Сетевое управление и мониторинг

Настройка Cisco

These materials are licensed under the Creative Commons *Attribution-Noncommercial 3.0 Unported* license (http://creativecommons.org/licenses/by-nc/3.0/) as part of the ICANN, ISOC and NSRC Registry Operations Curriculum.

Темы

- Режимы командной строки
- Доступ к конфигурации
- Базовая настройка (имя узла и DNS)
- Аутентификация и авторизация (AAA)
- Сбор логов
- Синхронизация времени (дата/временная зона)
- Настройка SNMP
- Обнаружение подключенных устройств (CDP)
- NetFlow потоки (версии 5 и 9)

Режимы командной строки

Пользовательский

- Ограниченный доступ к роутеру
- Может просматривать определенную информацию, но не может видеть и изменять конфигурацию

```
rtr>
```

Привилегированный

- Полный доступ к состоянию роутера, диагностика, изменение конфигурации и т.д.

```
rtr> enable
rtr#
```

Доступ к роутеру

До настройки SSH

- telnet 10.10.x.254
- логин “cisco” и “cisco” (имя и пароль)

Привилегированный пользователь может использовать привилегированный режим:

- `rtr> enable  (пароль по умолчанию “cisco”)`
- `rtr# configure terminal`
- `rtr(config)#`

Набирайте команды настройки

Выйдите и сохраните новую конфигурацию

- `rtr(config)# end`
- `rtr# write memory`

Доступ к конфигурации

Существует два набора конфигурации:

- ***Running config*** - активная конфигурация, находится в обычной памяти (RAM) и будет потеряна при перезагрузке:

```
rtr# configure terminal          (conf t)
rtr(config)# end
rtr# show running-config         (show run)
```

- ***Startup config***

  Конфигурация, используемая при загрузке. Хранится в NVRAM (сохраняется при перезагрузках):

```
rtr# copy running-config startup-config   (or)
rtr# write memory                 (wr mem)
rtr# show startup-config          (sh start)
```

Базовая настройка (имя узла и DNS)

- **Назначить имя узла**

```
rtr(config)# hostname rtrX
```

- **Назначить домен узла**

```
rtr(config)# ip domain-name ws.nsrc.org
```

- **Назначить сервер DNS**

```
rtr(config)# ip name-server 10.10.0.241
```

- **Или, запретить использование DNS**

```
rtr(config)# no ip domain-lookup
```

запрет dns *очень полезен* для избежания долгого времени отклика

Аутентификация и авторизация

Настройка паролей:

– Пароли хранятся в виде хеш-значений

Пример:

```
# enable secret 0 cisco
# user admin secret 0 cisco
```

Аутентификация и авторизация

Настройка SSH с ключом в 2048 бит (по крайней мере 768 бит для OpenSSH клиентов)

```
rtr(config)# aaa new-model
rtr(config)# crypto key generate rsa   (key size prompt)
```

Проверка создания ключа:

```
rtr# show crypto key mypubkey rsa
```

По желанию, регистрирование событий. Разрешить только SSH второй версии:

```
rtr(config)# ip ssh logging events
rtr(config)# ip ssh version 2
```

Используйте SSH, запретите *telnet* (используйте telnet только если нет другого выхода*)*:

```
rtr(config)# line vty 0 4
rtr(config)# transport input ssh
```

Замечание: в CatOS, вам потребуется запретить telnet явным образом

Сбор логов (syslog*)

Посылать логи на сервер *syslog*:

```
rtr(config)# logging 10.10.x.x
```

Определитесь, какой канал будет использован для логов (от local0 до local7):

```
rtr(config)# logging facility local5
```

События до какого уровня важности вы желаете сохранять?

```
rtr(config)# logging trap <уровень_важности>
```

<0-7>	**Уровни важности логов**	
emergencies	Система непригодна к использованию	(важность=0)
alerts	Нужна немедленная реакция	(важность=1)
critical	Критические ошибки	(важность=2)
errors	Ошибки	(важность=3)
warnings	Предупреждения	(важность=4)
notifications	Обычные, но значимые события	(важность=5)
informational	Информационные сообщения	(важность=6)
debugging	Отладочные сообщения	(важность=7)

*syslog, syslog-ng, rsyslog

Синхронизация времени

Очень важно, чтобы все устройства в сети были синхронизированы по времени

В режиме настройки:

```
rtr(config)# ntp server pool.ntp.org
rtr(config)# clock timezone <временная_зона>
```

Использовать время в UTC (всемирное координированное время):

```
rtr(config)# no clock timezone
```

Если в вашей местности используется переход на летнее время:

```
rtr(config)# clock summer-time recurring last Sun Mar 2:00 last Sun Oct 3:00
```

Проверка:

```
rtr# show clock
        22:30:27.598 UTC Tue Feb 15 2011
rtr# show ntp status
      Clock is synchronized, stratum 3, reference is 4.79.132.217
      nominal freq is 250.0000 Hz, actual freq is 249.9999 Hz, precision is 2**18
      reference time is D002CE85.D35E87B9 (11:21:09.825 CMT Tue Aug 3 2010)
      clock offset is 2.5939 msec, root delay is 109.73 msec…
```

Настройка SNMP

Начните с SNMP версии 2

- Её проще понимать и настраивать
- Пример:

```
rtr(config)# snmp-server community NetManage ro 99
rtr(config)# access-list 99 permit 10.10.0.0 0.0.255.255
```

Настройка SNMP

На машине под управлением Linux (вначале нужно установить snmp-утилиты), выполните:

```
snmpwalk -v2c -c NetManage 10.10.x.254 sysDescr
```

Обнаружение подключенных устройств (CDP)

Включено по умолчанию в большинстве современных роутеров

Если не включено:

```
Rtr(config)# cdp enable
Rtr(config)# cdp run
```

(в старых версиях CISCO IOS)

Посмотреть имеющиеся соседние устройства:

```
rtr# show cdp neighbors
```

Инструменты визуализации/просмотра CDP-оповещений:

tcpdump

cdpr

wireshark

tshark

Включение NetFlow версии 5

Сконфигурируйте потоки NetFlow версии 5 на FastEthernet interface 0/0 и экспортируйте их на 10.10.0.250, порт 9996:

```
rtr# configure terminal
rtr(config)# interface FastEthernet 0/0
rtr(config-if)# ip flow ingress
rtr(config-if)# ip flow egress
rtr(config-if)# exit
rtr(config-if)# ip flow-export destination 10.10.0.250 9996
rtr(config-if)# ip flow-export version 5
rtr(config-if)# ip flow-cache timeout active 5
```

Последняя команда разобьет долгоживущие потоки на пятиминутные фрагменты. Вы можете выбрать любое число минут между 1 и 60. Если вы оставите значение по умолчание (30 минут), отчеты о трафике будут содержать пики.

Note: Более новые версии Cisco IOS поменяли синтаксис этих команд.

Включение информации о наиболее активных пользователях, NetFlow в.5

```
rtr(config)# snmp-server ifindex persist
```

Делает так, что значения ifIndex сохраняются между перезагрузками и если вы добавляете/удаляете интерфейсные модули.

Теперь настройте, как будет выглядеть список наиболее активных пользователей:

```
rtr(config)#ip flow-top-talkers
rtr(config-flow-top-talkers)#top 20
rtr(config-flow-top-talkers)#sort-by bytes
rtr(config-flow-top-talkers)#end
```

Проверьте, что мы только что настроили:

```
rtr# show ip flow export
rt# show ip cache flow
```

Посмотрите список активных пользователей для всех интерфейсов:

```
rtr# show ip flow top-talkers
```

Настройка NetFlow версии 9 для IPv4

Настройте потоки NetFlow в.9 для IPv4 на FastEthernet interface 0/0 и экспортируйте их на 10.10.0.250, порт 9001:

```
rtrX# configure terminal
rtrX(config)# flow exporter EXPORTER-1
rtrX(config-flow-exporter)# description Export to NOC
rtrX(config-flow-exporter)# destination 10.10.0.250
rtrX(config-flow-exporter)# transport udp 9001
rtrX(config-flow-exporter)# template data timeout 300
rtrX(config-flow-exporter)# flow monitor FLOW-MONITOR-V4
rtrX(config-flow-monitor)# exporter EXPORTER-1
rtrX(config-flow-monitor)# record netflow ipv4 original-input
rtrX(config-flow-monitor)# cache timeout active 300
rtr(config)# snmp-server ifindex persist
rtrX(config)# interface FastEthernet 0/0
rtrX(config-if)# ip flow monitor FLOW-MONITOR-V4 input
rtrX(config-if)# ip flow monitor FLOW-MONITOR-V4 output
rtrX(config-if)# exit
rtrX# write memory
```

Настройка NetFlow версии 9 для IPv6

Настройте потоки NetFlow версии 9 для IPv6:

Для этого вам нужно создать новый монитор потоков для IPv6 и присоединить его к интерфейсу и существующим экспортерам.

```
rtrX(config-flow-exporter)# flow monitor FLOW-MONITOR-V6
rtrX(config-flow-monitor)# exporter EXPORTER-1
rtrX(config-flow-monitor)# record netflow ipv6 original-input
rtrX(config-flow-monitor)# cache timeout active 300
rtrX(config)# interface FastEthernet 0/0
rtrX(config-if)# ipv6 flow monitor FLOW-MONITOR-V6 input
rtrX(config-if)# ipv6 flow monitor FLOW-MONITOR-V6 output
rtrX(config-if)# exit
rtrX# write memory
```

Просмотр потоков NetFlow версии 9

Это не команды настройки, а просто несколько примеров просмотра потоков прямо на роутере.

Просмотреть текущую конфигурацию:

```
rtrX# show flow exporter EXPORTER-1
rtrX# show flow monitor FLOW-MONITOR-V4
```

Возможно просмотреть индивидуальные активные потоки на устройстве:

```
rtrX# show flow monitor FLOW-MONITOR-V4 cache
```

Это покажет слишком много потоков. Намжите ‘q’ для выхода. Вы можете видеть наиболее активных пользователей, сгруппированных по исходным и конечным адресам. Это довольно длинная команда:

```
rtrX# show flow monitor FLOW-MONITOR-V4 cache aggregate ipv4 \
      source address ipv4 destination address sort counter   \
      bytes top 20
```

Вопросы?

Для дополнительной информации, смотрите
http://www.cisco.com/en/US/docs/ios/12_2/configfun/configuration/guide/ffun_c.html