ЛАБОРАТОРНАЯ РАБОТА

Цель: познакомится с системой аутентификации авторизации и учета событий – AAA, в программе Cisco Packer Tracer.

Теоретические сведения

AAA (Authentication Authorization and Accounting) — система аутентификации авторизации и учета событий, встроенная в операционную систему Cisco IOS, служит для предоставления пользователям безопасного удаленного доступа к сетевому оборудованию Cisco. Она предлагает различные методы идентификации пользователя, авторизации, а также сбора и отправки информации на сервер.

Однако мало того, что ааа по умолчанию выключена; конфигурация этой системы — дело довольно запутанное. Недочеты в конфигурации могут привести либо к нестабильному, небезопасному подключению, либо к отсутствию какого-либо соединения в принципе

Преимущество конфигурации ааа в том, что она содержит множество методов аутентификации (в отличие от предыдущего случая). Включение ааа происходит путем добавления команды ааа new-model в режиме глобальной конфигурации. Далее предстоит выбор методов аутентификации. Все методы организуются в списки, которым присваивается либо значение default, либо конкретное имя списка (list-name). Таким образом, на разные типы линий (аих, vty, con...) можно «повесить» разные методы аутентификации, разграничив доступ между пользователями.

Пример настройки aaa new-model и списков аутентификации:

Router(config)#aaa new-model

Router(config)#aaa authentication login {default | list-name} method1 [method2...]

Router(config)#line {vty | aux | con...} line-numbers

Router(config-line)#login authentication {default | list-name}

Методы

Как было сказано ранее, методов аутентификации в ааа довольно много. Попробуем перечислить наиболее распространенные:

- Local база данных логинов и паролей храниться на самом сетевом устройстве. Требует username {password | secret}.
- Local-case тот же самый метод, что и local, но чувствительный к регистру при ввде логина.
 - Enable для аутентификации требуется enable {password | secret}.
- Line для аутентификации требуется пароль line (см. рис. 4 способ аутентификации "line")

- None аутентификация не требуется, доступ к устройству предоставляется без ввода логина и пароля.
- Group {tacacs+ | radius} подключение серверов с установленным Tacacs Наиболее интересным методом аутентификации является group: он довольно часто встречается в средних и крупных компаниях.

Ниже представлен пример настройки метода group, который обязательно должен реализовываться в совокупности со списками аутентификации.

Пример добавления группы серверов и частного сервера

Radius:Router(config)#aaa authentication login default group servradius1

Router(config)#aaa group server radius servradius1

Router(config-sg-radius)#server 192.168.1.1

Router(config-sg-radius)#server 192.168.1.2

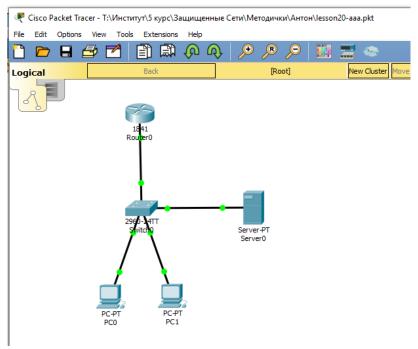
Router(config-sg-radius)#server 192.168.1.3

Router(config-sg-radius)#server-private 192.168.1.10

На этом примере видно, что настроены три Radius-сервера. Но возникает вопрос: как они будут работать? Первое, что приходит в голову: скорее всего, они будут работать по очереди: при недоступности 192.168.1.1 идет обращение к 192.168.1.2 и т. д. Но это не так. В данном примере допущена ошибка: 192.168.1.1, 192.168.1.2, 192.168.1.3 настроены некорректно, а поэтому в аутентификации использоваться не будут. В данной конфигурации не хватает команды Router(config)#radius-server host для каждого из серверов.

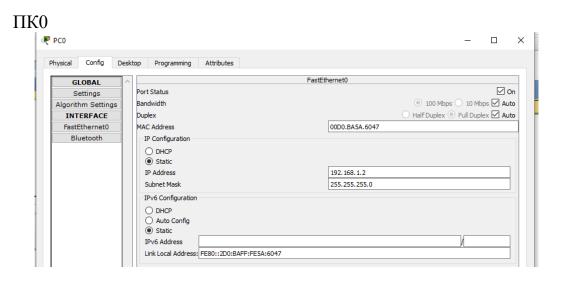
Практическое задание

Данная лабораторная работа может быть выполнена на реальном оборудовании или в Cisco Packet Tracer. Все необходимые действия указаны по порядку их выполнения.



Для начала создадим простую сеть, состоящую из 2 ПК, одного маршрутизатора, коммутатора и сервера, который будет выступать в роли AAA-сервера.

Настроим ір адреса на наших устройствах в соответствии со скриншотами ниже



ПК1

₹ PC1		- 🗆 X
Physical Config Desk	ktop Programming Attributes	
GLOBAL ^		FastEthernet0
Settings	Port Status	☑ On
Algorithm Settings	Bandwidth	100 Mbps 10 Mbps Auto
INTERFACE	Duplex	○ Half Duplex ◎ Full Duplex ☑ Auto
FastEthernet0	MAC Address	0001.43AE.0A0D
Bluetooth	IP Configuration	
	O DHCP	
	Static	
	IP Address	192.168.1.3
	Subnet Mask	255.255.255.0
	IPv6 Configuration	
	O DHCP	
	O Auto Config	
	Static	
	IPv6 Address	/
	Link Local Address: FE80::201:43FF	:FEAE:A0D

Маршрутизатор

Router0		– 🗆 X
Physical Config C	LI Attributes	
GLOBAL	^	FastEthernet0/1
Settings	Port Status	☑ On
Algorithm Settings	Bandwidth © 100 Mbps © 10 Mbps 🗹 A	
ROUTING	Duplex	○ Half Duplex ◎ Full Duplex ☑ Auto
Static	MAC Address	0001.9634.D802
RIP	IP Configuration	
SWITCHING	IP Address	192.168.1.1
VLAN Database	Subnet Mask	255.255.255.0
INTERFACE		
FastEthernet0/0	To Dine Limit	10
FastEthernet0/1	Tx Ring Limit	10

☑ On

Серве	ep –							
(₹ Server0						-	- 0
	Physical Config 5	Servio	es Desktop	Programming	Attributes			
	GLOBAL	^				FastEthernet0		
	Settings		Port Status					✓ On
	Algorithm Settings		Bandwidth				100 Mbps	10 Mbps 🗹 Auto
	INTERFACE		Duplex				O Half Duplex O Ful	l Duplex 🗹 Auto
	FastEthernet0		MAC Address			0060.3EE1.E04E		
			TP Configuration	nn .				

O DHCP
Static

IPv6 Configuration DHCP
Auto Config
Static IPv6 Address

Link Local Address: FE80::260:3EFF:FEE1:E04E

Первым делом настроим наш роутер. Зайдем в него, на вкладку CLI и настроим Local Database. Выполним следующие команды.

192.168.1.4 255.255.255.0

en conf t enable secret cisco username admin privilege 15 secret cisco aaa new-model aaa authentication login default local exit

```
Router#
Router#en
Router#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#enable secret cisco
Router(config)#username admin privilege 15 secret cisco
Router(config)#aaa new-model
Router(config)#aaa authentication login default local
Router(config)#exit
Router#
%SYS-5-CONFIG_I: Configured from console by console
```

Попробуем подключиться к роутеру через telnet, для этого зайдем на PC0, вкладка Desktop -> Command Prompt. Введем следующую команду.

telnet 192.168.1.1.

Логин – admin, пароль – cisco

```
Connection refused by remote host
PC>
PC>
PC>telnet 192.168.1.1
Trying 192.168.1.1 ...Open

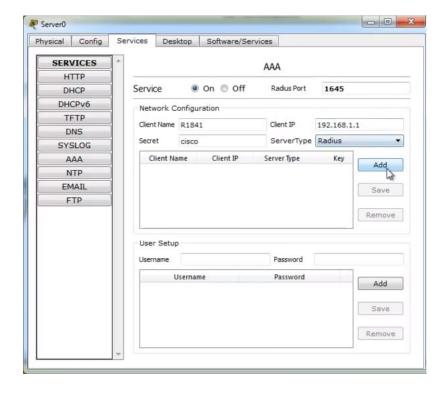
User Access Verification

Username: admin
Password:
Router>
Router>
```

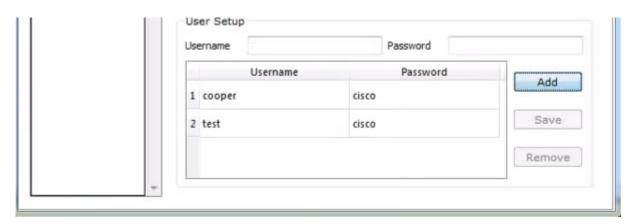
Видим, что подключение прошло.

Теперь настроим AAA-Сервер. Для этого зайдем на устройство Server-PT, на вкладку Services -> AAA.

Заполняем следующими данными, как на скриншоте ниже. И нажимаем на кнопку добавить.



Теперь создадим саму базу пользователей. Username – cooper, Password – cisco. И Username – test, password – cisco.



Возвращаемся на Router0, вкладка CLI и выполняем следующие команды.

```
en
conf t
no aaa authentication login default local
aaa authentication login default group radius local
end
exit
conf t
radius-server host 192.168.1.4 key cisco
end
```

Пробуем зайти под локальными данными. Логин – admin, пароль – cisco.

User Pass % Lo	Access Verification name: admin word: gin invalid	Ι	E	
			Copy Paste	

Видно, что аутентификация не проходит, потому что мы настроили аутентификацию, через Radius-сервер, а такой пользователь у нас там отсутствует.

Под пользователем cooper и паролем cisco, мы успешно попадаем на роутер.



Вывод: в данной лабораторной работе мы успешно настроили аутентификации через ААА-сервер

Контрольные вопросы

- 1. Сформируйте определение ААА-сервера.
- 2. Что такое аутентификация и авторизация?
- 3. Что такое telnet?
- 4. Перечислите методы аутентификации в ААА.