

Lab 0

ASA Firewall

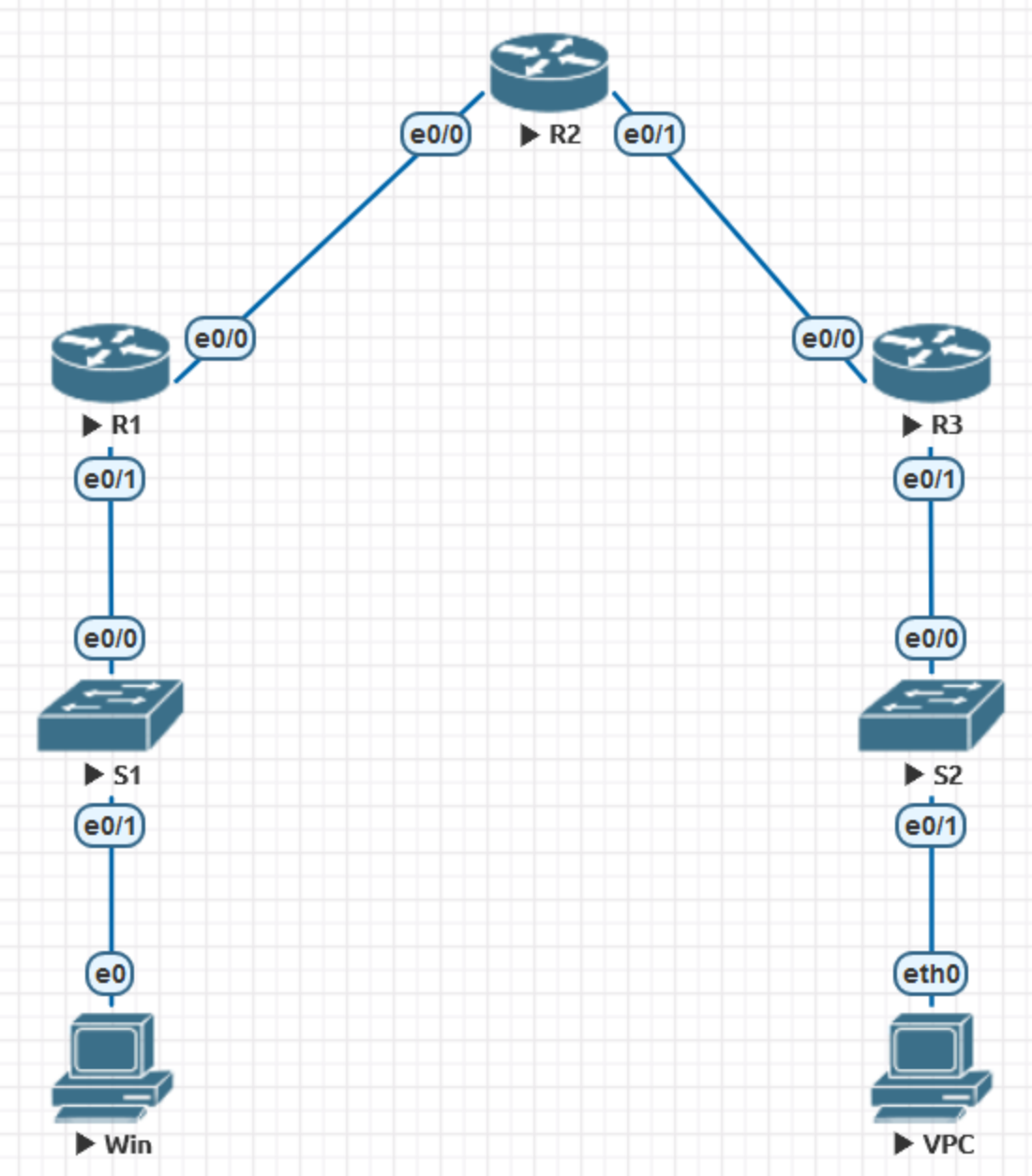
Lab Access

- SSID: ASAFirewall
- Password: Firewall

- George, Adam
 - <http://192.168.1.101>

- Matej, Bogdan
 - <http://192.168.1.102>

Topology



Topology

Device	Interface	IP Address	Subnet Mask	Default Gateway	Switch Port
R1	E0/1	192.168.1.1	255.255.255.0	N/A	S1 E0/0
	E0/0	10.1.1.1	255.255.255.252	N/A	N/A
R2	E0/0	10.1.1.2	255.255.255.252	N/A	N/A
	E0/1	10.2.2.2	255.255.255.252	N/A	N/A
R3	E0/1	192.168.3.1	255.255.255.0	N/A	S2 E0/0
	E0/0	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 E0/1
PC-C	NIC	192.168.3.3	255.255.255.0	192.168.3.1	S2 E0/1

Configure basic settings for each router

- Configure host names as shown in the topology.
- Configure the interface IP addresses as shown in the IP addressing table.

```
R1 (config) # interface E0/0
```

```
R1 (config-if) # ip address X.X.X.X M.M.M.M
```

- To prevent the router from attempting to translate incorrectly entered commands as though they were host names, disable DNS lookup.

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

Configure OSPF routing on the routers.

- Use the **router ospf** command in global configuration mode to enable OSPF on R1.

```
R1 (config) # router ospf 1
```

- Configure the **network** statements for the networks on R1. Use an area ID of 0.

```
R1 (config-router) # network 192.168.1.0 0.0.0.255 area 0
```

```
R1 (config-router) # network 10.1.1.0 0.0.0.3 area 0
```

- Configure OSPF on R2 and R3.
- Issue the **passive-interface** command to change the G0/1 interface on R1 and R3 to passive.

```
R1 (config) # router ospf 1
```

```
R1 (config-router) # passive-interface g0/1
```

```
R3 (config) # router ospf 1
```

```
R3 (config-router) # passive-interface g0/1
```

Verify OSPF neighbors and routing information.

- Issue the `show ip ospf neighbor` command to verify that each router lists the other routers in the network as neighbors.
- R1# `show ip ospf neighbor`

Neighbor ID	Pri	State	Dead Time	Address	Interface
10.2.2.2	0	FULL/ -	00:00:31	10.1.1.2	Serial0/0/0

Configure PC host IP settings.

- Configure a static IP address, subnet mask, and default gateway for PC-A
- PC-C, as shown in the IP addressing table.

Verify connectivity between PC-A and R3.

- Ping from R1 to R3.
- If the pings are not successful, troubleshoot the basic device configurations before continuing.
- Ping from PC-A on the R1 LAN to PC-C on the R3 LAN.

Configure and encrypt passwords on R1 and R3.

- Configure a minimum password length.
- Use the **security passwords** command to set a minimum password length of 10 characters.

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

- Configure the **enable secret** password on both routers. Use the type 9 (SCRYPT) hashing algorithm.

```
R1 (config) # enable algorithm-type scrypt secret cisco12345
```

Configure the basic console, auxiliary port, and vty lines.

- Configure a console password and enable login for router R1. For additional security, the **exec-timeout** command causes the line to log out after **5** minutes of inactivity. The **logging synchronous** command prevents console messages from interrupting command entry.
- **Note:** To avoid repetitive logins during this lab, the exec timeout can be set to 0, which prevents it from expiring. However, this is not considered a good security practice.

```
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
```

Configure the basic console, auxiliary port, and vty lines.

- Configure a password for the aux port for router R1.

```
R1 (config) # line aux 0
```

```
R1 (config-line) # password ciscoauxpass
```

```
R1 (config-line) # exec-timeout 5 0
```

```
R1 (config-line) # login
```

- Configure the password on the vty lines for router R1.

```
R1 (config) # line vty 0 4
```

```
R1 (config-line) # password ciscovtypass
```

```
R1 (config-line) # exec-timeout 5 0
```

```
R1 (config-line) # login
```

- Encrypt the console, aux, and vty passwords.

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

- Issue the **show run** command. Can you read the console, aux, and vty passwords

Configure a login warning banner on routers R1 and R3.

- Configure a warning to unauthorized users using a message-of-the-day (MOTD) banner with the **banner motd** command. When a user connects to the router, the MOTD banner appears before the login prompt. In this example, the dollar sign (\$) is used to start and end the message.

```
R1 (config) # banner motd $Unauthorized access strictly prohibited!$
```

```
R1 (config) # exit
```

- Exit privileged EXEC mode by using the **disable** or **exit** command and press **Enter** to get started.
- If the banner does not appear correctly, re-create it using the **banner motd** command.

Configure the local user database.

- Create a local user account with the type 9 (SCRYPT) hashing algorithm.

```
R1 (config) # username user01 algorithm-type scrypt secret  
user01pass
```

Configure local authentication for the console line and login

- Set the console line to use the locally defined login usernames and passwords.

```
R1 (config) # line console 0
```

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

- Exit to the initial router screen that displays:

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

- Log in using the **user01** account and password previously defined.

Test the new account by logging in from a Telnet session.

- From PC-A, establish a Telnet session with R1.

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

- Were you prompted for a user account? Explain.
- Set the vty lines to use the locally defined login accounts and configure the **transport input** command to allow Telnet.

```
R1 (config) # line vty 0 4
```

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

```
R1 (config-line) # transport input telnet
```

```
R1 (config-line) # exit
```

- From PC-A, telnet R1 to R1 again.

Configure a domain name.

- Enter global configuration mode and set the domain name.

```
R1# conf t
```

```
R1 (config)# ip domain-name local.lab
```

Configure a privileged user for login from the SSH client.

- Use the `username` command to create the user ID with the highest possible privilege level and a secret password.

```
R1 (config)# username Admin01 privilege 15 algorithm-type  
crypt secret Admin01pass
```

Configure the incoming vty lines.

- Specify a privilege level of **15** so that a user with the highest privilege level (15) will default to privileged EXEC mode when accessing the vty lines. Other users will default to user EXEC mode. Use the local user accounts for mandatory login and validation and accept only SSH connections.

```
R1 (config) # line vty 0 4
```

```
R1 (config-line) # privilege level 15
```

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

```
R1 (config-line) # transport input ssh
```

```
R1 (config-line) # exit
```

Erase existing key pairs on the router.

```
R1 (config) # crypto key zeroize rsa
```

- **Note:** If no keys exist, you might receive this message:

```
% No Signature RSA Keys found in configuration.
```

Generate the RSA encryption key pair for the router.

- The router uses the RSA key pair for authentication and encryption of transmitted SSH data.
- Configure the RSA keys with **1024** for the number of modulus bits. The default is 512, and the range is from 360 to 2048.

```
R1 (config) # crypto key generate rsa general-keys modulus 1024
```

- The name for the keys will be: `R1.local.lab`

```
% The key modulus size is 1024 bits
```

```
% Generating 1024 bit RSA keys, keys will be non-exportable...[OK]
```

```
R1 (config) #
```

```
*Dec 16 21:24:16.175: %SSH-5-ENABLED: SSH 1.99 has been enabled
```

- Issue the **ip ssh version 2** command to force the use of SSH version 2.

```
R1 (config) # ip ssh version 2
```

```
R1 (config) # exit
```

Verify the SSH configuration.

- Use the `show ip ssh` command to see the current settings.

```
R1# show ip ssh
```

- Fill in the following information based on the output of the `show ip ssh` command.

Configure SSH timeouts and authentication parameters.

- The default SSH timeouts and authentication parameters can be altered to be more restrictive using the following commands.

```
R1 (config) # ip ssh time-out 90
```

```
R1 (config) # ip ssh authentication-retries 2
```

Set Up the NTP Master using Cisco IOS commands.

- Use the **show clock** command to display the current time set on the router.

```
R2# show clock
```

```
*19:48:38.858 UTC Wed Feb 18 2015
```

- To set the time on the router, use the **clock set *time*** command.

```
R2# clock set 20:12:00 Dec 17 2014
```

```
R2#
```

```
*Dec 17 20:12:18.000: %SYS-6-CLOCKUPDATE: System clock has  
been updated from 01:20:26 UTC Mon Dec 15 2014 to 20:12:00  
UTC Wed Dec 17 2014, configured from console by admin on  
console.
```


Set Up the NTP Master using Cisco IOS commands.

- Configure NTP authentication by defining the authentication key number, hashing type, and password that will be used for authentication. The password is case sensitive.

```
R2# config t
```

```
R2 (config)# ntp authentication-key 1 md5 NTPpassword
```

- Configure the trusted key that will be used for authentication on R2.

```
R2 (config)# ntp trusted-key 1
```

- Enable the NTP authentication feature on R2.

```
R2 (config)# ntp authenticate
```

- Configure R2 as the NTP master using the **ntp master stratum-number** command in global configuration mode. The stratum number indicates the distance from the original source. For this lab, use a stratum number of **3** on R2. When a device learns the time from an NTP source, its stratum number becomes one greater than the stratum number of its source.

```
R2 (config)# ntp master 3
```

Configure R1 and R3 as NTP clients using the CLI.

- Configure NTP authentication by defining the authentication key number, hashing type, and password that will be used for authentication.

```
R1# config t
```

```
R1 (config)# ntp authentication-key 1 md5 NTPpassword
```

- Configure the trusted key that will be used for authentication. This command provides protection against accidentally synchronizing the device to a time source that is not trusted.

```
R1 (config)# ntp trusted-key 1
```

- Enable the NTP authentication feature.

```
R1 (config)# ntp authenticate
```

- R1 and R3 will become NTP clients of R2. Use the command **ntp server *hostname***. The host name can also be an IP address. The command **ntp update-calendar** periodically updates the calendar with the NTP time.

```
R1 (config)# ntp server 10.1.1.2
```

Configure R1 and R3 as NTP clients using the CLI.

- Verify that R1 has made an association with R2 with the **show ntp associations** command. You can also use the more verbose version of the command by adding the **detail** argument. It might take some time for the NTP association to form.

```
R1# show ntp associations
```

```
address      ref clock      st  when  poll reach  delay  offset  disp
~10.1.1.2    127.127.1.1    3   14   64    3   0.000  -280073 3939.7
*sys.peer, # selected, +candidate, -outlyer, x falseticker, ~ configured
```

- Issue the **debug ntp all** command to see NTP activity on R1 as it synchronizes with R2.

```
R1# debug ntp all
```

Install the syslog server.

- Tftpd32 includes a TFTP server, TFTP client, and a syslog server and viewer. The Kiwi Syslog Daemon is only a dedicated syslog server. You can use either with this lab. Both are available as free versions and run on Microsoft Windows.
- If a syslog server is not currently installed on the host, download the latest version of Tftpd32 from <http://tftpd32.jounin.net> or Kiwi from <http://www.kiwisyslog.com> and install it on your desktop. If it is already installed, go to Step 2.
- **Note:** This lab uses the Tftpd32 application for the syslog server functionality.

Configure R1 to log messages to the syslog server

- Verify that you have connectivity between R1 and PC-A by pinging the R1 G0/1 interface IP address 192.168.1.1. If it is not successful, troubleshoot as necessary before continuing.
- NTP was configured in Task 2 to synchronize the time on the network. Displaying the correct time and date in syslog messages is vital when using syslog to monitor a network. If the correct time and date of a message is not known, it can be difficult to determine what network event caused the message.
- Verify that the timestamp service for logging is enabled on the router using the **show run** command. Use the following command if the timestamp service is not enabled.

```
R1 (config) # service timestamps log datetime msec
```

- Configure the syslog service on the router to send syslog messages to the syslog server.

```
R1 (config) # logging host 192.168.1.3
```

Configure the logging severity level on R1.

- Use the `logging trap` command to determine the options for the command and the various trap levels available.
- Use the `logging trap` command to set the severity level for R1.

```
R1 (config) # logging trap warnings
```

Display the current status of logging for R1.

- Use the `show logging` command to see the type and level of logging enabled.

```
R1# show logging
```

Enable AAA

- On R3, enable services with the global configuration **aaa new-model** command. Because you are implementing local authentication, use local authentication as the first method, and no authentication as the secondary method.
- If you were using an authentication method with a remote server, such as TACACS+ or RADIUS, you would configure a secondary authentication method for fallback if the server is unreachable. Normally, the secondary method is the local database. In this case, if no usernames are configured in the local database, the router allows all users login access to the device.

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


Implement AAA services for console access using the local database.

- Create the default login authentication list by issuing the `aaa authentication login default method1 [method2] [method3]` command with a method list using the `local` and `none` keywords.

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

```
R3 (config)# aaa authentication enable default enable
```

- **Note:** If you do not set up a default login authentication list, you could get locked out of the router and be forced to use the password recovery procedure for your specific router.
- **Note:** The `local-case` parameter is used to make usernames case-sensitive.
- Exit to the initial router screen that displays:
 - `R3 con0 is now available`
- Press RETURN to get started.

Create an AAA authentication profile for Telnet using the local database.

- Create a unique authentication list for Telnet access to the router. This does not have the fallback of no authentication, so if there are no usernames in the local database, Telnet access is disabled. To create an authentication profile that is not the default, specify a list name of TELNET_LINES and apply it to the vty lines.

```
R3 (config) # aaa authentication login TELNET_LINES local
```

```
R3 (config) # line vty 0 4
```

```
R3 (config-line) # login authentication TELNET_LINES
```

Use debug to verify user access.

- Activate debugging for AAA authentication.

```
R3# debug aaa authentication
```

- AAA Authentication debugging is on
- Start a Telnet session from R2 to R3.
- Log in with username **Admin01** and password **Admin01pass**. Observe the AAA authentication events in the console session window. Debug messages similar to the following should be displayed.

```
R3#
```

```
Feb 20 08:45:49.383: AAA/BIND(0000000F): Bind i/f
```

```
Feb 20 08:45:49.383: AAA/AUTHEN/LOGIN (0000000F): Pick  
method list 'TELNET_LINES'
```

ReConfigure the default login authentication list.

- Configure the list to first use RADIUS for the authentication service, and then none. If no RADIUS server can be reached and authentication cannot be performed, the router globally allows access without authentication. This is a safeguard measure in case the router starts up without connectivity to an active RADIUS server.

```
R1 (config) # aaa authentication login default group radius
```

```
R1 (config) # aaa authorization exec default group radius if-authenticated
```

- You could alternatively configure local authentication as the backup authentication method instead.
- **Note:** If you do not set up a default login authentication list, you could get locked out of the router and need to use the password recovery procedure for your specific router.

Specify a RADIUS server.

- Use the `radius server` command to enter RADIUS server configuration mode.

```
R1(config)# radius server RADSERVERGROUP
```

- Use the `?` to view the sub-mode commands available for configuring a Radius server.

```
R1(config-radius-server)# ?
```

RADIUS server sub-mode commands:

<code>address</code>	Specify the radius server address
<code>automate-tester</code>	Configure server automated testing.
<code>backoff</code>	Retry backoff pattern(Default is retransmits with constant delay)
<code>exit</code>	Exit from RADIUS server configuration mode
<code>key</code>	Per-server encryption key
<code>no</code>	Negate a command or set its defaults
<code>non-standard</code>	Attributes to be parsed that violate RADIUS standard
<code>pac</code>	Protected Access Credential key
<code>retransmit</code>	Number of retries to active server (overrides default)
<code>timeout</code>	Time to wait (in seconds) for this radius server to reply (overrides default)

Specify address and key

- Use the **address** command to configure this IP address for PC-A

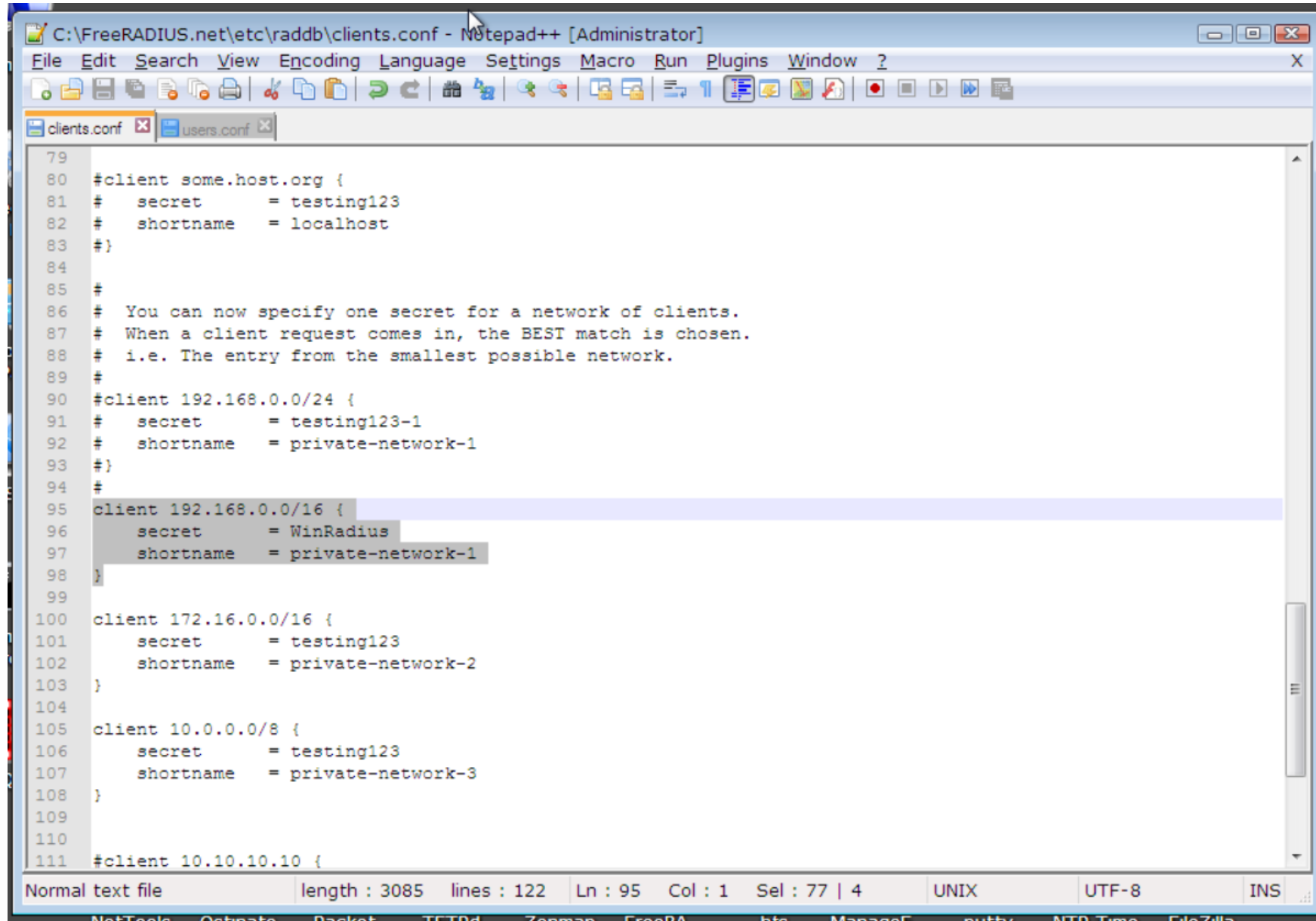
```
R1 (config-radius-server) #  
address ipv4 192.168.1.3 auth-port 1812 acct-port 1813
```

- The **key** command is used for the secret password that is shared between the RADIUS server and the router (R1 in this case) and is used to authenticate the connection between the router and the server before the user authentication process takes place. Use the default NAS secret password of **WinRadius** specified on the Radius server (see Task 2, Step 5). Remember that passwords are case-sensitive.

```
R1 (config-radius-server) # key WinRadius
```

```
R1 (config-radius-server) # end
```

FreeRadius Server 1



```
C:\FreeRADIUS.net\etc\raddb\clients.conf - Notepad++ [Administrator]
File Edit Search View Encoding Language Settings Macro Run Plugins Window ?
clients.conf x users.conf x
79
80 #client some.host.org {
81 #   secret      = testing123
82 #   shortname   = localhost
83 #}
84
85 #
86 # You can now specify one secret for a network of clients.
87 # When a client request comes in, the BEST match is chosen.
88 # i.e. The entry from the smallest possible network.
89 #
90 #client 192.168.0.0/24 {
91 #   secret      = testing123-1
92 #   shortname   = private-network-1
93 #}
94 #
95 client 192.168.0.0/16 {
96     secret      = WinRadius
97     shortname   = private-network-1
98 }
99
100 client 172.16.0.0/16 {
101     secret      = testing123
102     shortname   = private-network-2
103 }
104
105 client 10.0.0.0/8 {
106     secret      = testing123
107     shortname   = private-network-3
108 }
109
110
111 #client 10.10.10.10 {
```

Normal text file length : 3085 lines : 122 Ln : 95 Col : 1 Sel : 77 | 4 UNIX UTF-8 INS

NetTools Ostrato Packet TELPd Zenman FreeRA hts ManageE nutty NTP Time FileZilla

FreeRadius Server 2

```
C:\FreeRADIUS.net\etc\raddb\users.conf - Notepad++ [Administrator]
File Edit Search View Encoding Language Settings Macro Run Plugins Window ?
clients.conf x users.conf x
73 #
74
75 ##### RFC3580 #####
76 ## Also the "eap.conf" MUST be modified to include the follow line:
77 ## "use_tunneled_reply = yes"
78 ## the default is "use_tunneled_reply = no"
79 ## this allow the "Tunnel*" AV's to be passed outside the eap tunnel
80 ## otherwise the switch will NOT see the VLAN to place the port into
81 ##### Comments added by Jeff Reilly #####
82
83 pokus  User-Password == "POKUS"
84     Service-Type = NAS-Prompt-User,
85     cisco-avpair = "shell:priv-lvl=15"
86
87 testuser  User-Password == "testpw"
88
89 FreeRADIUS.net-Client  User-Password == "demo"
90
91 rfc3580 User-Password == "demo"
92     Tunnel-Type = "VLAN",
93     Tunnel-Medium-Type = "IEEE-802",
94     Tunnel-Private-Group-Id = "1",
95     Reply-Message = "Hello, %u"
96
97 #
98 # This is a complete entry for "steve". Note that there is no Fall-Through
99 # entry so that no DEFAULT entry will be used, and the user will NOT
100 # get any attributes in addition to the ones listed here.
101 #
102 #steve  Auth-Type := Local, User-Password == "testing"
103 #     Service-Type = Framed-User,
104 #     Framed-Protocol = PPP,
105 #     Framed-IP-Address = 172.16.3.33,
Normal text file      length : 7877  lines : 237  Ln : 86  Col : 1  Sel : 103 | 4  Dos\Windows  UTF-8  INS
NetTools  Ostinato  Packet  TFTPd  Zenmap  FreeRA...  hts  ManageE...  putty  NTP Time  FileZilla
```