

Документ подписан простой электронной подписью
Информация о владельце:
ФИО: Локтионова Оксана Геннадьевна
Должность: проректор по учебной работе
Дата подписания: 17.12.2021 11:16:49
Уникальный программный ключ:
0b817ca911e6668abb13a5d426d39e5f1c11eabbf73e943df4a4851fda56d089

МИНОБРНАУКИ РОССИИ

Федеральное государственное бюджетное образовательное
учреждения высшего образования
«Юго-Западный государственный университет»
(ЮЗГУ)

Кафедра информационной безопасности

УТВЕРЖДАЮ
Проректор по учебной работе
Локтионова
« 6 / 12 / 2017 г.



КОНФИГУРИРОВАНИЕ МАРШУТИЗАТОРОВ

Методические рекомендации по выполнению лабораторной
работы №3
для студентов направления подготовки бакалавриата
10.03.01 «Информационная безопасность»

Курск 2017

УДК 621.(076.1)

Составитель: А.Г. Спеваков

Рецензент

Кандидат технических наук, доцент кафедры
«Информационная безопасность» И.В. Калущкий

Конфигурирование маршрутизаторов [Текст] :
методические рекомендации по выполнению лабораторной работы
/ Юго-Зап. гос. ун-т; сост.: А.Г. Спеваков. – Курск, 2017. – 24 с.:
ил. 12. – Библиогр.: с. 24.

Содержат сведения по вопросам работы в программном
продукте Cisco Packet Tracer. Указывается порядок выполнения
лабораторной работы, правила содержания отчета.

Методические указания соответствуют требованиям
программы, утвержденной учебно-методическим объединением по
специальности.

Предназначены для студентов направления подготовки
бакалавриата 10.03.01 «Информационная безопасность».

Текст печатается в авторской редакции

Подписано в печать . Формат 60x84 1/16.
Усл.печ. л. 1,40. Уч.-изд. л. 1,26. Тираж 100 экз. Заказ. Бесплатно.
Юго-Западный государственный университет.
305040, г.Курск, ул. 50 лет Октября, 94.

1 Получение сведений о маршрутизаторе и его работе

Просмотр информации о маршрутизаторе, такой как модель, объемы памяти, версия IOS, число и тип интерфейсов, выполняется по команде (ниже приведен пример вывода команды и комментарии к нему):

```
Router>show version
```

```
Cisco Internetwork Operating System Software  
IOS (tm) C2600 Software (C2600-JS-M), Version  
12.0(3)T3, RELEASE SOFTWARE (fc1)
```

```
Copyright (c) 1986-1999 by cisco Systems, Inc.
```

```
Compiled Thu 15-Apr-99 17:05 by kpma
```

```
Image text-base: 0x80008088, data-base: 0x80C2D514
```

!Версия IOS, под управлением которой работает маршрутизатор.

```
ROM: System Bootstrap, Version 11.3(2)XA4, RELEASE  
SOFTWARE (fc1)
```

!Сокращенная версия IOS, которая используется в качестве загрузчика (Bootstrap) и находится в ПЗУ.

```
Router uptime is 0 minutes
```

```
System restarted by power-on
```

```
System image file is "flash:c2600-js-mz.120-3.T3.bin" !Файл с  
образом IOS, из которого система была загружена.
```

```
cisco 2621 (MPC860) processor (revision 0x101) with  
24576K/8192K bytes of memory
```

!Модель маршрутизатора.

!Объем оперативной памяти – он выводится в виде двух чисел: объема процессорной памяти (24576 К) и памяти ввода-вывода (8192 К). Общий размер RAM равен их сумме.

```
Processor board ID JAB0402040J (2308906173)
```

```
M860 processor: part number 0, mask 49 Bridging software.
```

```
X.25 software, Version 3.0.0.
```

```
SuperLAT software copyright 1990 by Meridian Technology  
Corp).
```

```
TN3270 Emulation software.
```

```
Basic Rate ISDN software, Version 1.1.
```

2 FastEthernet/IEEE 802.3 interface(s)

2 Serial network interface(s)

32K bytes of non-volatile configuration memory. !Объем NVRAM.

8192K bytes of processor board System flash (Read/Write)

!Объем флэш-памяти.

Configuration register is 0x2102

!Значение конфигурационного регистра.

ВЫПОЛНИТЬ!

1. Запустить в GNS3 образ маршрутизатора серии 7200, добавив в его системный слот расширения slot0 модуль C7200-IO-2FE (два порта Fast Ethernet). Установить с ним консольное соединение.

2. Получить сведения о модели маршрутизатора, версии IOS, файле образа ОС, объеме памяти RAM, NVRAM, значении конфигурационного регистра.

Просмотр содержимого флэш-памяти:

Router>show flash

System flash directory:

File Length Name/status 1 6399468 c2600-dos-mz_120-

4_T.bin

[6399532 bytes used, 1989076 available, 8388608 total]

8192K bytes of processor board System flash (Read/Write.

Мониторинг загрузки процессора (рисунок 1):

Router>show processes.

```

Telnet localhost
Router>show processes
CPU utilization for five seconds: 0%/0%; one minute: 0%; five minutes: 0%
PID QTy PC Runtime (ms) Invoked uSecs Stacks TTY Process
1 Cwe 6002D4AC 0 3 0 5492/6000 0 Chunk Manager
2 Csp 6071B9B4 1000 346 2890 2536/3000 0 Load Meter
3 M* 0 3700 388 9536 8632/12000 0 Exec
4 Mwe 61F19FA0 0 1 0 23392/24000 0 EDDRI_MAIN
5 Lst 6002A800 352 174 2022 5260/6000 0 Check heaps
6 Cwe 60032DFC 0 2 0 5432/6000 0 Pool Manager
7 Mst 61048D04 0 2 0 5496/6000 0 Timers
8 Mwe 600E68B8 0 2 0 8492/9000 0 ATM AutoUC Perio
9 Mwe 600E6238 0 2 0 5492/6000 0 ATM UC Auto Crea
10 Mwe 6011B908 0 30 0 5672/6000 0 IPC Dynamic Cach
11 Mwe 6010FC7C 0 1 0 5548/6000 0 IPC Zone Manager
12 Mwe 6010F7BC 4 1792 2 5700/6000 0 IPC Periodic Tim
13 Mwe 6010F65C 4 1792 2 5524/6000 0 IPC Deferred Por
14 Mwe 6010F9BC 4 1 4000 5496/6000 0 IPC Seat Manager
15 Mwe 60112EEC 0 1 0 5560/6000 0 IPC BackPressure
16 Msi 60267240 20 1791 11 5304/6000 0 EnvMon
17 Mwe 6026E788 0 1 0 8520/9000 0 OIR Handler
18 Mwe 603157DC 0 1 0 23436/24000 0 Crash writer
19 Mwe 60BBD3C4 16 34 470 5300/6000 0 ARP Input
20 Mwe 60C250F4 0 2 0 5492/6000 0 ATM Idle Timer
21 Mwe 61003170 0 2 0 5484/6000 0 AAA high-capacit
--More--

```

Рисунок 1 - Просмотр информации о процессах

Router>show processes cpu.

```

Telnet localhost
Router>show processes cpu
CPU utilization for five seconds: 0%/0%; one minute: 0%; five minutes: 0%
PID Runtime(ms) Invoked uSecs 5Sec 1Min 5Min TTY Process
1 0 3 0 0.00% 0.00% 0.00% 0 Chunk Manager
2 1000 357 2801 0.08% 0.02% 0.04% 0 Load Meter
3 3780 401 9426 0.00% 0.10% 0.27% 0 Exec
4 0 1 0 0.00% 0.00% 0.00% 0 EDDRI_MAIN
5 356 180 1977 0.00% 0.01% 0.00% 0 Check heaps
6 0 2 0 0.00% 0.00% 0.00% 0 Pool Manager
7 0 2 0 0.00% 0.00% 0.00% 0 Timers
8 0 2 0 0.00% 0.00% 0.00% 0 ATM AutoUC Perio
9 0 2 0 0.00% 0.00% 0.00% 0 ATM UC Auto Crea
10 0 31 0 0.00% 0.00% 0.00% 0 IPC Dynamic Cach
11 0 1 0 0.00% 0.00% 0.00% 0 IPC Zone Manager
12 4 1845 2 0.00% 0.00% 0.00% 0 IPC Periodic Tim
13 4 1845 2 0.00% 0.00% 0.00% 0 IPC Deferred Por
14 4 1 4000 0.00% 0.00% 0.00% 0 IPC Seat Manager
15 0 1 0 0.00% 0.00% 0.00% 0 IPC BackPressure
16 20 1844 10 0.00% 0.00% 0.00% 0 EnvMon
17 0 1 0 0.00% 0.00% 0.00% 0 OIR Handler
18 0 1 0 0.00% 0.00% 0.00% 0 Crash writer
19 16 35 457 0.00% 0.00% 0.00% 0 ARP Input
20 0 2 0 0.00% 0.00% 0.00% 0 ATM Idle Timer
21 0 2 0 0.00% 0.00% 0.00% 0 AAA high-capacit
--More--

```

Рисунок 2 - Просмотр информации об использовании процессора

Router>show processes memory.

```

Telnet localhost
Router>show processes memory
Processor Pool Total: 182614268 Used: 18020480 Free: 164593788
I/O Pool Total: 16777216 Used: 2648384 Free: 14128832

PID TTY Allocated Freed Holding Getbufs Retbufs Process
0 0 29945096 11703360 16468128 439 123 *Init*
0 0 12512 132604 12512 0 0 *Sched*
0 0 130516 255936 86824 25 0 *Dead*
1 0 5052 0 12232 0 0 Chunk Manager
2 0 252 252 4180 0 0 Load Meter
3 0 2329396 1998284 349404 4 4 Exec
4 0 65588 0 90768 0 0 EDDRI_MAIN
5 0 3352 252 10340 0 0 Check heaps
6 0 2692 0 9872 45 0 Pool Manager
7 0 252 252 7180 0 0 Timers
8 0 252 252 10180 0 0 ATM AutoUC Perio
9 0 252 252 7180 0 0 ATM UC Auto Crea
10 0 0 0 7180 0 0 IPC Dynamic Cach
11 0 0 0 7180 0 0 IPC Zone Manager
12 0 0 0 7180 0 0 IPC Periodic Tim
13 0 0 0 7180 0 0 IPC Deferred Por
14 0 744 0 7924 0 0 IPC Seat Manager
15 0 0 0 7180 0 0 IPC BackPressure
16 0 0 0 7180 0 0 EnvMon
--More--

```

Рисунок 3 - Просмотр информации об использовании памяти

Второй вариант команды (рисунок 2) выводит более подробную информацию о загрузке процессора (показывает общую усредненную загрузку по каждому процессу за последние 5 секунд, 1 и 5 минут), а третий – о загрузке процессами оперативной памяти (рисунок 3).

Мониторинг общей загрузки памяти (рисунок 4):

Router>show memory.

```

Telnet localhost
0 0 130516 255936 86824 25 0 *Dead*
1 0 5052 0 12232 0 0 Chunk Manager
2 0 252 252 4180 0 0 Load Meter
3 0 2329396 1998284 349404 4 4 Exec
4 0 65588 0 90768 0 0 EDDRI_MAIN
5 0 3352 252 10340 0 0 Check heaps
6 0 2692 0 9872 45 0 Pool Manager
7 0 252 252 7180 0 0 Timers
8 0 252 252 10180 0 0 ATM AutoUC Perio
9 0 252 252 7180 0 0 ATM UC Auto Crea
10 0 0 0 7180 0 0 IPC Dynamic Cach
11 0 0 0 7180 0 0 IPC Zone Manager
12 0 0 0 7180 0 0 IPC Periodic Tim
13 0 0 0 7180 0 0 IPC Deferred Por
14 0 744 0 7924 0 0 IPC Seat Manager
15 0 0 0 7180 0 0 IPC BackPressure
16 0 0 0 7180 0 0 EnvMon

Router>show memory
Head Total(b) Used(b) Free(b) Lowest(b) Largest(b)
Processor 641D8620 182614268 18021000 164593268 164263936 149059836
I/O F0000000 16777216 2648392 14128824 14128824 14128796
--More--

```

Рисунок 4 - Мониторинг общей загрузки памяти

Для каждого пула памяти (процессорного и ввода-вывода) указываются в байтах его объем (Total), объем памяти, используемой в настоящий момент (Used), объем свободной (Free),

а также наименьший объем памяти, когда-либо доступный для выделения из данного пула (Lowest), и размер наибольшего непрерывного блока, доступного для выделения в настоящий момент (Largest).

ВЫПОЛНИТЬ!

3. Получить сведения о используемых процессах, загрузке процессора и памяти.

2 Начальная конфигурация маршрутизатора

В данном пункте приведен набор команд первоначальной конфигурации маршрутизатора (рисунок 5). Для начала необходимо установить имя маршрутизатора, перейдя из пользовательского режима в режим администратора, открываемый командой **enable**, а затем в глобальный режим конфигурирования:

Router(config)#hostname <имя_маршрутизатора>.

Установить пароль администратора (пароль будет требоваться для выполнения команды **enable**):

lab1(config)#enable secret <enable>.

Отключить обращения в DNS (в том случае, если DNS-сервер не используется): **lab1(config)#no ip domain-lookup.**

```
Router(config)#hos
Router(config)#hostname lab1
lab1(config)#enable secret lab1
lab1(config)#no ip domain-lookup
lab1(config)#
```

Рисунок 5 – Начальная настройка маршрутизатора

Сконфигурировать консоль и виртуальные терминалы: отключить таймер неактивности и интерпретацию неизвестных команд как указаний открыть сеанс Telnet, включить режим синхронной регистрации:

lab1(config)#line con 0 lab1(config-line)#exec-timeout 0 0
lab1(config-line)#transport preferred none lab1(config-
line)#logging synchronous.

Обратите внимание, что по умолчанию маршрутизатор выводит сообщения на консоль поверх ввода оператора, и чтобы продолжить ввод команды, оператор должен помнить, в каком

месте его прервали. При использовании команды **logging synchronous** после каждого выведенного сообщения маршрутизатор будет заново выводить часть команды, уже введенной оператором к моменту появления сообщения, и оператор может легко продолжить ввод.

Виртуальный терминал назначается оператору, подключившемуся к маршрутизатору по протоколу Telnet. На доступ через виртуальный терминал следует назначить пароль. Это делается командами:

```
lab1(config-line)#line vty 0 4 lab1(config-line)#login  
lab1(config-line)#password <password>.
```

Из соображений безопасности, если маршрутизатор напрямую подключен к публичным сетям, например Интернет, виртуальные терминалы рекомендуется заблокировать, а доступ к маршрутизатору осуществлять только по консольной линии.

ВЫПОЛНИТЬ!

4. Установить имя маршрутизатора и пароль на вход в привилегированный режим (lab1, enable).

5. Отключить обращения в DNS, таймер неактивности и интерпретацию неизвестных команд.

6. Включить режим синхронной регистрации.

7. Назначить пароль на доступ к маршрутизатору через виртуальный терминал (password).

3 Настройка интерфейсов

Для перехода в режим настройки необходимого интерфейса следует, находясь в глобальном режиме, выполнить команду:

```
lab1(config)#interface <имя_интерфейса>.
```

По умолчанию все интерфейсы маршрутизатора выключены.

Интерфейс включается командой:

```
lab1(config-if)#no shutdown.
```

Работоспособность настроек физического и канального уровней можно проверить командой в контексте администратора:

```
lab1#show interface <имя_интерфейса>.
```

Сообщения об изменении состояния физического и канального уровней любого интерфейса выводятся

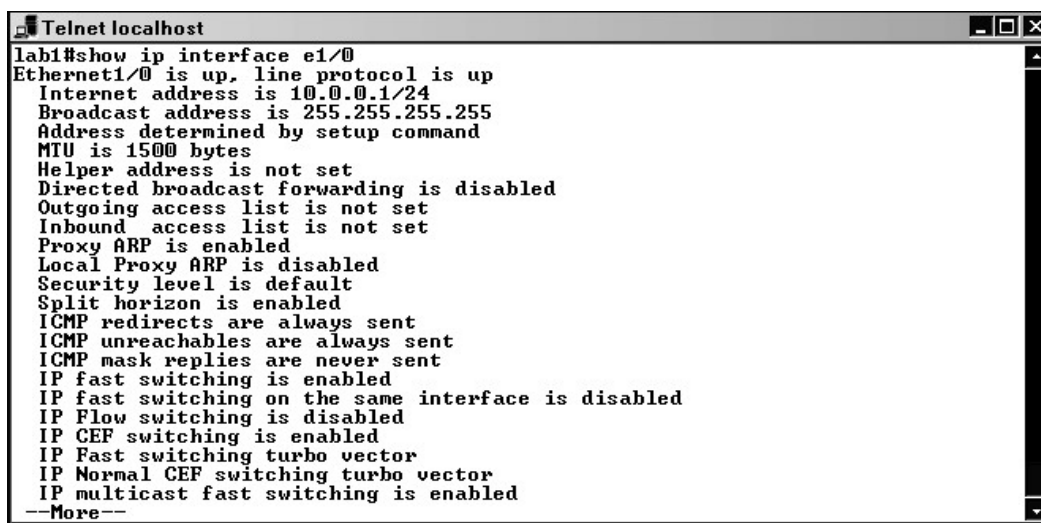
маршрутизатором на консоль. Команда **show interface** также выводит сведения об используемом протоколе канального уровня, IP-адресе и статистику отправленных и полученных данных и ошибок.

Настройка IP-адреса интерфейса (рисунок 6) производится командой: **lab1(config-if)#ip address <адрес> <маска>**.

```
lab1(config-if)#
lab1(config-if)#ip address 10.0.0.1 255.255.255.0
lab1(config-if)#no shu
lab1(config-if)#no shutdown
lab1(config-if)#
*Feb 13 10:32:49.999: %LINK-3-UPDOWN: Interface Ethernet1/0, changed state to up
*Feb 13 10:32:50.999: %LINEPROTO-5-UPDOWN: Line protocol on Interface Ethernet1/0, changed state to up
lab1(config-if)#
```

Рисунок 6 - Настройка IP-адреса интерфейса

Подробная информация о параметрах протокола IP (рисунок 7) доступна в контексте администратора по команде: **lab1#show ip interface <имя_интерфейса>**.



```
Telnet localhost
lab1#show ip interface e1/0
Ethernet1/0 is up, line protocol is up
Internet address is 10.0.0.1/24
Broadcast address is 255.255.255.255
Address determined by setup command
MTU is 1500 bytes
Helper address is not set
Directed broadcast forwarding is disabled
Outgoing access list is not set
Inbound access list is not set
Proxy ARP is enabled
Local Proxy ARP is disabled
Security level is default
Split horizon is enabled
ICMP redirects are always sent
ICMP unreachable are always sent
ICMP mask replies are never sent
IP fast switching is enabled
IP fast switching on the same interface is disabled
IP Flow switching is disabled
IP CEF switching is enabled
IP Fast switching turbo vector
IP Normal CEF switching turbo vector
IP multicast fast switching is enabled
--More--
```

Рисунок 7 - Подробная информация о параметрах протокола IP

Краткая сводная таблица состояний IP-интерфейсов (рисунок 8):

lab1#show ip interface brief.

```

Telnet localhost
IP Normal CEF switching turbo vector
IP multicast fast switching is enabled

lab1#show ip interface brief
Interface              IP-Address      OK? Method Status  Prot
ocol
FastEthernet0/0        unassigned      YES unset  administratively down down
Ethernet1/0            10.0.0.1        YES manual  up      up
Ethernet1/1            192.168.0.1     YES manual  up      up
Ethernet1/2            unassigned      YES unset  administratively down down
Ethernet1/3            unassigned      YES unset  administratively down down
Ethernet1/4            unassigned      YES unset  administratively down down
Ethernet1/5            unassigned      YES unset  administratively down down
Ethernet1/6            unassigned      YES unset  administratively down down
Ethernet1/7            unassigned      YES unset  administratively down down
lab1#

```

Рисунок 8 - Краткая сводная таблица состояний IP-интерфейсов

ВЫПОЛНИТЬ!

8. Произвести настройку интерфейсов FastEthernet 0/0 и FastEthernet 0/1 (192.168.0.1 и 10.0.0.1 со стандартными масками соответственно).

9. Изучить информацию о состоянии интерфейсов.

4 Назначение статических маршрутов

Маршруты, ведущие в сети, к которым маршрутизатор подключен непосредственно, автоматически добавляются в маршрутную таблицу после конфигурирования интерфейса при условии, что интерфейс работоспособен (line protocol up).

Для назначения дополнительных статических маршрутов в контексте глобальной конфигурации вводится команда (одна строка):

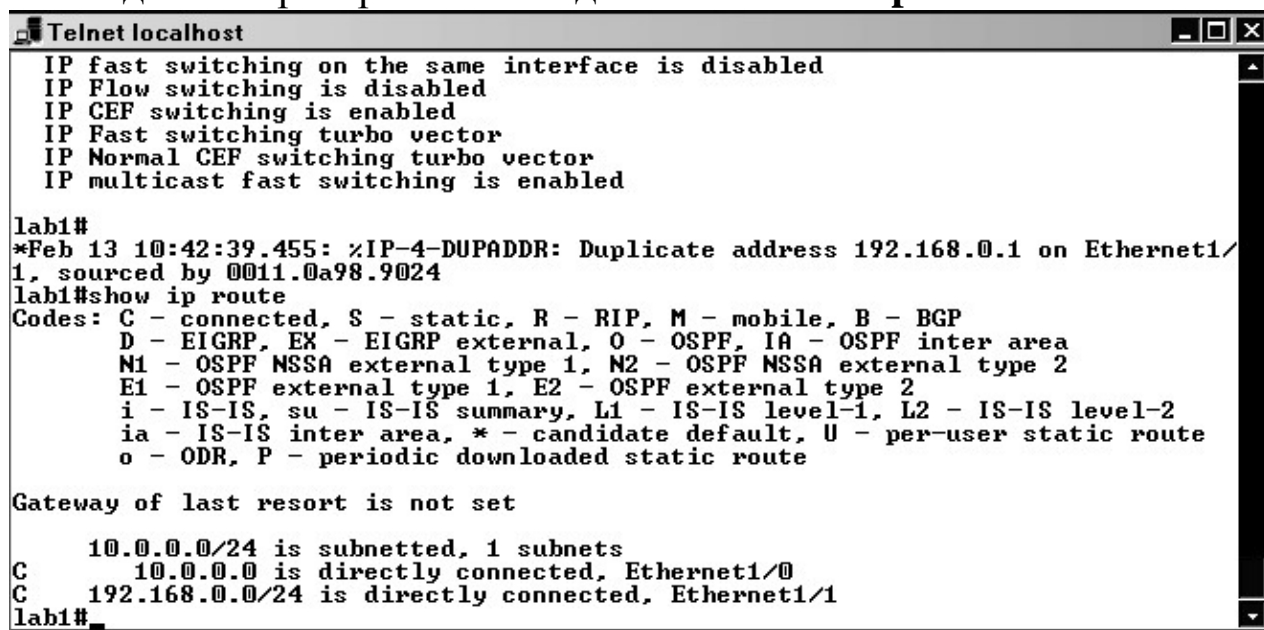
router(config)#ip route <IP-адрес> <маска> <интерфейс> <IP_адрес_следующего_маршрутизатора>.

Маршрут активен только тогда, когда следующий маршрутизатор достижим, то есть существует маршрут в сеть, где находится следующий маршрутизатор. Напротив, статический маршрут будет неактивен, если следующий маршрутизатор не достижим по разным причинам, например, когда его интерфейс находится в нерабочем состоянии.

Управление таблицей маршрутизации на маршрутизаторах в большой распределенной сети является сложной задачей. Поэтому часто используют специальные протоколы маршрутизации. Маршрут по умолчанию назначается командой:

```
router(config)#ip route 0.0.0.0 0.0.0.0 <интерфейс>  
<IP_адрес_следующего_маршрутизатора>.
```

Просмотреть таблицу маршрутов (рисунок 9) можно в контексте администратора по команде: **router#show ip route.**



```
Telnet localhost
IP fast switching on the same interface is disabled
IP Flow switching is disabled
IP CEF switching is enabled
IP Fast switching turbo vector
IP Normal CEF switching turbo vector
IP multicast fast switching is enabled

lab1#
*Feb 13 10:42:39.455: %IP-4-DUPADDR: Duplicate address 192.168.0.1 on Ethernet1/
1, sourced by 0011.0a98.9024
lab1#show ip route
Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route

Gateway of last resort is not set

 10.0.0.0/24 is subnetted, 1 subnets
C    10.0.0.0 is directly connected, Ethernet1/0
C    192.168.0.0/24 is directly connected, Ethernet1/1
lab1#
```

Рисунок 9 - Просмотр таблицы маршрутов

ВЫПОЛНИТЬ!

10. Добавить в схему сети такой же маршрутизатор. Соединить маршрутизаторы с использованием интерфейсов FastEthernet 0/1. Дать новому маршрутизатору имя lab2.

11. Произвести настройку интерфейсов FastEthernet 0/0 и FastEthernet 0/1 маршрутизатора lab2 (192.168.100.1 и 10.0.0.2 со стандартными масками соответственно) – в итоге должна получиться схема сети, изображенная на рисунке 10.

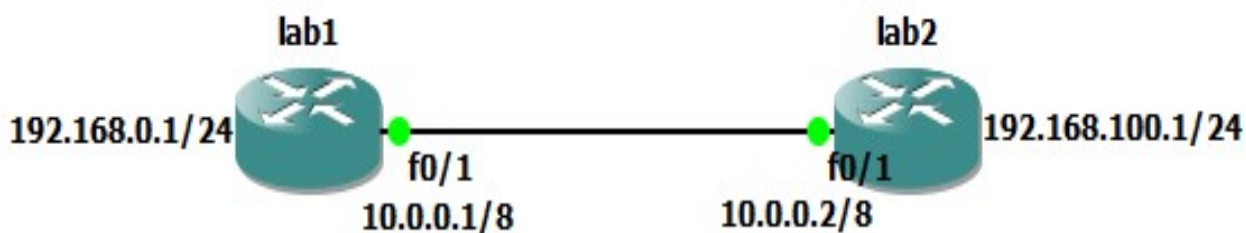


Рисунок 10 - Схема сети с двумя маршрутизаторами

ВЫПОЛНИТЬ!

12. На маршрутизаторе lab2 назначить статический маршрут к сети 192.168.0.0/24. Проверить достижимость 192.168.0.1.
13. Назначить для интерфейса FastEthernet 0/1 маршрутизатора lab1 маршрут по умолчанию. Проверить достижимость 192.168.100.1.
14. Изучить таблицу маршрутов на обоих маршрутизаторах.

5 Настройка точного времени

Часы маршрутизатора сбрасываются при перезагрузке или отключении питания. Старшие модели маршрутизаторов (7xxx и выше) оборудованы аппаратными часами (calendar), по которым программные часы устанавливаются после загрузки маршрутизатора [10]. В дальнейшем, говоря о часах, мы имеем ввиду только программные часы (clock) – именно их показания используются операционной системой, когда, например, ставятся метки времени в диагностических сообщениях.

Поскольку точное время исчисляется по Гринвичу, то предварительно следует установить часовой пояс (относительно Гринвича) и параметры перехода на летнее время (в случае необходимости): **lab1(config)#clock timezone <name> <offset>**
lab1(config)#clock summer-time <name> recurring.

Текущее время на маршрутизаторе можно установить и отобразить с помощью следующих команд соответственно:

lab1#clock set <time> <day> <month> <year> и **lab1#show clock.**

ВЫПОЛНИТЬ

15. Произвести настройку текущего времени на маршрутизаторах lab1 и lab2.

В ряде случаев текущее время на маршрутизаторах необходимо синхронизировать с сервером точного времени, для этого используется протокол NTP.

Маршрутизаторы младших моделей (серии 800, 1700) поддерживают также упрощенную версию этого протокола – SNTP. Естественно, чтобы синхронизация была возможной, необходимо наличие связи с NTP-сервером.

В крупных корпоративных сетях обычно устанавливается собственный сервер точного времени, который синхронизируется от публичных серверов, расположенных в Интернете (списки таких серверов, а также программное обеспечение можно найти на сайте www.ntp.org), в иных случаях можно воспользоваться публичными NTP-серверами напрямую.

Серверы, подключенные непосредственно к источникам точного времени (атомным часам и т. п.), имеют статус stratum 1. Серверы, синхронизирующиеся от этих серверов, имеют статус stratum 2 и т. д. Отсутствие синхронизации обозначается в Cisco как stratum 16.

Маршрутизатор с синхронизированными часами может и сам выступать в роли NTP-сервера: **lab1(config)#ntp master <stratum>**.

Для синхронизации времени с сервером NTP на клиенте используется следующая команда (может быть задан один или несколько серверов): **lab1(config)#ntp server <IP-адрес_NTP_сервера>**.

Обратите внимание, что после настройки NTP, в конфигурационном файле появится команда **ntp clock-period**, содержащая информацию о неточности хода часов, которая обновляется маршрутизатором автоматически и редактировать ее не рекомендуется.

16. Для выполнения следующих упражнений Вам необходимо удалить линк между маршрутизаторами и подключить к ним два облака (Cloud), настроенные на loopback интерфейс вашего

компьютера. Loopback интерфейсу необходимо присвоить ip 10.0.0.5/8. Схема полученной сети представлена на рисунке 11.

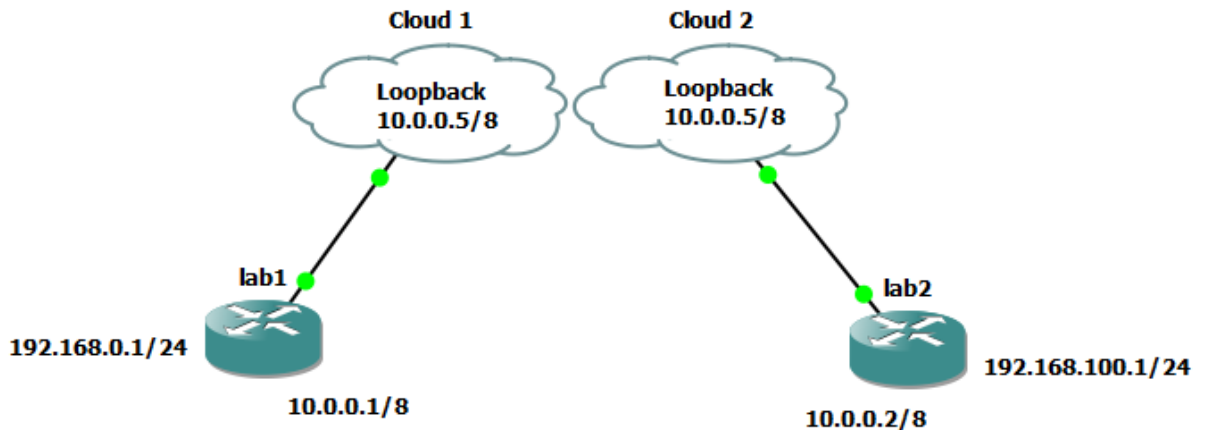


Рисунок 11 - «Улучшенная» схема сети с двумя маршрутизаторами

17. Произвести настройку сервера времени на маршрутизаторе lab1.

18. Настроить на маршрутизаторе lab2 синхронизацию времени с сервером.

Отобразить текущее состояние синхронизации по протоколу NTP можно с помощью команды: **lab1#show ntp status**

Clock is synchronized, stratum 3, reference is 217.107.53.5 ...

(первая строка вывода говорит об успешной синхронизации), а параметры взаимодействия и ассоциации с NTP-серверами выводятся по команде:

lab1#show ntp associations или **lab1#show ntp associations detail.**

19. Захватить сетевой трафик, изучить процесс взаимодействия маршрутизаторов по протоколу NTP.

20. Проанализировать информацию о статусе и ассоциациях NTP на маршрутизаторах lab1 и lab2, сравнить результаты для lab1 и lab2.

Кроме клиент-серверных отношений протокол NTP предусматривает равноправные отношения (symmetric active mode), когда участники процесса учитывают показания часов друг друга и выполняют взаимную синхронизацию, соответствующая конфигурация определяется командой: **lab1(config)#ntp peer <IP-адрес_участника>**.

ВЫПОЛНИТЬ!

21. Настроить взаимную синхронизацию времени по протоколу NTP между lab1 и lab2 (не забудьте предварительно удалить предыдущие настройки NTP).

22. Захватить сетевой трафик, изучить процесс взаимодействия маршрутизаторов по протоколу NTP.

23. Проанализировать информацию о статусе и ассоциациях NTP на маршрутизаторах lab1 и lab2, сравнить результаты lab1 и lab2.

6 Конфигурирование протоколов управления оборудованием

При выполнении заданий данного параграфа используйте схему сети, изображенную на рисунке 11.

7 Сохранение и загрузка файлов конфигурации с использованием протоколов tftp и ftp

ВЫПОЛНИТЬ!

1. Запустить программу 3C Daemon, перейти на вкладку tftp сервера. Запустить захват трафика. В привилегированном режиме на маршрутизаторе lab1 выполнить команду **copy run tftp://10.0.0.5/router-lab1.cfg**. Подтвердить запросы маршрутизатора и дождаться окончания копирования.

2. В окне анализатора трафика найти пакеты, принадлежащие протоколу tftp. Какой транспортный протокол использует tftp? Каким образом передаются команды и содержимое файла?

3. Перейти в рабочий каталог tftp-сервера 3C Daemon (Посмотреть его расположение или изменить можно во вкладке

Configure TFTP Server). Найти только что скопированный файл и открыть его любым текстовым редактором. Этот файл содержит текущую конфигурацию устройства. Найти в файле параметры, установленные Вами в ходе лабораторной работы.

4. На маршрутизаторе lab1 удалить файл стартовой конфигурации (команда **erase startup-config**).

5. Загрузить сохраненный на сервере файл **router-lab1.cfg** в качестве файла стартовой конфигурации (команда **copy tftp: startup-config**).

6. Выполнить пункты 1 ÷ 5 для маршрутизатора lab2, используя протокол ftp. Для возможности сохранения файла конфигурации по протоколу ftp необходимо создать соответствующую учетную запись на сервере (рисунок 12).

Доступ к маршрутизатору по протоколам Telnet и SSH

ВЫПОЛНИТЬ!

7. На маршрутизаторах lab1 и lab2 создать учетную запись пользователя с именем **cisco**, паролем **secret** и уровнем привилегий **0**.

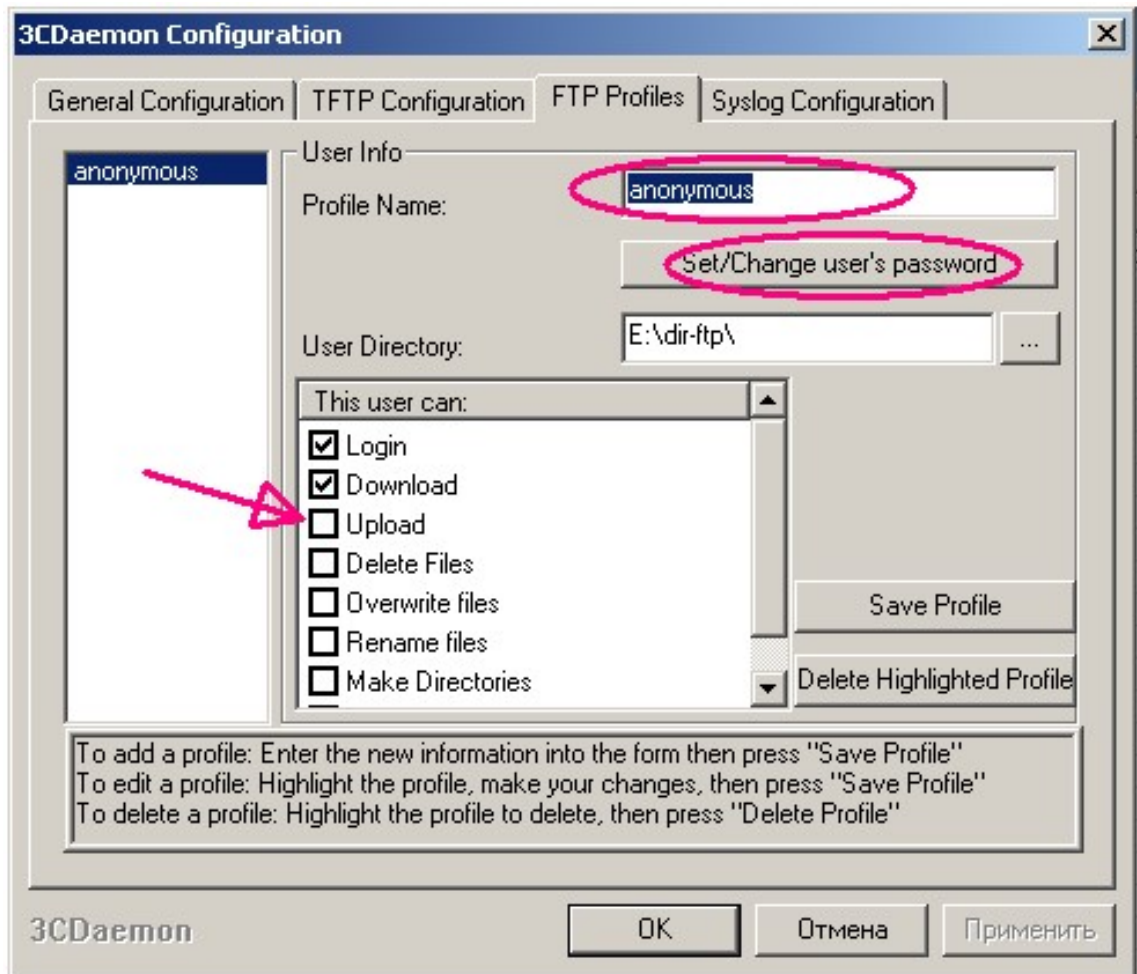


Рисунок 12 - Создание учетной записи на сервере FTP

8. На маршрутизаторах lab1 и lab2 установить пароль **enable** для входа в привилегированный режим.

9. На маршрутизаторах lab1 и lab2 сконфигурировать линии виртуальных терминалов vty0 ÷ vty4 на аутентификацию с использованием локальной базы устройства.

10. Подключиться к маршрутизатору lab1 по протоколу Telnet. В Wireshark проанализировать трафик сессии.

11. Указать на маршрутизаторе lab2 имя домена с помощью команды **ip domain-name <имя>**, где параметр <имя> – это имя произвольного домена, например, lab.net.

12. Сгенерировать ключ шифрования RSA длиной более 1024 бит с помощью команды **crypto key generate rsa**. После выполнения этой команды на маршрутизаторе начинает функционировать сервер SSH.

13. Подключиться к маршрутизатору lab2 по протоколу SSH, используя программу Putty (ярлык на рабочем столе).

В Wireshark проанализировать трафик сессии.

14. Установить для линий виртуальных терминалов маршрутизатора lab2 возможность подключения только с использованием протокола SSH, выполнив команду **transport input ssh**. Убедитесь, что подключение пользователя по протоколу Telnet сбрасывается маршрутизатором.

15. Отобразить и проанализировать с помощью команд **show ssh** и **show ip ssh** информацию о сессиях по протоколу SSH и настройках сервера SSH по умолчанию. **2.3.3. Доступ к маршрутизатору по протоколу HTTP и HTTPS**

ВЫПОЛНИТЬ!

16. На маршрутизаторе lab1 сконфигурировать доступ по протоколу HTTP на аутентификацию с использованием локальной базы устройства с помощью команды **ip http authentication local**.

17. Проверить в текущей конфигурации маршрутизатора запущен ли HTTP-сервер (команда **ip http server**) и в случае необходимости запустить его. Подключиться к маршрутизатору по web-интерфейсу. В Wireshark проанализировать трафик сессии. Изучить возможности web-доступа по конфигурированию устройства.

18. Остановить на маршрутизаторе HTTP-сервер и запустить HTTPS-сервер (команда **ip http secure-server**). Подключиться к маршрутизатору по web-интерфейсу.

В Wireshark проанализировать трафик сессии.

8 Регистрация событий

Диагностические сообщения о системных событиях выводятся маршрутизатором по умолчанию только на консольную линию. Для того чтобы эти сообщения дублировались в виртуальные терминалы (то есть в telnet-соединения), в контексте администратора в соответствующем сеансе используется команда **lab1#terminal monitor**.

При конфигурировании линий виртуальных терминалов для этой цели выполняется команда **monitor**. Вывод сообщений можно направить также во внутренний буфер устройства или на syslog-сервер. Направление в буфер: **lab1(config)#logging buffered <размер>**.

Буфер организован в виде очереди указанного размера (в байтах), самые старые сообщения удаляются из него при поступлении новых. Размер буфера по умолчанию – 4096 байт. Просмотр буфера (и параметров процесса регистрации событий): **lab1#show logging**.

Очистка буфера производится командой **lab1#clear logging**.

Пример отправки сообщений на syslog-сервер:

lab1(config)#logging <IP-адрес сервера> lab1(config)#logging facility local7 lab1(config)#logging trap debugging.

Последние две команды определяют источник сообщений (facility в терминах syslog, используется для определения способа обработки сообщений на сервере) и степень важности (debugging – минимальная) сообщений, протоколируемых в системном журнале.

По умолчанию диагностические сообщения имеют метки времени, которые отсчитываются с момента загрузки устройства (system uptime), поэтому для того чтобы время выводилось в обычном формате (дата, время суток), в конфигурации необходимо указать:

lab1(config)#service timestamps log datetime localtime

lab1(config)#service timestamps debug datetime localtime.

ВЫПОЛНИТЬ!

19. Реализовать вывод диагностических сообщений в виртуальный терминал.

20. Запустить syslog-сервер 3CDaemon.

21. Сконфигурировать маршрутизаторы lab1 и lab2 для отправки на сервер сообщений о **всех** системных событиях, указав различные источники для идентификации маршрутизаторов, например, для lab1 – local1, а для lab2 – local2.

22. Запустить захват сетевого трафика. На маршрутизаторах перейти в режим конфигурации интерфейса FastEthernet0/1, выключить его, а затем через некоторое время снова включить. Какие сообщения получил syslog сервер?

23. Сравнить диагностические сообщения, выводимые в виртуальном терминале и на syslog-сервере.

24. В анализаторе сетевого трафика найти пакеты, относящиеся к протоколу syslog. Какой транспортный протокол используется для их передачи? Какая информация содержится в этих пакетах? Какие механизмы позволяют отследить отправителя пакета, и насколько они надежны?

9 Протокол обнаружения соседних устройств CDP

Протокол CDP используется устройствами Cisco по умолчанию, поэтому в целях безопасности для запрета его функционирования на маршрутизаторе в целом в режиме глобальной конфигурации необходимо ввести команду **no cdp run**. Для использования протокола на конкретных интерфейсах устройства применяется команда **cdp enable** в режиме конфигурирования интерфейса. Параметры функционирования CDP отображаются командой **show cdp** в режиме глобального конфигурирования.

ВЫПОЛНИТЬ!

25. Убедиться, что команда **no cdp run** отсутствует в текущей конфигурации устройства (**show runningconfig**). Запросить у маршрутизатора lab1 информацию о его соседях: **show cdp neighbors**. Какие устройства и каким образом соединены с маршрутизатором? Какую опасность может представлять протокол CDP?

26. Отобразить и проанализировать параметры функционирования протокола CDP по умолчанию.

27. Выполнить команду **show cdp detail**. Какая информация из выведенного перечня была бы полезна для потенциального злоумышленника? Найти в выведенных параметрах IP-адреса соседних устройств.

28. На узле XP_VMnet2 захватить CDP-пакеты, передающиеся через его интерфейс локальной сети. Какой

транспорт используется протоколом CDP? С какой периодичностью передаются сообщения протокола?

10 Использование маршрутизатора в качестве DHCP-сервера

ВЫПОЛНИТЬ!

30. Для запуска на маршрутизаторе сервера DHCP необходимо перейти в режим глобальной конфигурации и включить его командой **service dhcp** (прекращение функционирования сервера производится, соответственно, командой **no service dhcp**). Запустить DHCP-сервер на маршрутизаторе lab1.

31. Создать пул с именем POOL10, из которого будет производиться раздача параметров функционирования клиентов. Для создания пула необходимо в режиме глобальной конфигурации ввести команду **ip dhcp pool <имя>**, где параметр <имя> – название пула, который используется при дальнейшей настройке. После выполнения команды устанавливается режим конфигурирования пула DHCP.

32. Указать сеть, из которой необходимо выдавать адреса, командой **network <сеть> <маска сети>** (используйте 10.0.0.0 255.0.0.0).

33. Указать шлюз по умолчанию для клиентов DHCP:
default-router <IP-адрес> (используйте адрес lab2).

34. Выйти из контекста конфигурации пула. Для настройки исключений DHCP в контексте глобального конфигурирования ввести команду

ip dhcp excluded-address <IP-low> <IP-high>, где IP-low – начальный адрес запрещенного диапазона, а IP-high – его конечный адрес. Данная команда для одной подсети может быть введена несколько раз. Настроить исключения таким образом, чтобы сервер выдавал клиентам адреса с 40 по 90 включительно, кроме адресов 60 ÷ 70 (последний байт адреса).

35. Запустить анализатор Wireshark. На узле XP_VMnet2 в настройках сетевого адаптера указать автоматическое получение IP-адреса. С помощью утилиты **ipconfig** определить, какие настройки получил клиент. Какой срок аренды IP-адреса

устанавливает сервер? В какой момент времени клиент отправит запрос на продление аренды адреса, если подключение к сети будет оставаться активным?

36. Проанализировать сессию захвата трафика. Найти все пакеты, относящиеся к протоколу DHCP. Какие типы DHCP-сообщений были использованы, какие значения установлены в полях адресов отправителя и получателя в кадре Ethernet и пакете IP? Какой транспортный протокол используется для передачи сообщений и какой идентификатор в нем указывает на сообщения протокола DHCP? Какая информация содержится непосредственно в DHCP-пакете?

37. На узле XR_VMnet2 с помощью команды **ipconfig** принудительно обновить адрес. В Wireshark определить, какие типы пакетов были использованы клиентом при обновлении параметров? Какие поля DHCP-пакетов заполнены и какие значения они имеют? Какой адрес получил узел XR_VMnet2 после обновления адреса?

38. С помощью команды **ipconfig** принудительно освободить адрес. В анализаторе трафика определить, какие типы пакетов были использованы при отказе от адреса. Какие поля DHCP-пакетов заполнены и какие значения они имеют?

39. Отключить сетевой адаптер и снова включить его. Какой IP-адрес получил узел XR_VMnet2?

40. На маршрутизаторе lab1 в привилегированном режиме просмотреть список адресов, выданных из пула в аренду (команда **show ip dhcp binding**). Какую информацию

об арендаторах хранит маршрутизатор? Посмотреть статистику работы сервера (команда **show ip dhcp server statistics**) и статистику пула адресов (команда **show ip dhcp pool**). Какие из выведенных параметров Вы можете интерпретировать?

41. С помощью анализатора протоколов определить маршрут передачи пакетов при выполнении команды **ping** с узла XR_VMnet2 в адрес интерфейса FastEthernet 0/0 маршрутизатора lab1 (192.168.0.1).

Вопросы для проверки знаний

1. Какие VLAN существуют по умолчанию в коммутаторе и к каким из них принадлежат его интерфейсы?
2. Можно ли в сети с несколькими коммутаторами при конфигурировании VLAN обойтись без использования стандарта IEEE802.1Q?
3. Каково назначение функции Port Security?
4. В чем преимущество каналов EtherChannel?
5. Для чего необходим протокол STP?
6. Для чего и каким образом конфигурируются статические маршруты?
7. В каких случаях целесообразно использовать маршруты по умолчанию?
8. Каково назначение протокола CDP, в чем преимущества и недостатки его использования в сети?
9. Каковы основные возможности протокола управления сетью SNMP?
10. На основе каких протоколов можно получить удаленный доступ к командной строке IOS устройства, в чем преимущества и недостатки каждого из них?
11. Для какого количества сетей DHCP-сервер на маршрутизаторе может выдавать конфигурационные параметры клиентам?
12. В каких случаях на маршрутизаторах необходимо конфигурировать промежуточные агенты при использовании серверов DHCP?

Библиографический список

1. Защита информации в компьютерных сетях. Практический курс : учеб. пособие / А. Н. Андрончик, В. В. Богданов, Н. А. Домуховский [и др.] ; под ред. Н. И. Синадского. – Екатеринбург : УГТУ-УПИ, 2008. – 248 с.
2. Americas Headquarters Cisco Security MARS Initial Configuration and Upgrade Guide, Release 6.x. – USA : Cisco Systems, 2009. – 136 p.
3. Gary Hallen, G. Kellogg Security Monitoring with Cisco Security MARS. – USA : Cisco Press, 2007. – 335 p.
4. James Burton, Ido Dubrawsky, Vitaly Osipov Cisco Security Professional's Guide to Secure Intrusion Detection Systems. – USA : Syngress Publishing, 2003. – 673 p.
5. Installation Guide for the Cisco Secure PIX Firewall Version 5.2. [Электронный ресурс]. Режим доступа: <http://www.cisco.com>.
6. Install and Setup Guide for Cisco Security Monitoring Analysis and Response System. Release 4.3.x., 2008. [Электронный ресурс]. Режим доступа: <http://www.cisco.com>.
7. Стивенс У. Р. Протоколы TCP/IP. Практическое руководство / пер. с англ. – СПб. : БХВ-Петербург, 2003. – 672 с.
8. Кульгин М. Практика построения компьютерных сетей. Для профессионалов. – СПб. : Питер, 2001. – 320 с.