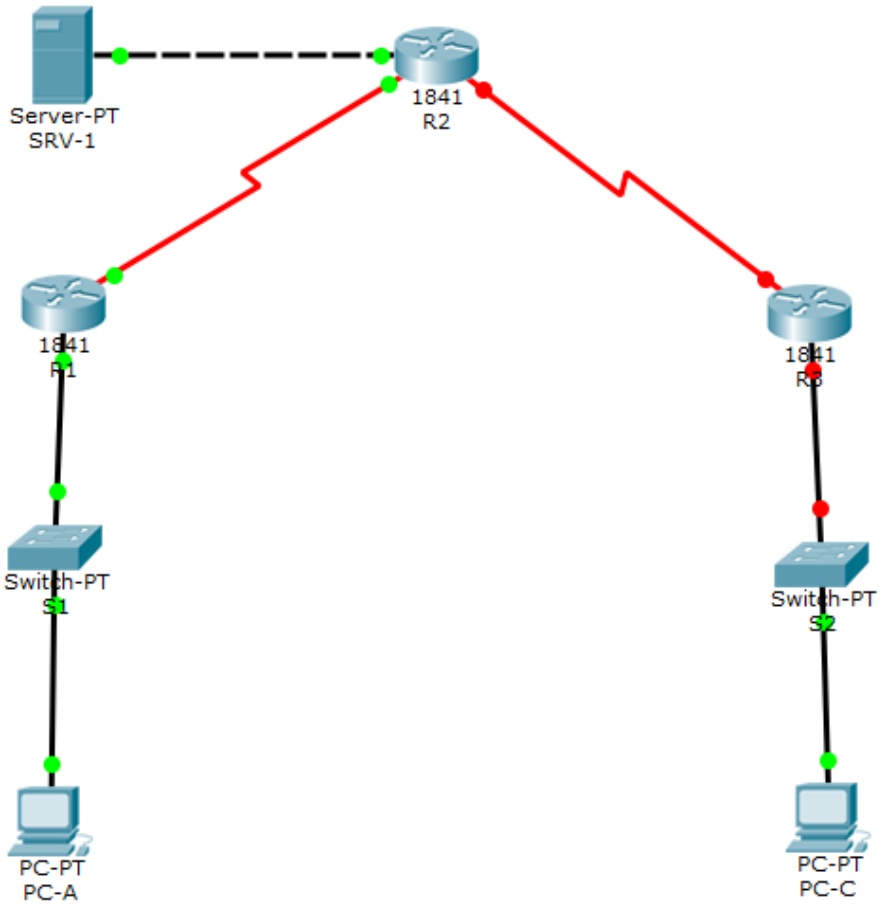
Конфигуриране на AAA

Топология



IP Addressing Table

Device	Interface	IP Address	Subnet Mask	Default Gateway	Switch Port
R1	FA0/1	192.168.1.1	255.255.255.0	N/A	S1 FA0/5
	S0/0/0 (DCE)	10.1.1.1	255.255.255.252	N/A	N/A
R2	S0/0/0	10.1.1.2	255.255.255.252	N/A	N/A
	S0/0/1 (DCE)	10.2.2.2	255.255.255.252	N/A	N/A
	FA0/1	192.168.4.1	255.255.255.0	N/A	N/A
R3	FA0/1	192.168.3.1	255.255.255.0	N/A	S3 FA0/5
	S0/0/1	10.2.2.1	255.255.255.252	N/A	N/A
PC-A	NIC	192.168.1.3	255.255.255.0	192.168.1.1	S1 FA0/6
PC-C	NIC	192.168.3.3	255.255.255.0	192.168.3.1	S3 FA0/18
SRV-1	NIC	192.168.4.4	255.255.255.0	192.168.4.1	R2 FA0/0

Цел на упражнението

Запознаване с основите на технологиите AAA (authentication, authorization, accounting) и протокола RADIUS, както и приложението им в Cisco устройства. За целта ще се използва симулационна програма Cisco Packet Tracer.

Теория

1. Аутентикация

Аутентикацията (Authentication) е проверка на идентичността, която даден потребител, процес или машина твърдят, че имат. Следващите нива при контрола на достъпа зависят от аутентикацията. На базата на нея се извършва оторизацията, т.е дават се права на точно дадената идентичност. Отчетността също няма да работи, без да я има аутентикацията.

Нивото на аутентикация, необходимо за дадена система, зависи от изискванията за сигурност, идващи от самата нея. Например публично достъпните уеб сървъри могат да позволяват анонимен достъп, както и достъп за гости. Финансовите транзакции трябва да изискват много силна аутентикация. Пример за слаба форма на аутентикация е използването на IP адрес за определянето на идентичност. Подмяната или нелегалното използване на IP адреса може лесно да излъже този механизъм. Силната форма на аутентикация изисква поне два фактора за доказване на идентичността:

- Какво знае човек: пароли и лични идентификационни номера (PIN кодове) са пример за това какво човек може да знае. Паролите могат да бъдат за еднократно или многократно използване. S/Key е пример за система за еднократни пароли (http://en.wikipedia.org/wiki/S/KEY).

- Какво притежава човек: Различни хардуерни устройства или софтуерни приложения: Смарт карти, SecureID, CRYPTOCard и SafeWord.

- Кой е човекът: Биометричните характеристики са това, което показва кой точно е човекът, защото разпознаването на идентичността се базира на физическите му характеристики: например сканиране на дланта, геометрия на ръката, сканиране от ириса на окото, модел на ретината, отпечатъци от пръсти, модел на гласа, разпознаване на лице или подпис.

Съществуват много системи за мрежова аутентикация. TACACS+ (Terminal Access Controller Access System), Kerberos и RADIUS (Remote Access Dial In User Service) са протоколи за аутентикация, поддържани от Сиско. Тези системи за аутентикация могат да бъдат конфигурирани да използват много от примерите за установяване на идентичността, посочени по-горе.

Няколко протокола за маршрутизация, които се използват от Сиско устройства, поддържат аутентикация:

- Open Shortest Path First (OSPF)
- Routing Information Protocol version 2 (RIPv2)
- Enhanced Interior Gateway Routing Protocol (Enhanced IGRP)
- Border Gateway Protocol (BGP)
- Intermediate System-to-Intermediate System (IS-IS)

2. Оторизация

Оторизацията (Authorization) е привилегията да се разрешава достъп до услуги или информация само за определени групи или личности. За системи, които трябва да поддържат високо ниво на сигурност, нивото на достъп по принцип трябва да бъде забранено за всички, като изключенията се добавят допълнително. Дори и добавени допълнително, правилата за достъп трябва да са на принципа на най-малкото, което е нужно на даден човек. За публични системи оторизация може да се даде и на гости или анонимни потребители. Нужно е да се определят изискванията за сигурност, за да се изяснят подходящите граници на оторизация.

3. Отчетност

Отчетността (Accounting) е записването на цялата мрежова дейност и всички опити -успешни и неуспешни за достъп до мрежовите ресурси. Въпреки, че тази информация може да се използва за сметки и фактуриране, от гледна точка на сигурността, тя е най-важна за засичане, анализиране и реагиране на инциденти със сигурността в мрежата. Системни логове, периодични прегледи и оценки на състоянието на компонентите на мрежата, както и различните софтуери, заедно могат да се използват за следене какво се случва, когато даден потребител се логне в системата.

4. RADIUS

RADIUS (Remote Access Dial In User Service) се ползва като стандарт за идентификация и отчет на потребителите. Той се базира на модел клиент/сървър, предполагащ, че промишленият комутатор се явява клиент. Комутаторът изпраща запитване до централния RADIUS сървър и на базата на съществуващата информация за потребителя разрешава достъп до определени мрежови ресурси или да откаже такъв. Защитеното взаимодействие между комутатора и RADIUS сървъра се обезпечава чрез взаимна автентификация с използване на „общ секрет“ и шифриране на предаваните данни. RADIUS поддържа редица процеси за автентификация и е способен да обработва и предава множество разширяеми атрибути на потребителите.

RADIUS може да служи за решаване на следните задачи за автентификация:

- контрол на достъпа по MAC адрес;
- IEEE 802.1x;
- отчет;
- администриране посредством Telnet.

В последния случай RADIUS сървърът определя кой от потребителите има право на четене или четене/запис при достъпа до интерфейса за управление на комутатора. Това изключва необходимостта от конфигуриране на пароли за отделните промишлени комутатори.

Required Resources

- 3 routers (Cisco 1841 with Cisco IOS Release 12.4(20)T1 or comparable)
- 2 switches (Cisco 2960 or comparable)
- PC-A: Windows XP, Vista or Windows 7 with CCP 2.5 & RADIUS server software available
- PC-C: Windows XP, Vista or Windows 7 with CCP 2.5
- Serial and Ethernet cables as shown in the topology
- Rollover cables to configure the routers via the console

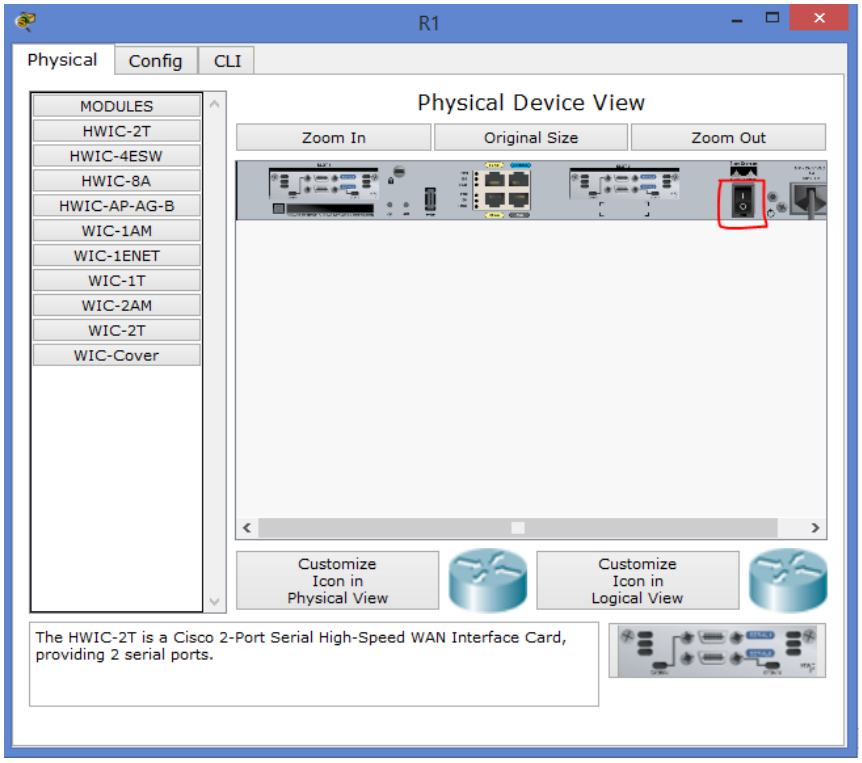
Практическа задача

Част 1: Базова конфигурация на устройствата

В първата част на упражнението ще се конфигурират имена и адреси на отделните интерфейси на рутери, статични пътища по подразбиране, парола за telnet сесии, конзолата и различните режими на работа.

Стъпка 1: Свързване на кабелите и пускане на устройствата.

Свържете устройствата как е показано на топологията. След като това кликнете на R1 и в раздела Physical може да видите самият рутер. Кликнете на Power бутона, за да го включите.



Стъпка 2: Основни настройки за всички рутери.

a. При първоначално зареждане ще ви опита: Continue with configuration dialog? [yes/no]: no

b. Конфигурирайте имена на устройствтата R1, R2 и R3.

c. Конфигурирайте адреси на интерфейсите на рутерите, като използвате таблицата в началото на упражнението.

d. За да предотвратите рутера да се опитва да превежда неправилно въведените команди, като имена на хостове, деактивирайте DNS търсенето на всички рутери.

R1(config)# **no ip domain-lookup**

Стъпка 3: Конфигуриране на EIGRP протокол на R1, R2, и R3.

a. На R1, използвайте следните команди.

R1(config)# **router eigrp 101**
R1(config-router)# **network 192.168.1.0 0.0.0.255**
R1(config-router)# **network 10.1.1.0 0.0.0.3**
R1(config-router)# **no auto-summary**

b. На R2, използвайте следните команди.

R2(config)# **router eigrp 101**
R2(config-router)# **network 10.1.1.0 0.0.0.3**
R2(config-router)# **network 10.2.2.0 0.0.0.3**
R2(config-router)# **network 192.168.4.0 0.0.0.255**
R2(config-router)# **no auto-summary**

c. На R3, използвайте следните команди.

R3(config)# **router eigrp 101**
R3(config-router)# **network 192.168.3.0 0.0.0.255**
R3(config-router)# **network 10.2.2.0 0.0.0.3**
R3(config-router)# **no auto-summary**

Стъпка 4: Конфигурирайте компютрите PC-A и PC-C.

Конфигурирайте статични адреси. (в таблицата по-горе са показани адресите

Стъпка 5: Проверете връзката между компютрите и рутерите.

a. Ping от R1 до R3 (192.168.3.1).

b. Ping от PC-A до R1 LAN (192.168.1.1) от PC-C до R3 LAN (192.168.3.1).

Стъпка 6: Конфигурирайте минимална дължина на използваните пароли.

Изполвайте командата **security passwords, за да конфигурирате минимална дължина паролата от 10.**

R1(config)# **security passwords min-length 10**

Стъпка 7: Конфигурирайте конзолата и VTY сесиите.

Използвайте командата exec-timeout, за да конфигурирате при 5 минути неактивност да ви изключи автоматично. За да синхронизирате нежелани съобщения и съобщенията от debug-а използвате командата logging synchronous.

a. Парола за конзолата

```
R1(config)# line console 0
R1(config-line)# password ciscoconpass
R1(config-line)# exec-timeout 5 0
R1(config-line)# login
R1(config-line)# logging synchronous
```

b. Парола за Telnet сесии

```
R1(config)# line vty 0 4
R1(config-line)# password ciscovtypass
R1(config-line)# exec-timeout 5 0
R1(config-line)# login
```

a. Повторете командаите и на R2 и R3.

Стъпка 8: Криптирайте паролите, които са в чист текстови вид на всичко три устройства.

Използвайте командата **service password-encryption, за да криптирате паролите на конзолата, VTU и AUX**.

```
R1(config)# service password-encryption
```

Стъпка 9: Запате текущата конфигурацията на всичи три устройства.

```
R1# copy running-config startup-config
```

Част 2: Конфигуриране на локална аутентикация

Във втората част на упражнението ще конфигурирате локална база с потребители и техните пароли. Ще промените достъпа през конзолата и телнет сесиите, за да използват локалните потребители на рутера.

Стъпка 1: Конфигуриране на локален потребител.

```
R1(config)# username user01 secret user01pass
```

Стъпка 2: Конфигуриране на локална аутентикация за конзолата и входа на R1.

a. Конфигуриране на конзолата.

```
R1(config)# line console 0
R1(config-line)# login local
```

b. Излезте от устройството:

```
R1 con0 is now available. Press RETURN to get started.
```

Стъпка 3: Конфигуриране на локална аутентикация на телнет сесиите на R1.

a. Конфигуриране на телнет сесиите:

```
R1(config)# line vty 0 4
R1(config-line)# login local
```

b. Влезте от PC-A, чрез telnet в R1.

```
PC-A> telnet 192.168.1.1
```

c. Ако е успешен входа прекратете сесията с командата **exit**.

Стъпка 4: Запазете конфигурацията на R1.

```
R1# copy running-config startup-config
```

Стъпка 5: Направете стъпки от 1 до 4 и за R3 и

```
R3# copy running-config startup-config
```

Част 3: Конфигуриране на локална аутентикация използвайки AAA на рутер R3

Задача 1: Конфигуриране на локален потребител в базата използвайки Cisco IOS

Стъпка 1: Конфигуриране на локален потребител.

```
R3(config)# username Admin01 privilege 15 secret Admin01pass
```

Задача 2: Конфигурирайте AAA.

Стъпка 1: Стартирайте услугата AAA.

```
R3(config)# aaa new-model
```

Стъпка 2: Имплементирайте AAA за конзилата, така че да използва локалните потребители.

a. Конфигуриране.

```
R3(config)# aaa authentication login default local none
```

b. Излезте от устройството: **R3 con0 is now available, Press RETURN to get started**.

Стъпка 3: Създайте профил за телнет сесии, които да ползват локални потребители.

a.

```
R3(config)# aaa authentication login TELNET_LINES local
R3(config)# line vty 0 4
R3(config-line)# login authentication TELNET_LINES
```

b. Проверете дали можете да се свържете от PC-C до R3 чрез телнет.

```
PC-C> telnet 192.168.3.1
Trying 192.168.3.1 ... Open
```

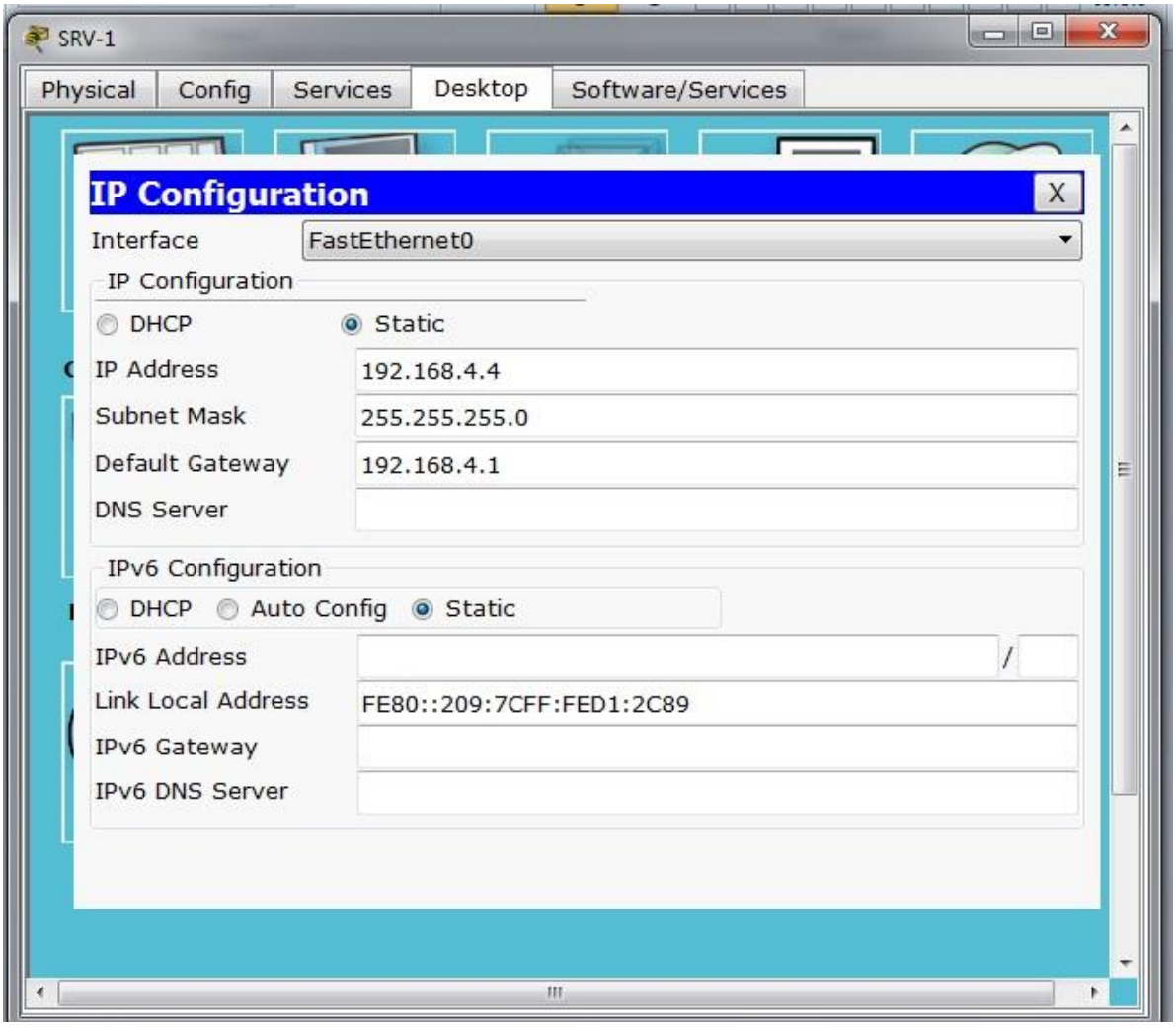
Част 4: Конфигуриране на централизирана аутентикация чрез AAA и RADIUS.

В четвъртата част на упражнението ще се конфигурира R2 да изпозлва Radius сървър.

Задача 1: Конфигурирайте SRV-1.

Стъпка 1: Конфигурирайте адреси на SRV-1.

Използвайте данните от таблицата в началото на упражнението, за да конфигурирате адресите на SRV-1.



Стъпка 2: Добавете клиенти в конфигурацията на radius-а.

a. Добавете клиент за връзка към radius-а. Отваряте SRV-1, кликате на Services и избирате от менюто в ляво AAA. След това трябва да добавите клиент, с параметри:

   Client Name: R2

   Client IP: 192.168.4.1

   Secret: radius

   ServerType: Radius

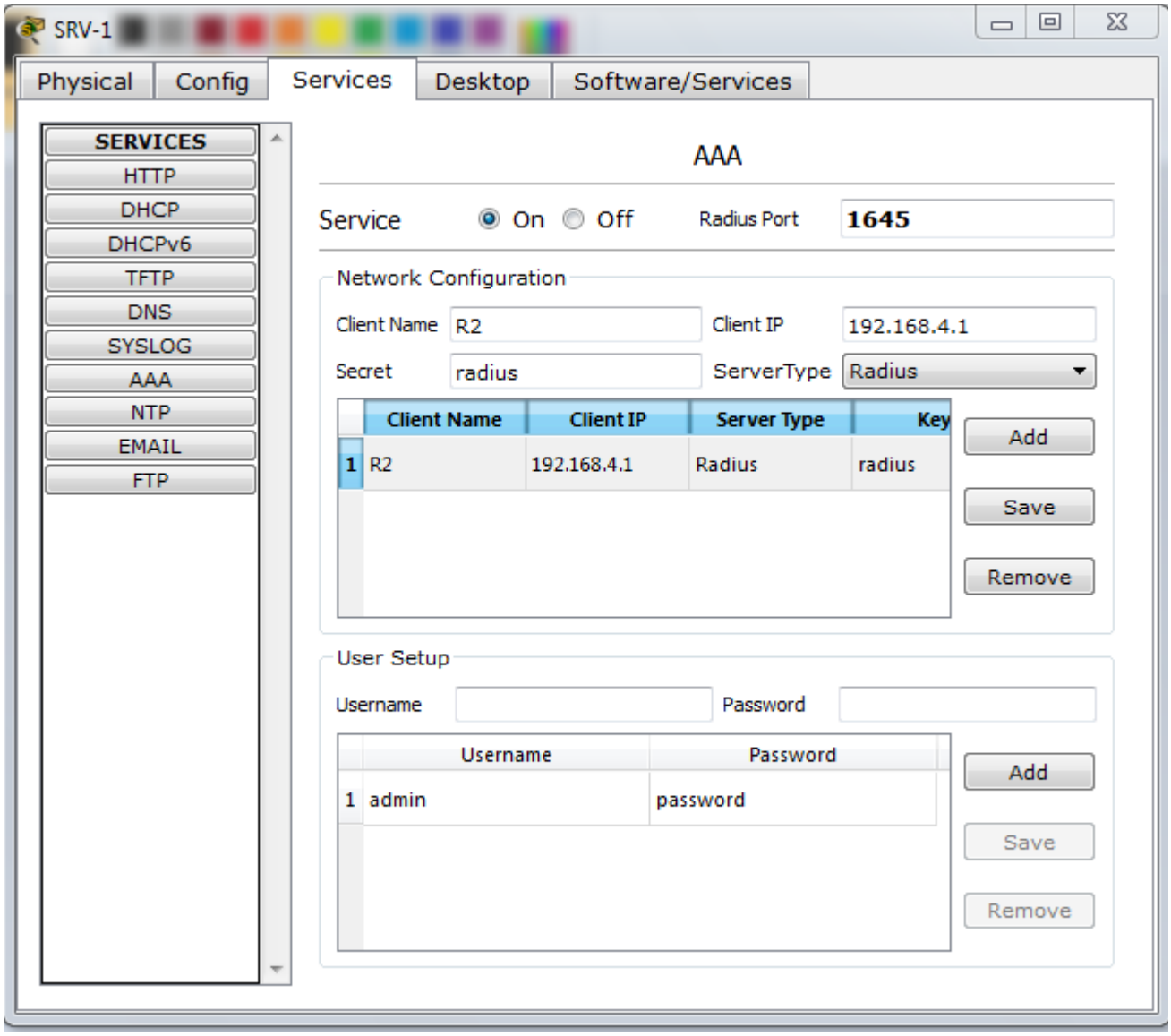
   И натиснете бутона Add.

b. Добавете потребител:

   Username: admin

   Password: password

   И натиснете бутона Add.



a. Close the RadiusTest application.

Задача 2: Конфигуриране на R2 AAA и Radius използвайки Cisco IOS.

Стъпка 1: Стартирайте услугата AAA.

```
R2(config)# aaa new-model
```

Стъпка 2: Конфигурирайте лист по подразбиране за аутентикация.

a. Конфигурирате листа в която указвате реда на аутентикация – първо да бъде radius. Ако няма съвпадение в радиус сървъра, то не ви допуска в устройството.

```
R2(config)# aaa authentication login default group radius none
```

Стъпка 3: Конфигуриране на връзката към RADIUS сървъра.

```
R2(config)# radius-server host 192.168.4.4 key radius
```

Задача 3: Тествайте конфигурацията.

Стъпка 1: Проверет дали имате връзка до RADIUS server от PC-A.

Направете ping от PC-A до SRV-1 (192.168.4.4).

Стъпка 2: Тествайте връзка до R2.

a. Влезте в PC-A и от Command Promnt направете телнет връзка към R2. Използвайте командата: **telnet 192.168.4.1** и потребителското име и парола, които зададохте в Radius сървъра**.**

PC>telnet 192.168.4.1

Trying 192.168.4.1 ...Open

User Access Verification

Username:

b. Имате ли успешна връзка?

Резултати

След приключване на упражнението студентите ще имат познания в изграждането на сигурни мрежи с локален или отдалечен контрол на достъп чрез технологията AAA и радиус и приложението им върху Cisco устойства.

Използвана литература

1. Cisco Security v1.1
2. Компютърни мрежи и комуникации – Иван Цонев, Станимир Станев
3. Дебра Литълджон Шиндър – „Компютърни мрежи”
4. James S Tiller :VPN - A Technical Guide to IPSec Virtual Private Networks
5. WWW
   - www.cisco.com