [terminal]?
Enter configuration commands one per line. End with
CNTL/Z.
San Jose(config)#radius-server host 131.108.110.33
```

```
San Jose(config)#radius-server key Radius4Me
San Jose(config)#AZ
```

Протокол TACACS+. TACACS+ представляет собой AAA-протокол, который концептуально подобен протоколу RADIUS. TACACS+ – это третья ревизия протокола TACACS. Вторая ревизия называлась Extended TACACS или XTACACS (расширенный протокол TACACS). Протокол TACACS+ является протоколом собственной разработки компании Cisco, и все устройства, работающие с ОС IOS, имеют родной TACACS+-клиент.

Серверное программное обеспечение протокола TACACS+ доступно из многих источников, включая компанию Cisco (в продукте CiscoSecure) и других поставщиков, и для многих аппаратных платформ рабочих станций. Задать IP-адрес TACACS+-сервера, с которым будет общаться клиент из ОС IOS, можно с помощью команды глобального конфигурирования tacacs-server host.

Протокол TACACS+ шифрует всю коммуникацию между клиентом и сервером. Для такого шифрования сообщений необходимо сконфигурировать на TACACS+-сервере и в ОС IOS секретную цепочку. Чтобы сконфигурировать эту цепочку в клиенте ОС IOS, следует воспользоваться командой глобального конфигурирования tacacs-server key.

Маршрутизатор сети компании ZIP SF-1 конфигурируется адресом TACACS+-сервера и ключом шифрования следующим образом:

```
SF-Core-l#configure
Configuring from terminal memory or network [termi-
nal]?
Enter configuration commands one per line. End with
CNTL/Z.
SF-Core-l(config)#tacacs-server host 131.108.110.33
SF-Core-1(config)#tacacs-server key ZIPSecure
SF-Core-l(config)#^Z
```

Сравнение протоколов RADIUS и TACACS+. Различий между протоколами RADIUS и TACACS+ достаточно много, но выполняемые ими функции, по сути, одинаковы. Протокол RADIUS, являющийся стандартом, использует на транспортном уровне протокол UDP. Протокол же TACACS+, являясь частной разработкой, применяет на транспортном уровне протокол TCP. Протокол RADIUS хорошо работает только в IP-средах, тогда как протокол TACACS+ полезен в многопротокольных средах. В настоящее время протоколом RADIUS поддерживается больше количество атрибутов, и он позволяет передавать клиен-

ту и серверу больше информации, чем протокол TACACS+ Наконец, RADIUS шифрует только пароль, пересылаемый между клиентом и сервером, тогда как TACACS+ шифрует всю пересылаемую информацию.

Многие поставщики, поддерживающие тот или иной протокол, яростно спорят о преимуществах «своего» протокола. Компания Cisco поддерживает оба протокола. Если сеть в значительной степени гетерогенна, то лучше всего выбрать протокол RADIUS, так как его поддерживают многие поставщики. Если сеть использует главным образом устройства компании Cisco, то, скорее всего, правильным решением будет применение протокола TACACS+.

2.2. Основы предотвращения атак

Имеющиеся в ОС IOS функции TCP-перехвата и одноадресной пересылки по обратному пути позволяют сконфигурировать некоторые базовые средства защиты от двух типов атак отказов в обслуживании: заполнение сети пакетами TCP SYN и подделка IP-адреса отправителя.

Атака отказов в обслуживании представляет собой ситуацию, когда хакер переполняет сетевые ресурсы трафиком, который не повреждает данные, но использует достаточный объем ресурсов сети, чтобы она не могла выполнять свою основную задачу. Например, атака заполнением пакетами TCP SYN (синхронизации) возникает, когда хакер заполняет сервер большим количеством TCP SYN-запросов (используемых для инициализации TCP-соединений) из некорректного IP-адреса отправителя. Каждый из этих запросов имеет недостижимый IP-адрес отправителя, т. е. соединения не могут быть установлены. Большое количество неустановленных открытых соединений переполняет сервер и может привести к тому, что он будет отказывать в обслуживании корректных запросов, не давая пользователям подключиться к серверу.

TCP-перехват. Функция TCP-перехвата помогает предотвратить заполнение сети SYN-запросами путем перехвата и проверки достоверности запросов на установление TCP-соединений при их прохождении через маршрутизатор. Функция TCP-перехвата может работать на перехват входящих TCP SYN-сообщений или отслеживать TCP-соединения, когда маршрутизатор пересылает их.

В режиме перехвата маршрутизатор активно перехватывает каждый входящий TCP SYN-запрос и отвечает за реальный сервер-получатель пакетом подтверждения TCP ACK и пакетом SYN. Это является первым шагом в стандартном процессе установления TCP-соединения, называемом *трехсторонним рукопожатием.* Затем маршрутизатор ожидает получения пакета TCP ACK на второй пакет TCP SYN от отправителя. После получения подтверждения ACK маршрутизатор устанавливает

правильное TCP-соединение с отправителем и завершает трехстороннее рукопожатие. Затем маршрутизатор посылает начальный пакет TCP SYN реальному серверу-получателю и выполняет второе трехстороннее рукопожатие. После этого маршрутизатор прозрачным образом объединяет эти два TCP-соединения, пересылая пакеты между двумя соединениями в течение всего времени жизни соединения.

Режим перехвата функции TCP помогает не допустить атаки заполнением пакетами TCP SYN, так как пакеты от недостижимой хост-машины никогда не попадут серверу-получателю. Сконфигурировать маршрутизатор на перехват запросов можно путем применения расширенного IP-списка доступа, который позволяет задать подлежащие перехвату маршрутизатором запросы.

Чтобы не перехватывать каждое TCP-соединение, можно сделать так, что функция TCP-перехвата будет наблюдать за запросами на соединение при их пересылке маршрутизатором. Если в течение сконфигурированного временного интервала TCP-соединение не будет инициализировано, то программное обеспечение ОС IOS перехватит и оборвет попытку такого соединения.

Функция TCP-перехвата конфигурируется с помощью команды глобального конфигурирования ip tcp intercept mode. Команда глобального конфигурирования ip tcp intercept list назначает расширенный IP-список доступа, задающий те запросы, которые маршрутизатор должен перехватывать. Команда ip tcp intercept watch-timeout задает количество секунд, допускаемых маршрутизатором до сброса TCP-соединения, не завершившего процесс корректного трехстороннего рукопожатия с сервером-получателем. По умолчанию маршрутизатор будет сбрасывать TCP-соединение, если трехстороннее рукопожатие не завершится за 30 секунд. В примере ниже маршрутизатор SF-Core-1 конфигурируется на наблюдение за всеми TCP-соединениями из сета 131.108.0.0 и сброс соединений, которые не устанавливаются за 15 секунд:

```
SF-Core-l#configure
Configuring from terminal memory or network [terminal]?
Enter configuration commands one per line. End with
CNTL/Z.
SF-Core-1(config)#access-list 120 permit ip any
131.108.0.0 0.0.255.25
SF-Core-1(config)#ip tcp intercept mode watch
SF-Core-1(config)tip tcp intercept list 120
SF-Core-1(config)lip tcp intercept watch -timeout 15
SF-Core-1(config)#^Z
```

Команда режима EXEC show tcp intercept connections выводит на экран незавершенные и установленные TCP-соединения. Другая команда режима E) show tcp intercept statistics показывает статистические данные о поведении функции TCP-перехвата.

Одноадресная пересылка по обратному пути. Функция одноадресной пересылки по обратному пути (unicast reverse path forwarding) может помочь в предотвращении атак отказов в обслуживании из-за фальшивых IP-адресов отправителя (иногда называемых *IP-спуфингом).* При атаке на сеть фальшивыми IP-адресами отправителя используются искаженные IP-адреса отправителя или быстро меняющийся IP-адрес отправителя. Если сеть подвергается атаке такими искаженными IP-адресами отправителя или набором быстро изменяющихся IP-адресов отправителя, то может оказаться невозможным сконфигурировать список доступа, который остановит атаку.

Функция одноадресной пересылки по обратному пути решает эту проблему за счет автоматического уничтожения пакетов, которые не имеют поддающегося верификации IP-адреса отправителя. Проверяя, есть ли адрес и интерфейс маршрутизатора отправителя в таблице IP-маршрутизации, и согласуется ли этот интерфейс с тем, на который этот пакет был принят, маршрутизатор верифицирует IP-адрес отправителя. Принятый маршрут и маршрут в обратном направлении к IP-адресу отправителя, как он показан в таблице маршрутизации, должны быть симметричными. Маршрут симметричен, если пакет поступает на интерфейс маршрутизатора, стоящего в одном из наилучших путей возврата к отправителю пакета, при этом не является ограничением точное соответствие с интерфейсом маршрутизатора отправителя, что позволяет использовать такие методики маршрутизации, как балансировка нагрузки по путям равной стоимости.

Если нет маршрута обратного пути на тот же интерфейс отправителя или пути возврата для того пути, с которого пакет был принят, то это, вероятно, означает, что адрес отправителя был модифицирован или подделан, и пакет уничтожается. Верификация достижимости IP-адреса отправителя с помощью обратного пути, на который будет переадресовываться пакет, помогает не допустить подделки IP-адреса отправителя.

Функция одноадресной пересылки по обратному пути может использоваться в сети с любой конфигурацией, в которой есть только один путь, по которому можно взаимодействовать с сетью извне. Если такой путь единственный, даже если существует несколько путей разделения нагрузки, то маршрутизация в сети почти всегда симметрична. Такая конфигурация часто возникает в точке выхода восходящего потока данных сети к сети Internet.

Не следует использовать функцию одноадресной переадресации по обратному пути во внутренней сети организации, когда существуют несколько различных маршрутов к IP-адресам получателей. Конфигурирование функции одноадресной пересылки по обратному пути осуществляется с помощью единственной интерфейсной субкоманды ip verify unicast reverse-path. В обыкновенной среде эта команда используется в отношении только того интерфейса (или интерфейсов, если это среда с разделением нагрузки) маршрутизатора, через который проходит восходящий поток данных в сеть Internet.

Устройства, работающие под управлением ОС IOS, имеют возможность вести журнал сообщений о деятельности в системе. Эти регистрируемые в журнале сообщения могут быть полезны при отслеживании действий в системе, ошибок и извещений. При ведении журнала используются восемь уровней извещающих сообщений, которые сведены в табл. 1.

Таблица 1

Регистрируемые в журнале сообщения ОС IOS

Уровень	Описание
Уровень 0 – аварийные	Система стала непригодной для использования
Уровень 1 – тревожные	Требуется немедленное действие для восстановления стабильности системы
Уровень 2 – критические	Сложились критические условия, которые могут потребовать внимания
Уровень 3 – ошибки	Возникли ошибки, которые могут помочь в отслеживании проблем
Уровень 4 – предупреждения	Сложились предпосылочные условия, но они не носят серьезного характер
Уровень 5 – извещения	Нормальные, но важные в смысловом плане условия, подразумевающие наличие извещений
Уровень 6 – информационные	Эти информационные сообщения не требуют действий
Уровень 7 – отладочные	Эти отладочные сообщения предназначены только для процесса устранения неполадок

В ОС IOS устанавливается минимальный уровень протоколируемых сообщений (в терминах серьезности), которые желательно заносить в журнал. Это делается путем указания в команде конфигурирования уровня серьезности по названию. Аварийные сообщения (уровень 0) об-

ладают наивысшим приоритетом, тогда как отладочные (уровень 7) – наименьшим. Все сообщения с заданным уровнем серьезности и выше отсылаются в одно из четырех мест.

- Сервер системного журнала, который конфигурируется командой logging trap.
- Внутренний буфер устройства, который конфигурируется с помощью команды logging buffered.
- Порт консоли устройства, который конфигурируется с помощью команды logging console.
- Терминальные каналы устройства, который конфигурируются командой logging monitor.

Стоящая впереди команда logging является командой глобального конфигурирования, что позволяет задавать уровень сообщений, отсылаемых в каждое место ведения журнала. Сервер системного журнала – это превосходное место для ведения журнала, так как система обычно сохраняет сообщения на жестком диске. Кроме того, поскольку системный журнал представляет собой средство общего назначения, которым пользуются разнообразные программы, можно иметь один центральный источник для протоколирования сообщений от различных устройств.

Внутренний буфер устройства полезен, если отсутствует сервер системного журнала или нужно, чтобы каждое устройство вело свой отдельный журнал событий. Размер внутреннего буфера устройства по умолчанию составляет 4096 байт. Но, используя команду logging buffered, можно изменять его размер. Например, команда logging buffered 8192 задает размер внутреннего буфера устройства в 8192. Будучи полезным в некоторых ситуациях, внутренний буфер размещается в ОЗУ устройства, и поэтому его содержимое теряется при каждой перезагрузке устройства.

Пересылка журнальных сообщений на консоль или в терминальные канал устройства (включая сеансы виртуального терминала) полезна для организации немедленного извещения о критических событиях. Четыре различных места ведения журнала не являются взаимоисключающими, и можно одновременно использовать несколько средств ведения журнала.

Конфигурирование пересылки сообщений на сервер системного журнала можно выполнить командой logging trap. Для активации в ОС IOS функции пересылки журнальных сообщений в системный журнал следует воспользоваться командой глобального конфигурирования logging, чтобы задать IP-адрес хост-машины, на которой будет осуществляться ведение журнала.

Возможно протоколирование сообщений сразу в нескольких местах. Например, можно отсылать все сообщения уровня 7 и выше на

сервер системного журнала. Одновременно аварийные сообщения из-за их критической природы можно отсылать на консоль устройства. В примере ниже маршрутизатор сети компании ZIP Seoul-1 конфигурируется на выполнение протоколирования как раз таким способом, как было описано выше:

```
Seoul-1#configure
Configuring from terminal memory or network [termi-
nal]?
Enter configuration commands one per line. End with
CNTL/Z.
Seoul-1(config)#logging 131.108.110.33
Seoul-1(config)#logging trap debugging
Seoul-1(config)#logging console emergencies
Seoul-1(config)#^Z
```

Если устройство с ОС IOS сконфигурировано на протоколирование во внутреннем буфере, то результаты можно просматривать с помощью команды режима EXEC show logging. Если предположить, что маршрутизатор Seoul-1 сконфигурирован на протоколирование в буфере, а также в системном журнале и на консоли, то результат исполнения команды show logging будет выглядеть следующим образом:

```
Seoul-1>show logging
Syslog logging: enabled (0 messages dropped 0
flushes 0 overruns)
Console logging: level debugging 2 messages logged
Monitor logging: level debugging 2 messages logged
Trap logging: level debugging 2 message lines
logged Logging to
131.108.110.33 2 message lines logged
Buffer logging: level debugging 2 messages logged
Log Buffer (4096 bytes):
Mar 17 17:45:56: %LINK-3-UPDOWN: Interface Serial0,
changed state to down
Mar 17 18:23:10: %LINK-3-UPDOWN: Interface Serial0,
changed state to up
```

В выводимой информации показывается, что активирована функция протоколирования в системном журнале. Она также выводит количество сообщений, отправленных на консоль устройства, в терминальные каналы устройства (строка monitor logging) и в системный журнал.

Кроме того, показывается количество сообщений, занесенных в буфер. Последние две строки показывают содержание буфера журнала с двумя запротоколированными сообщениями об изменении состояния канала (сообщения уровня 6). Следует отметить наличие в выводимой информации временных меток.

2.3. Основы управления сетью

Управление сетью – это процесс управления отказами, контроля конфигураций, мониторинга производительности, обеспечения защиты и учета деятельности в сети передачи данных. Каждая из этих задач необходима для полного контроля над средой сети данных, которая является важной составляющей структуры организации. Форум по управлению сетями Международной организации стандартизации (ISO Network Management Forum) определил управление сетью как сумму всех действий, требующихся для управления отказами, конфигурацией, производительностью, средствами защиты и учетом данных в сети.

Платформы управления сетью представляют собой программные системы, спроектированные для выполнения действий по управлению сетью. Некоторыми примерами таких систем являются продукты OpenView компании Hewlett-Packard, Spectrum компании Cabletron, Solstice Enterprise Manager компании Sun, NetView/AIX компании IBM и CiscoWorks2000 компании Cisco. Платформы управления сетью обеспечивают программную архитектуру для приложений по сетевому управлению, которые выполняют разнообразные задачи. Их нельзя сгруппировать в одну категорию. Некоторые формируют карту сети и контролируют статус всех сетевых устройств, обеспечивают реализацию функции управления отказами. Некоторые, являясь средствами для управления производительностью, строят диаграммы использования каналов и посылают сообщения, если на интерфейсе локальной сети возникают ошибки. Другие же следят за моментами, связанными с защитой сети, и посылают сообщения по электронной почте или на алфавитно-цифровые пейджеры.

Приложения управления сетью общаются с программным обеспечением сетевых устройств, называемых *агентами.* Обмен данными между менеджером и агентом возможность менеджеру собирать стандартный набор информации, который определен в базе данных информации для управления сетью (management information Base-MIB). Каждая порция информации, существующая в базе данных, называется *объектом.* База данных информации для управления сетью содержит объекты, которые нужны менеджеру для управления сетью. На рис. 4 показаны взаимоотношения между менеджером и агентом.

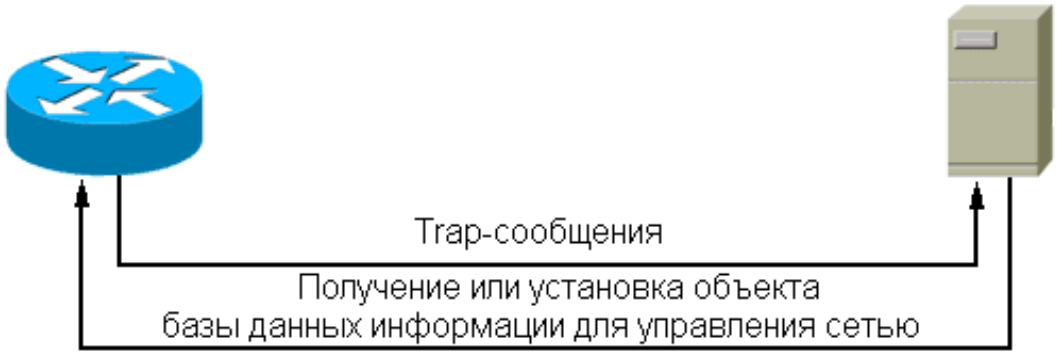


Рис. 4. В соответствии с протоколом управления сетью менеджер запрашивает и выполняет установки относительно информации в базе данных управления сетью, а агент посылает менеджеру захваченные сообщения, которые содержат информацию о событиях в устройстве

Существует два типа баз данных управления сетью: стандартные и собственной разработки поставщика. Стандартные базы данных, например типа MIB-II, обеспечивают наличие основных объектов, применимых почти ко всем устройствам в сети передачи данных. К примеру, база данных MIB-II содержит такую системную информацию об устройстве, как время нахождения в рабочем состоянии и имя, данные о трафике по интерфейсам и счетчики ошибок, а также информацию протокола IP. Технологически специализированные базы данных, которые тоже относятся к стандартным, ориентированы на конкретные протоколы, например, на Frame Relay или на Token Ring. Они содержат объекты, связанные с конкретной технологией, используемой на сетевом устройстве. Специализированные на поставщика базы данных, которые относятся к классу собственных разработок, задают определения объектов, которые специфичны для сетевых устройств одного поставщика.

Приложения управления сетью собирают информацию в базу данных из устройств и изменяют поведение этих сетевых устройств с помощью протокола управления сетью. Стандартным и наиболее распространенным протоколом управления сетью является простой протокол управления сетью – SNMP. Протокол SNMP использует на транспортном уровне протокол UDP и протокол IP на сетевом уровне. Существуют протоколы управления сетью собственной разработки, и некоторые поставщики реализовали их в своих сетевых устройствах.

Обмен данными между SNMP-агентом и менеджером происходит с помощью пяти типов пакетов:

- Get-Request (запрос на получение);
- Get-Next-Request (запрос на получение следующего);
- Set-Request (запрос на установку);

- Get-Response (ответ на запрос);
- Trap (перехват).

Get-Request представляет собой сообщение от менеджера агенту, запрашивающее набор конкретных объектов базы данных информации для управления сетью, например, имя устройства, местоположение, количество физических интерфейс так далее. Get-Next-Request – это сообщение от менеджера агенту с запросом порции табличных данных, ссылка на которые производится из конкретной точки в базе данных информации для управления сетью. Этот тип сообщений полезен при проходах по таблицам базы данных и при извлечении данных из таких лиц, как таблица IP-маршрутизации. Сообщение типа Set-Request содержит запрос агенту на изменение значения конкретного объекта базы данных, например, на изменение статуса интерфейса устройства. Агент на каждое сообщение Get-Request, Get-Next-Request или Set-Request отвечает менеджеру сообщением Get-Response, которое содержит запрашиваемые значения объектов базы данных информации для управления сетью или показывает значение объекта, которое было изменено. Сообщение типа Trap представляет собой сообщение о событии, посылаемое менеджеру по инициативе агента.

В каждом SNMP-агенте устанавливается верификационная последовательность, называемая *цепочкой сообщества* (community string). Цепочка сообщества включает каждый запрос менеджера на получение или установку информации в базе данных информации для управления сетью. Перед ответом агент проверяет ее. Цепочка сообщества является слабым средством аутентификации и закодирована в кодах ASCII. Не следует полагаться на нее как на единственное средство защиты доступа к SNMP-агенту.

Конфигурирование агента цепочкой сообщества осуществляется командой глобального конфигурирования ОС IOS snmp-server community. Опции этой команды позволяют ставить условия, чтобы цепочка сообщества применялась к сообщениям, которые имеют статус «только для чтения», или к сообщениям со статусом «чтение-запись». Сообщения Get-Request и Get-Next-Request являются сообщениями только для чтения; сообщения Set-Request относятся к сообщениям чтения-записи. Ключевыми словами, используемыми для задания условий только для чтения и для чтения-записи, являются RO и RW, соответственно. Во многих приложениях управления сетью цепочкой сообщества по умолчанию для сообщений только для чтения является public, а для сообщений с чтением-записью по умолчанию часто используется слово private. Последняя опция этой команды глобального конфигурирования задает стандартный IP-список доступа хост-машин, которым разрешается запрашивать агента с использованием достоверных цепочек сообщества.

В примере ниже маршрутизатор в Сингапуре конфигурируется цепочкой сообщества сообщений только для чтения zipnet и цепочкой сообщества для сообщений с чтением-записью ZlPprivate. Кроме того, задается список доступа access-list 2, который позволяет менеджеру сети с адресом 131.108.20.45 использовать любую из двух цепочек сообщества.

Следует отметить, что номер списка доступа являете последним опционным параметром в обеих командах snmp-server community, показанных в этом примере.

```
Singapore#configure
Configuring from terminal memory or network [terminal]?
Enter configuration commands one per line. End with
CNTL/Z.
Singapore(config)#access-list 2 permit
131.108.20.45
Singapore(config)#snmp-server community Zipnet RO 2
Singapore(config)#snmp-server community ZlPprivate RW 2
Singapore(config)#^Z
```

Для отправки SNMP-сообщений типа Trap необходимо выполнить конфигурирование устройства с ОС IOS. Определены шесть стандартных SNMP-сообщений, посылаемых всеми агентами:

- coldStart (холодный старт);
- warmStart (теплый старт);
- linkUp (канал в рабочем состоянии);
- HnkDown (канал в нерабочем состоянии);
- authenticationFailure (аутентификация не прошла);
- egpNeighborLoss (потеря EGP-соседа).

Сообщение coldStart означает, что агент был только что запущен. Сообщение warmStart указывает, что само программное обеспечение агента только что было перезапущено. На практике большинство агентов посылают только сообщение coldStart, так как обычно после включения питания устройства, на котором исполняется агент, сам агент перезапускается. Сообщения linkUp и HnkDown обращают внимание менеджера на изменение статуса канала на устройстве. Сообщение authenticationFailure указывает, что менеджер послал агенту SNMP-запрос с неправильной цепочкой сообщества. И, наконец, сообщение egpNeighborLoss говорит менеджеру о том, что сосед протокола внешних шлюзов (EGP) стал недостижимым. Это последнее Trap-сообщение используется редко, так как протокол EGP перекрывается протоколом BGP4.

Приведенные выше шесть Trap-сообщений являются стандартными, но не единственными Trap-сообщениями SNMP, которые может посылать агент. Многие базы данных информации для управления сетью содержат определения Trap-сообщений, специфичных для протокола, например: сообщения для протоколов ISDN, Frame Relay или BGP4. ОС IOS поддерживает Trap-сообщения для разнообразных протоколов и функций IOS, включая сообщения для протоколов BGP, Frame Relay, ISDN, X.25, сообщения монитора среды и изменений конфигурации ОС IOS.

ОС IOS может быть настроена на отправку Trap-сообщений SNMP любому количеству менеджеров. Для задания IP-адреса и цепочки сообщества менеджеру, которому надо будет посылать Trap-сообщения, следует использовать команду snmp-server host. В примере ниже маршрутизатор сети компании ZIP в Сингапуре конфигурируется на отправку Trap-сообщений SNMP менеджеру с IP-адресом 131.108.20.45 с использованием цепочки сообщества Zipnet. Опционные параметры команды snap-server host также задают, чтобы агент отсылал Trap-сообщения для протоколов SNMP, Frame Relay и сообщения об изменениях в конфигурации ОС IOS.

```
Singapore#configure
Configuring from terminal memory or network [terminal]?
Enter onfiguration commands cone per line. End with
CNTL/Z.
Singapore(config)#snrap-server host 131.108.20.45
Zipnet snmp frame-ralay config
Singapore(config)#^Z
```

В ОС IOS в SNMP-агенте можно вручную сконфигурировать физическое местоположение и контактную персону по устройству. В этом случае приложения управления сетью могут извлекать эту информацию. Для занесения этой информации следует использовать команды глобального конфигурирования snmp-server location и snmp-server contact. Каждая из этих команд позволяет ввести текстовую строку из 255 символе описывающую местоположение и контактную персону. В примере ниже осуществляете занесение в конфигурацию маршрутизатора в Сингапуре информации о местополо-жении и контактной персоне:

```
Singapore#configure
Configuring from terminal memory or network [terminal]?
Enter configuration commands one per line. End with
CNTL/Z.
Singapore(config)#snmpserver
```

```
location 1 Raffles Place, Singapore
Singapore(config)#snmp-server contact
Allan Leinwand, allan@telegis.net
Singapore(config)#^Z
```

Команда режима EXEC show snmp демонстрирует статистические данные протокола SNMP для заданного устройства. Эта команда полезна для наблюдения за работой протокола SNMP на устройстве. Ниже приведен результат исполнения этой команды на маршрутизаторе в Сингапуре:

```
Singapore>show snmp
Chassis: 25014624
Contact: Allan Leinwand allan@digisle.net
Location: 45 Raffles Place Singapore
4620211 SNMP packets input
0 Bad SNMP version errors
0 Unknown community name
0 Illegal operation for community name supplied
0 Encoding errors
23493606 Number of requested variables
0 Number of altered variables
576553 Get-request PDUs
4043613 Get-next PDUs
0 Set-request PDUs 4623230 SNMP packets output
0 Too big errors (Maximum packet size 1500)
1757 No such name errors
0 Bad values errors
0 General errors
4620166 Get-response PDUs 3064 SNMP trap PDUs SNMP
logging: enabled
Logging to 131.108.20.45 0/10 3064 sent, 0 dropped.
```

В приведенном выше результате присутствуют статистические данные относительно работы протокола SNMP. В первой строке результата показан серийный номер системной платы, который находится в базе данных информации для управления сетью разработки компании Cisco. Вторая и третья строки содержат текстовые последовательности, определяющие местоположение и контактную персону по устройству в соответствии с той информацией, которая была сконфигурирована командами глобального конфигурирования snmp-server contact и snmpserver location. В начале выводимого результата стоят данные об общем количестве

SNMP-пакетов на входе, общем количестве SNMP-пакетов на входе, которые были посланы с неправильной цепочкой сообщества и общем количестве SNMP-объектов (названных здесь переменными), запрошенных менеджерами. Также здесь показана разбивка принятых SNMP-пакетов по типам.

Во второй части результата содержатся данные об общем количестве SNMP-пакетов на выходе, различных сообщениях о стандартных ошибках протокола SNMP и об общем количестве отправленных ответов и Trap-сообщений. Последние две строки результата показывают, был ли агент настроен на отправку Trap-сообщений (здесь эта процедура называется «протоколирование SNMP»), IP-адреса каждого менеджера, принимающего Trap-сообщения и количество Trap-сообщений, отосланных каждому конкретному менеджеру.

2.4. Основы управления временем

ОС IOS компании Cisco позволяет устройству отслеживать текущее время и дату, используя системные часы. Системные часы запускаются в момент подачи питания на устройство и могут распространять данные о времени в различные внутренние системы, например, для регистрации времени и даты изменений конфигурации, вывода на экран времени занесения в буфер журнала сообщений и отправки времени и даты в сообщениях протокола SNMP. Только в маршрутизаторе Cisco 7000 время системных часов устанавливается аппаратным образом. Во всех других моделях системные часы устанавливаются по умолчанию на полночь 1 марта 1993 года.

После установки времени системные часы определяют надежность источника даты и времени. Если источник времени надежен, то время становится доступным другим процессам ОС IOS, в противном случае оно используется только для демонстрации. В последующих разделах показано, как сделать выбранный источник времени, например атомные часы, надежным.

Дату и время на системных часах можно посмотреть, если воспользоваться командой режима EXEC show clock:

```
SF-1>show clock
06:56:50.314 PST Fri Mar 30 2001
```

В маршрутизаторах серии Cisco 7000 имеется календарь, который ведет дату и время, в том числе при перезапусках системы и отказах по питанию. При перезапуске системы для установки системных часов всегда используется календарь. После этого другой протокол может изме-

нять или обновлять показания часов. В сети, в которой нет другого авторитетного источника времени, в качестве такового может использоваться календарь, и его показания могут передаваться другим процессам (например, протоколу сетевого времени Network Time Protocol, NTP, который рассматривается в разделе ниже). Увидеть текущие значения системы календаря можно, воспользовавшись командой режима EXEC show calendar:

```
SF-l>show calendar
06:57:26 PST Fri Mar 30 2001
```

Системные часы ведут отсчет времени внутренним образом, основываясь на универсальном скоординированном времени, также называемом средним гринвичским. ОС IOS позволяет вводить в конфигурацию устройства локальный часовой пояс и, если это имеет место, счисление времени со сбережением светового дня (в синтаксисе ОС IOS это называется летним временем – summer-time). Таким образом, устройство показывает правильное время на протяжении всего года.

Для установки системных часов могут использоваться несколько источников. Самыми распространенными являются следующие:

- установка вручную;
- протокол сетевого времени NTP;
- простой протокол сетевого времени SNTP.

Конфигурирование даты и времени вручную. Если устройство, работающее под управлением ОС IOS, стоит обособленно и не может использовать внешний авторитетный источник времени, то время и дата устройстве могут устанавливаться вручную. Эти установки достоверны до момента сброса и перезагрузки устройства. Службы управления временем вручную следует использовать только тогда, когда другой авторитетный источник времени недоступен.

Чтобы вручную установить часовой пояс для устройств с ОС IOS, используют команду глобального конфигурирования clock timezone. Эта команда воспринимает в качестве опций часовой пояс, в котором находится устройство, и разницу в часах между этим часовым поясом и универсальным скоординированным временем. Например, для стандартного тихоокеанского времени (Pacific Standard Time – PST), которое на восемь часов отстает от универсального скоординированного времени, вводится следующая глобальная команда: clock, timezone PST-8.

Если в часовом поясе, в котором стоит устройство, используется летнее время, воспользуйтесь командой глобального конфигурирования clock summer-time recurring. Аргументом этой команды конфигурирова-

ния является название летнего времени часового пояса, например, тихоокеанское летнее время (Pacific Daylight Time – PDT). Системные часы устанавливаются с помощью команды глобального конфигурирования clock set. В примере ниже в маршрутизаторе SF-1 устанавливается часовой пояс PST, активируется режим летнего времени (в данном случае это PDT) и выполняется установка часов на 17 марта 2001 года, 14:25:

```
SF-1#configure
Configuring from terminal memory or network [termi-
nal]?
Enter configuration commands one per line. End with
CNTL/Z.
SF-1(config)#clock timezone PST -8
SF-1(config)#clock summer-time PDT recurring
SF-1(config)#clock set 14:25 17 3 2001
SF-1(config)#AZ
```

В маршрутизаторах серии Cisco 7000 для установки календаря вручную применяется команда глобального конфигурирования calendar set. Чтобы этот календарь играл роль достоверного источника времени и даты для других функций ОС IOS, воспользуйтесь командой глобального конфигурирования clock calendar-valid.

Протокол сетевого времени. Протокол сетевого времени (Network Time Protocol – NTP) синхронизирует время в устройствах, работающих в IP-сети передачи данных. ОС IOS компании Cisco содержит NTP-процесс, который позволяет устройству посылать и принимать NTP-пакеты. Многие поставщики наделяют свои устройства подобными NTP-процессами, что делает этот протокол оптимальным механизмом для решения задачи синхронизации времени во всей сети.

Протокол NTP распространяет установку времени, которую он получает по сети от авторитетного источника времени. Как уже отмечалось ранее, устройство с ОС IOS может быть настроено так, чтобы оно само играло роль такого источника времени, но предпочтительнее, чтобы источником времени были атомные часы, подключенные к серверу службы времени. Для использования протокола NTP не обязательно иметь собственные атомные часы. Можно синхронизировать время с другим источником, который получает его от атомных часов.

Как и во многих часах телефонных сетей, протокол NTP измеряет расстояние между устройством, на котором он исполняется, и авторитетным источником времени в инкрементах, называемых *стратами.* Часы, являющиеся источником времени *страты 1,* подключены к

атомным часам непосредственно, источник *страты 2* синхронизируется с источником *страты 1* и так далее. Вы не можете подключить свое устройство непосредственно к источнику времени *страты 1*. Однако NTP-процесс в ОС IOS компании Cisco автоматически выполняет синхронизацию с источником времени с наименьшей стратой. NTP-процесс, реализованный компанией Cisco, не подстраивает системное время устройства к времени источника, относящегося к той же страте или большей. Если протокол NTP сталкивается с источником времени, у которого время существенно отличается от времени в других устройствах сети, то он не выполняет синхронизацию с таким источником, даже если у него более низкая страта.

Одно устройство, исполняющее протокол NTP, обменивается информацией с другим NTP-устройством, образуя ассоциацию. В ОС IOS компании Cisco ассоциации конфигурируются с использованием команд глобального конфигурирования ntp server или ntp peer. *Серверная ассоциация* означает, что устройство с ОС IOS образует ассоциацию со сконфигурированным устройством, а не наоборот. При *одноранговой ассоциации* устройства образуют ассоциацию друг с другом. Наиболее распространенным типом ассоциаций является серверная, в которой одним авторитетным источником времени для нескольких NTP-процессов на разных устройствах является сервер. На рис. 5 показана серверная ассоциация между NTP-клиентами и устройством, работающим под управлением ОС IOS.

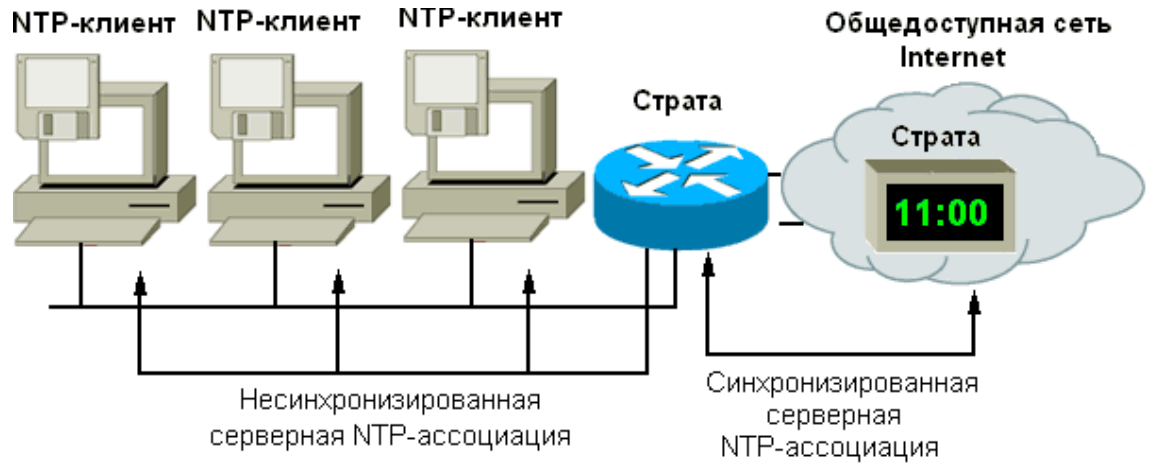


Рис. 5. Эти NTP-клиенты входят в серверную ассоциацию с устройством, работающим под управлением ОС IOS, которое синхронизируется с авторитетным источником времени общего пользования Internet

В маршрутизаторах серии Cisco 7000 с помощью протокола NTP можно периодически осуществлять синхронизацию системы календаря. Для выполнения этой задачи используется команда глобального конфигурирования ntp update-calendar.

В локальной сети отправка и прием NTP-сообщений осуществляется с использованием широковещательных сообщений, что исключает необходимость в конфигурировании и образовании ассоциации с каждым NTP-устройством, находящимся в локальной сети. Для прослушивания широковещательных NTP-сообщений на интерфейсе используется субкоманда конфигурирования интерфейса ntp broadcast client. Чтоб передавать широковещательные NTP-сообщения в заданный сегмент локальной сети, необходимо воспользоваться интерфейсной субкомандой ntp broadcast. В самой распространенной конфигурации устройства, работающие под управлением ОС IOS, настраиваются так, чтобы они могли образовывать серверную ассоциацию с находящимся в сети Internet авторитетным источником времени, а затем рассылают широковещательные NTP-сообщения на все интерфейсы, на которых размещаются другие NTP-устройства. В примере ниже на маршрутизаторе SF-1 конфигурируется NTP-процесс с использованием двух авторитетных источников времени из сети Internet, находящихся в Северной Калифорнии, с периодическим обновлением показаний системы календаря на основе даты и времени протокола NTP и с широковещательной отправкой NTP-сообщений на интерфейс (Ethernet0):

```
SF-1#configure
Configuring from terminal memory or network [terminal]?
Enter configuration commands one per line. End with
CNTL/Z.
SF-l(config)#ntp server 192.216.191.10
SF-1(config)#ntp server 129.189.134.11
SF-1(config)#ntp update-calendar
SF-l(config)#interface (Ethernet0)
SF-1(config)#ntp broadcast
SF-1(config)#^Z
```

NTP-ассоциации, сконфигурированные в устройстве, работающем с ОС IOS, можно просмотреть с помощью команды режима EXEC show ntp associations. Первый символ в каждой строке выводимого результата говорит, является ли конкретная ассоциация синхронизированной (ключом к значению символов из первого столбца служит последняя строка результата). В результате также показывается адрес каждой сконфигурированной ассоциации, страта источника времени и ведущий сервер. Ниже показан соответствующий пример:

```
SF-l>show ntp assoc
address ref lock st when poll reach delay offset disp
```

```
*~192.216.191.10 .GPS. 1 127 512 377 285.5 7.57 32.8
+~129.189.134.11 .PPS. 1 207 512 377 147.2 -22.19 18.4
* master (synced) # master (unsynced) + selected -
candidate ~ configured
```

Используя команду режима EXEC show ntp status, можно узнать статус протокола NTP. В примере результата исполнения этой команды ниже показано, что протокол NTP синхронизирован, относится к страте 2 и в качестве опорного авторитетного источника времени использует источник с IP-адресом 192.216.191.10:

```
SF-l>show ntp status
Clock is synchronized stratum 2 reference is
192.216.191.10
nominal freq is 250.0000 Hz actual freq is 250.0003
Hz precision is 2**24
reference time is B853B821.9813EB8D (06:58:10 PST
Fri Mar 30 2001)
lock offset is -7.3067 msec root delay is 285.46 msec
root dispersion is 41.95 msec peer dispersion is
32.82 msec
```

Деактивировать работу протокола NTP можно на конкретном интерфейсе с помощью команды ntp disable. Команда глобального конфигурирования ntp access-group вводит ограничение на тип NTP-ассоциации, которую может иметь устройство, работающее под управлением ОС IOS. Эта команда требует задать тип ассоциации, разрешенной с другими устройствами из конкретного множества IP-адресов, указанного в IP-списке доступа. Можно разрешить устройству образовывать одноранговую или серверную ассоциацию. Также можно разрешить ему только системные запросы времени или только NTP-сообщения. В примере, приведенном ниже, на маршрутизаторе SF-1 разрешаются серверные ассоциации со всеми системами из сети 131.108.0.0:

```
SF-1#configure
Configuring from terminal memory or network [terminal]?
Enter configuration commands one per line. End with
CNTL/Z.
SF-1(config)#access-list 50 permit 131.108.0.0
0.0.255.255
SF-1(config)#ntp access-group serve 50
SF-1(config)#^Z
```

Простой протокол сетевого времени. Маршрутизаторы моделей Cisco 1003, 1004 и 1005 работают только с простым протоколом сетевого времени (Simple Network Time Protocol – SNTP). SNTP – это упрощенная версия протокола NTP, которая может получать время только от NTP-серверов. Протокол SNTP не может быть авторитетным источником времени для других устройств. Такие ограниченные функциональные возможности, по мнению компании Cisco, были приемлемы в данном случае, так как эти маршрутизаторы серии Cisco 1000 являются малыми устройствами с фиксированным количеством интерфейсов и относительно низкой производительностью. Протокол SNTP обеспечивает получение информации о времени с точностью приблизительно в 100 миллисекунд. Эта информация предназначается для использования в устройствах ОС IOS.

Протокол SNTP можно сконфигурировать на запрос и прием пакетов от сконфигурированных серверов с помощью команды глобального конфигурирования sntp server. Организовать SNTP-процесс в маршрутизаторе, который бы слушал широковещательные пакеты протокола NTP, можно путем применения команды глобального конфигурирования sntp braodcast client. Если ввести в конфигурацию как конкретный сервер, так и возможность маршрутизатора принимать широковещательную информацию, то устройство предпочтет сервер более низкой страты или сконфигурированный сервер, если страты нескольких источников равны. Статистические данные о работе протокола SNTP можно просмотреть, воспользовавшись командой режима EXEC show sntp.

3. ОСНОВНЫЕ ПРИНЦИПЫ ПОИСКА НЕИСПРАВНОСТЕЙ В СЕТЯХ CISCO

3.1. Общее описание процесса поиска

Несмотря на то, что количество сетевых конфигураций и настроек фактически ничем не ограничено, методология, применяемая при проработке каждой проблемы, почти всегда одинакова. Независимо от сложности отдельного компьютера или сети, процедура поиска неисправностей, на которую всегда можно положиться, делится на четыре основных этапа. Они проиллюстрированы на рис. 6: сначала вы определяетесь с симптомами, потом выявляете и локализуете возможный источник (или местонахождение) неисправности, заменяете подозрительную подсистему, и, наконец, чтобы убедиться в исчезновении проблемы, повторно проводите полное тестирование системы. Если разрешить проблему не удалось, смело начинайте с шага № 1.

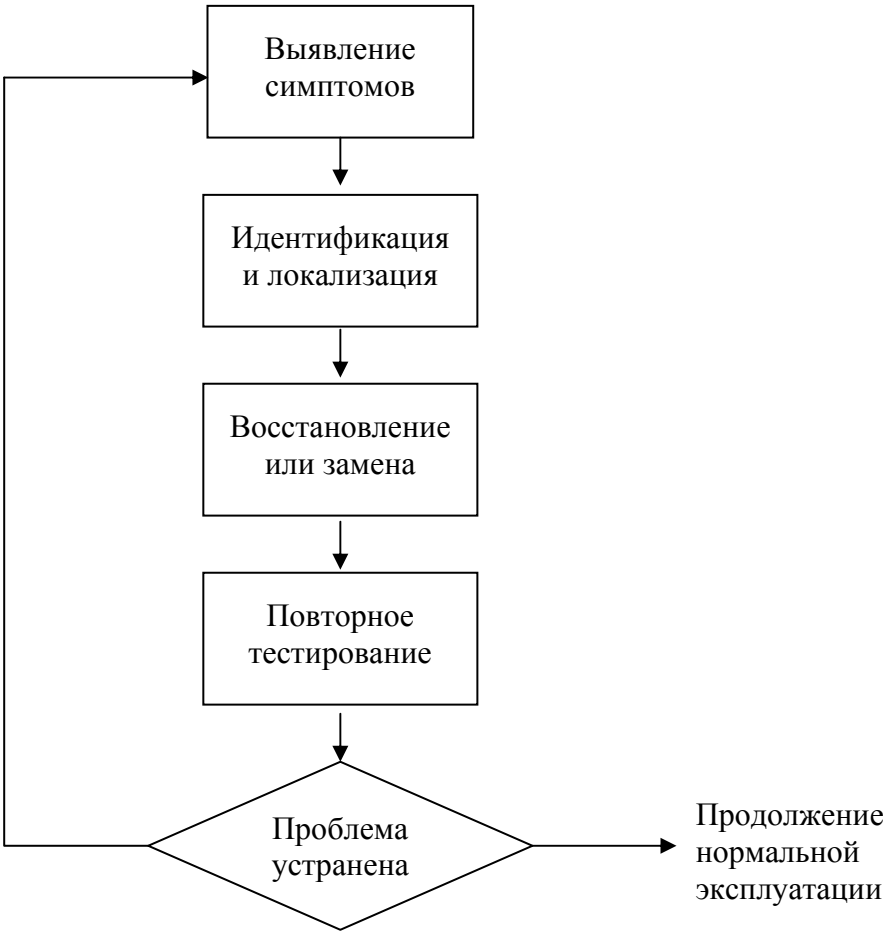


Рис. 6. Универсальный процесс поиска неисправностей

1. Выявление симптомов. Причина выхода сети из строя может быть как простой, например, плохо зафиксированный провод или разъем (коннектор), так и сложной, к примеру, сбой в микросхеме или в подсистеме. Хорошо подумайте, в чем заключаются симптомы. К примеру, можно задаться следующими вопросами.

- Удается ли рабочим станциям обращаться к серверу или маршрутизатору?
- Не сложилась ли ситуация, при которой Ping-запрос, отправленный на одну сторону маршрутизатора или сети, завершается успешно, а аналогичный запрос, отправленный на другую сторону, завершается ничем?
- Зажигаются ли светодиоды питания или активности?
- Не возникает ли неисправность только тогда, когда компьютер подключают к сети или удаляют?

Выявив симптомы и разобравшись в их сути, вы значительно упрощаете задачу локализации неисправности в рамках конкретного компоновочного блока или компонента.

2. Идентификация и локализация. Прежде чем пытаться изолировать проблему в рамках сети или аппаратного устройства, необходимо убедиться в том, что причиной ее возникновения послужило именно оборудование. Во многих случаях это оказывается очевидным, но бывают ситуации, допускающие двоякое толкование (например, при отсутствии питания, отсутствии командной строки DOS и т. д.). Всегда помните, что сеть функционирует благодаря тесному взаимодействию аппаратного и программного обеспечения. Неисправный или неверно настроенный программный блок может вызывать появление сбивающих с толку системных ошибок с тем же успехом, с каким это может делать вышедшее из строя аппаратное устройство. Только лишь выявив возможную проблемную область, вы сможете приступить к самому процессу ремонта – заменить подозрительную подсистему или провести повторную конфигурацию подозрительного программного обеспечения.

3. Замена. Так как сети замышлялись как совокупности подсистем, в большинстве случаев сразу заменить подсистему оказывается проще, чем пытаться устранить ее неполадки на компонентном уровне. В современных условиях сети часто оказываются необходимым элементом нормального функционирования предприятий, так что замена неисправного компонента (например, вышедшей из строя сетевой платы или концентратора) зачастую оказывается наиболее экономически эффективным способом возврата сети в работоспособное состояние. Производители и связанные с ними распространители часто предлагают подсистемы и оборудование в ассортименте. Имейте в виду: для того, чтобы

заказать новую подсистему, вам, вероятно, придется узнать производственный шифр компонента старой подсистемы.

Другой проблемой, связанной с быстрым технологическим прогрессом, является то, что компоненты редко остаются в продаже надолго. Когда компьютер выходит из строя, и перед вами встает задача замены неисправного устройства, вероятнее всего, вам придется проводить модернизацию – по той простой причине, что взамен старого устройства вы не сможете найти идентичное. С этой точки зрения, модернизация зачастую замещает процессы поиска неисправностей и восстановления.

4. Повторное тестирование. Когда ремонт наконец будет завершен, сетевые устройства придется установить заново, а после этого протестировать. Прежде чем проводить окончательные испытания, необходимо поставить на свои места всю защиту, корпуса, кабели и фильтры. Если симптомы сохранятся, придется провести их переоценку и локализовать неисправность в другой части сети. Если нормальное функционирование удастся восстановить (или значительно улучшить), нужно протестировать различные функции сети. Когда вы сможете убедиться в том, что при работе системы все симптомы исчезли, оборудование можно вновь запускать в работу. Как правило, имеет смысл позволить системе поработать, по меньшей мере, 24 часа – это позволяет удостовериться в том, что новая подсистема не выйдет из строя преждевременно. Это называется приработкой системы.

Не отчаивайтесь, обнаружив, что сеть до сих пор работает плохо. Возможно, вы забыли о каком-то соединении. Быть может, для того, чтобы система могла приспособиться к новой подсистеме, программные настройки и драйверы устройств нужно обновить. Помните, что сеть – это лишь некое количество систем, каждая из которых тоже состоит из некоторых компонентов. Обычно все они прекрасно работают друг с другом, но, когда одна система приходит в негодность, она может инициировать неисправности еще в одной или в нескольких

Практическое руководство по поиску неисправностей

Начало. Процесс поиска неисправности лучше всего начинать с количественного анализа – это поможет разобраться в ее сущности. Вероятно, сразу выявить причину возникновения проблемы не удастся, но понимание того, что и где происходит, поможет вам своими силами воспроизвести неисправность и определиться с тем, что нужно предпринять впоследствии. В большинстве случаев ознакомление с проблемой происходит при участии пользователей (вероятно, с ними придется говорить по телефону, или они придут к вам сами). К примеру, вполне возможно, что напуганный пользователь сообщит вам о том, что, придя

на работу в 7:30 утра, ему не удалось зарегистрировался на сервере. Помимо всего прочего, в такой ситуации вам представляется возможность получить довольно подробные данные о конкретных условиях, окружающих пользователя, его учетной записи и аппаратном обеспечении. Кроме того, для того чтобы ознакомиться с местной проводкой кабелей, узнать о наличии концентраторов/коммутаторов и смежных рабочих станций, следует обратиться к любым логическим или физическим картам сети.

Проблемы отдельного компьютера. Если неисправность поражает отдельно взятую рабочую станцию, в то время как рабочие станции, серверы и другие ресурсы функционируют в нормальном режиме, вполне возможно, что сбой локализован в данной рабочей станции, ближайших к ней элементах подключения к сети или в конфигурации ее программного обеспечения. В случае, когда неисправность наблюдается только на одном персональном компьютере, необходимо выполнить следующие действия.

Проверьте питание. Возможно, это покажется слишком очевидным, но вы удивитесь, узнав, какое количество пользователей приходят на работу, предполагая, что их компьютеры включены – они даже не представляют, что их могли выключить. Если пользователь говорит, что система отключена или не желает включаться, в первую очередь проверьте, подключены ли компьютер и монитор к источнику питания, и находятся ли они во включенном состоянии. Если система включена, но не может выйти из режима ожидания, попробуйте перезагрузить ее. Корректному восстановлению после нахождения в энергосберегающих режимах зачастую препятствует несовместимое аппаратное обеспечение и устаревшие драйверы. Если система включена, но ей не удается загрузиться, вам придется заменить компьютер, чтобы пользователь смог возобновить работу, а затем, находясь на своем рабочем месте, починить неисправную систему.

Проведите проверку на предмет вирусов. Это стандартный этап поиска неисправностей – его необходимо проводить всякий раз при возникновении сетевых проблем. Для того чтобы проверить, насколько чист неисправный компьютер (и не воспроизводит ли он инфицированные файлы или макросы по всей сети), запустите недавно обновленную антивирусную программу. В случае обнаружения на станции вируса обязательно выполните комплексную процедуру поиска вирусов в масштабах всей сети.

Проверьте соединение. Взгляните на кабель, проложенный между рабочей станцией и соответствующим портом концентратора/ коммутатора (возможно, для того чтобы получить данные об этом соединении,

вам придется обратиться к физической карте). Проверьте, горит ли светодиод линии. Если он не работает, значит, кабель отсоединен или поврежден, и для восстановления нормального соединения, вам, вероятно, придется чинить кабельную проводку.

Проверьте учетную запись. Трудности, возникающие при попытках регистрации в сети (особенно в отдельные дни и часы), могут свидетельствовать о том, что проблема заключается в учетной записи. Возможно, ограничены часы регистрации, или в результате превышения лимита ошибок при регистрации заблокирована учетная запись (быть может, кто-то пытался выполнить несанкционированную регистрацию). Убедитесь в правильности настроек учетной записи и проверьте журналы безопасности сервера на предмет подозрительной активности. Кроме того, вы можете попросить пользователя попытаться зарегистрироваться с другой рабочей станции, располагающей необходимыми для этого полномочиями.

Отправьте на станцию Ping-запрос. Для тестирования IP-адреса проблемной станции нужно пользоваться утилитами, подобными Ping. Если станция не сможет ответить, значит, существует неисправность кабеля, порта концентратора/коммутатора, или сетевой платы, и именно в этом направлении вам предстоит копать. Если станция отвечает на Ping-запрос (и, более того, сама может отправить такие запросы другим станциям), но во всех прочих отношениях ее поведение в сети оказывается некорректным, вполне возможно, что соединение и оборудование сетевой платы работают в нормальном режиме, а проблема исходит от программного обеспечения. Еще раз проверьте настройки, и исправьте все недочеты.

Проверьте порт концентратора/коммутатора. Если станция подключена к «управляемому», концентратору или коммутатору, вполне возможно, что ее порт отключен. Откройте служебную программу управления и проверьте состояние соответствующего данной станции порта. Если порт отключен, попытайтесь включить его. Если попытки повторного включения порта ни к чему не приведут (а также, если порт будет обозначаться как неисправный или недоступный), попытайтесь подключить рабочую станцию к другому незанятому порту (с другой стороны, вы можете полностью заменить концентратор/коммутатор). Если концентратор/коммутатор не является «управляемым», то, для того чтобы проверить исправность порта, имеет смысл перезагрузить концентратор/коммутатор или попробовать подключить рабочую станцию к другому свободному порту.

Проблемы в сегменте. Предположим, что проблема затрагивает несколько сетевых станций. Логика диктует, что проблема является общей для всех этих станций. В большинстве подобных случаев причина

заключается в неисправности кабеля или концентратора/коммутатора. Для примера рассмотрим четыре станции, находящиеся в одной части офиса и подключенные к одному концентратору, который, в свою очередь, подсоединен к коммутатору, обеспечивающему работу сервера и прочих небольших групп, подключенных к локальным концентраторам по всему офису.

Проверьте питание локального концентратора. Убедитесь в том, что небольшой концентратор, к которому подключены все четыре удаленных рабочих станции, получает питание. Можете попытаться перезагрузить этот концентратор, отключив питание на несколько секунд, а затем, возобновив его и предоставив концентратору возможность провести самотестирование. Кроме того, проверьте, светятся ли светодиоды линий, соответствующих каждой рабочей станции, подключенной к локальному концентратору. Если эти светодиоды не работают, вполне возможно, что локальный концентратор неисправен и нуждается в замене.

Проверьте активность и наличие конфликтов. Необычно высокие уровни активности и избыточные конфликты способны оказать негативное воздействие на станции, расположенные в рамках отдельного сегмента. Взгляните на светодиоды активности и конфликтов, соответствующие всем затронутым рабочим станциям. Возможно, что станция Ethernet с необычно высоким уровнем активности приводит к возникновению чрезмерного количества конфликтов. Если умышленные операции передачи со станции-нарушителя не проводятся, значит, возможно, ее сетевая плата передает сбойные пакеты и требует замены. Обоснованный трафик, приводящий к возникновению избыточного количества конфликтов, возможно, свидетельствует о необходимости обеспечения более серьезной пропускной или своего перемещения в другой сегмент (т. е. подключения сильно занятой станции к какому-то другому концентратору).

Проверьте магистральный кабель. Взгляните на кабель, проложенный между локальным портом и соответствующим ему портом коммутатора (возможно, для того, чтобы получить данные об этом соединении, вам придется обратиться к физической карте). Проверьте, светится ли светодиод канала. Если он не функционирует, значит, кабель отсоединен или поврежден – вероятно, для восстановления нормального соединения вам придется чинить кабель.

Отправьте Ping-запросы на локальные станции. Пользуясь утилитой Ping, проверьте возможность передачи данных между локальными станциями. Если отправка Ping-запроса с одной локальной станции на другую не приведет к успеху, значит, концентратор неисправен и требует замены.

Отправьте Ping-запросы на удаленные станции. Если локальные станции сохраняют возможность взаимной отправки Ping-запросов через концентратор, попробуйте отправить Ping-запросы на коммутатор, сервер или другие станции, являющиеся внешними по отношению к коммутатору. Если отправка Ping-запросов с любой локальной станции через коммутатор не приведет к успеху, значит, коммутатор, возможно, неисправен и требует замены. Попробуйте подключиться к другому свободному порту коммутатора. Если коммутатор является «управляемым», откройте служебную программу управления, проверьте состояние рассматриваемого порта, и, если представится такая возможность, попробуйте разблокировать его. В противном случае замените коммутатор.

Проблемы масштаба всей сети. Наиболее обременительные и серьезные типы неисправностей распространяются на всю сеть. К примеру, может сложиться ситуация, при которой ни один из пользователей не сможет зарегистрироваться на сервере домена, подключиться к сети Интернет или воспользоваться сетевым принтером. На первый взгляд, проблемы подобного рода производят впечатление крайне сложных, требующих наличия высокопрофессионального оборудования и многих лет опыта работы специалиста; как бы то ни было, самым эффективным вашим оружием является знание схемы сети и понимание причинно-следственных связей.

Если проблема распространяется на отдельно взятую станцию, естественная логика подсказывает, что все внимание нужно обратить именно на эту станцию (начиная с качества сетевого соединения и корректности настройки учетной записи). С другой стороны, предположим, что зарегистрироваться на сервере домена не удается всем пользователям. Определить, что все эти станции сохраняют способность к передаче информации (к примеру, они обеспечивают коллективный доступ к файлам и каталогам на других серверах или персональных компьютерах), не составляет сложности. В таком случае общей нитью является сам сервер домена. Возможно, он отключен или неверно настроен; не исключено присутствие некоей аппаратной неисправности, требующей конфигурации или починки.

3.2. Инструментальные средства поиска

Применение диагностических команд маршрутизатора. В маршрутизаторах Cisco предусмотрено множество встроенных команд, позволяющих контролировать работу и выполнять поиск неисправностей в объединенной сети. В следующих разделах описаны основные области применения этих команд.

- Команды show позволяют контролировать работу оборудования и определять характеристики сети, а также выявлять проблемные области.

- Команды debug позволяют диагностировать проблемы, возникающие из-за неправильной настройки конфигурации протоколов и оборудования.
- Команды ping позволяют проверить возможность взаимодействия устройств в сети.
- Команды trace дают возможность определить маршрут, по которому проходят пакеты от одного устройства к другому на пути к месту назначения.

Применение команд show. Команды show представляют собой мощное инструментальное средство текущего контроля и поиска неисправностей. Команды show могут применяться для выполнения следующих функций:

- текущий контроль характеристик маршрутизатора в процессе инсталляции;
- текущий контроль нормального функционирования сети;
- выявление интерфейсов, узлов, компонентов передающей среды или приложений, которые являются причиной неисправности;
- определение наличия заторов в сети;
- определение состояния смежных серверов, клиентов или других смежных устройств.

Ниже перечислены некоторые наиболее широко применяемые команды show.

- show version. Показывает конфигурацию аппаратных средств системы, версию программного обеспечения, имена файлов конфигурации, а также загрузочные образы.
- show running-config. Отображает применяемую в настоящий момент конфигурацию маршрутизатора.
- show startup-config. Показывает конфигурацию маршрутизатора, которая хранится в энергонезависимом ОЗУ (оперативное запоминающее устройство).
- show interfaces. Выводит статистические данные по всем интерфейсам, которые входят в конфигурацию маршрутизатора или сервера доступа. Отображаемые данные зависят от типа сети, для использования в которой настроен конкретный интерфейс.
- show controllers. Показывает статистические данные о контроллерах интерфейсных плат.
- show flash. Отображает компоновку и содержимое флэш-памяти.
- show buffers. Выводит статистические данные о буферных пулах маршрутизатора.
- show memory summary. Выводит статистические данные о пулах оперативной памяти и итоговую информацию о действиях про-

граммы распределения системной памяти, а также предоставляет отчет об использовании каждого блока памяти.

- show process cpu. Показывает информацию об активных процессах в маршрутизаторе.
- show stacks. Выводит информацию об использовании стека процессами и процедурами прерывания, а также показывает причину последней перезагрузки системы.
- show cdp neighbors. Предоставляет определенную информацию о возможности доступа к непосредственно подключенным (соседним, или смежным) устройствам Cisco. Эта команда – исключительно полезное инструментальное средство, позволяющее определить состояние функционирования физического уровня и уровня передачи данных. CDP представляет собой собственный протокол уровня передачи данных.
- show debugging. Выводит информацию о том, какой режим отладки разрешен для данного маршрутизатора.

Рис. 7. Команды show running-config и show startup-config

Для получения списка подкоманд любых команд всегда можно ввести вопросительный знак (?) в командной строке.

Как и команды debug, некоторые команды show, перечисленные выше, доступны только в привилегированном режиме выполнения exec-команд маршрутизатора (в режиме enable). Кроме перечисленных, имеются также сотни других команд show. Дополнительные сведения об использовании и интерпретации вывода конкретных команд show приведены в справочниках по командам IOS (Internetwork Operating System – операционная система для объединенных сетей) корпорации Cisco.

Применение команд debug. Привилегированные exec-команды debug позволяют получить значительный объем информации о том, какой трафик наблюдается (или не наблюдается) в определенном интерфейсе, перехватить сообщения об ошибках, вырабатываемых узлами сети, сформировать диагностические пакеты, относящиеся к конкретному про-

токолу, а также ознакомиться с другими данными, необходимыми для поиска неисправностей. Чтобы получить доступ к перечню привилегированных exec-команд и ознакомиться с ним, введите следующий код:

```
Router>
enable Password: XXXXXX
Router# ?
```

Команды debug должны применяться только для поиска причин неисправностей, а не для контроля над нормальным функционированием сети. Команды debug требуют больших затрат процессорного времени, поэтому должны применяться исключительно при анализе трафика определенного типа или при устранении неисправностей, если они позволят сузить круг поиска возможных причин неисправностей.

Формат вывода результатов зависит от конкретной команды debug. Некоторые команды вырабатывают по одной строке вывода для каждого пакета, а другие при обработке каждого пакета вырабатывают несколько строк вывода. Одни команды генерируют большой объем выходной информации, а другие выводят данные лишь время от времени. Одни команды выдают текст построчно, а другие формируют отчеты с данными, представленными в отдельных полях.

Чтобы свести к минимуму негативное влияние, связанное с использованием команд debug, соблюдайте следующие рекомендации.

Шаг 1. Используйте в маршрутизаторе глобальную команду конфигурации no logging console, которая отменяет весь вывод журнала на терминал консоли.

Шаг 2. Подключитесь по протоколу Telnet к порту маршрутизатора и введите exec-команду enable, которая переводит маршрутизатор в режим привилегированных exec-команд. После ввода пароля enable, обеспечивающего доступ, вы получите приглашение к вводу информации, которое состоит из имени маршрутизатора и знака фунта (#).

Шаг 3. Используйте команду terminal monitor для копирования вывода команды debug и сообщений системы об ошибках на дисплей своего текущего терминала.

Перенаправив вывод на дисплей своего текущего терминала, вы сможете дистанционно просматривать вывод команды debug, не подключаясь через порт консоли.

Если команды debug выполняются через порт консоли, то при передаче каждого символа активизируется прерывание процессора, поэтому и без того значительная нагрузка процессора, вызванная использованием команды debug, возрастает до предела.

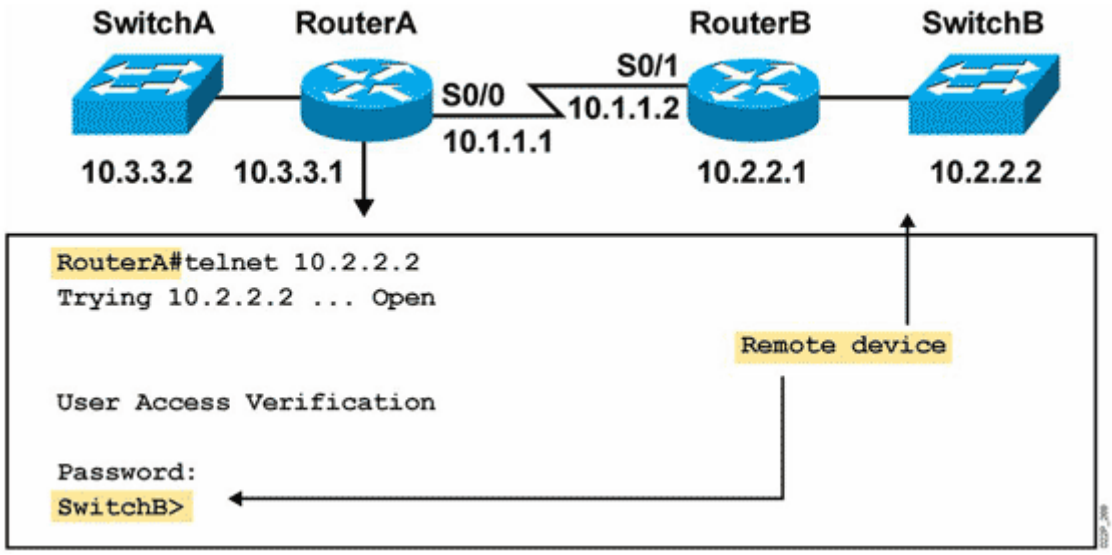


Рис. 8. Тестирование уровня приложений с помощью команды telnet

Если вывод команды debug необходимо сохранить для справок, выведите его в файл.

Применение команд ping. Команда ping, которая может быть вызвана на выполнение в режиме непривилегированных и привилегированных exec-команд, применяется для проверки доступности хоста и связи по сети. После регистрации на маршрутизаторе или сервере доступа автоматически устанавливается режим непривилегированных exec-команд. Доступные на непривилегированном уровне exec-команды являются подмножеством exec-команд, применяемых на привилегированном уровне. Как правило, непривилегированные exec-команды позволяют подключаться к удаленным устройствам, изменять на время установки терминала, выполнять простейшие проверки и выводить на экран информацию о системе. Команда ping позволяет выполнять простые проверки наличия связи в сетях AppleTalk, CLNS (Connectionless Network Service – сетевое обслуживание без установления соединения) по стандарту ISO, IP, Novell, Apollo, VINES, DECnet или XNS.

В сетях IP при выполнении команды ping происходит отправка запросных сообщений эхо-тестирования ICMP. ICMP – это протокол Internet, с помощью которого передаются сообщения об ошибках и предоставляется информация, касающаяся адресации IP-пакетов. При получении запросного сообщения эхо-тестирования ICMP станция передает отправителю этого сообщения ответное сообщение эхо-тестирования ICMP.

Расширенный командный режим команды ping позволяет указать поддерживаемые опции заголовка IP-пакета. При этом в маршрутизаторе может быть выполнен ряд проверок, предусматривающих более широкий

набор функций. Для перехода в расширенный командный режим ping введите yes в ответ на приглашение extended commands команды ping.

Рекомендуем воспользоваться командой ping при нормальном функционировании сети, чтобы узнать, как работает эта команда в обычных условиях, и сравнить полученные при этом результаты с результатами, характерными для нарушений в работе.

Применение команд trace. Непривилегированная exec-команда trace позволяет определить, по каким маршрутам следуют пакеты определенного маршрутизатора на пути к месту назначения. Привилегированная exec-команда trace дает возможность указать поддерживаемые опции заголовков IP-пакетов, в результате чего в маршрутизаторе может быть применен более широкий набор опций проверки.

В команде trace используются сообщения об ошибках, вырабатываемые маршрутизаторами при достижении дейтаграммой минимального значения срока жизни TTL. Вначале рассылаются пакеты запросов (специальные дейтаграммы) со значением TTL, равным 1. В результате первый маршрутизатор отбрасывает запросы и возвращает сообщения об ошибках «time exceeded», которые указывают, что срок жизни пакета истек. На следующем этапе выполнения команды trace передается еше несколько запросов и для каждого из них отображается время кругового обращения. После отправки каждого третьего запроса значение TTL увеличивается на 1.

Отправка каждого исходящего пакета может привести к получению одного из двух сообщений об ошибках. Сообщение об ошибке «time exceeded» указывает, что промежуточный маршрутизатор получил и отбросил запрос, поскольку истек срок жизни пакета. Сообщение об ошибке «port unreachable» указывает, что узел назначения получил и отбросил пакет, поскольку не мог доставить его приложению. А если установка таймера истекла до того, как поступил ответ, команда trace выводит символ звездочки (*).

Выполнение команды trace заканчивается после получения ответа от хоста назначения, при превышении максимального значения TTL или при вводе пользователем управляющей последовательности, которая прерывает трассировку.

Как и при использовании команды ping, рекомендуем выполнить команду trace при нормальном функционировании сети, чтобы узнать, как работает эта команда в обычных условиях, и сравнить полученные при этом результаты с результатами, характерными для нарушений в работе.

Инструментальные средства управления сетью, предоставляемые корпорацией Cisco. Корпорация Cisco поставляет семейство программных продуктов управления сетью CiscoWorks 2000, в состав кото-

рого входят инструментальные средства проектирования, текущего контроля и поиска неисправностей, позволяющие упростить управление объединенной сетью.

При поиске неисправностей в объединенной сети могут применяться следующие инструментальные средства управления объединенной сетью.

- Программа CiscoView выполняет функции динамического текущего контроля и поиска неисправностей, в частности, позволяет получить графическую схему соединений устройств Cisco, статистические данные и исчерпывающую информацию о конфигурации.
- Монитор производительности объединенной сети (IPM – Internetwork Performance Monitor) позволяет сетевым инженерам заблаговременно определять отклонения характеристик сетевого отклика от нормы с использованием отчетов, полученных в настоящее время и в прошлом.
- Инструментальное средство дистанционного текущего контроля (RMON – Remote MONitoring) TrafficDirector дает возможность накапливать данные, контролировать действия, происходящие в сети, и диагностировать потенциальные проблемы.
- Приложение управления коммутатором VlanDirector представляет собой инструментальное средство управления, которое позволяет получить полное представление о состоянии виртуальных локальных сетей.

Программа CiscoView. Графические средства управления программы CiscoView позволяют получить в оперативном режиме сведения о состоянии, статистические данные и исчерпывающую информацию о конфигурации продуктов корпорации Cisco для объединенных сетей (коммутаторов, маршрутизаторов, концентраторов и серверов доступа). Программа CiscoView дает возможность упростить управление сетью, поскольку схематически отображает информацию о состоянии устройств Cisco, в частности, предоставляет схему портов устройства с цветовой кодировкой, позволяющую быстро получить сведения о состоянии портов и охватить одним взглядом всю необходимую информацию. Ниже описаны основные возможности программы.

- Просмотр на графическом экране из центрального пункта информации о продуктах Cisco; это средство позволяет сетевым администраторам получить полное представление о работе устройств Cisco без физической проверки каждого устройства на удаленных узлах.

- Непрерывно обновляемая схема с информацией о маршрутизаторах, концентраторах, коммутаторах или серверах доступа в сети, полнота которой не зависит от их физического расположения.
- Постоянное обновление данных текущего контроля в реальном времени и отслеживание основной информации и данных, характеризующих производительность устройств, объем трафика и степень загрузки. Эти данные содержат такие ключевые характеристики, как процент использования, число переданных и полученных фреймов, относительное количество ошибок, а также целый ряд других показателей, касающихся каждого конкретного устройства.
- Возможность изменять такие опции конфигурации, как прерывания, IP-маршруты, параметры настройки виртуальных локальных сетей и мостов.

Монитор производительности объединенной сети. Приложение управления сетью IPM (Internetwork Performance Monitor – монитор производительности объединенной сети) обеспечивает текущий контроль над производительностью мультипротокольных сетей. Приложение IPM позволяет измерять время отклика и определять характеристики доступа сетей IP на каждом транзитном переходе (от одного маршрутизатора к другому). Это приложение позволяет также измерять время отклика на участках между маршрутизаторами и мэйнфреймом в сетях SNA (Systems Network Architecture – системная сетевая структура).

Приложение IPM применяется для выполнения следующих задач.

- Поиск неисправностей в сети путем проверки сетевой задержки на участках между устройствами.
- Передача прерываний SNMP (Simple Network Management Protocol – простой протокол управления сетью) и предупреждающих сообщений SNA при превышении порогового значения, установленного пользователем, при разрыве и восстановлении соединения или при возникновении тайм-аута.
- Анализ данных о потенциальных проблемах еше до их возникновения путем накопления статистических данных, которые могут использоваться для моделирования и прогнозирования характеристик будущих сетевых топологий.
- Текущий контроль времени отклика на участке между двумя оконечными точками.

Программный продукт IPM состоит из трех частей: серверного и клиентского приложения IPM, а также модуля генератора отчетов о времени отклика (RTR – Response Time Reporter), который входит в состав программного обеспечения Cisco IOS.

Приложение RMON TrafficDirector. Усовершенствованные фильтры пакетов приложения TrafficDirector дают возможность пользователям контролировать сетевой трафик на всех семи уровнях протоколов. С использованием встроенных агентов RMON операционной системы Cisco IOS и средств формирования автономных запросов SwitchProbe сетевые администраторы могут просматривать сетевой трафик в масштабах всего предприятия на канальном, сетевом, транспортном или прикладном уровнях. Итоговый отчет о многоуровневом трафике приложения TrafficDirector позволяет быстро получить общую оценку степени загрузки сети и определить относительный объем трафика различных протоколов. Затем сетевые администраторы могут перейти к подробному изучению конкретного сегмента, кольца, порта коммутатора или магистрального канала и применить инструментальные средства анализа и диагностики в реальном времени для просмотра информации о хостах и конкретных сеансах обмена данными, а также для перехвата пакетов.

Средства текущего контроля пороговых значений приложения TrafficDirector позволяют создать среду управления, которая обеспечивает заблаговременное устранение возможных неисправностей. Для этого прежде всего в агенте RMON устанавливаются пороговые значения важных переменных MIB (Management Information Base – информационная база управления). При превышении этих пороговых значений на соответствующую станцию управления передаются прерывания, позволяющие предупредить сетевого администратора о потенциальной проблеме.

Приложение управления коммутатором VlanDirector. Приложение управления коммутатором VlanDirector позволяет упростить распределение портов виртуальной локальной сети и обеспечивает управление виртуальными локальными сетями. Приложение VlanDirector выполняет следующие функции.

- Точное отображение физической сети, позволяющее разработать проект виртуальной локальной сети и выполнить проверку конфигурации.
- Сбор информации о конфигурации виртуальной локальной сети, которая относится к конкретному устройству или канальному интерфейсу.
- Формирование отчетов о несоответствиях при наличии противоречивой информации о конфигурации.
- Поиск неисправностей и выявление отдельных конфигураций устройств, которые не соответствуют характеристикам виртуальных локальных сетей на уровне всей системы.
- Своевременное обнаружение изменений в состоянии портов коммутаторов виртуальной локальной сети.

- Проверка подлинности пользователей и защита данных.

Инструментальные средства поиска неисправностей, предоставляемые независимыми поставщиками. Диагностические инструментальные средства независимых поставщиков часто могут оказаться более полезными по сравнению с командами, встроенными в маршрутизатор. Например, применение команды debug, требующей большого объема процессорного времени, в сетевой среде с исключительно интенсивным трафиком может привести к разрушительным последствиям. Но подключение сетевого анализатора к исследуемой сети практически не нарушает ее работу и позволяет с большей вероятностью получить необходимую информацию, не препятствуя нормальному функционированию маршрутизатора. Ниже перечислены некоторые типичные инструментальные средства поиска неисправностей, предоставляемые независимыми поставщиками, которые применяются для устранения нарушений в работе объединенных сетей.

- Для проверки физических характеристик кабельной сети применяются вольтомметры, цифровые мультиметры и кабельные тестеры.
- Поиск обрывов в кабелях, рассогласований импедансов и других технических неисправностей кабельной сети осуществляется с использованием динамических рефлектометров и оптических динамических рефлектометров.
- Для поиска неисправностей периферийных интерфейсов применяются коммутационные боксы, генераторы тестовых последовательностей и тестеры частоты ошибочных битов/частоты ошибочных блоков.
- Сетевые мониторы позволяют получить полное представление о функционировании сети на протяжении определенного периода времени путем непрерывного отслеживания пакетов, проходящих по сети.
- Такие сетевые анализаторы, как перехватчики сетевых пакетов, автоматически декодируют информацию, передаваемую на всех семи уровнях эталонной модели OSI, и способствуют выявлению нарушений в работе в реальном масштабе времени, позволяя получить полное представление о функционировании сети и классифицируя проблемы по степени важности.

Вольтомметры, цифровые мультиметры и кабельные тестеры. Вольтомметры и цифровые мультиметры относятся к числу наиболее простых инструментальных средств, предназначенных для измерения физических характеристик кабельной сети. Эти устройства измеряют такие параметры, как напряжение переменного и постоянного тока, силу тока, сопротивление и емкость, а также позволяют определить нали-

чие обрывов в кабеле. Они применяются для проверки физического состояния сети.

Кабельные тестеры (сканеры) также позволяют проверить физическое состояние сети. Для проверки экранированной витой пары (STP), неэкранированной витой пары (UTP), кабелей lOBaseT, одинарных и двойных коаксиальных кабелей применяются кабельные тестеры соответствующего типа. Как правило, кабельные тестеры обеспечивают выполнение следующих функций.

- Проверка состояния кабеля и предоставление отчета, в том числе с результатами измерения перекрестной наводки на ближнем конце, затухания и шума.
- Выполнение функций динамического рефлектометра, текущий контроль трафика и подготовка схемы кабельной системы.
- Предоставление информации уровня MAC (Media Access Control – управление доступом к передающей среде) о трафике в локальной сети, накопление статистических данных, которые необходимы для расчета таких показателей, как коэффициент использования сети и частота ошибочных пакетов, а также выполнение некоторых функций проверки работы протокола (например, такой проверки связи по протоколу TCP/I P, как эхо-тестирование).

Аналогичное испытательное оборудование предусмотрено и для волоконно-оптических кабелей. В связи с относительно высокой стоимостью и самого кабеля, и его монтажа, волоконно-оптический кабель должен проверяться перед монтажом (на кабельном барабане) и после монтажа. Для проверки стекловолокна на обрыв требуется источник видимого света или рефлектометр. Источники света, способные излучать свет с тремя основными значениями длины волны, 850, 1300 и 1550 нанометров (нм), применяются в сочетании с измерителями мощности, позволяющими проводить измерения на той же длине волны, проверять затухание и потери на отражение в стекловолокне.

Динамические рефлектометры и оптические динамические рефлектометры. К числу наиболее сложных приборов, применяемых для проверки характеристик медного кабеля, относятся динамические рефлектометры. Эти устройства позволяют быстро находить обрывы и короткозамкнутые цепи, скрутки, петли, острые изгибы, рассогласования импедансов и другие дефекты монтажа кабелей.

Динамический рефлектометр действует по принципу приема сигнала, отраженного от противоположного конца кабеля. При наличии обрывов, короткозамкнутых цепей и других дефектов амплитуда отраженного сигнала изменяется по-разному, в зависимости от дефекта. Динамический рефлектометр измеряет время, по истечении которого по-

ступает отраженный сигнал, и вычисляет расстояние до дефекта в кабеле. Динамические рефлектометры могут также применяться для измерения длины кабеля. Некоторые динамические рефлектометры позволяют вычислить скорость распространения сигнала путем измерения характеристик эталонного участка кабеля.

Для измерения характеристик волоконно-оптических кабелей применяются оптические динамические рефлектометры, которые позволяют точно измерить длину стекловолокна, найти обрывы в кабеле, определить затухание сигнала в стекловолокне, а также измерить величину потерь в стыке (месте сращивания волокна) или разъеме. Оптический динамический рефлектометр может применяться для подготовки протокола испытания смонтированной кабельной системы, в котором отмечены значения затухания и указаны потери в каждом стыке. Эти эталонные результаты измерений могут затем сравниваться с результатами текущей проверки кабельной системы для обнаружения неисправностей.

Коммутационные боксы, генераторы тестовых последовательностей и тестеры частоты ошибочных битов/частоты ошибочных блоков. Коммутационные боксы, генераторы тестовых последовательностей и тестеры частоты ошибочных битов/частоты ошибочных блоков представляют собой инструментальные средства проверки с цифровым интерфейсом, которые часто применяются для измерения цифровых сигналов в интерфейсах периферийного оборудования персональных компьютеров, принтеров, модемов, модулей обслуживания канала/модулей обработки данных (CSU/DSU) и других аппаратных средств. Эти устройства позволяют контролировать характеристики каналов передачи данных, анализировать и перехватывать передаваемые данные, а также диагностировать неисправности, которые часто возникают в системах передачи данных. С их помощью можно исследовать трафик, передаваемый от терминального оборудования (DTE – Data Terminal Equipment) через терминальное оборудование канала передачи данных (DCE – Data Circuit-terminating Equipment) для ускорения поиска неисправностей, выявления типичных последовательностей двоичных сигналов и проверки правильности монтажа кабельных соединений. Эти устройства не могут применяться для проверки сигналов в такой сетевой среде, как Ethernet, Token Ring или FDDI.

Сетевые мониторы. Сетевые мониторы непрерывно отслеживают пакеты, проходящие по сети, и позволяют получить точное представление о функционировании сетей в любой момент времени или сформировать хронологический отчет об активности сети за определенный период времени. Мониторы не декодируют содержимое фреймов. Они могут применяться для накопления эталонных данных. При этом в течение

определенного времени фиксируются данные о характеристиках работы сети для формирования так называемого *эталонного профиля производительности,* т. е. данных о работе сети при нормальных условиях.

Сетевые мониторы собирают информацию о размерах и количестве пакетов, включая ошибочные. Они позволяют определить общие показатели использования соединения, выяснить количество хостов и их MAC-адреса, а также получить подробные сведения о сеансах обмена данными между хостами и другими устройствами. Эти данные могут использоваться для создания профилей трафика локальной сети, а также для обнаружения участков с чрезмерным объемом трафика, планирования расширения сети, обнаружения нарушителей правил зашиты сети, накопления эталонных данных о производительности, а также для более эффективного распределения трафика.

Сетевые анализаторы. *Сетевые анализаторы* (или *анализаторы протокола)* декодируют информацию о разных уровнях протокола в зарегистрированных фреймах и представляют накопленную информацию в виде удобных для чтения кратких отчетов или сводок, по которым можно определить, на каких уровнях осуществлялась обработка данных (физическом, канальном и т. д.) и какие функции выполняет каждый байт заголовка или информационного наполнения.

Большинство сетевых анализаторов в основном выполняет следующие функции:

- отбирают трафик, который соответствует определенным критериям; это позволяет, например, перехватывать все фреймы, входящие или исходящие из конкретного устройства;
- регистрируют время перехвата данных;
- представляют информацию об уровнях протокола в форме, удобной для чтения;
- генерируют фреймы и выводят их в сеть;
- предоставляют возможность воспользоваться «экспертной» системой, в которой применяется набор правил в сочетании с информацией о конфигурации и функционировании сети для диагностики и устранения нарушений в работе сети или для выработки рекомендаций по улучшению ее работы.

4. УСТРАНЕНИЕ НАРУШЕНИЙ В РАБОТЕ АППАРАТНЫХ СРЕДСТВ, СРЕДСТВ ЗАГРУЗКИ И ПЕРЕДАЮЩЕЙ СРЕДЫ

4.1. Нарушения в работе аппаратных средств и средств загрузки

Загрузка маршрутизатора. Для инициализации системы (начальной загрузки) маршрутизаторов Cisco предусмотрено четыре способа.

- **Начальная загрузка по сети.** Маршрутизаторы можно загружать с сервера с помощью протокола TFTP, протокола MOP (Maintenance Operation Protocol – протокол обслуживания) корпорации DEC или протокола RCP (Remote Copy Protocol – протокол дистанционного копирования) по любому из поддерживаемых видов передающей среды, таким как Ethernet, Token Ring, FDDI, HSSI (High-Speed Serial Interface – высокоскоростной последовательный интерфейс) и по последовательным каналам.
- **Загрузка из флэш-памяти.** Маршрутизаторы могут загружаться из флэш-памяти – энергонезависимого носителя данных, который можно стирать и перепрограммировать с помощью электронных средств.
- **Загрузка** из **ПЗУ.** Начальная загрузка операционной системы маршрутизаторов может осуществляться с помощью встроенного постоянного запоминающего устройства (ПЗУ).
- **Загрузка с помощью платы флэш-памяти.** Для начальной загрузки маршрутизаторов может применяться съемная плата флэш-памяти.

В настоящем разделе приведены общие сведения о загрузке маршрутизаторов.

Рекомендации по загрузке через сеть. Во время сеансов начальной загрузки по сети маршрутизаторы действуют как обычные хосты. Их трафик маршрутизируется с помошью информации протокола ARP, SLARP (Serial Line Address Resolution Protocol – протокол преобразования адресов последовательного канала), перенаправлений протокола ICMP или с применением шлюза, заданного по умолчанию. Во время загрузки по сети маршрутизаторы игнорируют динамическую информацию маршрутизации, статические IP-маршруты и информацию о перенаправлении фреймов мостами. Поэтому успешная загрузка маршрутизатора в основном зависит от функционирования промежуточных

маршрутизаторов, которые должны правильно обрабатывать запросы ARP и UDP. При использовании в качестве передающей среды последовательных каналов и интерфейса HSSI протокол ARP не применяется.

Перед выполнением начальной загрузки по сети с сервера необходимо выполнить эхо-тестирование сервера с помощью программного обеспечения, записанного в ПЗУ. Если эхо-тестирование сервера невозможно выполнить, обратитесь к процедурам, описанным ниже, в разделе «Начальная загрузка: маршрутизатор не может загрузиться по сети от TFTP-сервера». Если и после этого невозможно выполнить эхо-тестирование сервера, то, вероятно, имеются ошибки в конфигурации сервера или неисправности аппаратных средств. Изучите документацию по TFTP-серверу или обратитесь за помощью к представителю службы технической поддержки.

Надежные методы начальной загрузки. Метод начальной загрузки по сети является очень удобным, но его применение может стать невозможным при нарушениях в работе сети или сервера. После установки и настройки флэш-памяти маршрутизатора необходимо правильно определить последовательность начальной загрузки маршрутизатора, чтобы свести к минимуму влияние нарушений в работе сервера или сети. Рекомендуется следующий порядок загрузки.

1. Загрузка образа системы из флэш-памяти.
2. Загрузка образа системы по сети.
3. Начальная загрузка с применением образа системы, записанного в ПЗУ.

Ниже приведен пример того, как нужно выполнить настройку конфигурации маршрутизатора с учетом указанной последовательности начальной загрузки.

```
goriot#configure terminal
Enter configuration commands, one per line. End
with CNTL/Z.
goriot(config)#boot system flash gsxx
goriot(config)#boot system gsxx 131.108.1.101
goriot(config)#boot system rom
goriot(config)#^Z
goriot#%SYS-5-C0NFIG_I: Configured from console by
console
goriot#copy running-config startup-config
[ok]
goriot#
```

Если применяется описанный метод, то маршрутизатор имеет три источника информации для начальной загрузки: он может загружаться

из флэш-памяти, по сети, а также из ПЗУ. Предоставление альтернативных источников загрузочной информации позволяет уменьшить влияние любых нарушений в работе TFTP-сервера или сети.

Тайм-ауты и пакеты, поступающие с нарушением порядка следования. Во время начальной загрузки по сети клиенту может потребоваться повторно передавать запросы перед получением ответа на определенный ARP-запрос. При таких повторных передачах могут возникать тайм-ауты и появляться пакеты, поступающие с нарушением порядка следования.

Тайм-ауты (показанные точками на дисплее начальной загрузки по сети) и пакеты с нарушением порядка следования (показанные прописными буквами О) не всегда препятствуют успешной начальной загрузке по сети. Поэтому в процессе начальной загрузки по сети вполне допустимо появление тайм-аутов или пакетов с нарушением порядка следования, или тех и иных.

В следующих примерах показан вывод на консоль во время сеансов начальной загрузки по сети, которые оказались успешными, даже несмотря на появление тайм-аутов и пакетов с нарушением порядка следования (восклицательными знаками указаны успешно принятые пакеты):

```
Booting gs3-bfx from 131.108.1.123:
!.!!!!!!!!!!!!!!!!!!!!
Booting gs3-bfx from 131.108.1.123:
!O.O!!!!!!!!!!!!!!!!!!!!
```

Но если в ходе начальной загрузки по сети появляется слишком много тайм-аутов и пакетов с нарушением порядка следования, то могут возникнуть проблемы.

Информация для службы технической поддержки. Если вы не можете решить проблему начальной загрузки с использованием процедур, описанных в настоящей главе, подготовьте следующую информацию для представителя службы технической поддержки.

- Версии образов системы, записанных в ПЗУ. (Используйте exec-команду show version.)
- Надписи на программируемых ПЗУ. (Эта информация отпечатана на корпусе микросхемы и пример ее показан на рис. 9.)
- Конфигурации энергонезависимых ОЗУ для клиентского маршрутизатора и смежных маршрутизаторов.
- Отладочный вывод, полученный со смежных маршрутизаторов с использованием следующих привилегированных exec-команд:
  - `debug ip packet;`

- `debug arp;`
- `debug ip udp;`
- `debug tftp.`

Запуск коммутаторов ряда Catalyst 2900. При запуске LAN-коммутатора ряда Catalyst 2900 должно произойти следующее.

- Светодиод PS на лицевой панели блока управления должен загореться и продолжать гореть зеленым светом до тех пор, пока в систему подается питание.
- Блок вентиляторов системы должен включиться, а светодиод Fan – загореться. Они должны оставаться в таком состоянии до тех пор, пока в систему подается питание.
- Светодиоды Status на блоке управления и на каждом интерфейсе должны гореть оранжевым светом до тех пор, пока не закончится начальная загрузка.

После завершения начальной загрузки системы блок управления должен инициализировать коммутационные модули. Светодиод Status на каждом коммутационном модуле после завершения инициализации загорается и на экране консоли отображаются сценарий и системная заставка, примерно так:

```
BOOTROM Version 2.1, Dated May 22 1996 15:17:09
Boot date: 05/22/96 BOOT time: 15:17:09 Executing
from RAM
Cisco Systems Console
Sending RARP request with address 00:40:0b:a0:05:b8
Sending bootp request with address
00:40:0b:a0:05:b8
Sending RARP request with address 00:40:0b:a0:05:b8
Sending bootp request with address
00:40:0b:a0:05:b8
No bootp or rarp response received
Enter password:
```

При обнаружении неисправности попытайтесь выяснить, в какой именно подсистеме она возникла. LAN-коммутатор ряда Catalyst 2900 имеет следующие подсистемы.

- Подсистема питания. Эта подсистема включает источники питания и вентиляторы источников питания.
- Подсистема охлаждения. Эта подсистема включает блок вентиляторов корпуса, который должен работать, если в систему подается питание.

- Подсистема процессора и интерфейсов. Эта подсистема включает блок управления (который содержит операционное программное обеспечение системы), сетевые интерфейсы и всю соответствующую кабельную систему.

В табл. 2 перечислены основные области, в которых могут возникать проблемы при запуске LAN-коммутатора ряда Catalyst 2900, и описаны решения этих проблем.

Таблица 2

Проблемы при запуске LAN-коммутатора ряда Catalyst 2900 их решения

Проблема		Решение
Подсистема питания	**Шаг 1**	Проверьте светодиод Power. Если он не горит, убедитесь в том, что кабель питания не поврежден и присоединен должным образом к блоку питания и к штепсельной розетке сети переменного тока.
	Шаг 2	Если светодиод горит красным светом, это означает, что прервана подача электроэнергии или обнаружена неисправность блока питания и требуется его обслуживание. Для получения дальнейших указаний обратитесь к представителю службы технической поддержки.
Подсистема охлаждения	**Шаг 1**	Выясните, горит ли зеленым светом светодиод Fan на блоке управления. Если светодиод не горит зеленым светом, проверьте подсистему питания, чтобы определить, нормально ли она функционирует.
	Шаг 2	Если светодиод Fan горит красным светом, обратитесь за помощью к представителю службы технической поддержки.
Подсистема процессора и интерфейсов	**Шаг 1**	Проверьте светодиоды Link и Status блока управления. Оба они должны гореть зеленым светом, если все функции диагностики и самоконтроля были выполнены успешно и порты находятся в работоспособном состоянии.
	Шаг 2	Проверьте светодиоды на отдельных модулях интерфейса. В большинстве случаев они должны гореть зеленым светом (или должны мерцать зеленым светом, в случае светодиодов Transmit и Receive), если интерфейс функционирует правильно. Для получения дополнительной информации о назначении светодиодов модуля интерфейса обратитесь к руководству пользователя коммутатора.
	Шаг 3	Проверьте всю кабельную проводку и все соединения. Замените всю неисправную кабельную проводку.

Проверка и аттестация сменного оборудования. Если для поиска неисправности применяется метод, предусматривающий замену компонентов или плат, выполняйте каждый раз только одну замену.

Для проверки системы выполните ее запуск в самой простой аппаратной конфигурации и постепенно добавляйте по одной плате, пока не будет обнаружен или изолирован неисправный интерфейс. Используйте простую программную конфигурацию и проверяйте наличие связи по сети с помощью команды ping.

Если будет обнаружено, что требуется замена компонента или платы, обратитесь к представителю службы технической поддержки. Конкретные инструкции по монтажу компонента или платы приведены в рекомендациях по настройке, которые входят в комплект компонента или платы, предназначенных для замены.

Выполняя поиск неисправностей в модульных маршрутизаторах, следите за правильной установкой всех плат. Если система не загружается должным образом, проверьте установку плат в разъемах. С помощью эжекторного рычага приподнимите, а затем снова установите в гнезда все процессорные модули, после чего выполните перезагрузку.

4.2. Устранение нарушений в работе передающей среды

Устранение нарушений в работе сети Ethernet. В табл. 3 приведены процедуры поиска неисправностей, связанных с обычными нарушениями в работе передающей среды Ethernet.

Таблица 3

Процедуры поиска неисправностей, связанных с обычными нарушениями в работе передающей среды Ethernet

Нарушение	Рекомендации по устранению неисправности	
Слишком высокий уровень шума	**Шаг 1**	Воспользуйтесь exec-командой show interfaces Ethernet для определения состояния интерфейсов Ethernet маршрутизатора. На наличие слишком высокого уровня шума указывает значительное количество ошибок CRC при небольшом количестве коллизий.
	Шаг 2	Проверьте кабели, чтобы убедиться в том, что в них отсутствуют повреждения.
	Шаг 3	Найдите места подключения компьютеров к кабелю, расположенные через неправильные интервалы, которые могут вызвать зеркальное отражение сигнала.
	Шаг 4	При использовании протокола 100BaseTX убедитесь в том, что применяемая кабельная разводка относится к категории 5, а не к другому типу, например, к категории 3

Продолжение табл. 3

Нарушение	Рекомендации по устранению неисправности	
Слишком высокое значение относительного количества коллизий	**Шаг 1**	Воспользуйтесь командой show interfaces ethernet для проверки относительного количества коллизий. Отношение количества коллизий к общему количеству принятых фреймов не должно превышать приблизительно 0,1 %.
	Шаг 2	Воспользуйтесь динамическим рефлектометром для поиска всех кабелей Ethernet, на которых не установлены терминаторы (заглушки).
	Шаг 3	Найдите подключенный к хосту трансивер, передающий искаженные данные. (Для этого может потребоваться осмотр каждого хоста или применение анализатора протокола.)
Чрезмерное количество слишком коротких фреймов		В разделяемой среде Ethernet причиной появления слишком коротких («карликовых») фреймов почти всегда являются коллизии. Если относительное количество коллизий велико, обратитесь к приведенному выше в данной таблице разделу с описанием проблемы, связанной с обнаружением слишком высокого значения относительного количества коллизий. Если «карликовые» фреймы появляются при небольшом относительном количестве коллизий или обнаруживаются в коммутируемой среде Ethernet, они могут быть вызваны недобором данных или некачественным программным обеспечением сетевой интерфейсной платы. Воспользуйтесь анализатором протокола, чтобы попытаться определить исходный адрес фреймов с размерами меньше минимально допустимого.
Запоздалые коллизии	**Шаг 1**	Воспользуйтесь анализатором протокола, чтобы проверить наличие запоздалых коллизий. *(Запоздалыми* называются коллизии, возникающие за пределами первых 64 байтов фрейма.) Запоздалые коллизии никогда не должны возникать в правильно спроектированной сети Ethernet. Они обычно появляются, если кабели Ethernet имеют слишком большую длину или в сети установлено слишком много повторителей.
	Шаг 2	Проверьте диаметр сети и убедитесь в том, что он соответствует спецификации

Окончание табл. 3

Нарушение	Рекомендации по устранению неисправности	
Отсутствие связи по каналу в сети 10BaseT, 100BaseT4 или 100BaseTX	**Шаг 1**	Убедитесь в том, что не используется протокол 100BaseT4 при наличии в кабеле только двух пар проводов. Для протокола 100BaseT4 требуется кабель с четырьмя парами проводов.
	Шаг 2	Проверьте в сети 10BaseT, 100BaseT4 или 100BaseTX соответствие типов аппаратных средств (например, убедитесь в том, что в порту концентратора не установлена неподходящая для него плата).
	Шаг 3	Определите, применяются ли там, где это требуется, перекрестные кабели. (Например, убедитесь в том, что между станцией и концентратором не установлены прямые кабели.)
	Шаг 4	Проверьте, не наблюдается ли в сети слишком высокий уровень шума (см. описание проблемы, связанной с наличием стишком высокого уровня шума, приведенное выше в этой таблице)

При поиске неисправностей передающей среды Ethernet в среде маршрутизатора Cisco можно воспользоваться командой show interfaces ethernet, которая предоставляет большой объем важной информации, позволяющей легко находить причины неисправностей.

Команда show interfaces Ethernet. Привилегированная exec-команда show interfaces ethernet применяется для вывода информации об интерфейсе Ethernet маршрутизатора.

- show interfaces ethernet unit [accounting].
- show interfaces ethernet [slot \ port] [accounting] (для маршрутизаторов ряда Cisco 7200 и Cisco 7500).
- show interfaces ethernet [type slot \ port-adapter \ port] (для портов плат универсального интерфейсного процессора маршрутизаторов ряда Cisco 7500).
- *Описание синтаксической структуры.*
- unit. В качестве этого параметра должен быть указан номер порта на выбранном интерфейсе.
- accounting. (Необязательный параметр.) При использовании этого параметра отображается число пакетов, относящихся к протоколу каждого типа, проходящих через интерфейс.
- slot. Для получения информации о гнездах и портах устройства обратитесь к соответствующему руководству по аппаратным средствам.
- port. Для получения информации о гнездах и портах устройства обратитесь к соответствующему руководству по аппаратным средствам.

- port-adapter. Для получения информации о совместимости адаптера порта обратитесь к соответствующему руководству по аппаратным средствам.

Эта команда впервые появилась в выпуске Cisco IOS 10.0. Если при вызове ее на выполнение не будет приведено значение параметра *unit* (параметров slot и port применительно к маршрутизатору ряда Cisco 7200 или параметров *slot* и *port-adapter* применительно к маршрутизатору ряда Cisco 7500), команда отображает статистические данные по всем сетевым интерфейсам. Необязательное ключевое слово accounting означает, что должно быть показано число пакетов, передаваемых через интерфейс по протоколу каждого типа.

Устранение нарушений в работе сети FDDI. В настоящем разделе описаны процедуры поиска неисправностей при решении обычных проблем передающей среды FDDI. В табл. 4 перечислены проблемы, которые наиболее часто встречаются в сетях FDDI, и приведены общие рекомендации по решению этих проблем.

Таблица 4

Проблемы передающей среды: спецификация FDDI

Нарушение		Рекомендации по устранению неисправности
Неработоспособное кольцо FDDI	**Шаг 1**	Воспользуйтесь exec-командой show interfaces fddi для определения состояния интерфейсов FDDI маршрутизатора.
	Шаг 2	Если команда show interfaces fddi показывает, что интерфейс и протокол канала передачи данных функционируют, выполните команду ping на каждом из маршрутизаторов.
	Шаг 3	Если интерфейс и протокол канала передачи данных функционируют, убедитесь в том, что MAC-адреса предыдущего и следующего смежных устройств соответствуют установленным требованиям.
	Шаг 4	Если в полях адреса одного из указанных смежных устройств присутствуют все нули, это может быть связано с неисправностью физического соединения.
	В этом случае (или если строка информации о состоянии не показывает, что интерфейс и протокол канала передачи данных находятся в работоспособном состоянии) проверьте, соединения коммутационной панели или воспользуйтесь оптическим динамическим рефлектометром или экспонометром, чтобы проверить наличие соединения между смежными устройствами. Убедитесь в том, что мощность сигнала соответствует требованиям спецификаций.	

Окончание табл. 4

Нарушение		Рекомендации по устранению неисправности
Произошел отказ предыдущего смежного устройства и установлено реле транзитной передачи	Реле транзитной передачи могут вызывать снижение уровня сигнала, поскольку они не ретранслируют сигналы, как обычные трансиверы.	
	Шаг 1	Проверьте предыдущее смежное устройство, чтобы определить, работоспособно ли оно.
	Шаг 2	Если этот узел не функционирует и установлено реле транзитной передачи, устраните все неисправности, обнаруженные в предыдущем смежном устройстве

Во время поиска неисправностей передающей среды FDDI, функционирующей при поддержке маршрутизатора Cisco, можно воспользоваться командой show interfaces fddi, которая предоставляет большой объем важной информации, позволяющей легко находить причины неисправностей.

Команда show interfaces fddi. Воспользуйтесь exec-командой show interfaces fddi для получения информации об интерфейсе FDDI.

Описание синтаксической структуры.

- number. Номер порта на выбранном интерфейсе.
- accounting. (Необязательный параметр.) Отображает число пакетов, переданных через данный интерфейс по протоколу каждого типа.
- slot. Для получения информации о гнездах и портах устройства обратитесь к соответствующему руководству по аппаратным средствам.
- port. Для получения информации о гнездах и портах устройства обратитесь к соответствующему руководству по аппаратным средствам.
- port-adapter. Для получения информации о совместимости адаптера порта обратитесь к соответствующему руководству по аппаратным средствам.

Рекомендации по использованию.

Эта команда впервые появилась в выпуске Cisco IOS 10.0. В выпуске Cisco IOS 11.3 внесены изменения для включения варианта вывода, касающегося дуплексных, одно- и многомодовых адаптеров порта для FDDI (PA-F/FD-SM и PA-F/FD-MM).

Устранение нарушений в работе сети Token Ring. В настоящем разделе описаны процедуры поиска неисправностей при решении обычных проблем передающей среды Token Ring. Здесь рассматриваются конкретные признаки неисправностей в сети Token Ring, перечислены проблемы, которыми может быть обусловлено появление каждого признака неисправности, и показаны способы решения этих проблем.

Таблица 5

Нарушения в работе передающей среды сети Token Ring

Нарушение	Рекомендации по устранению неисправности	
Неработоспособное кольцо Token Ring	**Шаг 1**	Воспользуйтесь командой show interfaces token для определения состояния интерфейсов маршрутизатора Token Ring.
	Шаг 2	Если строка с информацией о состоянии не указывает, что интерфейс и протокол канала передачи данных функционируют нормально, проверьте кабель от маршрутизатора к модулю многостанционного доступа MSAU (Multistation Access Unit). Убедитесь в том, что кабель полностью исправен. Если кабель неисправен, замените его.
	Шаг 3	Если нарушения в работе обнаружены после установки нового сетевого оборудования, проверьте, была ли должным образом выполнена инициализация модуля MSAU. Для получения информации об инициализации модуля MSAU обратитесь к документации изготовителя
Несоответствие спецификаций скорости кольца	**Шаг 1**	Проверьте спецификацию скорости кольца на всех узлах, подключенных к опорной сети Token Ring. В параметрах конфигурации всех станций должна быть установлена одинаковая скорость кольца (4 Мбит/с или 16 Мбит/с). Воспользуйтесь привилегированной exec-командой show running-config, чтобы определить, какая скорость указана в маршрутизаторе.
	Шаг 2	В случае необходимости измените спецификации скорости кольца для клиентов, серверов и маршрутизаторов. На маршрутизаторах для изменения скорости кольца воспользуйтесь командой конфигурации интерфейса ring-speed. Если это потребуется, переставьте перемычки на модульных маршрутизаторах, которые не обеспечивают настройку скорости кольца программным путем. Для получения дополнительной информации о спецификациях скорости кольца обратитесь к руководству по монтажу и техническому обслуживанию аппаратных средств для конкретной системы

Продолжение табл. 5

Нарушение	Рекомендации по устранению неисправности	
Открытый ретранслятор в модуле MSAU	**Шаг 1**	Если на консоли во время включения системы появляется сообщение «open lobe fault», проверьте кабельное соединение с модулем MSAU.
	Шаг 2	Воспользуйтесь привилегированной exec-командой clear interface, чтобы выполнить сброс интерфейса Token Ring и снова вставить маршрутизатор в кольцо.
	Шаг 3	Для всех плат Token Ring, кроме CTR и маршрутизаторов доступа необходимо применить команду clear interface для повторной инициализации интерфейса Token Ring, если произошел останов интерфейса.
	Шаг 4	Воспользуйтесь exec-командой show interfaces token, чтобы проверить, исправно ли функционируют интерфейс и протокол канала передачи данных.
	Шаг 5	Если интерфейс функционирует нормально, но сообщение «open lobe fault» продолжает появляться и маршрутизатор все еще не может соединиться с кольцом, подключите маршрутизатор к другому порту MSAU.
	Шаг 6	Если и в этом случае сообщение «open lobe fault» продолжает появляться, отключите от модуля MSAU все устройства и выполните сброс ретранслятора MSAU с помощью инструментального средства, предоставленного поставщиком модуля MSAU.
	Шаг 7	Снова подключите маршрутизатор и определите, может ли он соединиться с кольцом. Если сброс ретранслятора не позволил устранить неисправность, попытайтесь заменить модуль MSAU заведомо исправным.
	Шаг 8	Если маршрутизатор все еще не может соединиться с кольцом, проверьте внутренние кабельные соединения плат маршрутизатора Token Ring. Убедитесь в том, что провода кабелей, относящихся к портам с соответствующими номерами, правильно подключены к разъемам и что кабели не переставлены местами.

Продолжение табл. 5

Нарушение	Рекомендации по устранению неисправности	
	Шаг 9	Если маршрутизатор все еще не может соединиться с кольцом, замените кабели подключения маршрутизатора к модулю MSAU заведомо исправными кабелями.
	Шаг 10	Воспользуйтесь командой clear interface, чтобы выполнить сброс интерфейса и снова вставить маршрутизатор в кольцо. Выполните команду show interfaces token, чтобы проверить, исправно ли функционируют интерфейс и протокол канала передачи данных.
	Шаг 11	Еще один вариант состоит в том, что маршрутизатор может быть подключен к резервному модулю MSAU, к которому не присоединены какие-либо станции. Если маршрутизатор сможет подключиться к кольцу, замените основной модуль MSAU
Повторяющийся MAC-адрес	Эта проблема может возникнуть, если в маршрутизаторах используются адреса, назначаемые на месте сетевым администратором.	
	Шаг 1	Воспользуйтесь сетевым анализатором, чтобы проверить наличие контрольного фрейма Duplicate Address, поступающего от загружаемой станции. Если станция получает ответ, то в кольце есть другая станция, в конфигурации которой определен MAC-адрес загружаемой станции.
	Шаг 2	Если в кольце есть две станции с одинаковыми MAC-адресами, измените MAC-адрес одной из станций и повторно инициализируйте сетевой узел
Перегруженное кольцо	**Шаг 1**	Вставьте маршрутизатор в кольцо в тот период, когда в сети нет пиковой нагрузки.
	Шаг 2	Если в период вне пиковых нагрузок вставка маршрутизатора осуществляется успешно, а во время пиковой нагрузки завершается неудачей, сегментируйте объединенную сеть для достижения более равномерного распределения трафика

Окончание табл. 5

Нарушение	Рекомендации по устранению неисправности	
Конфликт между реализациями RPS	**Шаг 1**	Воспользуйтесь командой конфигурации интерфейса no lnm rps, чтобы отменить функцию RPS (Ring Parameter Server – сервер параметров кольца) в маршрутизаторе, который вы пытаетесь вставить в кольцо.
	Шаг 2	Попытайтесь вставить маршрутизатор в кольцо.
	Шаг 3	Если попытка вставить в кольцо маршрутизатор с заблокированной функцией RPS завершается успешно, то причиной неисправности является конфликт между реализациями RPS. Обратитесь к представителю службы технической поддержки для получения дополнительной информации

Команда show interfaces tokenring. При поиске неисправностей передающей среды Token Ring в среде маршрутизатора Cisco можно воспользоваться командой show interfaces tokenring, которая предоставляет большой объем важной информации, позволяющей легко находить причины неисправностей.

Воспользуйтесь привилегированной exec-командой show interfaces tokenring для просмотра информации об интерфейсе Token Ring и состоянии мостового перенаправления от отправителя:

- show interfaces tokenring unit [accounting];
- show interfaces tokenring slot \ port [accounting] (для маршрутизаторов ряда Cisco 7200 и Cisco 7500);
- show interfaces tokenring [slot | port-adapter \ port] (для портов плат универсального интерфейсного процессора маршрутизаторов ряда Cisco 7500).
- *Описание синтаксической структуры.*
- unit. В качестве этого параметра должен быть указан номер порта на выбранном интерфейсе.
- accounting. (Необязательный параметр.) При использовании этого параметра отображается число проходящих через интерфейс пакетов, относящихся к протоколу каждого типа.
- slot. Для получения информации о гнездах и портах устройства обратитесь к соответствующему руководству по аппаратным средствам.
- port. Для получения информации о гнездах и портах устройства обратитесь к соответствующему руководству по аппаратным средствам.

- port-adapter. Для получения информации о совместимости адаптера порта обратитесь к соответствующему руководству по аппаратным средствам.

Рекомендации по использованию.

Эта команда впервые появилась в выпуске Cisco IOS 10.0.

В выпуске Cisco IOS 11.3 определение команды изменилось с учетом необходимости поддержки новых дуплексных адаптеров порта Token Ring.

Если при вызове команды на выполнение не будут приведены значения параметров slot и port, отображаются статистические данные по всем сетевым интерфейсам. Необязательное ключевое слово accounting означает, что должно быть показано число пакетов, передаваемых через интерфейс по протоколу каждого типа.

5. РЕВИЗИИ РАЗЛИЧНЫХ ТИПОВ И СОЗДАНИЕ КАРТ СЕТИ

Может показаться, что после того, как сеть установлена и работает, можно расслабиться. Но опытный администратор знает, что это совершенно неправильный подход. Прежде всего необходимо задокументировать сеть. Далее, точное знание о предположительных характеристиках работы сети значительно облегчит работу в случае возникновения проблем. Поэтому необходимо воспользоваться нормальной работой сети и выполнить комплексную проверку. Фактически необходимо сделать пять различных ревизий сети: инвентаризационную, установленного оборудования, эксплуатации, эффективности и средств защиты сети.

Все эти пять типов ревизий описываются в данной главе. Инвентаризационную ревизию и ревизию установленного оборудования можно начать сразу. Информация для эксплуатационной ревизии и ревизий эффективности и средств защиты сети может и должна быть получена после начала функционирования сети, поскольку эти ревизии требуют данных, которые могут быть обеспечены только посредством мониторинга и анализа поведения и производительности сети.

Инвентаризационная ревизия. *Инвентаризационная ревизия* позволяет инвентаризовать все сетевое оборудование и программное обеспечение. В идеале эта информация должна быть получена в момент закупки аппаратуры и программного обеспечения еще до их установки. Это сбережет время и усилия и снизит количество неудобств, которые будут испытывать пользователи сети.

Инвентаризационная ревизия сетевого оборудования должна включать сбор данных о серийных номерах устройств, их типе и фамилиях лиц, которые используют каждую конкретную единицу оборудования. Она также предусматривает составление перечня установок на различных рабочих станциях и сетевых устройствах. Некоторые администраторы считают полезным держать инвентаризационную информацию непосредственно прикрепленной к каждому сетевому устройству. Другие предпочитают хранить ее в письменном виде или в компьютеризированной базе данных, где она легко доступна для персонала технической поддержки.

Инвентаризационная ревизия прикладного программного обеспечения должна включать сбор данных о типах используемого программного обеспечения, количестве пользователей каждого приложения и эксплутационных требованиях к каждому из приложений. Во время выполнения

инвентаризационной ревизии также необходимо удостовериться, что количество пользователей каждого приложения не превосходит количества лицензий, которым располагает данная рабочая площадка.

Ревизия установленного оборудования. *Ревизия установленного оборудования* позволяет зафиксировать, где все находится. Она должна включать учет проложенных кабелей, рабочие станции, принтеры и устройства межсетевого взаимодействия (такие как концентраторы, мосты и маршрутизаторы). Короче говоря, она должна в конечном итоге дать подробную информацию о местонахождении всех составляющих элементов сети. В идеале вся эта информация должна быть внесена в рабочую версию документа с названием *карта нарезки* еще во время монтажа сети. После завершения этой ревизии самое время перенести нанесенные на карты нарезки данные на комплект чертежей здания.

Карта сети. После завершения инвентаризационной ревизии и ревизии установленного оборудования необходимо воспользоваться собранной информацией и составить *карту сети,* которая по внешнему виду похожа на чертеж. Карта должна включать данные о физическом местонахождении и схеме размещения всех устройств, включенных в сеть, и выполняемых на них приложениях. Она также должна включать IP- и MAC-адреса каждого устройства. Наконец, карта сети должна содержать сведения о длине каждого отрезка кабеля между узлами сети. Законченная карта сети должна храниться рядом с рабочим местом, выбранным для администрирования и мониторинга сети.

Когда программы мониторинга и устройства сообщают о проблеме с какими-либо физическими компонентами сети, часто они указывают место проблемы, например обрыва или короткого замыкания, путем предоставления информации о расстоянии между точкой возникновения проблемы и местом расположения контролирующего устройства. В других случаях программа мониторинга сообщает адрес устройства (или устройств), где возникла проблема. Совершенно очевидно, что локализация и решение проблемы существенно облегчаются, если информация готова и находится под рукой.

Ревизия эксплуатации. Ревизия эксплуатации позволяет наблюдать за повседневной работой сети. Она требует применения специализированного программного обеспечения и аппаратуры. Кроме устройства, осуществляющего мониторинг сети, в ходе ревизии эксплуатации могут потребоваться и такие устройства, как анализатор сети, измеритель отраженного сигнала, разветвительные коробки, измерители мощности и генератор. Устройства, подобные мониторам сети, и анализаторы используют для выполнения своих функций специализированное программное обеспечение.

Все это оборудование и программное обеспечение позволяют администратору сети отслеживать сетевой трафик путем пересчета количества посланных пакетов, повторно переданных пакетов, а также определять размер пакетов и уровень загруженности сети. Проще говоря, эти устройства и программное обеспечение, которым они пользуются, позволяют обнаруживать такие события, как возникновение короткого замыкания и разрывов в кабеле, шум в сетевой среде передачи данных и узкие места в сети.

Из всех упомянутых здесь аппаратных средств управления для получения информации, требующейся при выполнении ревизии эксплуатации, ревизии эффективности и ревизии средств защиты, наиболее часто используются сетевые мониторы и анализаторы. Ниже в данной главе эти два типа устройств будут рассмотрены более подробно. Сейчас же достаточно сказать, что обычно они размещаются на центральной площадке, где легко доступны для персонала службы технической поддержки.

Мониторинг сети. Каждодневный контроль работы сети позволяет установить, что для нее является нормальным состоянием. Например, отслеживая информацию за период времени, можно узнать, насколько в среднем загружена сеть. Также администратор может выяснить, в какое время суток, день недели и месяца трафик достигает своего пика. Можно определить наиболее и наименее популярные приложения в сети и как они используются. В некоторых случаях можно даже идентифицировать тех пользователей, которые чаще всего сталкиваются с проблемами при работе в сети. Вся эта информация должна храниться в соответствующих журналах. Позднее, когда администратор заметит что-либо, что, возможно, является проблемой, он сможет сравнить ее с этой информацией базового уровня, которая показывает, какой должна быть нормальная работа сети.

Ревизия эффективности. *Ревизия эффективности* позволяет определить, работает ли сеть в соответствии со своими потенциальными возможностями. Как и ревизию эксплуатации, эту ревизию лучше всего выполнять после того, как сеть начала предоставлять услуги своим клиентам.

Что до кабельной системы сети, то набор опорных измерений, удовлетворяющих стандартам Института инженеров по электротехнике и электронике (IEEE) и/или Ассоциации электронной промышленности/Ассоциации телекоммуникационной промышленности США (EIA/TIA), должна предоставить та организация, которая выполняла установку сети. Чтобы иметь уверенность в том, что кабельная система продолжает работать эффективно, необходимо периодически проводить

соответствующие измерения и сравнивать их результаты с этими базовыми данными.

К другим показателям, которые должны быть включены в ревизию эффективности, относятся стоимостной анализ сети, анализ легкости, с которой сеть способна давать информацию, анализ способности сети обеспечивать целостность данных, а также оценка количества персонала для поддержки сети. Наконец, ревизия эффективности должна включать и оценку того, как клиенты сети умеют пользоваться программными и аппаратными ресурсами сети.

Ревизия средств защиты. Ревизия средств защиты сети предусматривает просмотр требований по защите данных в сети и определение аппаратных и программных защитных систем, которые в наибольшей степени удовлетворяют им. Предоставить информацию, необходимую для выполнения этой ревизии, может только наблюдение и практика того, как сеть и ее клиенты используют данные и обращаются за ними.

Информация, которая должна собираться при выполнении ревизии этого типа, включает список сегментов, требующих ограниченного доступа или шифрования данных, перечень устройств, файлов и каталогов, требующих блокирования или защиты паролями, данные о файлах, архивные резервные копии которых должны создаваться, анализ необходимой частоты выполнения процедур резервного копирования, тип используемой защиты от вирусов и, что наиболее важно, сведения о тех процедурах, которые будут использоваться в сети в случае возникновения аварийных ситуаций и катастрофических отказов.

Если у вас нет точного представления о той информации, которая должна быть собрана в ходе той или иной ревизии, то следует проконсультироваться с другими сетевыми администраторами и узнать у них, как они проводят ревизии своих сетей и какие типы инструментальных средств управления сетью они находят наиболее пригодными для выполнения подобных задач. Можно также связаться с поставщиками сетевой операционной системы, которые смогут порекомендовать подходящее программное обеспечение для аудита сети, которое само проведет по процессу организации адекватной защиты сети и поможет выполнить полный мониторинг и анализ сети.

ТЕРМИНОЛОГИЧЕСКИЙ СЛОВАРЬ

AppleTalk – стек протоколов, разработанных Apple Computer для компьютерной сети. Он был изначально включён в Macintosh (1984), сейчас компания отказалась от него в пользу TCP/IP.

ARP (англ. Address Resolution Protocol – протокол разрешения адресов) – сетевой протокол, предназначенный для преобразования IP-адресов (адресов сетевого уровня) в MAC-адреса (адреса канального уровня) в сетях TCP/IP.

ATM (англ. Asynchronous Transfer Mode – асинхронный способ передачи данных) – сетевая технология, основанная на передаче данных в виде ячеек (cell) фиксированного размера (53 байта), из которых 5 байтов используется под заголовок.

CDP (англ. Cisco Discovery Protocol) – проприетарный протокол второго уровня, разработанный компанией Cisco Systems, позволяющий обнаруживать подключенное (напрямую или через устройства первого уровня) сетевое оборудование Cisco, его название, версию IOS и IP-адреса. Поддерживается многими устройствами компании, почти не поддерживается сторонними производителями.

Cisco IOS (англ. Internetwork Operating System – Межсетевая Операционная Система) – программное обеспечение, используемое в маршрутизаторах Cisco, и некоторых сетевых коммутаторах. Cisco IOS это многозадачная операционная система выполняющая функции сетевой организации, маршрутизации, коммутации и передачи данных.

CRC (англ. cyclic redundancy check – проверка избыточности циклической суммы) – способ цифровой идентификации некоторой последовательности данных, который заключается в вычислении контрольного значения её циклического избыточного кода.

DES (англ. Data Encryption Standard) – симметричный алгоритм шифрования, в котором один ключ используется как для зашифрования, так и для расшифрования сообщений.

EGP (англ. Exterior Gateway Protocol – протокол внешнего шлюза) – устаревший протокол обмена информации между маршрутизаторами нескольких автономных систем.

Ethernet – пакетная технология компьютерных сетей, преимущественно локальных.

Frame Relay (англ. «ретрансляция кадров», FR) – протокол канального уровня сетевой модели OSI. Служба коммутации пакетов Frame Relay в настоящее время широко распространена во всём мире.

FTP (англ. File Transfer Protocol – протокол передачи файлов) – протокол, предназначенный для передачи файлов в компьютерных сетях. FTP позволяет подключаться к серверам FTP, просматривать содержимое каталогов и загружать файлы с сервера или на сервер; кроме того, возможен режим передачи файлов между серверами.

ICMP (англ. Internet Control Message Protocol – межсетевой протокол управляющих сообщений) – сетевой протокол, входящий в стек протоколов TCP/IP. В основном ICMP используется для передачи сообщений об ошибках и других исключительных ситуациях, возникших при передаче данных.

IP (англ. Internet Protocol – межсетевой протокол) – маршрутизируемый сетевой протокол, основа стека протоколов TCP/IP.

IP-спуфинг (от англ. spoof – мистификация) – вид хакерской атаки, заключающийся в использовании чужого IP-адреса с целью обмана системы безопасности.

IPX (англ. Internetwork Packet Exchange) – протокол сетевого уровня модели OSI в стеке протоколов SPX. Он предназначен для передачи датаграмм, являясь неориентированным на соединение (так же, как IP и NetBIOS), и обеспечивает связь между NetWare-серверами и конечными станциями.

NTP (англ. Network Time Protocol) – сетевой протокол для синхронизации внутренних часов компьютера с использованием сетей с переменной латентностью.

Ping – служебная компьютерная программа, предназначенная для проверки соединений в сетях на основе TCP/IP.

RADIUS (англ. Remote Authentication in Dial-In User Service) – протокол AAA (Authentication, Authorization и Accounting), разработанный для передачи сведений между центральной платформой AAA и оборудованием Dial-Up доступа (NAS, Network Access Server) и системой биллинга (то есть, системой тарификации использованных ресурсов конкретным абонентом/пользователем).

RMON (англ. Remote MONitoring) – протокол мониторинга компьютерных сетей, расширение SNMP, в основе которого, как и в основе SNMP, лежит сбор и анализ информации о характере информации, передаваемой по сети.

RSA – криптографический алгоритм с открытым ключом. RSA стал первым алгоритмом такого типа, пригодным и для шифрования и для цифровой подписи. Алгоритм используется в большом числе криптографических приложений.

SNA (англ. Systems Network Architecture – системная сетевая архитектура) – разработанная компанией IBM в 1974 г. общее описание структуры, форматов, протоколов, используемых для передачи информации между программами IBM и оборудованием, создавалось для объединения в глобальные сети мейнфреймов IBM.

SNMP (англ. Simple Network Management Protocol – простой протокол управления сетью) – протокол управления сетями связи на основе архитектуры TCP/IP.

SNTP (англ. Simple Network Time Protocol) – протокол синхронизации времени по компьютерной сети. Является упрощённой реализацией протокола NTP. Используется во встраиваемых системах и устройствах, не требующих высокой точности, а также в пользовательских программах точного времени.

SSH (англ. Secure Shell «безопасная оболочка») – сетевой протокол прикладного уровня, позволяющий производить удалённое управление операционной системой и туннелирование TCP-соединений (например, для передачи файлов).

TACACS (англ. Terminal Access Controller Access Control System) – сеансовый протокол, использовавшийся на серверах доступа ARPANET. Центральный сервер, который принимает решение, разрешить или не разрешить определённому пользователю подключиться к сети.

TCP/IP (англ. Transmission Control Protocol/Internet Protocol) – собирательное название для сетевых протоколов разных уровней, используемых в сетях.

TELNET (англ. TELecommunication NETwork) – сетевой протокол для реализации текстового интерфейса по сети (в современной форме – при помощи транспорта TCP).

TFTP (англ. Trivial File Transfer Protocol – простой протокол передачи файлов) – используется главным образом для первоначальной загрузки бездисковых рабочих станций.

Token Ring (англ. «маркерное кольцо») – архитектура кольцевой сети с маркерным (эстафетным) доступом.

TTL (англ. Time-To-Live) – время жизни дейтаграммы в секундах, то есть предельно допустимое время её пребывания в системе.

UDP (англ. User Datagram Protocol – протокол пользовательских датаграмм) – это транспортный протокол для передачи данных в сетях IP. Он является одним из самых простых протоколов транспортного уровня модели OSI.

X.25 – семейство протоколов канального уровня сетевой модели OSI. Предназначалось для организации WAN на основе телефонных сетей с линиями с достаточно высокой частотой ошибок, поэтому содержит развитые механизмы коррекции ошибок. Ориентирован на работу с установлением соединений.

Авторизация – процесс, определяющий полномочия идентифицированного субъекта на доступ к определенным объектам или сервисам.

Аутентификация – процесс идентификации и проверки личности пользователя.

Буфер – область памяти, используемая для временного хранения данных ввода-вывода.

Виртуальный терминал – одно логическое соединение терминала с устройством, работающим под управлением ОС IOS.

Дейтаграмма (датаграмма) – блок информации, посланный как пакет сетевого уровня, через передающую среду, без предварительного установления виртуального канала.

Зуммер – сигнальное устройство, электро-механическое или электронное.

Инкапсуляция – метод согласования сетей, применимый только для согласования транспортных протоколов. Инкапсуляция (тоннель) может быть использована, когда две сети с одной транспортной технологией необходимо соединить через сеть, использующую другую транспортную технологию.

Коммутатор – устройство, предназначенное для соединения нескольких узлов компьютерной сети в пределах одного сегмента. Коммутатор передает данные только непосредственно получателю. Это повышает производительность и безопасность сети, избавляя остальные сегменты сети от необходимости (и возможности) обрабатывать данные, которые им не предназначались.

Маршрутизатор – сетевое устройство, на основании информации о топологии сети и определённых правил принимающее решения о пересылке пакетов сетевого уровня между различными сегментами сети.

Мост – сетевое оборудование для объединения сегментов локальной сети.

Пакет – форматированный блок информации, передаваемый по вычислительной сети.

Прерывание – сигнал, сообщающий процессору о совершении какого-либо асинхронного события. При этом выполнение текущей последовательности команд приостанавливается, и управление передаётся обработчику прерывания, который выполняет работу по обработке события и возвращает управление в прерванный код.

Протокол – стандарт, определяющий поведение функциональных блоков при передаче данных.

Сервер – узел сети, принимающий и обрабатывающий запросы пользователей.

Скрипт – программа, которая автоматизирует некоторую задачу, которую без сценария пользователь делал бы вручную, используя интерфейс программы.

Слот – щелевой разъём для установки печатной платы.

Терминал – рабочее место на многопользовательских ЭВМ, монитор с клавиатурой.

Транзакция (англ. transaction) – в информатике, группа последовательных операций, которая представляет собой логическую единицу работы с данными. Транзакция может быть выполнена целиком либо успешно, соблюдая целостность данных и независимо от параллельно идущих других транзакций, либо не выполнена вообще и тогда она не должна произвести никакого эффекта.

Трафик – объём информации или поток информации, передаваемой по сети.

Шлюз – сетевое устройство, которое передаёт протоколы одного типа физической среды в протоколы другой физической среды (сети).

СПИСОК ЛИТЕРАТУРЫ

1. Амато Вито. Основы организации сетей Cisco, том 1, испр. изд. / пер. с англ. – М.: Издательский дом «Вильямс», 2004. – 512 с.: ил.
2. Амато, Вито. Основы организации сетей Cisco, том 2., испр. изд. / пер. с англ. – М.: Издательский дом «Вильямс», 2004. – 464 с.: ил.
3. Cisco Sistems и др. Руководство по поиску неисправностей в объединенных сетях / пер. с анл. – М. Издательский дом «Вильямс», 2003. – 1040 с.: ил.
4. Леинванд А., Пински Б. Конфигурирование маршрутизаторов Cisco, 2-е изд. / пер. с англ. – М.: Издательский дом «Вильямс», 2001. – 368 с.: ил.
5. Бигелоу С. Сети: поиск неисправностей, поддержка и восстановление / пер. с англ. – Спб.: БХВ-Петербург, 2005. – 1200 с.: ил.
6. Хьюкаби Д., Мак-Квери Сю Руководство Cisco по конфигурированию коммутаторов Catalyst / пер. с англ. – М.: Издательский дом «Вильямс», 2004. – 560 с.: ил.
7. http://www.snip-info.ru/Rd_50-34_698-90.htm
8. http://www.abn.ru/inf/siemon/standard13.shtml
9. http://exams.com.ua/administration/cisco/
10. http://www.cisco.com
11. http://www.opennet.ru/mp/cisco/
12. http://citforum.ru/nets/
13. http://osp.ru/lan/index.html

Учебное издание

ТОМАШЕВСКИЙ Алексей Сергеевич

АДМИНИСТРИРОВАНИЕ В ТЕЛЕКОММУНИКАЦИОННЫХ СИСТЕМАХ

Учебное пособие

Ассистент каф. ОСУ А.С. Томашевский