CSG 1105 / 5130 - Applied Communications

Module 10 Tutorial

Objectives

- To learn about the types of firewalls and their purpose
- To learn about authentication methods

By the end of this workshop you should be able to

- Discuss the different kinds of firewalls
- Discuss the different methods of user authentication on a network

Required Downloads

- Activity Module 1 - Packet Filtering Firewall.pkt
  - A Packet Tracer file with *some* pre-configured hardware already laid out.
- Activity Module 2 - Authentication.pkt
  - A Packet Tracer file with *some* pre-configured hardware already laid out.

Optional Downloads

- Packet Tracer Simulation Guide found in the Unit Documents
- A recording of this Tutorial from blackboard; discussions are held in class and clarifications are made too.

Learning Module 1 - Firewalls

Firewalls are a component of a network which can either be a physical device, or a server running firewall software, that is used to control the incoming and outgoing traffic at differing layers of the OSI model depending on the type and ruleset enabled on it.

Firewalls are the boundary and virtual barrier between a known, trusted, secure internal network and another network, such as the Internet or potentially another section of the internal network.

Firewalls were created relatively early in the lifespan of internetworking and came about in a generational style progression.

The first generation of firewalls were the **Packet Filtering** firewalls that worked by analysing the traffic based on the IP addresses, port numbers or protocol in use. They allowed or denied access based on the rules that restrict or enable the specific requirements. Tunnelling traffic through a particular port number or masking the IP address is a way to bypass or exploit this firewall.

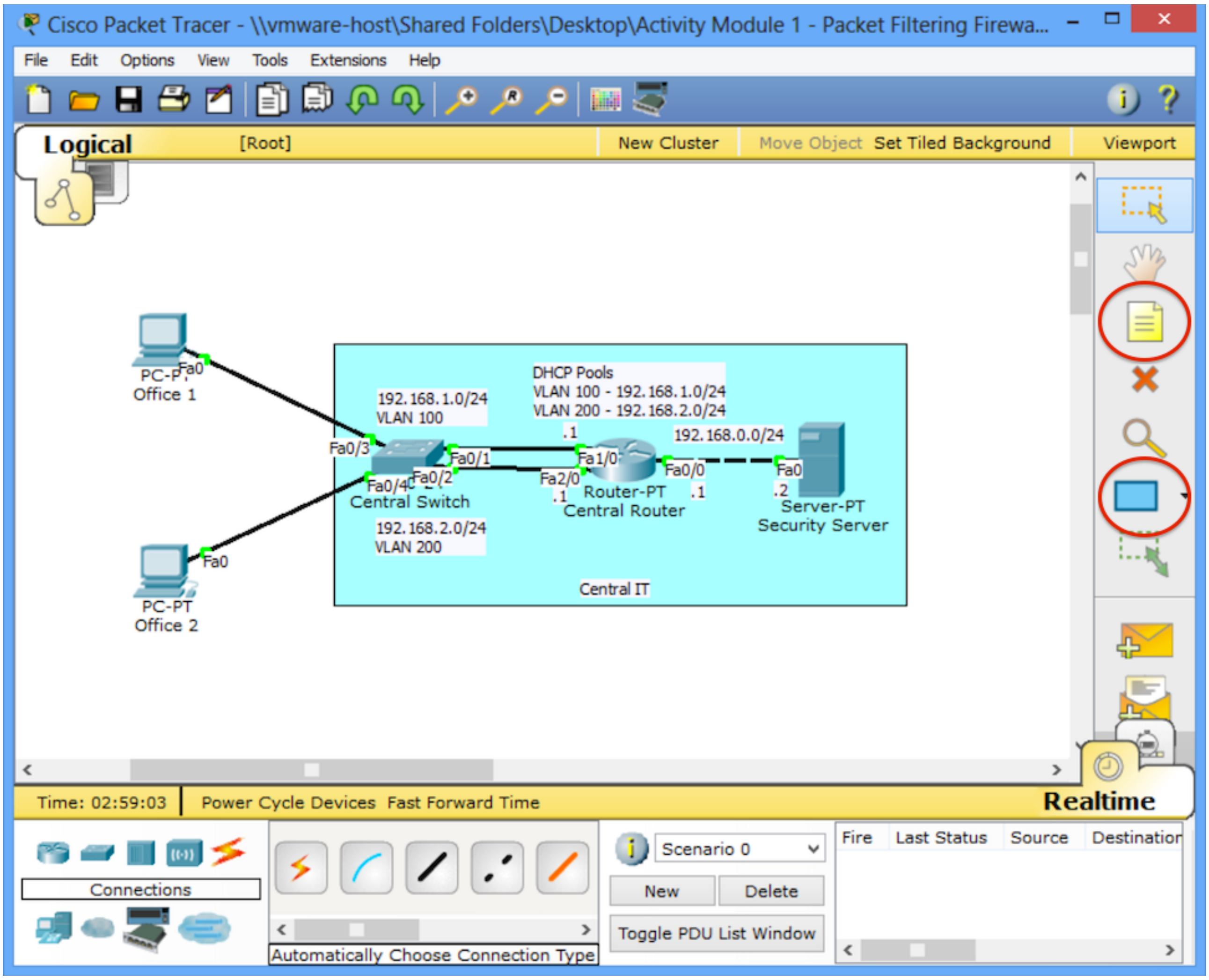
The next generation of firewalls to come out are the **Proxy Service** firewalls which operate on the Session or Application Layer of the OSI model and monitor them for proper sequencing or protocols. Proxies can allow authentication to be used in order to enforce access to the rest of the network, or to the outside network (such as in ECU's public network).

The last kind of firewall to come about is the **Stateful Inspection** firewall which is a combination of both of the previous generations of firewall. It operates in the same way that both the Packet Filtering and Proxy Service firewalls operate in a co-operative manner. A particularly common attack on these kinds of firewalls is the Denial-of-Service attack, in which the attacker(s) attempt to fill the connection state log of the firewall causing it run out of memory.

In the first Activity Module we'll be configuring a **Packet Filtering** firewall in Packet Tracer. You'll need to have the file, '*Activity Module 1 - Packet Filtering Firewall.pkt*'.

Activity Module 1 - Packet Filtering Firewall
Firstly, open the file ‘Activity Module 1 - Packet Filtering Firewall.pkt’ in Packet Tracer and have a look at the network. It’s a very basic network and it’s currently got no security in place what-so-ever.

I’ve placed all the key information on the logical space to aid in finding it quickly and easily. This is all done by making use of the Shape Tool and the Note Tool (circled in the picture below).


Cisco Packet Tracer - \\vmware-host\Shared Folders\Desktop\Activity Module 1 - Packet Filtering Firewa...
File Edit Options View Tools Extensions Help
Logical [Root] New Cluster Move Object Set Tiled Background Viewport
PC-PT Office 1
Fa0
Fa0/3
192.168.1.0/24
VLAN 100
DHCP Pools
VLAN 100 - 192.168.1.0/24
VLAN 200 - 192.168.2.0/24
.1
192.168.0.0/24
Fa0/1
Fa1/0
Fa0/0
Fa0
Fa0/4
Fa0/2
Fa2/0
.1
Router-PT
.1
.2
Central Switch
Central Router
Server-PT
Security Server
192.168.2.0/24
VLAN 200
Central IT
PC-PT Office 2
Time: 02:59:03 Power Cycle Devices Fast Forward Time
Realtime
Connections
Automatically Choose Connection Type
Scenario 0
New Delete
Toggle PDU List Window
Fire Last Status Source Destination

We’ll look at the configuration of the Central Router and Switch first. This sort of configuration should be familiar from Week 8’s Tutorial. It is in use here to allow the DHCP pools to allocate on a per VLAN basis. You can see the DHCP pools listed in the blue square.

On the Central Router we have the three interfaces configured with the three different networks, two of which are included in the DHCP pools, the third, leads to the server which has a static IP address. The configuration is as follows:

Router:

```
ip dhcp pool pool1 (VLAN 100)
network 192.168.1.0 255.255.255.0
default-router 192.168.1.1

ip dhcp pool pool2 (VLAN 200)
network 192.168.2.0 255.255.255.0
default-router 192.168.2.1
```

```
        FastEthernet 0/0 (Server Connection)
        ip address 192.168.0.1 255.255.255.0

        FastEthernet 1/0 (VLAN 100)
        ip address 192.168.1.1 255.255.255.0

        Fast Ethernet 2/0 (VLAN 200)
        ip address 192.168.2.1 255.255.255.0
```

Switch:

```
        VLAN 100
        VLAN 200

        FastEthernet 0/1
        access VLAN 100

        Fast Ethernet 0/2
        access VLAN 200

        FastEthernet 0/3
        access VLAN 100

        FastEthernet 0/4
        access VLAN 200
```

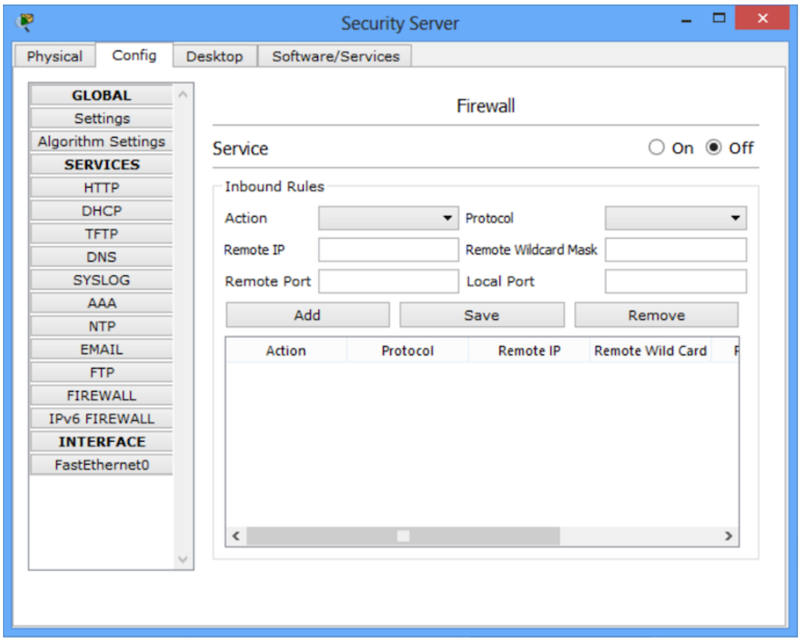
All pretty standard configurations with what we have come to learn! Now, let's enter the two computers (Office 1 & Office 2) and ensure that we have obtained an IP address each from the DHCP server. We should get and IP address in the following subnets:

Office 1 - 192.168.1.0/24
Office 2 - 192.168.2.0/24

Once we have verified that our DHCP works, we'll start adding some security onto the network! If we try pinging the Server (192.168.0.2) from any point we will get successful results - let's make it so Office 1 cannot ping our server. (For help using ping see the Packet Tracer Simulation Guide found in the Unit Documents and follow 'Single Packet Simulation').

Open the Server's configuration window and go to the **Config** tab. Along the left hand side you should see the **Firewall** option (not the IPv6 version). Go into this tab (pictured to the right) and we'll start configuring the Firewall. We'll be limiting the ICMP (which is what ping uses) so that only the 192.168.0.0 (Server Network) and 192.168.2.0 (Office 2 Network) can ping our server.

Firstly, let's **turn on** the firewall and then modify our inbound rules. I'll show you the settings you'll need to configure them on the next page.



Firewall

Service ○ On ● Off

When creating firewall rules you have to explicitly state what to **allow** and what to **deny**. If you forget to state what is allowed, it will also be automatically denied. So be sure to add in all of the following information:

Action	Protocol	Remote IP	Wildcard Mask
Allow	ICMP	192.168.0.0	0.0.0.255
Allow	ICMP	192.168.2.0	0.0.0.255
Deny	ICMP	192.168.1.0	0.0.0.255

What is this **Wildcard Mask**? The wildcard mask is basically the opposite of the subnet mask in which the 255 means that any value from here may change. The easiest way to convert them is to minus the values in the octet from 255. See some examples below:

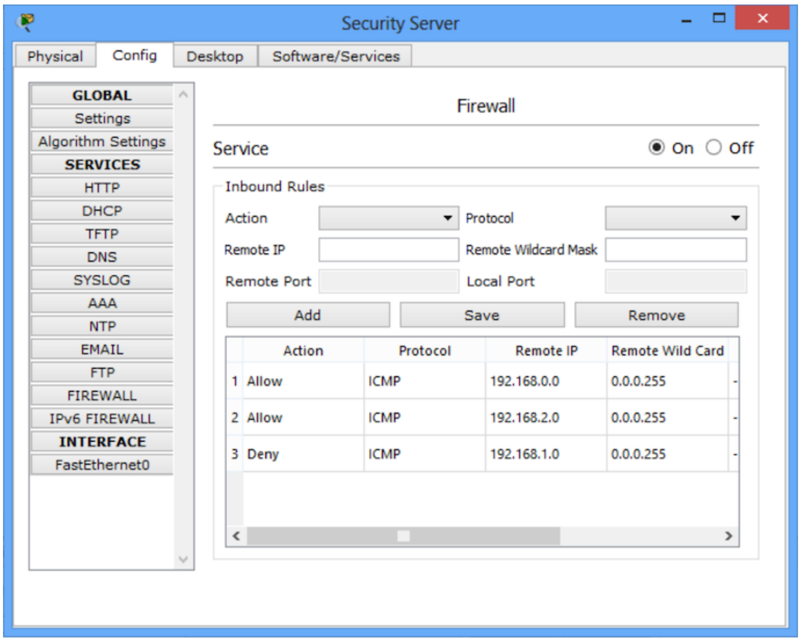
/24 = 255.255.255.0

First Octet:	255 - 255 = 0	
Second Octet:	255 - 255 = 0	
Third Octet:	255 - 255 = 0	
Fourth Octect:	255 - 0 = 255	therefore, Wildcard Mask /24 = 0.0.0.255

/26 = 255.255.255.192

First Octet:	255 - 255 = 0	
Second Octet:	255 - 255 = 0	
Third Octet:	255 - 255 = 0	
Fourth Octet:	255 - 192 = 63	therefore, Wildcard Mask /26 = 0.0.0.63

Your firewall settings should look like this once you have added the information in the table above.



Firewall

Service ● On ○ Off

Inbound Rules

Action | Protocol
Remote IP | Remote Wildcard Mask
Remote Port | Local Port

	Action	Protocol	Remote IP	Remote Wild Card
1	Allow	ICMP	192.168.0.0	0.0.0.255
2	Allow	ICMP	192.168.2.0	0.0.0.255
3	Deny	ICMP	192.168.1.0	0.0.0.255

Now, try going back to your Office 1 and Office 2 computers and once again ping the server from them. Office 1 should now show ‘Request timed out’ for all of it’s pings, this is because the server is simply ignoring the incoming ICMP request.

Done with the firewalls! Onwards to authentication.

Learning Module 2 - Authentication
Authentication has been around in one form or another since the need to restrict access to a location or information. It may have been a spoken password or phrase, or a key word to mention during a conversation before computers were invented, but since computing's invention it has taken a huge leap in improvements.

Authentication methods range from passwords, to certificates and even biometrics or key generators to supplement a password. Regardless of the authentication in place, making use of multiple is always more secure than simply have one-step authentication.

The authentication methods we'll be looking at today come in the form of RADIUS and AAA.

RADIUS stands for '*Remote Authentication Dial In User Service*' and is a networking protocol that provides the second protocol which allows centralised authentication of users, called **AAA** which means *Authentication, Authorization, and Accounting*'. It is basically a server that stores all the authentication details for every user that will connect to any of the routers or switches, or even to the wireless access points.

Authentication - Providing the username and password or secret key to ensure only the desired users are accessing the information on the network.
Authorization - Limiting the access to sections of the network based on the user authentication details (staff, student, guest etc.)
Accounting - Who does what and when?

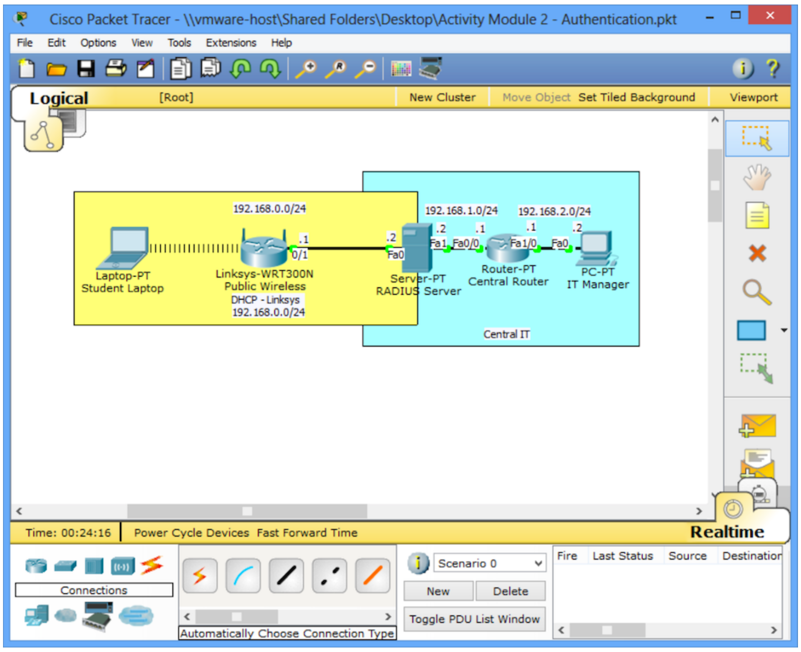
For the upcoming activity module we'll be making use of the packet tracer file '*Activity Module 2 - Authentication.pkt*'.

Activity Module 2 - Authentication

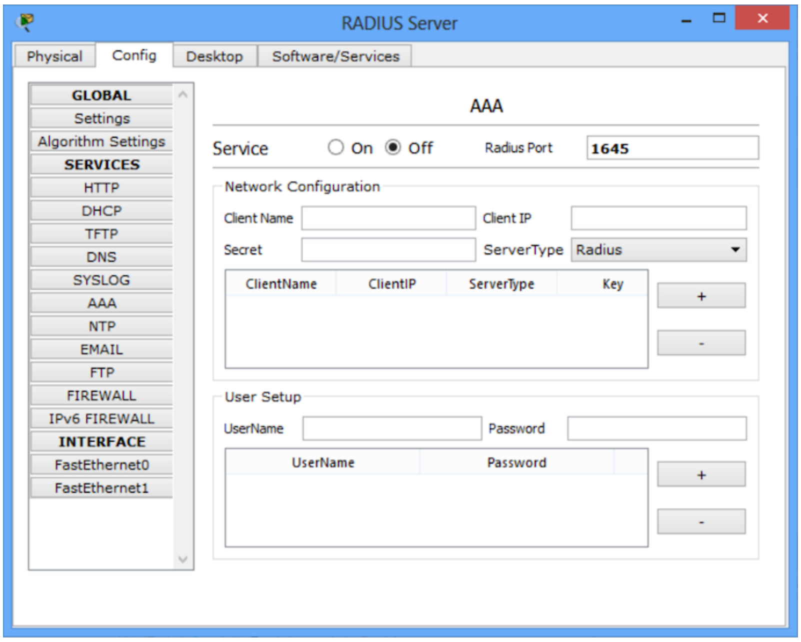
Open the file ‘Activity Module 2 - Authentication.pkt’ and have a look at the setup. You should be greeted with the project to the right.

Have a look at the network implemented here. We have two different sections to the network, once again with 3 subnets in use.

Let’s have a look at how secure the network is. Starting with the Laptop called ‘Student Laptop’, click on it and then go to the **Config** tab and look at it’s **Wireless0** interface. It’s go no security and it just connects right into the network as is. We’ll change that to WPA2-Enterprise so that we can have AAA in place.



Now have a look at the ‘Central Router’, try clicking on it, go to the **CLI** tab and press return. Did it ask for a username or password at all? No? Not exactly the best setup to have considering this is the **central** router.



AAA

Service ○ On ● Off Radius Port 1645

Network Configuration

Client Name | Client IP

Secret | ServerType Radius

ClientName	ClientIP	ServerType	Key

User Setup

UserName | Password

UserName	Password

Seems like we have a bit of work to fix this. Let’s open the ‘RADIUS Server’ in the center of the network and go to it’s **Config** tab, once there you should see a button on the left called **AAA**. Click on that and we’ll begin configuring it. You should see the window to the left.

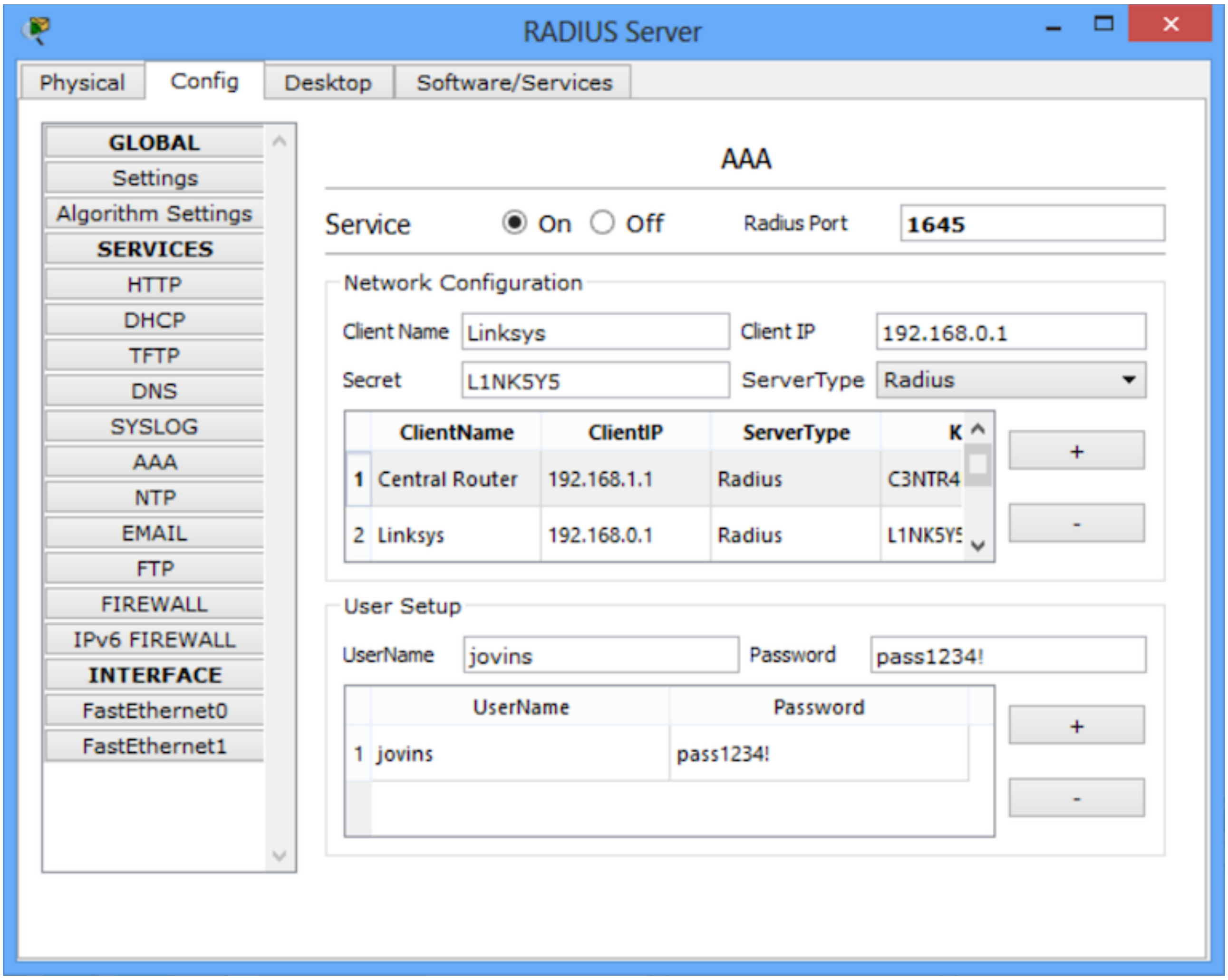
Firstly, set the service to **On** and leave the port at 1645. Then input the following two entires below into the **Network Configuration** section:

Client Name	Client IP	Secret	ServerType
Central Router	192.168.1.1	C3NTR4Lrouter	Radius
Linksys	192.168.0.1	L1NK5Y5	Radius

Once you have entered those, go ahead and enter a user into the **User Setup**. I have put the following into mine:

Username: jovins
Password: pass1234!

My configuration looks as follows.



AAA

Service ● On ○ Off Radius Port 1645

Network Configuration

Client Name Linksys Client IP 192.168.0.1

Secret L1NK5Y5 ServerType Radius

	ClientName	ClientIP	ServerType	K
1	Central Router	192.168.1.1	Radius	C3NTR4
2	Linksys	192.168.0.1	Radius	L1NK5Y5

User Setup

UserName jovins Password pass1234!

	UserName	Password
1	jovins	pass1234!

Now, try clicking on the router again and go to it's **CLI** tab once more. We'll now set up it's authentication for the server.

Type in the following commands exactly as they are to configure the AAA on the router, this will mean that the router will need the correct username and password we entered on the server in order to be configured in the future:

```
enable
configure terminal
aaa new-model
radius-server host 192.168.1.2 key C3NTR4Lrouter
aaa authentication login default group radius local
exit
exit
```

Now, try pressing the return key. You should see the immediate prompt for User Access Verification and asking for a Username. Enter the username we have on our server, and then the password at the next prompt. Congratulations! You have secured the central router!

Now onwards to the Wireless Access Point. Click on the Linksys called 'Public Wireless' and go to it's **Config** tab. Then click on the button saying **Wireless**. In here we are going to enable WPA2 for user authentication to join the WiFi.

To do so, change the Authentication to **WPA2** (not WPA2-PSK), and then enter the server IP of **192.168.0.2** and the shared secret we created above **L1NK5Y5**. Leave the encryption as AES. You should see the configuration on the following page.

Once you close it’s window you should notice the Laptop has stopped connecting. We’ll now configure the laptop!

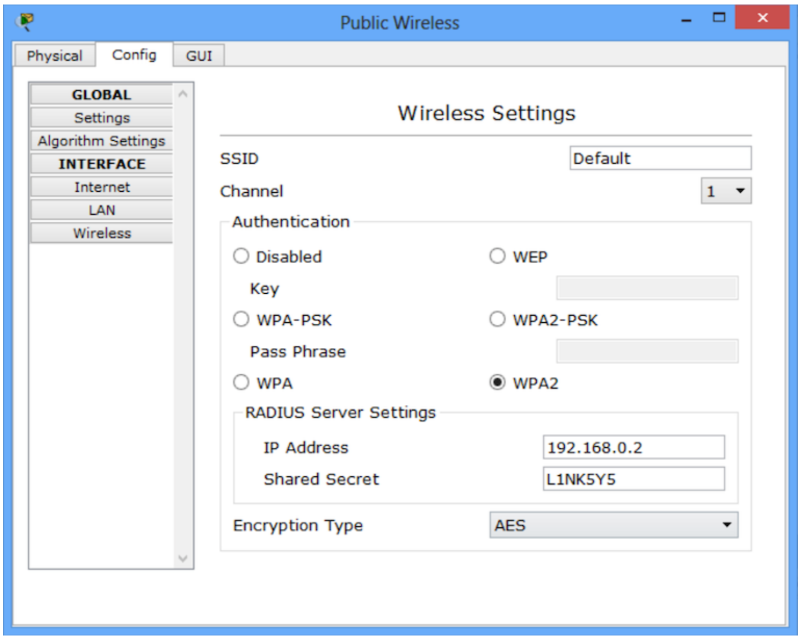
Click on the ‘Student Laptop’ and go to it’s **Config** tab. Now click on the **Wireless0** button to access the wireless options. Change it’s Authentication to **WPA2** and then enter the username and password we created on the server.

You can see my configuration of the Student Laptop in the second screenshot below to the right.

After a short while it should automatically reconnect once again now that we have authenticated!

You have now successfully setup AAA on a RADIUS server!

This concludes this tutorial - use the remainder of your time on your Assignment 2 or for Exam Revision.



Wireless Settings

SSID: Default

Channel: 1

Authentication

○ Disabled ○ WEP

Key

○ WPA-PSK ○ WPA2-PSK

Pass Phrase

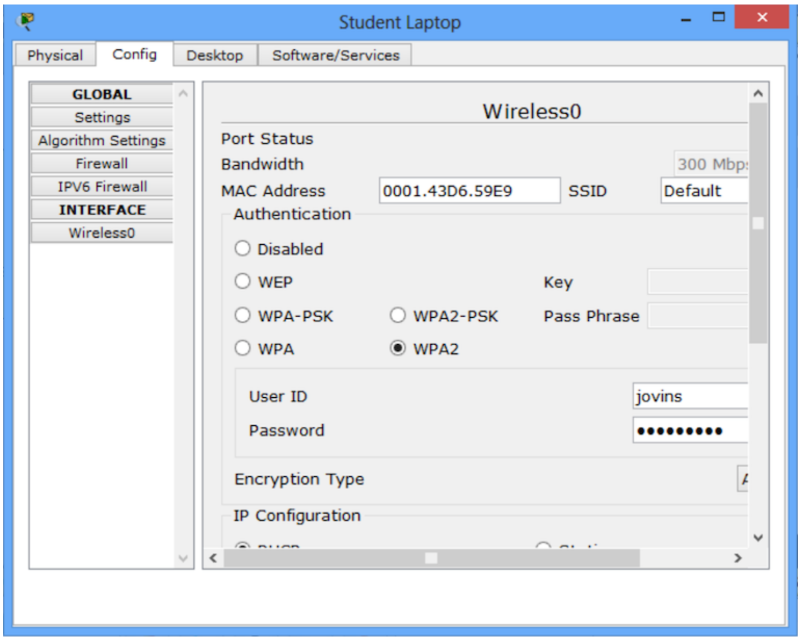
○ WPA ● WPA2

RADIUS Server Settings

IP Address: 192.168.0.2

Shared Secret: L1NK5Y5

Encryption Type: AES



Wireless0

Port Status

Bandwidth: 300 Mbp

MAC Address: 0001.43D6.59E9 SSID: Default

Authentication

○ Disabled

○ WEP Key

○ WPA-PSK ○ WPA2-PSK Pass Phrase

○ WPA ● WPA2

User ID: jovins

Password: •••••••••

Encryption Type

IP Configuration