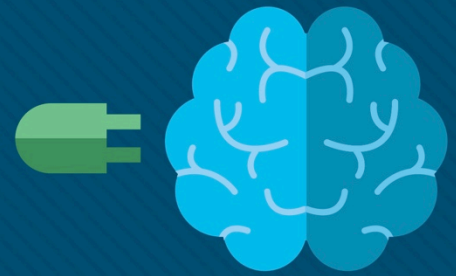


Глава 10. Устройства — обнаружение, управление и обслуживание

Материалы для инструктора

CCNA Routing and Switching

Routing and Switching Essentials v6.0

Материалы для инструкторов. Глава 10. Руководство по планированию

- Эта презентация PowerPoint состоит из двух частей:
- Руководство по планированию для инструкторов
  - Ознакомительная информация по главе
  - Методические пособия
- Презентация перед классом для инструктора
  - Дополнительные слайды, которые можно использовать в классе
  - Начало на слайде № 12

- **Примечание.** Перед предоставлением общего доступа удалите руководство по планированию из данной презентации.

Глава 10. Устройства — обнаружение, управление и обслуживание

Routing and Switching Essentials 6.0.
Руководство по планированию

Глава 10. Упражнения

Какие упражнения относятся к данной главе?

Страница №	Тип упражнения	Название упражнения	Необязательно?
10.1.1.4	Packet Tracer	Создание карты сети с помощью протокола CDP	Рекомендуется
10.1.2.2	Инструмент проверки синтаксиса	Настройка и проверка протокола LLDP	Рекомендуется
10.1.2.4	Интерактивное упражнение	Сравнение протоколов CDP и LLDP	Рекомендуется
10.1.2.5	Лабораторная работа	Настройка протоколов CDP и LLDP	Рекомендуется
10.2.1.3	Инструмент проверки синтаксиса	Настройка и проверка NTP	Рекомендуется
10.2.1.4	Cisco Packet Tracer	Настройка и проверка NTP	Рекомендуется
10.2.2.5	Интерактивное упражнение	Интерпретация выходных данных системного журнала Syslog	Рекомендовано
10.2.3.4	Инструмент проверки синтаксиса	Настройка и проверка Syslog	Рекомендуется
10.2.3.5	Cisco Packet Tracer	Настройка протоколов Syslog и NTP	Рекомендуется
10.2.3.6	Лабораторная работа	Настройка протоколов Syslog и NTP	Рекомендуется

В этой главе для выполнения упражнений в программе Packet Tracer используйте следующий пароль: **PT_ccna5**.

Глава 10. Упражнения (продолжение)

Какие упражнения относятся к данной главе?

Страница №	Тип упражнения	Название упражнения	Необязательно?
10.3.1.7	Syntax Checker (Средство проверки синтаксиса)	Восстановление пароля на маршрутизаторе	Рекомендуется
10.3.1.8	Cisco Packet Tracer	Резервное копирование файлов конфигурации	Рекомендуется
10.3.1.9	Лабораторная работа	Управление файлами конфигурации маршрутизатора с помощью программы Tera Term	Рекомендуется
10.3.1.10	Лабораторная работа	Управление файлами конфигурации устройства с помощью TFTP-сервера, флеш-памяти и USB-накопителя	Рекомендуется
10.3.1.11	Лабораторная работа	Изучение процедур восстановления пароля	Рекомендуется
10.3.3.2	Syntax Checker (Средство проверки синтаксиса)	Создание резервной копии образа IOS на TFTP-сервере	Рекомендуется
10.3.3.5	Cisco Packet Tracer	Использование TFTP-сервера для обновления образа Cisco IOS	Рекомендуется
10.3.3.6	Демонстрационный видеоролик	Управление образами Cisco IOS	Рекомендуется
10.3.4.4	Инструмент проверки синтаксиса	Отображение уникального идентификатора устройства лицензии на R2	Рекомендуется

В этой главе для выполнения упражнений в программе Packet Tracer используйте следующий пароль: **PT_ccna5**.

Глава 10. Упражнения (продолжение)

Какие упражнения относятся к данной главе?

Страница №	Тип упражнения	Название упражнения	Необязательно?
10.3.4.5	Инструмент проверки синтаксиса	Установка лицензии на функции обеспечения безопасности на R2	Рекомендуется
10.3.5.2	Инструмент проверки синтаксиса	Активация оценочной лицензии на право использования	Рекомендуется
10.3.5.3	Инструмент проверки синтаксиса	Резервная копия лицензии	Рекомендуется
10.3.5.4	Инструмент проверки синтаксиса	Удаление лицензии	Рекомендуется
10.3.5.5	Демонстрационный видеоролик	Работа с лицензиями для образов IOS 15	Рекомендуется
10.4.1.1	Packet Tracer	Отработка комплексных практических навыков	Рекомендовано

В этой главе для выполнения упражнений в программе Packet Tracer используйте следующий пароль: **PT_ccna5**.

Глава 10. Проверочная работа

- После прохождения главы 10 учащиеся должны пройти проверку на знание материала главы 10.
- Для неформальной оценки успехов учащихся можно использовать контрольные работы, лабораторные работы, работу с симулятором Packet Tracer и другие упражнения.

Глава 10. Практические рекомендации

Прежде, чем излагать материал главы 10, обратите внимание на следующее:

- Инструктор должен пройти проверку на знание материала главы 10 «Проверочная работа».
- Цели этой главы:
  - Использовать протокол CDP для составления топологии сети.
  - Использовать протокол LLDP для составления топологии сети.
  - Внедрить NTP между клиентом NTP и сервером NTP.
  - Объяснить принцип работы системного журнала.
  - Настроить серверы и клиенты syslog.
  - Использовать команды резервного копирования и восстановления файла конфигурации IOS.
  - Объяснить стандарты именования образов IOS, используемых компанией Cisco.
  - Обновить образ системы IOS.
  - Описать процесс лицензирования ПО Cisco IOS в сетях предприятий малого или среднего бизнеса.
  - Настроить маршрутизатор для установки лицензии на образ ПО IOS.

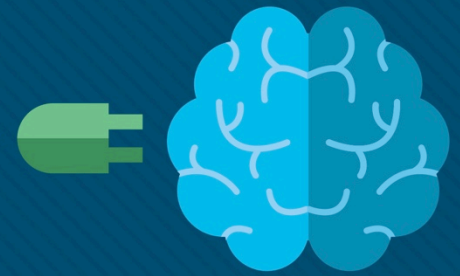
Глава 10. Практические рекомендации (продолжение)

- Докажите, что сервер TFTP можно использовать для хранения и резервного копирования образа IOS и конфигурации маршрутизатора.
- Продемонстрируйте резервное копирование IOS на сервер TFTP.
- Покажите, как получить доступ к правильному образу и загрузить его с веб-сайта http://www.cisco.com, убедившись, что он соответствует требованиям маршрутизатора и сети в отношении платформы, набора функций и программного обеспечения. Также убедитесь, что маршрутизатор имеет достаточный объем памяти для новой или обновленной IOS.

Глава 10. Дополнительная помощь

- Дополнительные справочные материалы, содержащие различные стратегии обучения, в том числе планы занятий, описание аналогий для сложных понятий и темы обсуждений, доступны на веб-сайте сообщества сертифицированных сетевых специалистов (CCNA) по адресу https://www.netacad.com/group/communities/community-home.
- Практические рекомендации специалистов со всего мира для обучения по программе CCNA Routing and Switching. https://www.netacad.com/group/communities/ccna
- Если вы хотите поделиться с другими преподавателями планами занятий и другой полезной информацией, вы можете разместить её на сайте сообщества CCNA.
- Студенты могут записаться на курс **Introduction to Packet Tracer** (для самостоятельного изучения).


CISCO



Глава 10. Устройства — обнаружение, управление и обслуживание

CCNA Routing and Switching

Routing and Switching Essentials v6.0

Глава 10. Разделы и задачи

- 10.1. Обнаружение устройств
  - Для составления топологии сети используйте протоколы обнаружения.
    - Использовать протокол CDP для составления топологии сети.
    - Использовать протокол LLDP для составления топологии сети.
- 10.2. Управление устройствами
  - Настройте NTP и Syslog в сетях предприятий малого и среднего бизнеса.
    - Внедрить NTP между клиентом NTP и сервером NTP.
    - Объяснить принцип работы системного журнала.
    - Настроить серверы и клиенты syslog.

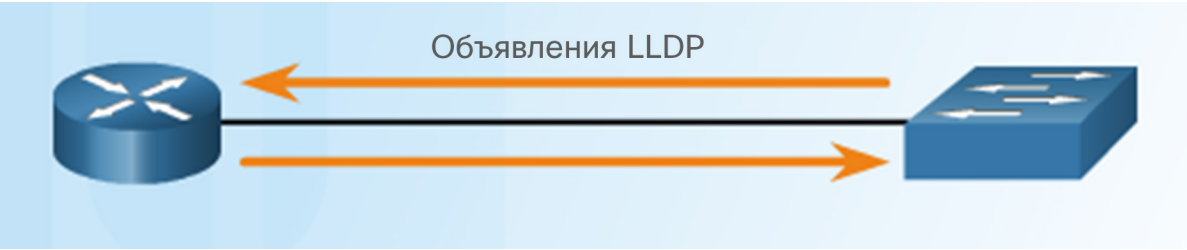
Глава 10. Разделы и цели (продолжение)

- 10.3. Обслуживание устройств
  - Поддерживать конфигурации маршрутизатора и коммутатора, а также файлы IOS.
    - Использовать команды резервного копирования и восстановления файла конфигурации IOS.
    - объяснять стандарты именования образов IOS, используемых компанией Cisco;
    - Обновить образ системы IOS.
    - описывать процесс лицензирования Cisco IOS в сетях предприятий малого или среднего бизнеса;
    - Настроить маршрутизатор для установки лицензии на образ ПО IOS.

10.1. Обнаружение устройств

Общие сведения о протоколе CDP

- CDP (Cisco Discovery Protocol)
  - Принадлежащий компании Cisco протокол уровня 2, используемый для сбора информации об устройствах Cisco, подключенных к одному каналу
  - Периодические объявления CDP, отправляемые на подключенные устройства
  - Предоставление информации о типе обнаруженного устройства, имени устройства и типу его интерфейсов
  - Определение сведений о соседних устройствах для создания логической топологии, если отсутствует документация



Настройка и проверка протокола CDP

```
Router# show cdp
Global CDP information:
        Sending CDP packets every 60 seconds
        Sending a holdtime value of 180 seconds
        Sending CDPv2 advertisements is enabled
```

Проверка состояния и вывод информации

```
Switch(config)# interface gigabitethernet 0/1
Switch(config-if)# cdp enable
```

Включает протокол CDP на интерфейсе (отключает команда **no CDP enable**)

```
Router(config)# no cdp run
Router(config)# exit
Router# show cdp
% CDP is not enabled
Router# conf t
Router(config)# cdp run
```

Глобально отключает команда **no cdp run** (включает команда **cdp run**)

```
Router# show cdp neighbors
Capability Codes: R - Router, T - Trans Bridge, B - Source Route Bridge
                  S - Switch, H - Host, I - IGMP, r - Repeater, P - Phone,
                  D - Remote, C - CVTA, M - Two-port Mac Relay

Device ID        Local Intrfce     Holdtme    Capability  Platform  Port ID

Total cdp entries displayed : 0
```

Соседние устройства не обнаружены

```
Router# show cdp interface
Embedded-Service-Engine0/0 is administratively down, line protocol is down
  Encapsulation ARPA
  Sending CDP packets every 60 seconds
  Holdtime is 180 seconds
GigabitEthernet0/0 is administratively down, line protocol is down
  Encapsulation ARPA
  Sending CDP packets every 60 seconds
  Holdtime is 180 seconds
GigabitEthernet0/1 is up, line protocol is up
  Encapsulation ARPA
  Sending CDP packets every 60 seconds
  Holdtime is 180 seconds
Serial0/0/0 is administratively down, line protocol is down
  Encapsulation HDLC
  Sending CDP packets every 60 seconds
  Holdtime is 180 seconds
Serial0/0/1 is administratively down, line protocol is down
  Encapsulation HDLC
  Sending CDP packets every 60 seconds
  Holdtime is 180 seconds
```

Указывает интерфейсы с включенным протоколом CDP

Поиск устройств с помощью протокола CDP


```
R1# show cdp neighbors
Capability Codes: R - Router, T - Trans Bridge, B - Source Route Bridge
                  S - Switch, H - Host, I - IGMP, r - Repeater, P - Phone,
                  D - Remote, C - CVTA, M - Two-port Mac Relay

Device ID        Local Intrfce     Holdtme    Capability  Platform  Port ID
S1               Gig 0/1           122              S I   WS-C2960- Fas 0/5
```

Команда **show cdp neighbors** обнаруживает:

- S1 (идентификатор устройства)
- Gig 0/1 (идентификатор локального порта)
- Fas 0/5 (идентификатор удаленного порта)
- S обозначает коммутатор (R — маршрутизатор)
- WS-C2960 (аппаратная платформа)

```
R1# show cdp neighbors detail
-------------------------
Device ID: S1
Entry address(es):
  IP address: 192.168.1.2
Platform: cisco WS-C2960-24TT-L,  Capabilities: Switch IGMP
Interface: GigabitEthernet0/1,  Port ID (outgoing port): FastEthernet0/5
Holdtime : 136 sec

Version :
Cisco IOS Software, C2960 Software (C2960-LANBASEK9-M), Version 15.0(2)SE7,
RELEASE SOFTWARE (fc1)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2014 by Cisco Systems, Inc.
Compiled Thu 23-Oct-14 14:49 by prod_rel_team

advertisement version: 2
Protocol Hello:  OUI=0x00000C, Protocol ID=0x0112; payload len=27,
value=00000000FFFFFFFF010221FF0000000000000002291210380FF0000
VTP Management Domain: ''
Native VLAN: 1
Duplex: full
Management address(es):
  IP address: 192.168.1.2


Total cdp entries displayed : 1
```

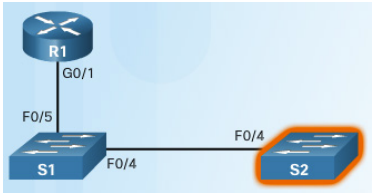
Команда **show cdp neighbors detail** предоставляет дополнительную информацию:

- IPv4-адрес
- версию IOS

Поиск устройств с помощью протокола CDP (продолжение)


```
S1# show cdp neighbors
Capability Codes: R - Router, T - Trans Bridge, B - Source Route Bridge
                  S - Switch, H - Host, I - IGMP, r - Repeater, P - Phone,
                  D - Remote, C - CVTA, M - Two-port Mac Relay

Device ID        Local Intrfce     Holdtme    Capability  Platform  Port ID
S2               Fas 0/4           158              S I   WS-C2960- Fas 0/4
R1               Fas 0/5           136            R B S I CISCO1941 Gig 0/1
```

- Можно определить другие устройства, подключенные к коммутатору S1
- В выходных данных обнаруживается коммутатор S2!




```
S2# show cdp neighbors
Capability Codes: R - Router, T - Trans Bridge, B - Source Route Bridge
                  S - Switch, H - Host, I - IGMP, r - Repeater, P - Phone,
                  D - Remote, C - CVTA, M - Two-port Mac Relay

Device ID        Local Intrfce     Holdtme    Capability  Platform  Port ID
S1               Fas 0/4           173              S I   WS-C2960- Fas 0/4
```

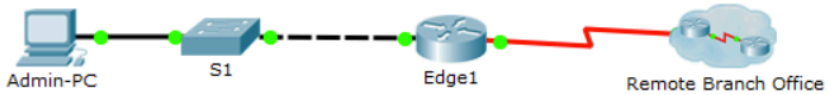
- Все устройства обнаружены!

Packet Tracer. Создание карты сети с помощью протокола CDP

Cisco Networking Academy® Mind Wide Open™

Packet Tracer – Map a Network Using CDP

Topology

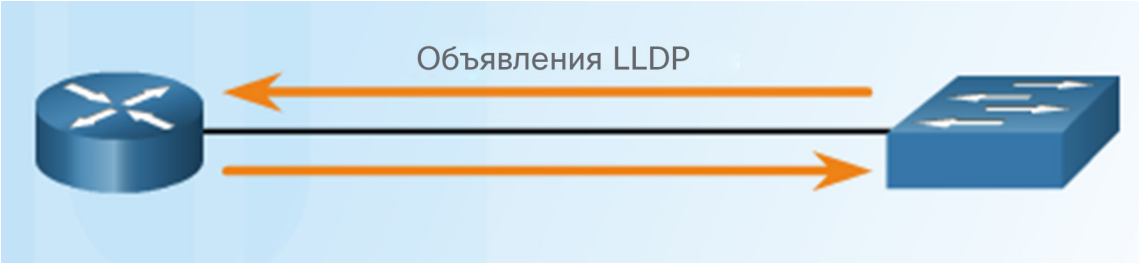


Addressing Table

Device	Interface	IP Address	Subnet Mask	Local Interface and Connected Neighbor
Edge1	G0/0	192.168.1.1	255.255.255.0	G0/1 - S1
	S0/0/0			S0/0/0 - ISP
	S0/0/1	209.165.200.10		S0/0/1 - ISP

Общие сведения о протоколе LLDP

- Протокол LLDP (Link Layer Discovery Protocol)
  - Обнаружение соседних устройств независимо от поставщиков аналогично протоколу CDP
  - Работает с маршрутизаторами, коммутаторами и беспроводными точками доступа к локальной сети
  - Объявляет себя и свои возможности другим устройствам и получает данные от подключенных устройств уровня 2

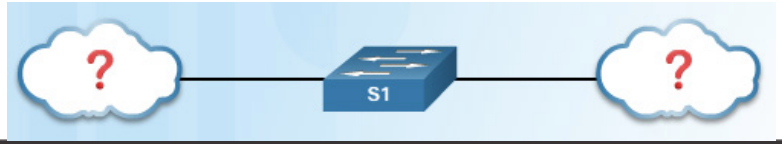


Настройка и проверка протокола LLDP

```
Switch# conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)# lldp run
Switch(config)# interface gigabitethernet 0/1
Switch(config-if)# lldp transmit
Switch(config-if)# lldp receive
Switch# show lldp

Global LLDP Information:
    Status: ACTIVE
    LLDP advertisements are sent every 30 seconds
    LLDP hold time advertised is 120 seconds
    LLDP interface reinitialisation delay is 2 seconds
```

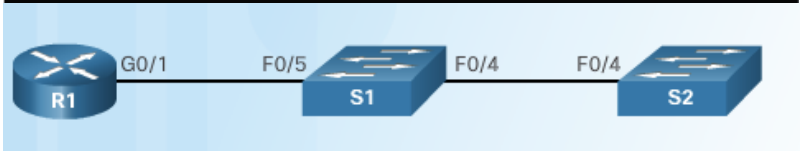
- Команда **lldp run** включает протокол глобально
- Протокол LLDP можно настроить на отдельных интерфейсах, раздельно настроенных для передачи и получения
- Для глобального отключения протокола LLDP используется команда **no lldp run**

Поиск устройств с помощью протокола LDP




```
S1# show lldp neighbors
Capability codes:
    (R) Router, (B) Bridge, (T) Telephone, (C) DOCSIS Cable Device
    (W) WLAN Access Point, (P) Repeater, (S) Station, (O) Other

Device ID           Local Intf      Hold-time     Capability      Port ID
R1                  Fa0/5           99            R               Gi0/1
S2                  Fa0/4           120           B               Fa0/4

Total entries displayed: 2
```

```
S1# show lldp neighbors detail
------------------------------------------------
Chassis id       : fc99.4775.c3e0
Port id          : Gi0/1
Port Description : GigabitEthernet0/1
System Name      : R1

System Description:
Cisco IOS Software, C1900 Software (C1900-UNIVERSALK9-M), Version 15.4(3)M2,
  RELEASE SOFTWARE (fc2)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2015 by Cisco Systems, Inc.
Compiled Fri 06-Feb-15 17:01 by prod_rel_team

Time remaining        : 101 seconds
System Capabilities   : B,R
Enabled Capabilities  : R
Management Addresses:
    IP: 192.168.1.1
Auto Negotiation - not supported
Physical media capabilities - not advertised
Media Attachment Unit type - not advertised
Vlan ID: - not advertised

------------------------------------------------
Chassis id        : 0cd9.96d2.3f80
Port id           : Fa0/4
Port Description  : FastEthernet0/4
System Name       : S2
```

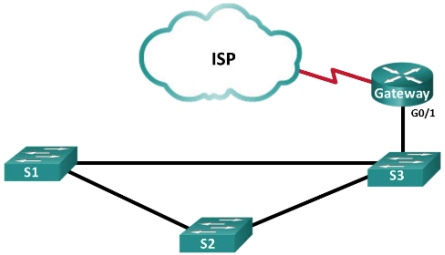


Лабораторная работа. Настройка протоколов CDP и LLDP

Cisco Networking Academy® Mind Wide Open™

Lab - Configure CDP and LLDP

Topology



Addressing Table

Device	Interface	IP Address	Subnet Mask
Gateway	G0/1	192.168.1.254	255.255.255.0
	S0/0/1	209.165.200.226	255.255.255.252
ISP	S0/0/1 (DCE)	209.165.200.225	255.255.255.252

Objectives

Part 1: Build the Network and Configure Basic Device Settings

Part 2: Network Discovery with CDP

Part 3: Network Discovery with LLDP

Background / Scenario

Cisco Discovery Protocol (CDP) is a Cisco proprietary protocol for network discovery on the data link layer. It can share information such as device names and IOS versions, with other physically connected Cisco devices. Link Layer Discovery Protocol (LLDP) is vendor-neutral protocol using on the data link layer for network discovery. It is mainly used with network devices in the local area network (LAN). The network devices advertise information, such as their identities and capabilities to their neighbors.

In this lab, you must document the ports that are connected to other switches using CDP and LLDP. You will document your findings in a network topology diagram. You will also enable or disable these discovery protocols as necessary.

Note: The routers used with CCNA hands-on labs are Cisco 1941 Integrated Services Routers (ISRs) with Cisco IOS Release 15.2(4)M3 (universalk9 image). The switches used are Cisco Catalyst 2960s with Cisco IOS Release 15.0(2) (lanbasek9 image). Other routers, switches, and Cisco IOS versions can be used.

10.2. Управление устройствами

Настройка системных часов

```
R1# clock set 20:36:00 dec 11 2015
R1#
*Dec 11 20:36:00.000: %SYS-6-CLOCKUPDATE: System clock has been updated from 21:32:31
UTC Fri Dec 11 2015 to 20:36:00 UTC Fri Dec 11 2015, configured from console by
console.
```

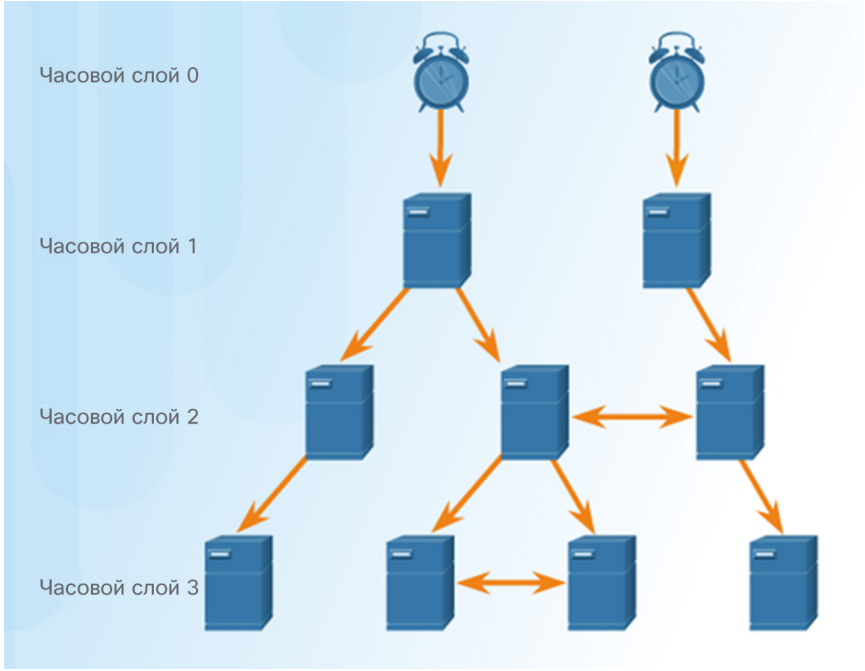
Для управления, обеспечения безопасности, поиска и устранения неполадок, а также планирования сетей требуются точные метки времени

Настроить дату и время на маршрутизаторе или коммутаторе можно одним из двух способов:

- вручную настройте дату и время, как показано на рисунке;
- настройте протокол сетевого времени (NTP).
  - Протокол NTP использует порт UDP 123
  - Клиенты NTP получают время и дату из одного источника

Принципы работы протокола NTP

- Слой 0 — верхний уровень иерархической системы, доверенные источники времени, считающиеся точными.
- Слой 1 — устройства, напрямую подключенные к доверенным источникам; выступают в роли основного стандарта времени в сети
- Слой 2 и более низкие слои — устройства, подключенные к устройствам слоя 1 по сети; выступают в роли серверов для устройств слоя 3
- Чем меньше номер слоя, тем ближе устройство к доверенному источнику времени
- Чем больше номер слоя, тем ниже уровень слоя (не более 15 переходов)
- Слой 16, самый низкий уровень, указывает, что устройство не синхронизировано.



Настройка и проверка протокола NTP

- Настройка NTP-сервера, слой 2

```
R1# show clock detail
20:55:10.207 UTC Fri Dec 11 2015
Time source is user configuration
R1(config)# ntp server 209.165.200.225
R1(config)# end
R1# show clock detail
21:01:34.563 UTC Fri Dec 11 2015
Time source is NTP
```

- Проверка настройки NTP-сервера

```
R1# show ntp associations

  address         ref clock       st   when   poll reach  delay  offset   disp
*~209.165.200.225 .GPS.           1     61     64   377  0.481   7.480  4.261
 * sys.peer, # selected, + candidate, - outlyer, x falseticker, ~ configured

R1# show ntp status
Clock is synchronized, stratum 2, reference is 209.165.200.225
nominal freq is 250.0000 Hz, actual freq is 249.9995 Hz, precision is 2**19
ntp uptime is 589900 (1/100 of seconds), resolution is 4016
reference time is DA088DD3.C4E659D3 (13:21:23.769 PST Tue Dec 1 2015)
clock offset is 7.0883 msec, root delay is 99.77 msec
root dispersion is 13.43 msec, peer dispersion is 2.48 msec
loopfilter state is 'CTRL' (Normal Controlled Loop), drift is 0.000001803 s/s
system poll interval is 64, last update was 169 sec ago.
```

- Маршрутизатор R1 синхронизирован с сервером NTP слоя 1 по адресу 209.165.200.225, который синхронизирован с часами GPS

Настройка и проверка протокола NTP (продолжение)

- Настройка NTP-сервера, слой 3

```
S1(config)# ntp server 192.168.1.1
S1(config)# end
S1# show ntp associations

  address         ref clock       st   when   poll reach  delay  offset   disp
*~192.168.1.1     209.165.200.225  2     12     64   377  1.066  13.616  3.840
 * sys.peer, # selected, + candidate, - outlyer, x falseticker, ~ configured

S1# show ntp status
Clock is synchronized, stratum 3, reference is 192.168.1.1
nominal freq is 119.2092 Hz, actual freq is 119.2088 Hz, precision is 2**17
reference time is DA08904B.3269C655 (13:31:55.196 PST Tue Dec 1 2015)
clock offset is 18.7764 msec, root delay is 102.42 msec
root dispersion is 38.03 msec, peer dispersion is 3.74 msec
loopfilter state is 'CTRL' (Normal Controlled Loop), drift is 0.000003925 s/s
system poll interval is 128, last update was 178 sec ago.
```

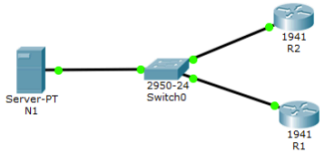
- Маршрутизатор R1 является устройством слоя 2 и сервером NTP для коммутатора S1
- Коммутатор S1 является устройством слоя 3, которое может предоставлять сервис NTP оконечным устройствам

Packet Tracer. Настройка и проверка протокола NTP

Cisco Networking Academy® Mind Wide Open™

Packet Tracer - Configure and Verify NTP

Topology



Addressing Table

Device	Interface	IP Address	Subnet Mask
N1	NIC	209.165.200.225	255.255.255.0
R1	G0/0	209.165.200.226	255.255.255.0
R2	G0/0	209.165.200.227	255.255.255.0

Objectives

In this activity, you will configure NTP on R1 and R2 to allow time synchronization.

Background / Scenario

Network Time Protocol (NTP) synchronizes the time of day among a set of distributed time servers and clients. While there are a number of applications that require synchronized time, this lab will focus on correlating events that are listed in the system log and other time-specific events from multiple network devices. NTP uses the User Datagram Protocol (UDP) as its transport protocol. All NTP communications use Coordinated Universal Time (UTC).

An NTP server usually receives its time from an authoritative time source, such as an atomic clock attached to a time server It then distributes this time across the network. NTP is extremely efficient; no more than one packet per minute is necessary to synchronize two machines to within a millisecond of each other.

Step 1: NTP Server

a. Server N1 is already configured as the NTP Server for this topology. Verify its configuration under **Services > NTP**.

b. From R1, ping N1 (209.165.200.225) to verify connectivity. The ping should be successful.

c. Repeat the ping to N1 from R2 to verify connectivity to N1.

Step 2: Configuring the NTP Clients

Cisco devices can be configured to refer to an NTP server to synchronize their clocks. This is important to keep time consistent among all devices. Configure R1 and R2 as NTP clients so their clocks are

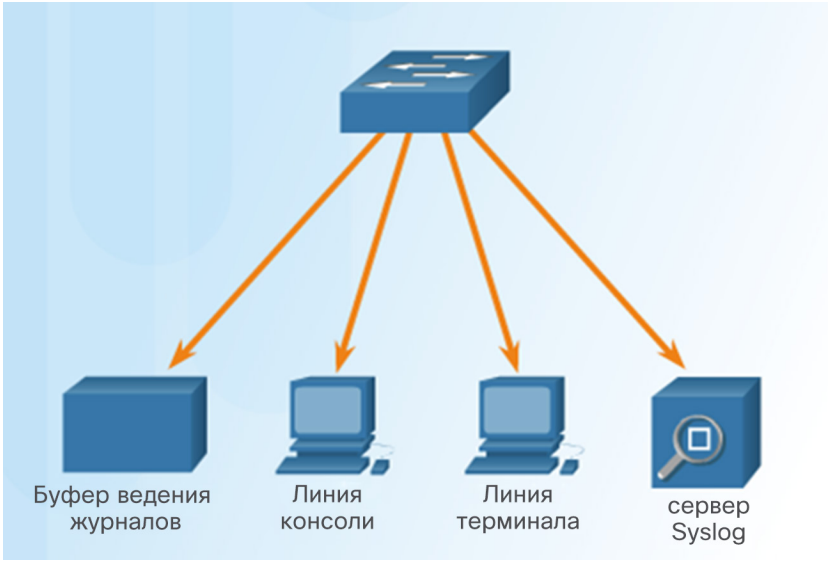
Общие сведения о системном журнале

- Системный журнал (Syslog)
  - Описывает стандарты и протоколы
  - Использует порт UDP 514
  - Отправляет сообщения с уведомлениями о событиях по сетям IP на средства сбора сообщений о событиях
  - Маршрутизаторы, коммутаторы, серверы, межсетевые экраны поддерживают системный журнал

- Сервис ведения системного журнала выполняет три основные функции:
  - сбор информации журнала для мониторинга, а также поиска и устранения неполадок;
  - выбор типа собираемой информации журнала;
  - указание получателей собранных сообщений системного журнала.

Принципы работы системного журнала

- Протокол системного журнала (syslog) начинает с отправки системных сообщений и выходных данных команд **debug** в локальный процесс ведения журналов соответствующего устройства.
- Каким образом процесс ведения журналов управляет этими сообщениями и выводом, зависит от настроек устройства.
- Сообщения системного журнала могут отправляться по сети на внешний сервер системного журнала. Могут включаться в различные отчеты.
- Сообщения системного журнала могут отправляться во внутренний буфер. Просматривать эти сообщения можно только через интерфейс командной строки устройства.



- Получателями сообщений системного журнала могут быть:
  - буфер ведения журналов (ОЗУ в маршрутизаторе или коммутаторе);
  - порт консоли;
  - линия терминала;
  - Сервер Syslog.

Формат сообщений системного журнала

- Устройства Cisco создают сообщения системного журнала при определенных сетевых событиях.
- Во всех сообщениях syslog указывается уровень важности (severity level) и объект (facility).
  - Чем меньше уровень, тем больше важность

Название уровня серьезности	Уровень серьезности	Описание
Чрезвычайная ситуация	Уровень 0	Систему нельзя использовать
Предупреждение	Уровень 1	Требуется принять немедленные меры
Критический	Уровень 2	Критическое состояние
Ошибка	Уровень 3	Состояние ошибки
Предупреждение	Уровень 4	Состояние предупреждения
Уведомление	Уровень 5	Нормальное, но требующее внимания состояние
Информационный	Уровень 6	Информационное сообщение
Отладка	Уровень 7	Сообщение отладки

Формат сообщений системного журнала (продолжение)

- Каждый уровень syslog имеет собственный смысл:
  - **Уровень предупреждения 4 (warning) — уровень критического состояния 0 (emergency)**: сообщения об ошибке программного или аппаратного обеспечения; затрагивается работоспособность устройства.
  - **Уровень уведомлений 5 (notification)**: уведомления об обычных событиях. На уровне уведомлений отображаются сообщения об изменении состояния интерфейса на активное или неактивное или о перезапуске системы.
  - **Информационный уровень 6 (informational)**: обычные информационные сообщения, которые не влияют на работу устройства. Например, при загрузке устройства Cisco может появиться следующее информационное сообщение: %LICENSE-6-EULA_ACCEPT_ALL: The Right to Use End User License Agreement is accepted.
  - **Уровень отладки 7 (debugging)**: сообщения этого уровня содержат выходные данные, полученные в результате выполнения различных команд **debug**.

Формат сообщений системного журнала (продолжение)

- Формат сообщений системного журнала по умолчанию в ПО Cisco IOS:

```
seq no: timestamp: %facility-severity-MNEMONIC: description
```

- Пример выходных данных об изменении состояния канала EtherChannel коммутатора Cisco на активное:

```
00:00:46: %LINK-3-UPDOWN: Interface Port-channel1, changed state to up
```

- Объектом является LINK, назначен уровень критичности 3, в качестве MNEMONIC указан UPDOWN.

Поле	Описание
seq no	Добавляет к сообщениям журнала порядковый номер, если в режиме глобальной настройки конфигурации использовалась команда **`service sequence-numbers`**.
timestamp	Отображает дату и время сообщения или события, только если в режиме глобальной настройки конфигурации использовалась команда **`service timestamp`**.
facility	Объект, к которому относится сообщение.
severity	Однозначный код (цифра от 0 до 7), обозначающий уровень серьезности сообщений.
MNEMONIC	Текстовая строка, которая однозначным образом описывает сообщение.
Описание	Текстовая строка, содержащая подробные сведения о событии, о котором получено уведомление.

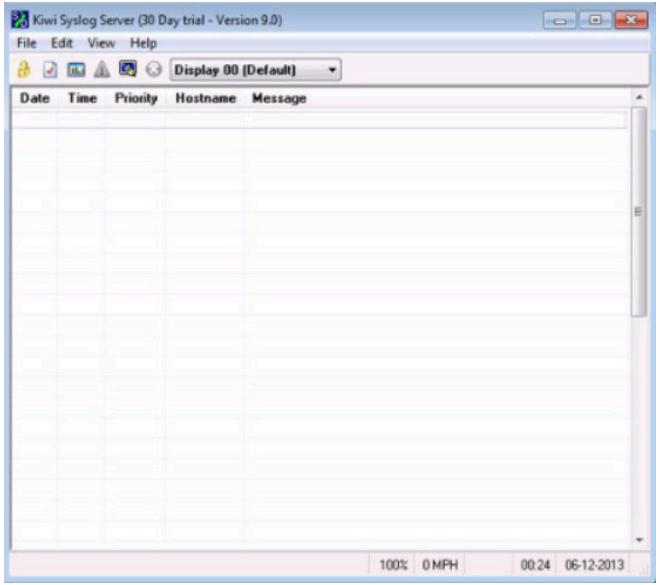
Метка времени службы

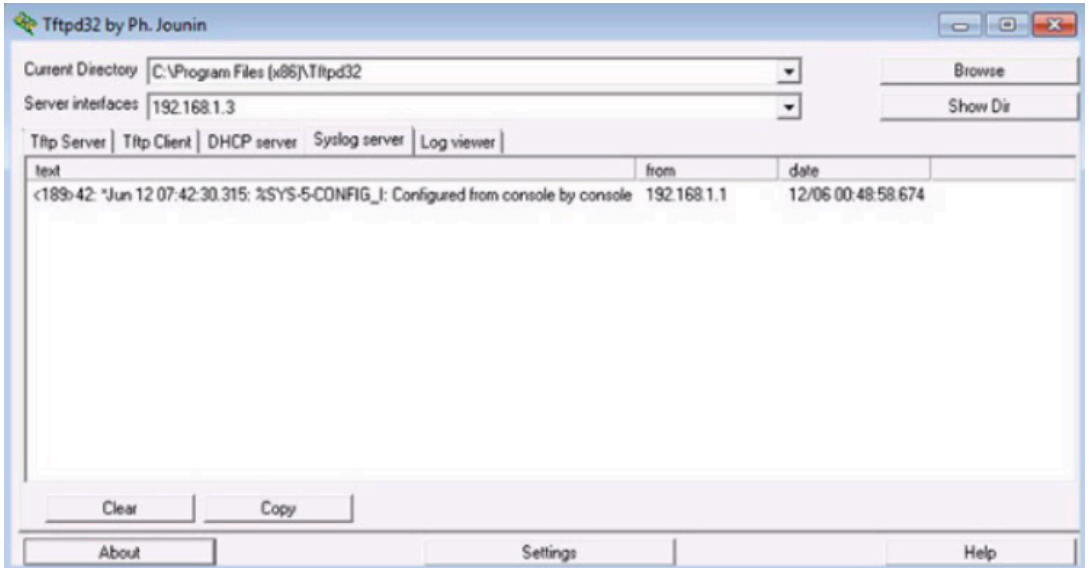
- По умолчанию в сообщениях журнала нет метки времени
- Метка времени в сообщениях журнала нужна для того, чтобы при отправке получателю (на сервер системного журнала) была запись о времени формирования сообщения
- После активации метки времени обратите внимание на приведенную ниже дату

```
R1# conf t
R1(config)# interface g0/0
R1(config-if)# shutdown
%LINK-5-CHANGED: Interface GigabitEthernet0/0, changed state to administratively down
%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/0, changed state to dow
R1(config-if)# exit
R1(config)# service timestamps log datetime
R1(config)# interface g0/0
R1(config-if)# no shutdown
*Mar  1 11:52:42: %LINK-3-UPDOWN: Interface GigabitEthernet0/0, changed state to down
*Mar  1 11:52:45: %LINK-3-UPDOWN: Interface GigabitEthernet0/0, changed state to up
*Mar  1 11:52:46: %LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/0,
changed state to up
R1(config-if)#
```

Сервер системного журнала

- Для просмотра сообщений системного журнала на подключенный к сети ПК необходимо установить сервер системного журнала





Ведение журнала по умолчанию

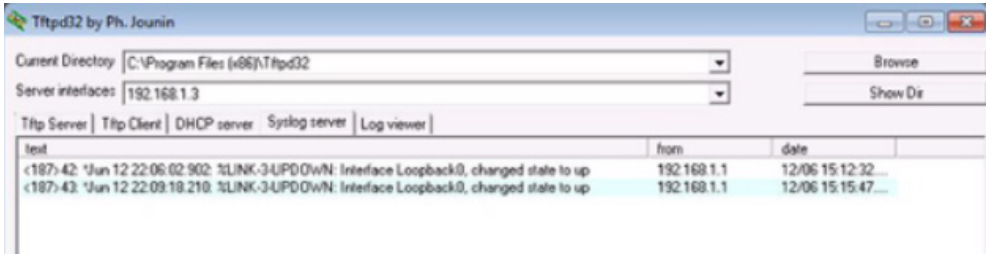
```
R1# show logging
Syslog logging: enabled (0 messages dropped, 2 messages rate-limited, 0 flushes, 0
overruns, xml disabled, filtering disabled)

No Active Message Discriminator.

No Inactive Message Discriminator.

        Console logging: level debugging, 32 messages logged, xml disabled,
                         filtering disabled
        Monitor logging: level debugging, 0 messages logged, xml disabled,
                         filtering disabled
        Buffer logging: level debugging, 32 messages logged, xml disabled,
                         filtering disabled
        Exception Logging: size (4096 bytes)
        Count and timestamp logging messages: disabled
        Persistent logging: disabled

No active filter modules.

    Trap logging: level informational, 34 message lines logged
        Logging Source-Interface:       VRF Name:

Log Buffer (8192 bytes):

*Jan 2 00:00:02.527: %LICENSE-6-EULA_ACCEPT_ALL: The Right to Use End User License
Agreement is accepted
*Jan 2 00:00:02.631: %IOS_LICENSE_IMAGE_APPLICATION-6-LICENSE_LEVEL: Module name =
c1900 Next reboot level = ipbasek9 and License = ipbasek9
*Jan 2 00:00:02.851: %IOS_LICENSE_IMAGE_APPLICATION-6-LICENSE_LEVEL: Module name =
c1900 Next reboot level = securityk9 and License = securityk9
*Jun 12 17:46:01.619: %IFMGR-7-NO_IFINDEX_FILE: Unable to open nvram:/ifIndex-table No
such file or directory

<output omitted>
```

- По умолчанию сообщения журнала отправляются на консоль.
- В некоторых версиях IOS сообщения журнала также по умолчанию записываются в буфер.
- В первой выделенной строке указано, что данные журнала этого маршрутизатора отправляются на консоль и содержат сообщения уровня отладки.
  - Все сообщения уровня отладки, а также любые сообщения более низкого уровня регистрируются на консоли
- Во второй выделенной строке указано, что журнал этого маршрутизатора сохраняется во внутренний буфер.
- Зарегистрированные системные сообщения находятся в конце выходных данных.

Настройка системного журнала
Команды маршрутизатора и коммутатора для клиентов системного журнала

```
R1(config)# logging 192.168.1.3
R1(config)# logging trap 4
R1(config)# logging source-interface g0/0
R1(config)# interface loopback 0
R1(config-if)#
*Jun 12 22:06:02.902: %LINK-3-UPDOWN: Interface Loopback0, changed state to up
*Jun 12 22:06:03.902: %LINEPROTO-5-UPDOWN: Line protocol on Interface Loopback0,
changed state to up
*Jun 12 22:06:03.902: %SYS-6-LOGGINGHOST_STARTSTOP: Logging to host 192.168.1.3
port 514 started - CLI initiated
R1(config-if)# shutdown
R1(config-if)#
*Jun 12 22:06:49.642: %LINK-5-CHANGED: Interface Loopback0, changed state to
administratively down
*Jun 12 22:06:50.642: %LINEPROTO-5-UPDOWN: Line protocol on Interface Loopback0,
changed state to down
R1(config-if)# no shutdown
R1(config-if)#
*Jun 12 22:09:18.210: %LINK-3-UPDOWN: Interface Loopback0, changed state to up
*Jun 12 22:09:19.210: %LINEPROTO-5-UPDOWN: Line protocol on Interface Loopback0,
changed state to up
R1(config-if)#
```

- На маршрутизаторе R1 настроена отправка сообщений журнала уровня 4 и ниже на сервер системного журнала по адресу 192.168.1.3
- В качестве интерфейса источника задан интерфейс G0/0
- Интерфейс обратной петли создается, затем выключается, а затем снова переводится в активное состояние
- Эти действия отражены в выходных данных на консоли



Проверка системного журнала

```
R1# show logging | include changed state to up
*Jun 12 17:46:26.143: %LINK-3-UPDOWN: Interface
GigabitEthernet0/1, changed state to up
*Jun 12 17:46:26.143: %LINK-3-UPDOWN: Interface Serial0/0/1,
changed state to up
*Jun 12 17:46:27.263: %LINEPROTO-5-UPDOWN: Line protocol on
Interface GigabitEthernet0/1, changed state to up
*Jun 12 17:46:27.263: %LINEPROTO-5-UPDOWN: Line protocol on
Interface Serial0/0/1, changed state to up
*Jun 12 20:28:43.427: %LINK-3-UPDOWN: Interface
GigabitEthernet0/0, changed state to up
*Jun 12 20:28:44.427: %LINEPROTO-5-UPDOWN: Line protocol on
Interface GigabitEthernet0/0, changed state to up
*Jun 12 22:04:11.862: %LINEPROTO-5-UPDOWN: Line protocol on
Interface Loopback0, changed state to up
*Jun 12 22:06:02.902: %LINK-3-UPDOWN: Interface Loopback0,
changed state to up
*Jun 12 22:06:03.902: %LINEPROTO-5-UPDOWN: Line protocol on
Interface Loopback0, changed state to up
*Jun 12 22:09:18.210: %LINK-3-UPDOWN: Interface Loopback0,
changed state to up
*Jun 12 22:09:19.210: %LINEPROTO-5-UPDOWN: Line protocol on
Interface Loopback0, changed state to up
*Jun 12 22:35:55.926: %LINK-3-UPDOWN: Interface Loopback0,
changed state to up
*Jun 12 22:35:56.926: %LINEPROTO-5-UPDOWN: Line protocol on
Interface Loopback0, changed state to up
```

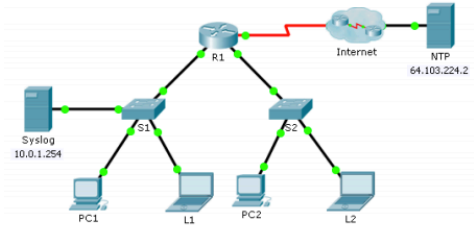
```
R1# show logging | begin Jun 12 22:35
*Jun 12 22:35:46.206: %LINK-5-CHANGED: Interface Loopback0,
changed state to administratively down
*Jun 12 22:35:47.206: %LINEPROTO-5-UPDOWN: Line protocol on
Interface Loopback0, changed state to down
*Jun 12 22:35:55.926: %LINK-3-UPDOWN: Interface Loopback0,
changed state to up
*Jun 12 22:35:56.926: %LINEPROTO-5-UPDOWN: Line protocol on
Interface Loopback0, changed state to up
*Jun 12 22:49:52.122: %SYS-5-CONFIG_I: Configured from console by
console
*Jun 12 23:15:48.418: %SYS-5-CONFIG_I: Configured from console by
console
R1#
```

Packet Tracer. Настройка системного журнала и протокола NTP

Cisco Networking Academy® Mind Wide Open™

Packet Tracer – Configuring Syslog and NTP

Topology



Objectives

Part 1: Configure Syslog Service

Part 2: Generate Logged Events

Part 3: Manually Set Switch Clocks

Part 4: Configure NTP Service

Part 5: Verify Timestamped Logs

Scenario

In this activity, you will enable and use the Syslog service and the NTP service so that the network administrator is able to monitor the network more effectively.

Part 1: Configure Syslog Service

Step 1: Enable the Syslog service.

a. Click **Syslog**, then **Services** tab.

b. Turn the **Syslog** service on and move the window so you can monitor activity.

Step 2: Configure the intermediary devices to use the Syslog service.

a. Configure **R1** to send log events to the **Syslog** server.

```
R1(config)# logging 10.0.1.254
```

b. Configure **S1** to send log events to the **Syslog** server.

c. Configure **S2** to send log events to the **Syslog** server.

Лабораторная работа. Настройка системного журнала и протокола NTP

Cisco Networking Academy® Mind Wide Open™

Lab – Configuring Syslog and NTP

Topology

Addressing Table

Device	Interface	IP Address	Subnet Mask	Default Gateway
R1	S0/0/0 (DCE)	10.1.1.1	255.255.255.252	N/A
R2	S0/0/0	10.1.1.2	255.255.255.252	N/A
	G0/0	172.16.2.1	255.255.255.0	N/A
PC-B	NIC	172.16.2.3	255.255.255.0	172.16.2.1

Objectives

Part 1: Configure Basic Device Settings

Part 2: Configure NTP

Part 3: Configure Syslog

Background / Scenario

Syslog messages that are generated by the network devices can be collected and archived on a syslog server. The information can be used for monitoring, debugging, and troubleshooting purposes. The administrator can control where the messages are stored and displayed. Syslog messages can be time-stamped for analysis of the sequence of network events; therefore, it is important to synchronize the clock across the network devices with a Network Time Protocol (NTP) server.

In this lab, you will configure R1 as the NTP server and R2 as a Syslog and NTP client. The syslog server application, such as Tftp32d or other similar program, will be running on PC-B. Furthermore, you will control the severity level of log messages that are collected and archived on the syslog server.

Note: The routers used with CCNA hands-on labs are Cisco 1941 Integrated Services Routers (ISRs) with Cisco IOS Release 15.2(4)M3 (universalk9 image). Other routers and Cisco IOS versions can be used. Depending on the model and Cisco IOS version, the commands available and output produced might vary from what is shown in the labs. Refer to the Router Interface Summary Table at the end of this lab for the correct interface identifiers.

Note: Make sure that the routers have been erased and have no startup configurations. If you are unsure, contact your instructor.

Required Resources

- 2 Routers (Cisco 1941 with Cisco IOS Release 15.2(4)M3 universal image or comparable)

10.3. Обслуживание устройств

Файловые системы маршрутизаторов

```
Router# show file systems
File Systems:

      Size(b)       Free(b)      Type  Flags  Prefixes
            -             -    opaque     rw   archive:
            -             -    opaque     rw   system:
            -             -    opaque     rw   tmpsys:
            -             -    opaque     rw   null:
            -             -   network     rw   tftp:
*    256487424     183234560      disk     rw   flash0: flash:#
            -             -      disk     rw   flash1:
       262136        254779     nvram     rw   nvram:
            -             -    opaque     wo   syslog:
            -             -    opaque     rw   xmodem:
            -             -    opaque     rw   ymodem:
            -             -   network     rw   rcp:
            -             -   network     rw   http:
            -             -   network     rw   ftp:
            -             -   network     rw   scp:
            -             -    opaque     ro   tar:
            -             -   network     rw   https:
            -             -    opaque     ro   cns:
```

- Команда **show file systems** перечисляет все доступные файловые системы
- Предоставляет такую информацию, как объем памяти, тип файловой системы и разрешения (только чтение (ro), чтение и запись (rw))
- Интересуют файловые системы tftp, flash и nvram
- Загружаемая IOS размещена во флеш-памяти, поэтому она обозначена символом *

Файловые системы маршрутизаторов (продолжение)

```
Router# dir
Directory of flash0:/

 1 -rw-     2903 Sep 7 2012 06:58:26 +00:00  cpconfig-
                                             19xx.cfg
 2 -rw-  3000320 Sep 7 2012 06:58:40 +00:00  cpexpress.tar
 3 -rw-     1038 Sep 7 2012 06:58:52 +00:00  home.shtml
 4 -rw-   122880 Sep 7 2012 06:59:02 +00:00  home.tar
 5 -rw-  1697952 Sep 7 2012 06:59:20 +00:00  securedesktop-
                                             ios-3.1.1.45-k9.pkg
 6 -rw-   415956 Sep 7 2012 06:59:34 +00:00  sslclient-win-
                                             1.1.4.176.pkg
 7 -rw- 67998028 Sep 26 2012 17:32:14 +00:00 c1900-
                                             universalk9-
                                             mz.SPA.152-4.M1.bin

256487424 bytes total (183234560 bytes free)
```

- **Команда** dir перечисляет содержимое флеш-памяти
- Последний пункт списка — имя текущего файла Cisco IOS, запущенного в ОЗУ

```
Router# cd nvram:
Router#pwd
nvram:/
Router#dir
Directory of nvram:/

  253  -rw-        1156      <no date>  startup-config
  254  ----           5      <no date>  private-config
  255  -rw-        1156      <no date>  underlying-config
    1  -rw-        2945      <no date>  cwmp_inventory
    4  ----          58      <no date>  persistent-data
    5  -rw-          17      <no date>  ecfm_ieee_mib
    6  -rw-         559      <no date>  IOS-Self-Sig#1.cer

262136 bytes total (254779 bytes free)
```

- Для просмотра содержания NVRAM измените текущую файловую систему по умолчанию с помощью команды **cd** (смена каталога)
- Команда **pwd** (представление рабочего каталога) подтверждает, что просматривается именно каталог NVRAM
- Команда **dir** перечисляет содержимое NVRAM, включая файл конфигурации запуска

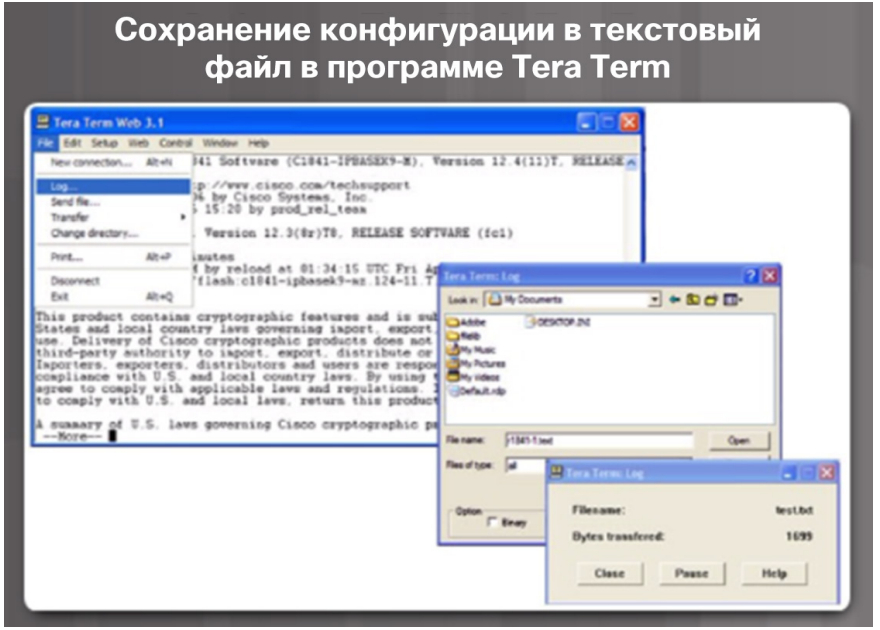
Файловые системы коммутаторов

```
Switch# show file systems
File Systems:

       Size(b)     Free(b)      Type  Flags  Prefixes
*     32514048    20887552     flash     rw    flash:
          -           -       opaque    rw       vb:
          -           -       opaque    ro       bs:
          -           -       opaque    rw   system:
          -           -       opaque    rw   tmpsys:
        65536       48897      nvram    rw    nvram:
          -           -       opaque    ro   xmodem:
          -           -       opaque    ro   ymodem:
          -           -       opaque    rw     null:
          -           -       opaque    ro      tar:
          -           -      network    rw     tftp:
          -           -      network    rw      rcp:
          -           -      network    rw     http:
          -           -      network    rw      ftp:
          -           -      network    rw      scp:
          -           -      network    rw    https:
          -           -      opaque     ro      cns:
```

Команда такая же, как для маршрутизатора!

Резервное копирование и восстановление с помощью текстовых файлов

1. В меню File (Файл) выберите пункт Log (Журнал).
2. Выберите путь для сохранения файла. Программа Tera Term запустит процесс захвата текста.
3. После начала данного процесса в командной строке привилегированного режима EXEC выполните команду show running-config или show startup-config. Текст, отображаемый в окне терминала, будет отправлен в выбранный файл.
4. По окончании захвата текста нажмите Close (Закрыть) в окне журнала Tera Term.
5. Просмотрите файл, чтобы убедиться в том, что он не поврежден.



Резервное копирование и восстановление с помощью текстовых файлов (продолжение)

Восстановление конфигураций из текстового файла

- Конфигурацию можно скопировать на устройство из файла.
- При копировании из текстового файла и вставке в окно терминала IOS выполняет каждую строку текста конфигурации как команду.
- В интерфейсе командной строки необходимо установить режим глобальной настройки устройства, чтобы команды из текстового файла вставлялись в окно терминала.

При использовании программы Tera Term необходимо выполнить следующие действия.

- Шаг 1. В меню File (Файл) выберите пункт Send file (Отправить файл).
- Шаг 2. Укажите путь к файлу, который необходимо скопировать на данное устройство, и нажмите Open (Открыть).
- Шаг 3. После этого программа Tera Term вставит этот файл в память устройства.
- Примечание. Текстовое содержимое файла будет применяться в интерфейсе командной строки в качестве команд и станет работающей конфигурацией на устройстве.

Резервное копирование и восстановление с помощью TFTP

- Необходимо выполнять резервное копирование файлов конфигурации и включать их в документацию сети
- Команды — **copy running-config tftp** (см. рисунок) или **copy startup-config tftp**
- Для восстановления текущей или начальной конфигурации с сервера TFTP используйте команду **copy tftp running-config** или **copy tftp startup-config**

```
R1# copy running-config tftp
Remote host []? 192.168.10.254
Name of the configuration file to write[R1-config]? R1-Jan-2016
Write file R1-Jan-2016 to 192.168.10.254? [confirm]
Writing R1-Jan-2016 !!!!!! [OK]
```

Использование портов USB на маршрутизаторе Cisco

- Некоторые модели маршрутизаторов Cisco поддерживают USB-накопители
- Такой накопитель можно использовать для хранения и загрузки.
- На USB-накопителе может храниться несколько копий Cisco IOS и несколько конфигураций маршрутизатора.
- Чтобы просмотреть содержимое USB-накопителя, выполните команду **dir**.

Резервное копирование и восстановление с помощью USB

```
R1# show file systems
File Systems:

      Size(b)       Free(b)      Type  Flags  Prefixes
            -             -    opaque     rw   archive:
            -             -    opaque     rw   system:
            -             -    opaque     rw   tmpsys:
            -             -    opaque     rw   null:
            -             -   network     rw   tftp:
*    256487424     184819712      disk     rw   flash0: flash:#
            -             -      disk     rw   flash1:
       262136        249270     nvram     rw   nvram:
            -             -    opaque     wo   syslog:
            -             -    opaque     rw   xmodem:
            -             -    opaque     rw   ymodem:
            -             -   network     rw   rcp:
            -             -   network     rw   http:
            -             -   network     rw   ftp:
            -             -   network     rw   scp:
            -             -    opaque     ro   tar:
            -             -   network     rw   https:
            -             -    opaque     ro   cns:
   4050042880    3774152704  usbflash     rw   usbflash0:
```

Отображение USB-порта и его имени: «usbflash0:»

- Команда **show file systems** проверяет USB-накопитель и имя

Резервное копирование и восстановление с помощью USB (продолжение)

```
R1# copy running-config usbflash0:
Destination filename [running-config]? R1-Config
5024 bytes copied in 0.736 secs (6826 bytes/sec)
```

Копирование на USB-накопитель, когда такого файла еще не существует на накопителе.

```
R1# copy running-config usbflash0:
Destination filename [running-config]? R1-Config
%Warning:There is a file already existing with this name
Do you want to over write? [confirm]
5024 bytes copied in 1.796 secs (2797 bytes/sec)
```

Копирование на USB-накопитель, когда такой файл конфигурации уже существует на накопителе.

- Команда **Copy run usbflash0:/** копирует файл текущей конфигурации на USB-накопитель (использовать косую черту не обязательно, она указывает корневой каталог USB-накопителя)
- IOS запросит имя файла
- Если этот файл уже существует на USB-накопителе, маршрутизатор предложит перезаписать его

Резервное копирование и восстановление с помощью USB (продолжение)

```
R1# dir usbflash0:/
Directory of usbflash0:/
    1  drw-     0  Oct 15 2010 16:28:30 +00:00  Cisco
   16  -rw-  5024   Jan 7 2013 20:26:50 +00:00  R1-Config

4050042880 bytes total (3774144512 bytes free)
R1# more usbflash0:/R1-Config
!
! Last configuration change at 20:19:54 UTC Mon Jan 7 2013 by
admin version 15.2
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname R1
!
boot-start-marker
boot-end-marker
!
!
logging buffered 51200 warnings
!
no aaa new-model
!
no ipv6 cef
```

- Чтобы просмотреть файл на USB-накопителе, выполните команду **dir**
- Чтобы просмотреть содержимое, выполните команду **more**
- Чтобы восстановить текущую конфигурацию, выполните команду **copy usbflash0:/R1-Config running-config**

Восстановление пароля

```
Readonly ROMMON initialized

monitor: command "boot" aborted due to user interrupt
rommon 1 > confreg 0x2142
rommon 2 > reset

System Bootstrap, Version 15.0(1r)M9, RELEASE SOFTWARE (fc1)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 2010 by cisco Systems, Inc.
<output omitted>
```

```
Router# copy startup-config running-config
Destination filename [running-config]?

1450 bytes copied in 0.156 secs (9295 bytes/sec)
Router# conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)# enable secret cisco
Router(config)# config-register 0x2102
Router(config)# end
Router# copy running-config startup-config
Destination filename [startup-config]?
Building configuration...
```

Шаг 1. Войдите в режим ROMMON.

- При наличии консольного доступа пользователь может войти в режим ROMMON, используя специальную комбинацию клавиш во время процесса загрузки или вынув внешнюю флеш-память, когда устройство отключено.

Шаг 2. Изменить значение регистра конфигурации на 0x2142, что позволит игнорировать файл загрузочной конфигурации.

- Выполните команду **confreg 0x2142**.
- Введите в командной строке reset, чтобы перезапустить устройство.

Шаг 3. Внесите в исходный файл загрузочной конфигурации необходимые изменения.

- Скопируйте начальную конфигурацию в текущую конфигурацию.
- Задайте все необходимые пароли.
- Измените значение регистра конфигурации обратно на 0X2102

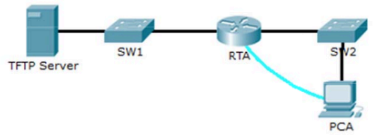
Шаг 4. Сохраните новую конфигурацию.

Packet Tracer. Резервное копирование файлов конфигурации

Cisco Networking Academy® Mind Wide Open™

Packet Tracer - Backing Up Configuration Files

Topology



Objectives

Part 1: Establish Connectivity to TFTP Server

Part 2: Transfer Configuration from TFTP Server

Part 3: Backup Configuration and IOS to TFTP Server

Background / Scenario

This activity is designed to show how to restore a configuration from a backup and then perform a new backup. Due to an equipment failure, a new router has been put in place. Fortunately backup configuration files have been saved to a Trivial File Transfer Protocol (TFTP) Server. You are required to restore the files from the TFTP Server to get the router back online with as little down time as possible.

Part 1: Establish Connectivity to the TFTP Server

Note: Because this is a new router, initial configuration will be performed using a console connection to the router.

a. Click **PCA**, then the **Desktop** tab, followed by **Terminal** to access the **RTA** command line.

b. Configure and activate the **Gigabit Ethernet 0/0** interface. The IP address should match the default gateway for the **TFTP Server**.

c. Test connectivity to **TFTP Server**. Troubleshoot, if necessary.

Part 2: Transfer Configuration from the TFTP Server

a. From privileged EXEC mode, issue the following command:

```
Router# copy tftp running-config
Address or name of remote host []? 172.16.1.2
Source filename []? RTA-confg
Destination filename [running-config]? <cr>
```

The router should return the following:

```
Accessing tftp://172.16.1.2/RTA-confg...
Loading RTA-confg from 172.16.1.2: !
```

Обслуживание файлов маршрутизаторов и коммутаторов

Лабораторная работа. Управление файлами конфигурации маршрутизатора с помощью программы Tera Term

Cisco Networking Academy® Mind Wide Open™

Lab – Managing Router Configuration Files with Terminal Emulation Software

Topology

Addressing Table

Device	Interface	IP Address	Subnet Mask	Default Gateway
R1	G0/1	192.168.1.1	255.255.255.0	N/A
S1	VLAN 1	192.168.1.11	255.255.255.0	192.168.1.1
PC-A	NIC	192.168.1.3	255.255.255.0	192.168.1.1

Objectives

Part 1: Configure Basic Device Settings

Part 2: Use Terminal Emulation Software to Create a Backup Configuration File

Part 3: Use a Backup Configuration File to Restore a Router

Background / Scenario

It is a recommended best practice to maintain backup configuration files for routers and switches in the event that they need to be restored to a previous configuration. Terminal emulation software can be used to easily back up or restore a router or switch configuration file.

In this lab, you will use Tera Term to back up a router running configuration file, erase the router startup configuration file, reload the router, and then restore the missing router configuration from the backup configuration file.

Note: The routers used with CCNA hands-on labs are Cisco 1941 Integrated Services Routers (ISRs) with Cisco IOS Release 15.2(4)M3 (universalk9 image). The switches used are Cisco Catalyst 2960s with Cisco IOS Release 15.0(2) (lanbasek9 image). Other routers, switches, and Cisco IOS versions can be used. Depending on the model and Cisco IOS version, the commands available and output produced might vary from what is shown in the labs. Refer to the Router Interface Summary Table at the end of this lab for the correct interface identifiers.

Note: Make sure that the routers and switches have been erased and have no startup configurations. If you are unsure, contact your instructor.

Required Resources

- 1 Router (Cisco 1941 with Cisco IOS Release 15.2(4)M3 universal image or comparable)
- 1 Switch (Cisco 2960 with Cisco IOS Release 15.0(2) lanbasek9 image or comparable)
- 1 PC (Windows 7, Vista, or XP with terminal emulation program, such as Tera Term)
- Console cables to configure the Cisco IOS devices via the console ports

Лабораторная работа. Управление файлами конфигурации устройств с помощью TFTP, флеш-памяти и USB

Cisco Networking Academy® Mind Wide Open™

Lab – Managing Device Configuration Files Using TFTP, Flash, and USB

Topology

Addressing Table

Device	Interface	IP Address	Subnet Mask	Default Gateway
R1	G0/1	192.168.1.1	255.255.255.0	N/A
S1	VLAN 1	192.168.1.11	255.255.255.0	192.168.1.1
PC-A	NIC	192.168.1.3	255.255.255.0	192.168.1.1

Objectives

Part 1: Build the Network and Configure Basic Device Settings

Part 2: (Optional) Download TFTP Server Software

Part 3: Use TFTP to Back Up and Restore the Switch Running Configuration

Part 4: Use TFTP to Back Up and Restore the Router Running Configuration

Part 5: Back Up and Restore Running Configurations Using Router Flash Memory

Part 6: (Optional) Use a USB Drive to Back Up and Restore the Running Configuration

Background / Scenario

Cisco networking devices are often upgraded or swapped out for a number of reasons. It is important to maintain backups of the latest device configurations, as well as a history of configuration changes. A TFTP server is often used to backup configuration files and IOS images in production networks. A TFTP server is a centralized and secure method used to store the backup copies of the files and restore them as necessary. Using a centralized TFTP server, you can back up files from many different Cisco devices.

In addition to a TFTP server, most of the current Cisco routers can back up and restore files locally from CompactFlash (CF) memory or a USB flash drive. The CF is a removable memory module that has replaced the limited internal flash memory of earlier router models. The IOS image for the router resides in the CF memory, and the router uses this IOS Image for the boot process. With the larger size of the CF memory, additional files can be stored for backup purposes. A removable USB flash drive can also be used for backup purposes.

In this lab, you will use TFTP server software to back up the Cisco device running configuration to the TFTP server or flash memory. You can edit the file using a text editor and copy the new configuration back to a Cisco device.

Лабораторная работа. Изучение процедур восстановления паролей

Cisco Networking Academy® Mind Wide Open™

Lab – Configure and Verify Password Recovery

Topology

Objectives

Part 1: Configure Basic Device Settings

Part 2: Reboot Router and Enter ROMMON

Part 3: Reset Password and Save New Configuration

Part 4: Verify the Router is Loading Correctly

Background / Scenario

The purpose of this lab is to reset the enable password on a specific Cisco router. The enable password protects access to privileged EXEC and configuration mode on Cisco devices. The enable password can be recovered, but the enable secret password is encrypted and will need to be replaced with a new password.

In order to bypass a password, a user must be familiar with the ROM monitor (ROMMON) mode, as well as the configuration register setting for Cisco routers. ROMMON is basic CLI software stored in ROM that can be used to troubleshoot boot errors and recover a router when an IOS is not found.

In this lab, you will change the configuration register in order to reset the enable password on a Cisco router.

Required Resources

- 1 Router (Cisco 1941 with Cisco IOS Release 15.2(4)M3 universal image or comparable)
- 1 PC (Windows 7, Vista, or XP with terminal emulation program, such as Tera Term)
- Console cable to connect to the Cisco IOS device via the console port

Part 1: Configure Basic Device Settings

In Part 1, you will set up the network topology and copy the basic configuration into R1. The password is encrypted to setup the scenario of needing to recover from an unknown enabled password.

Step 1: Cable the network as shown in the topology.

Step 2: Initialize and reload the routers as necessary.

Step 3: Configure basic settings on the router.

a. Console into the router and enter global configuration mode.

b. Copy the following basic configuration and paste it to the running-configuration on the router.

```
no ip domain-lookup
service password-encryption
hostname R1
enable secret 5 $1$SBb4$n.EuL28kPTzxMLFiyML15/
```

Комплектация образов системы IOS 15

- Маршрутизатор G2 поставляется с одной универсальной Cisco IOS, и для включения пакетов определенных наборов функций используется лицензия.

- Каждый маршрутизатор поставляется с одним из двух типов универсальных образов в ISR G2:
  - **"universalk9"** — позволяет пользоваться всеми функциями программного обеспечения Cisco IOS, включая функции стойкой криптографии полезных данных, такие как IPsec VPN, VPN на основе SSL и Secure Unified Communications
  - **"universalk9_npe"** — в некоторых странах существуют требования в отношении импорта, согласно которым платформа не должна поддерживать какие-либо функции стойкой криптографии; данный образ не поддерживает никакое стойкое шифрование полезных данных
- Функции активируются с помощью лицензии.
- Другие технологические пакеты включаются с помощью лицензионных ключей активации программного обеспечения Cisco.

Имена файлов образов IOS

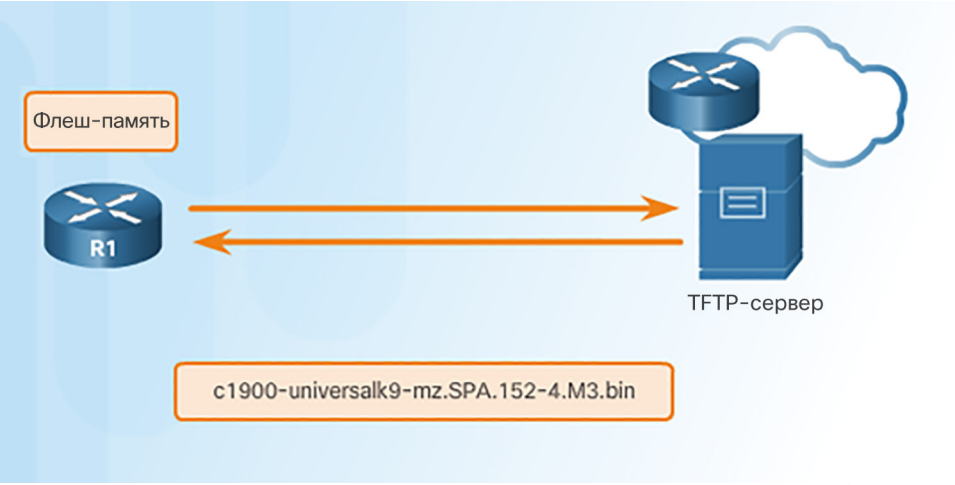
Отображаются файлы, хранящиеся во флеш-памяти

```
R1# show flash0:
-# - --length-- -----date/time------ path


8   68831808   Apr 2 2013 21:29:58 +00:00 c1900-universalk9-mz.SPA.152-4.M3.bin

182394880 bytes available (74092544 bytes used)

R1#
```

- mz — это наиболее распространенное обозначение для формата участка памяти и сжатия. Первая буква указывает, где маршрутизатор будет хранить образ во время работы. Возможные места:
  - f — флеш-память
  - m — ОЗУ
  - r — ПЗУ
  - l — переместимый
- Образ может быть сжат в формате z (zip) или x (mzip).

Использование серверов TFTP для хранения резервных копий

- Образы и файлы конфигурации ПО Cisco IOS могут храниться на центральном сервере TFTP.
- Рекомендуется сохранить резервную копию образа Cisco IOS на случай повреждения или случайного удаления образа системы на маршрутизаторе.
- Использование сетевого TFTP-сервера позволяет загружать файлы образов и конфигураций по сети. Такой TFTP-сервер может быть маршрутизатором, рабочей станцией или хостом.



Создание резервной копии образа IOS на сервере TFTP

- Сетевому администратору требуется создать резервную копию файла образа, который в данный момент используется в маршрутизаторе (c1900-universalk9-mz.SPA.152-4.M3.bin), на сервере TFTP по адресу 172.16.1.100.

Проверьте подключение к серверу.

```
R1# ping 172.16.1.100
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.16.1.100, timeout is 2
seconds:
!!!!!
Success rate is 100 percent (5/5),
round-trip min/avg/max = 56/56/56 ms
```

Создание резервной копии образа IOS на сервере TFTP (продолжение)

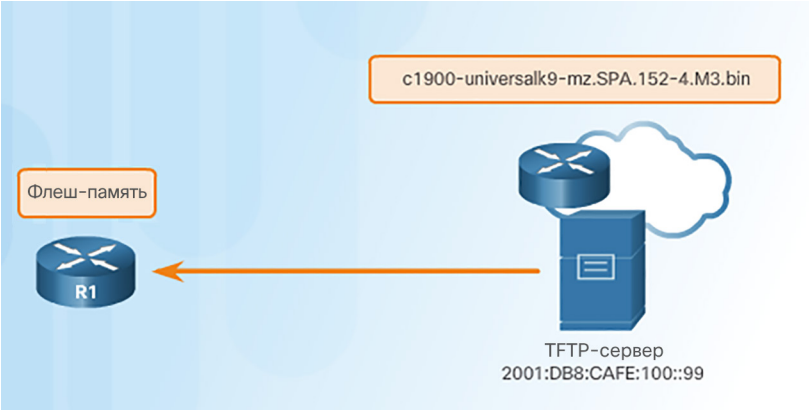
Проверьте размер образа.

```
R1# show flash0:
-# - --length-- -----date/time------ path
8    68831808   Apr 2 2013 21:29:58  +00:00
                        c1900-universalk9-mz.SPA.152-4.M3.bin

<output omitted>
```

Скопируйте образ на TFTP-сервер.

```
R1# copy flash0: tftp:
Source filename []? c1900-universalk9-mz.SPA.152-4.M3.bin
Address or name of remote host []? 172.16.1.100
Destination filename [c1900-universalk9-mz.SPA.152-4.M3.bin]?
Writing c1900-universalk9-mz.SPA.152-4.M3.bin...
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
<output omitted>
68831808 bytes copied in 363.468 secs (269058 bytes/sec)
```

Копирование образа IOS на устройство



- Новый файл образа (c1900-universalk9-mz.SPA.152-4.M3.bin) будет скопирован на маршрутизатор с TFTP-сервера по адресу 2001:DB8:CAFE:100::99.

Проверьте подключение к серверу.

```
R1# ping 2001:DB8:CAFE:100::99
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 2001:DB8:CAFE:100::99,
timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5),
round-trip min/avg/max = 56/56/56 ms
```

Копирование образа IOS на устройство (продолжение)

Проверьте свободный объём флеш-памяти.

```
R1# show flash0:
-# - --length-- -----date/time------ path
<output omitted>

182394880 bytes available (74092544 bytes used)

R1#
```

Скопируйте образ из TFTP-сервера.

```
R1# copy tftp: flash0:
Address or name of remote host []? 2001:DB8:CAFE:100::99
Source filename []? c1900-universalk9-mz.SPA.152-4.M3.bin
Destination filename []?
c1900-universalk9-mz.SPA.152-4.M3.bin
Accessing tftp://2001:DB8:CAFE:100::99/c1900-universalk9-
mz.SPA.152-4.M3.bin...
Loading c1900-universalk9-mz.SPA.152-4.M3.bin from
2001:DB8:CAFE:100::99 (via
GigabitEthernet0/0): !!!!!!!!!!!!!!!!!!!!
<output omitted>
[OK - 68831808 bytes]
68831808 bytes copied in 368.128 secs (265652 bytes/sec)
```

Команда boot system

- Чтобы выполнить обновление до скопированного образа IOS после его сохранения во флеш-памяти маршрутизатора, укажите маршрутизатору использовать новый образ во время загрузки с помощью команды **boot system**.

Укажите, какой образ следует загружать, и перезагрузите устройство.

```
R1# configure terminal
R1(config)# boot system
            flash0://c1900-universalk9-mz.SPA.152-4.M3.bin
R1(config)# exit
R1# copy running-config startup-config
R1# reload
```

```
R1# show version
Cisco IOS Software, C1900 Software (C1900-UNIVERSALK9-M), Version 15.2(4)M3,
RELEASE SOFTWARE (fc2)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2013 by Cisco Systems, Inc.
Compiled Tue 26-Feb-13 02:11 by prod_rel_team

ROM: System Bootstrap, Version 15.0(1r)M15, RELEASE SOFTWARE (fc1)

R1 uptime is 1 hour, 2 minutes
System returned to ROM by power-on
System image file is "flash0:
c1900-universalk9-mz.SPA.152-4.M3.bin"
```

- Чтобы проверить, загружен ли новый образ, используйте команду **show version**.
- Чтобы создать план отказоустойчивой загрузки, можно ввести несколько команд **boot system**.
- Если команды **boot system** отсутствуют, маршрутизатор по умолчанию загружает первый допустимый образ Cisco IOS из флеш-памяти.

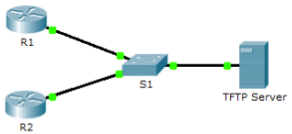
Управление образами IOS

Packet Tracer. Использование сервера TFTP для обновления образа Cisco IOS

Cisco Networking Academy® Mind Wide Open™

Packet Tracer – Using a TFTP Server to Upgrade a Cisco IOS Image

Topology



Addressing Table

Device	Interface	IP Address	Subnet Mask	Default Gateway
R1	F0/0	192.168.2.1	255.255.255.0	N/A
R2	G0/0	192.168.2.2	255.255.255.0	N/A
S1	VLAN 1	192.168.2.3	255.255.255.0	192.168.2.1
TFTP Server	NIC	192.168.2.254	255.255.255.0	192.168.2.1

Objectives

Part 1: Upgrade an IOS Image on a Cisco Device

Part 2: Backup an IOS Image on a TFTP Server

Scenario

A TFTP server can help manage the storage of IOS images and revisions to IOS images. For any network, it is good practice to keep a backup copy of the Cisco IOS Software image in case the system image in the router becomes corrupted or accidentally erased. A TFTP server can also be used to store new upgrades to the IOS and then deployed throughout the network where it is needed. In this activity, you will upgrade the IOS images on Cisco devices by using a TFTP server. You will also backup an IOS image with the use of a TFTP server.

Part 1: Upgrade an IOS Image on a Cisco Device

Step 1: Upgrade an IOS image on a router.

a. Access the TFTP server and enable the TFTP service.

b. Note the IOS images that are available on the TFTP server.

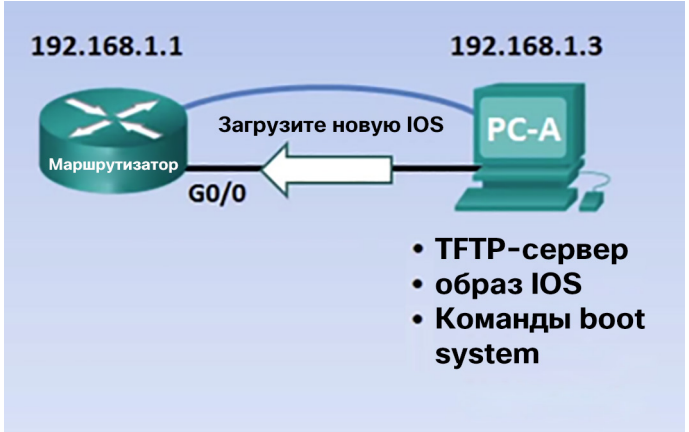
Which IOS images stored on the server are compatible with 1841?

c. From **R1**, issue the **show flash:** command and record the available flash memory.

Демонстрационный видеоролик. Управление образами Cisco IOS

Цель:

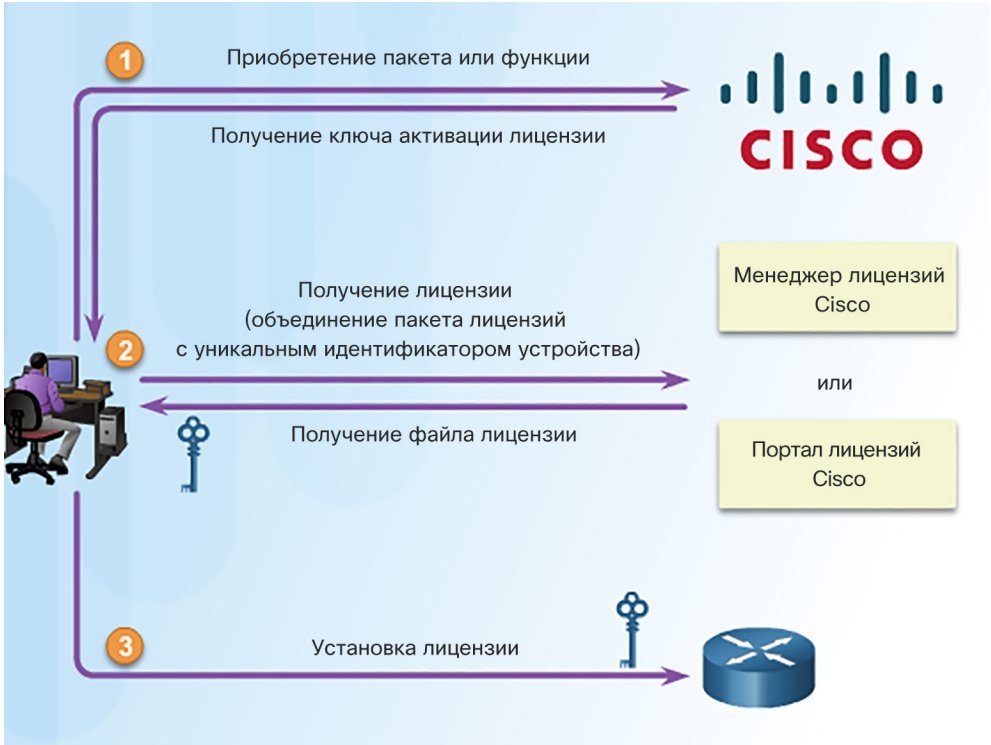
- Используйте сервер TFTP для передачи обновленного файла образа IOS на маршрутизатор Cisco.
- С помощью команды boot system задайте загрузку нового файла образа IOS на маршрутизаторе.
- Перезагрузите маршрутизатор и успешно загрузитесь с использованием нового файла образа IOS.



Общие сведения о лицензировании

- Каждое устройство поставляется с одним и тем же универсальным образом.
- Наборы функций универсального образа активируются ключом лицензирования с помощью ПО активации (Cisco Software Activation).
- Функция активации Cisco IOS позволяет пользователю активировать лицензированные функции и регистрировать лицензии.
- Доступные технологические пакеты:
  - IP Base
  - Данные
  - UC (унифицированные коммуникации)
  - SEC (система безопасности)

Процесс лицензирования



- На рисунке показаны три шага для активации на маршрутизаторе нового пакета ПО или функции на постоянной основе.
- PAK — ключ активации продукта
- UDI — уникальный идентификатор устройства

Шаг 1. Приобретение пакета ПО или дооснащения для установки

- Заказчики вместе с покупкой получают ключ активации (PAK), который служит в качестве чека и используется для получения лицензии.
- Ключ активации — это цифровой ключ из 11 цифр, сгенерированный производителем. Он определяет предоставляемый вместе с ним набор функций.
- Как показано на рисунке, для каждого пакета (IP Base, Data, UC и SEC) нужна отдельная лицензия.

Шаг 2. Получение лицензии

- UDI представляет собой комбинацию идентификатора продукта (PID), серийного номера (SN) и номера выпуска аппаратного обеспечения (VID). Серийный номер состоит из 11 цифр, идентифицирующих устройство. Идентификатор продукта определяет тип устройства. Для создания лицензии используются только идентификатор продукта и серийный номер.

- Этот уникальный идентификатор устройства (UDI) можно отобразить с помощью показанной команды **show license udi**.

```
R1#  show license udi
Device#  PID           SN            UDI
------------------------------------------------------------
*0       CISCO1941/K9  FTX1636848Z   CISCO1941/K9:FTX1636848Z

R1#
```

Шаг 3. Установка лицензии

Установка постоянной лицензии

```
R1# license install flash0:securityk9-CISCO1941-FHH12250057.lic
Installing licenses from "flash0:securityk9-CISCO1941-FHH12250057.lic"
Installing…Feature:securityk9…Successful:Supported
1/1 licenses were successfully installed
0/1 licenses were existing licenses
0/1 licenses were failed to install
R1#
*Jul 30 10:47:41.648: %IOS_LICENSE_IMAGE_APPLICATION-6-LICENSE_LEVEL: Module name =
c1941 Next reboot level = securityk9 and License = securityk9
*Jul 30 10:47:42.036: %LICENSE-6-INSTALL: Feature securityk9 1.0 was installed in this
device. UDI=CISCO1941:FHH12250057; StoreIndex=0:Primary License Storage
R1# reload
```

- Постоянная лицензия не истекает. Если на маршрутизаторе установлена постоянная лицензия, она действует для определенного набора функций в течение всего срока эксплуатации маршрутизатора, это распространяется на различные выпуски Cisco IOS.

Проверка лицензий

Проверка постоянной лицензии

```
R1# show version
<output omitted>
License Info:
License UDI:
------------------------------------------------------------------------------------------------
Device#           PID                 SN
------------------------------------------------------------------------------------------------
*0                CISCO1941/K9        FTX1636848Z
Technology        Package License     Information for Module:'c1900'
------------------------------------------------------------------------------------------------
Technology        Technology          Package             Technology-package
                  Current             Type                Next reboot
------------------------------------------------------------------------------------------------
ipbase            ipbasek9            Permanent           ipbasek9
security          seck9               Permanent           seck9
uc                None                None                None
data              None                None                None
```

Проверка лицензии

```
R1# show license
Index 1 Feature: ipbasek9
        Period left: Life time
        License Type: Permanent
        License State: Active, In Use
        License Count: Non-Counted
        License Priority: Medium
Index 2 Feature: securityk9
        Period left: Life time
        License Type: Permanent
        License State: Active, In Use
        License Count: Non-Counted
        License Priority: Medium
Index 3 Feature: datak9
        Period left: Not Activated
        Period Used: 0  minute  0  second
        License Type: EvalRightToUse
        License State: Not in Use, EULA not accepted
        License Count: Non-Counted
        License Priority: None

<output omitted>
```

Активация оценочной лицензии на право использования

Установка пробной лицензии

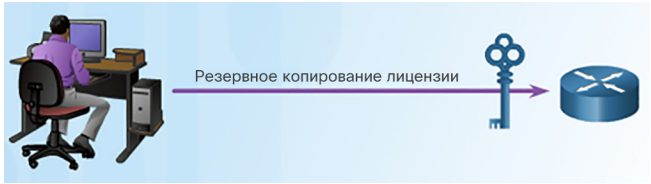
```
R1(config)# license accept end user agreement
R1(config)# license boot module c1900 technology-package
datak9
% use 'write' command to make license boot config take effect
on next boot
R1(config)#
*Apr 25 23:15:01.874: %IOS_LICENSE_IMAGE_APPLICATION-6-
LICENSE_LEVEL: Module name = c1900 Next reboot level = datak9
and License = datak9
*Apr 25 23:15:02.502: %LICENSE-6-EULA_ACCEPTED: EULA for
feature datak9 1.0 has been accepted.
UDI=CISCO1941/K9:FTX1636848Z; StoreIndex=1:Built-In License
Storage
R1(config)#
```

Проверка пробной лицензии

```
R1# show license
Index 1 Feature: ipbasek9
        Period left: Life time
        License Type: Permanent
        License State: Active, In Use
        License Count: Non-Counted
        License Priority: Medium
Index 2 Feature: securityk9
        Period left: Life time
        License Type: Permanent
        License State: Active, In Use
        License Count: Non-Counted
        License Priority: Medium
Index 3 Feature: datak9
        Period left: 8  weeks 4  days
        Period Used: 0  minute  0  second
        License Type: EvalRightToUse
        License State: Active, Not in Use, EULA accepted
        License Count: Non-Counted
        License Priority: Low
<output omitted >
```

Резервное копирование лицензий

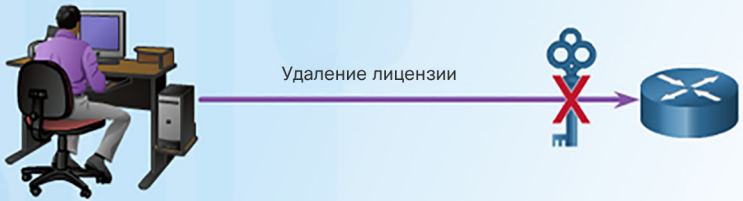
- Команда **license save** используется для копирования всех лицензий на устройстве и их сохранения.
- Чтобы восстановить сохраненные лицензии, используйте команду **license install**.
- Для создания резервной копии лицензии на устройстве используется следующая команда:
  - Router# **license save** *file-sys://lic-location*
- Чтобы проверить, сохранены ли лицензии, используйте команду show flash0:.




```
R1# license save flash0:all_licenses.lic
license lines saved ..... to flash0:all_licenses.lic

R1# show flash0:
-# - --length-- -----date/time------ path
<output omitted>
8   68831808 Apr 2 2013 21:29:58 +00:00
    c1900-universalk9-mz.SPA.152-4.M3.bin
9       1153 Apr 26 2013 02:24:30 +00:00 all_licenses.lic

182390784 bytes available (74096640 bytes used)

R1#
```

Удаление лицензии

Удаление активной и постоянной лицензии



Шаг 1. Отключите технологический пакет.

```
R1(config)# license boot module c1900 technology-package
seck9 disable
R1(config)# exit
R1# reload
```

Шаг 2. Удалите лицензию.

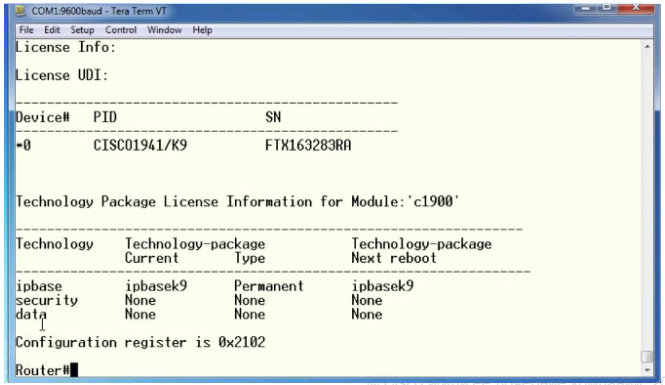
```
R1# license clear seck9
R1# configure terminal
R1(config)# no license boot module c1900 technology-package seck9 disable
R1(config)# exit
R1# reload
```

- Удалить можно только те лицензии, которые были добавлены с помощью команды **license install**.

Демонстрационный видеоролик. Работа с лицензиями на образ IOS 15

Цель:

- Определите дополнительные типы лицензирования маршрутизаторов Cisco ISR G2.
- Определите различия между постоянной лицензией и оценочной лицензией на право использования.
- Активируйте технологический пакет функций обеспечения безопасности на маршрутизаторе Cisco 1941.
- Примите лицензионное соглашение с конечным пользователем.
- Проверьте лицензию securityk9 и сохраните ее во флеш-память.



10.4. Обзор главы

Packet Tracer. Отработка комплексных практических навыков

Глава 10. Устройства — обнаружение, управление и обслуживание

- Для составления топологии сети используйте протоколы обнаружения.
- Настройте NTP и Syslog в сетях предприятий малого и среднего бизнеса.
- Поддерживать конфигурации маршрутизатора и коммутатора, а также файлы IOS.

Новые термины и команды

• CDP (Cisco Discovery Protocol)	• LLDP (Link Layer Discovery Protocol)

Новые термины и команды

• Системный журнал (Syslog) • NTP (Network Time Protocol) • NTP-клиент • NTP server (Сервер NTP) • Программные часы	• Часовой слой (stratum) • Доверенный источник времени • уровень серьезности • facility

Новые термины и команды

• Режим ROMMON • конфигурационный регистр • Услуги по требованию • Ключ активации продукта (PAK) • Активация ПО Cisco IOS • лицензии технологических пакетов • постоянные лицензии	• оценочная лицензия • Лицензионное соглашение с конечным пользователем (EULA) • Cisco License Manager (CLM) • Портал регистрации лицензий Cisco • Уникальный идентификатор устройства (UDI) • Оценочные лицензии на право использования (RTU)


CISCO