PRACTICAL LAB: BASIC FIREWALL IMPLEMENTATION

JORDAN ALLISON
jallison1@glos.ac.uk

Practical Lab: Basic Firewall Implementation - JA

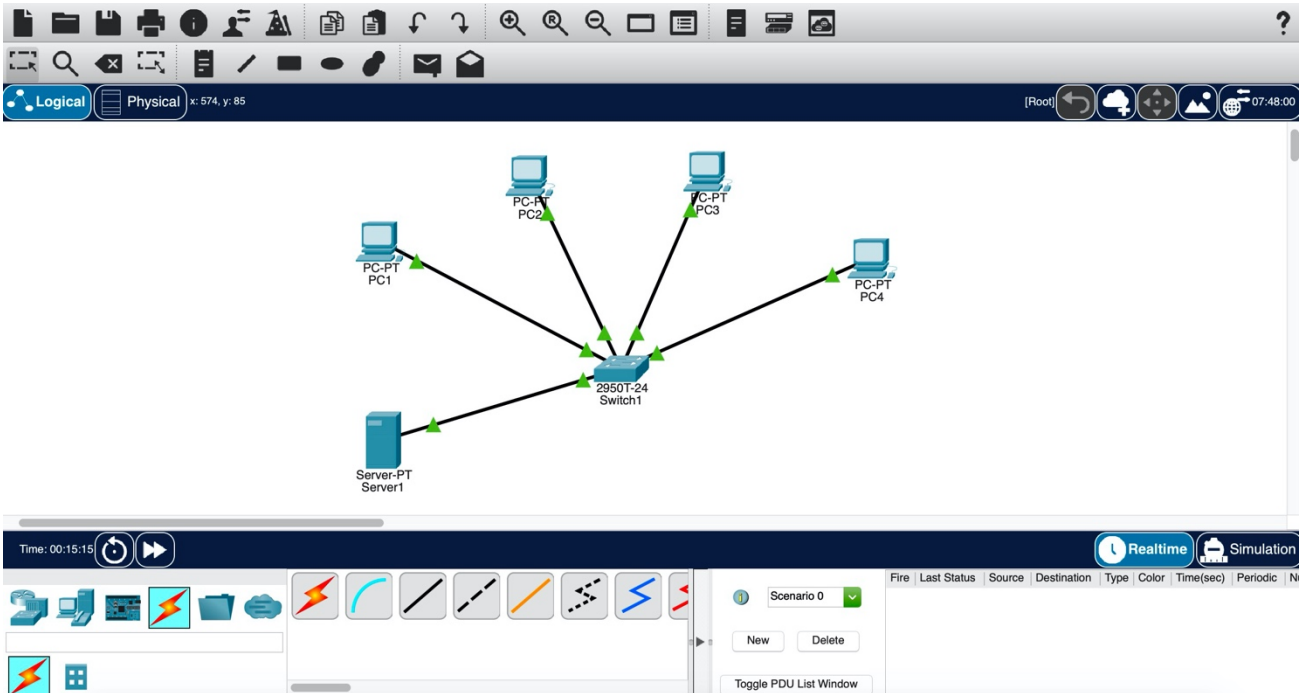
Table of Contents

1 Introduction

For this practical we will be using *Cisco Packet Tracer (student edition)*, a tool provided by Cisco to build and test Cisco networks. In this lab we are going to configure a network and implement some basic firewall settings.

2 Setting Up Devices

Set up the following devices. Name and device view:



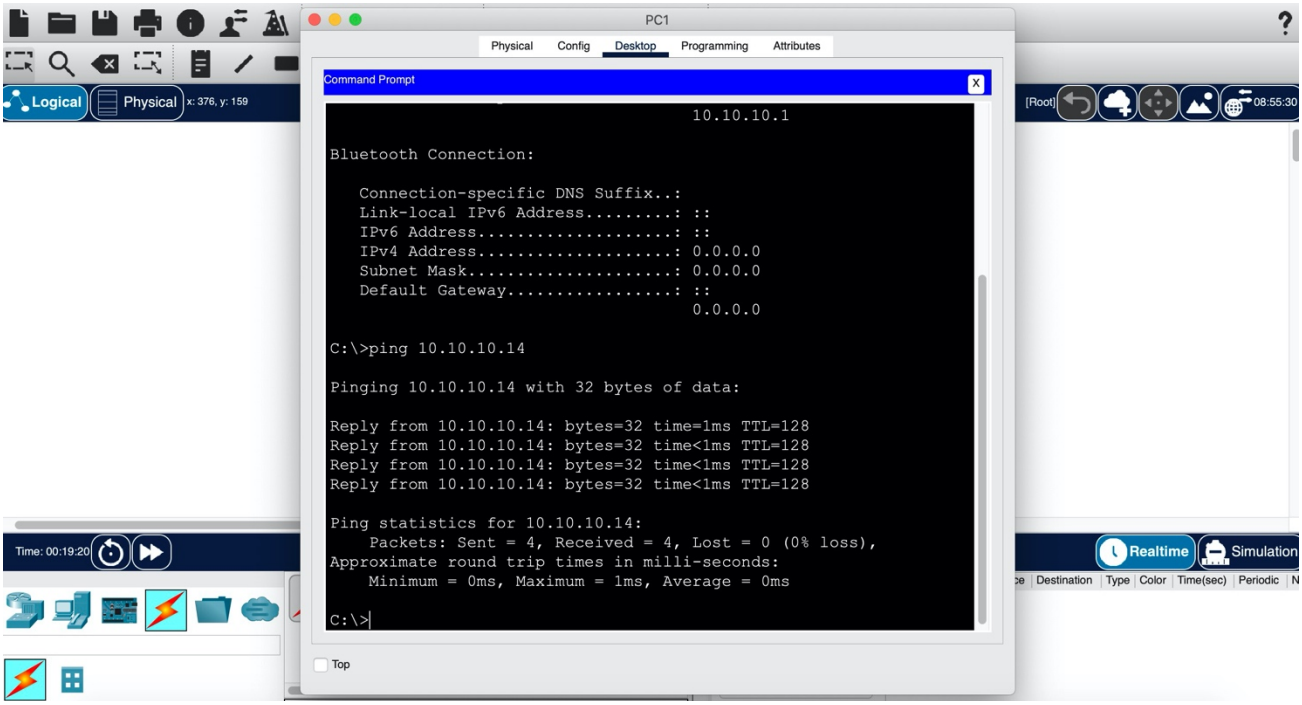
3 Configure Devices

Configure the devices as given below.

Device	Interface	IP Addresses	Subnet Mask	Default Gateway
PC1	N/A	10.10.10.10	255.0.0.0	10.10.10.1
PC2	N/A	10.10.10.11	255.0.0.0	10.10.10.1
PC3	N/A	10.10.10.12	255.0.0.0	10.10.10.1
PC4	N/A	10.10.10.13	255.0.0.0	10.10.10.1
Server1	N/A	10.10.10.14	255.0.0.0	10.10.10.1

4 Test Connectivity

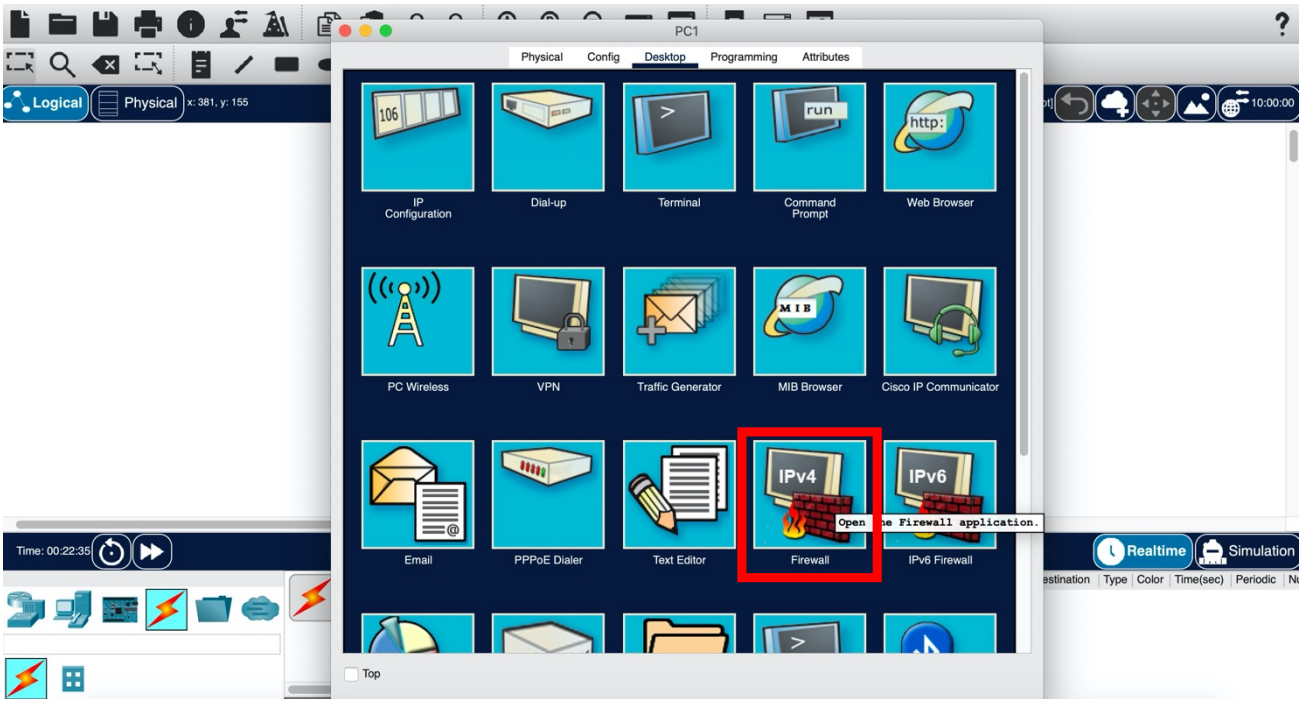
Try pinging the server from PC1.



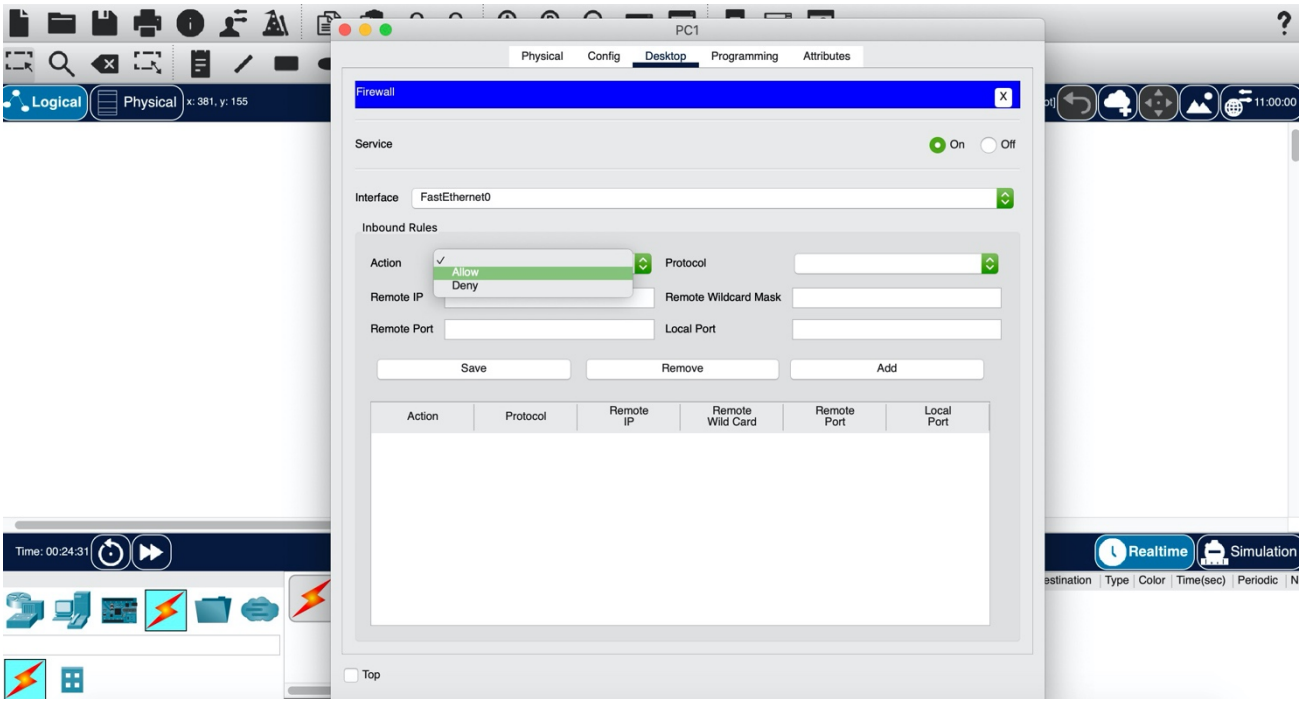
Test the connectivity for all other machines too and check they can ping each other.

5 Basic Firewall Implementation

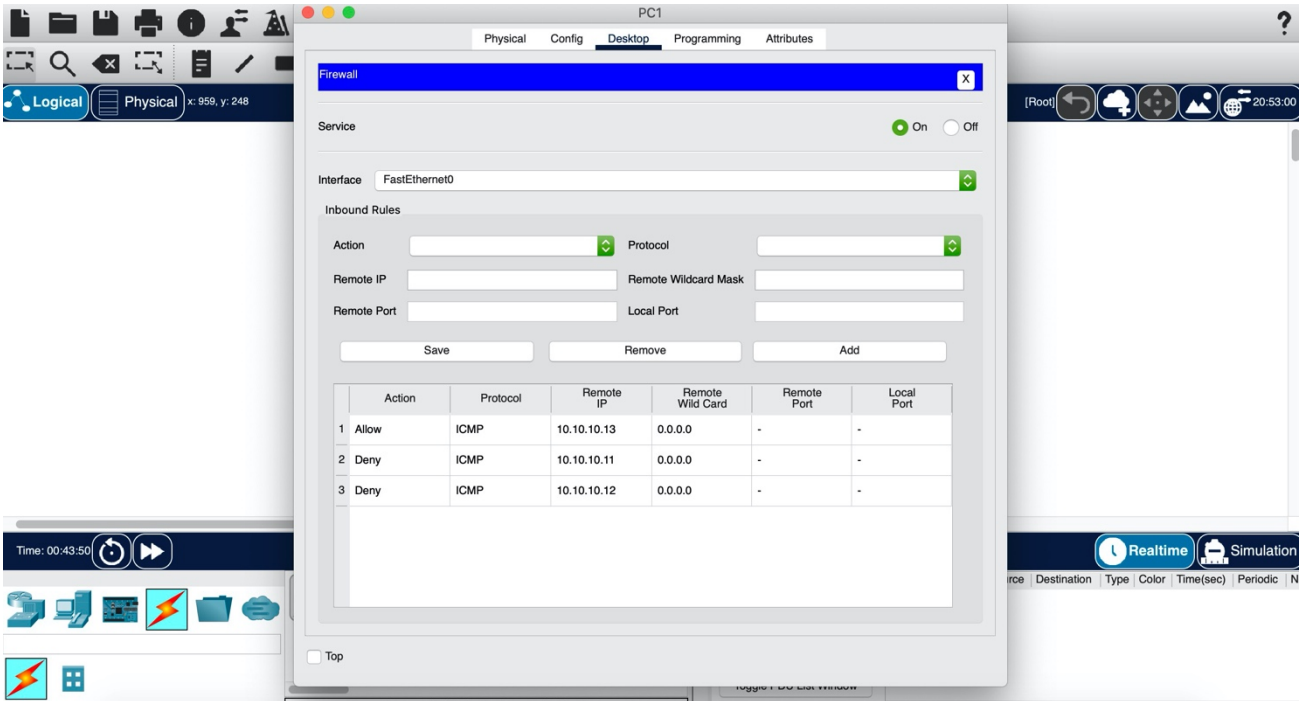
We are now going to implement some basic firewall settings so that PC1 cannot be pinged by any other computer in the network apart from PC4. To do this, click on PC1and then click on ‘Firewall’.



Now set ‘service’ to ‘On’. Then select the drop-down box for ‘Action’. Here is where you can set inbound rules to either allow or deny certain IP addresses.



Implement the following three rules to allow PC4 but deny PC2 and PC3.

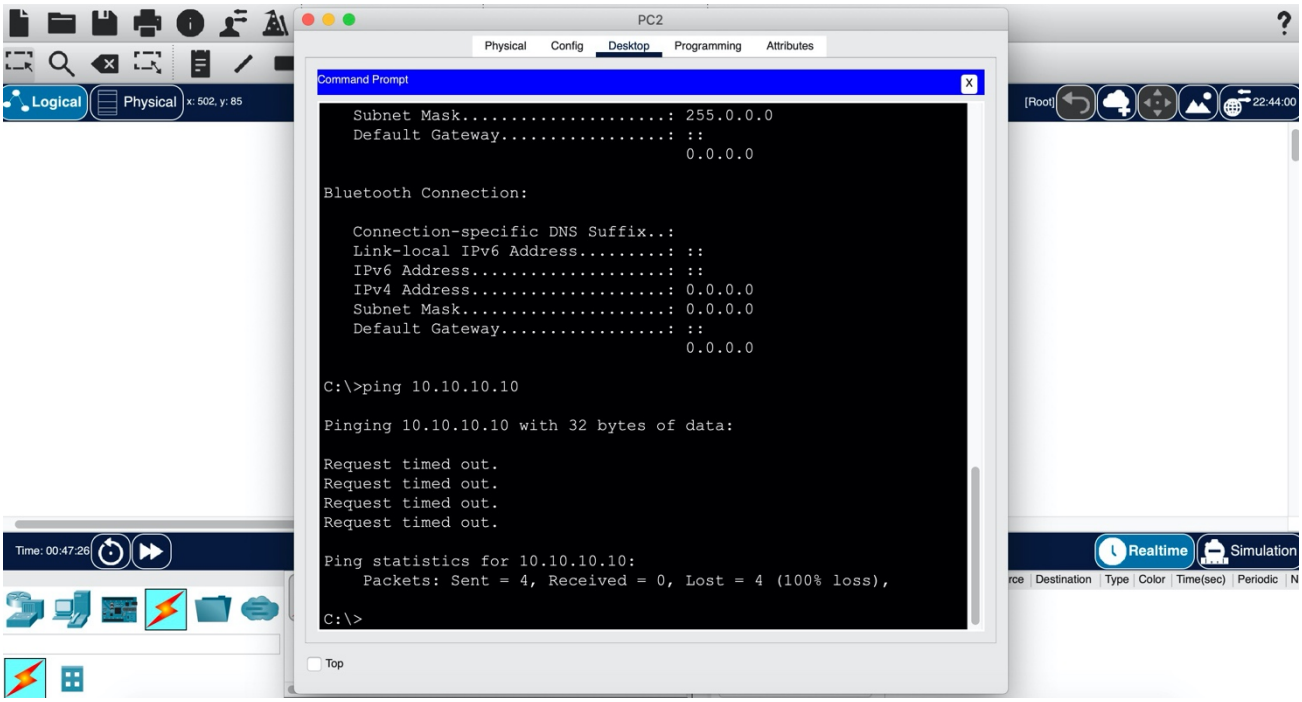


Research Task: What is meant by ‘remote wildcard mask’?

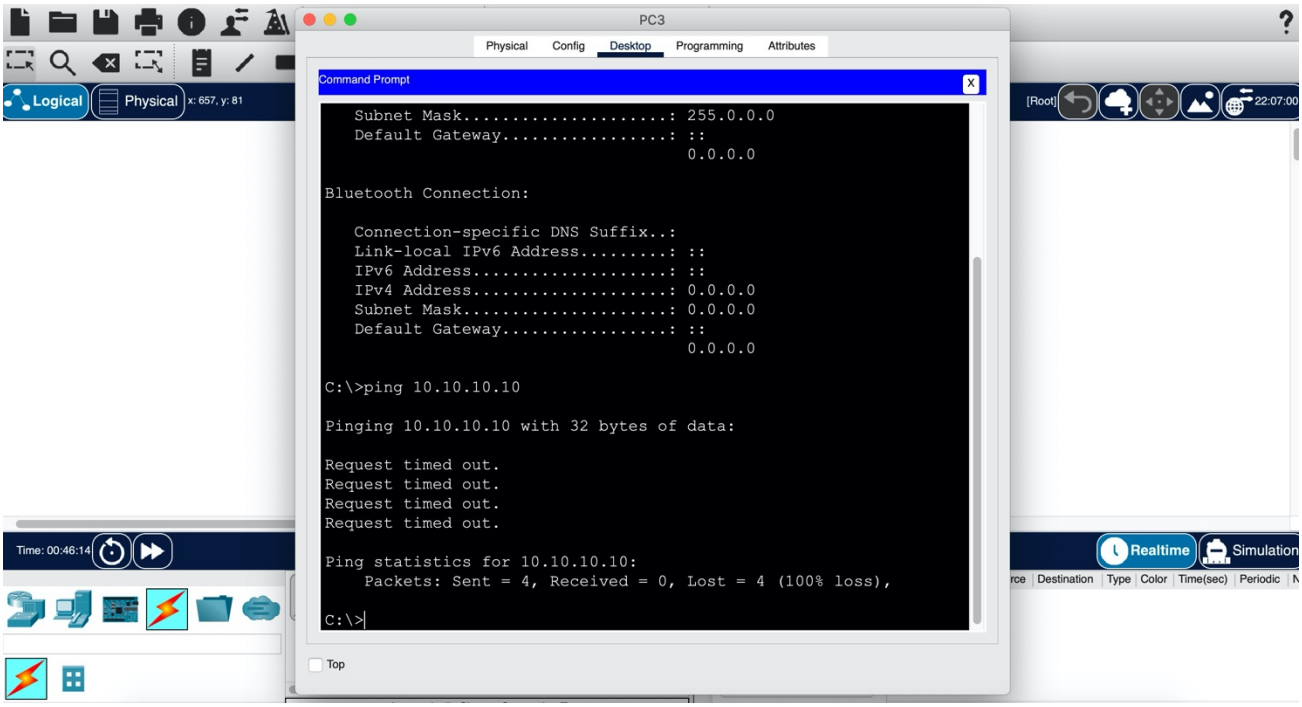
6 Testing Firewall Rules

Now the basic firewall settings have been implemented on PC1, try and ping PC1 from the other three devices. The ping should only be successful for PC4 (i.e., the PC which is allowed).

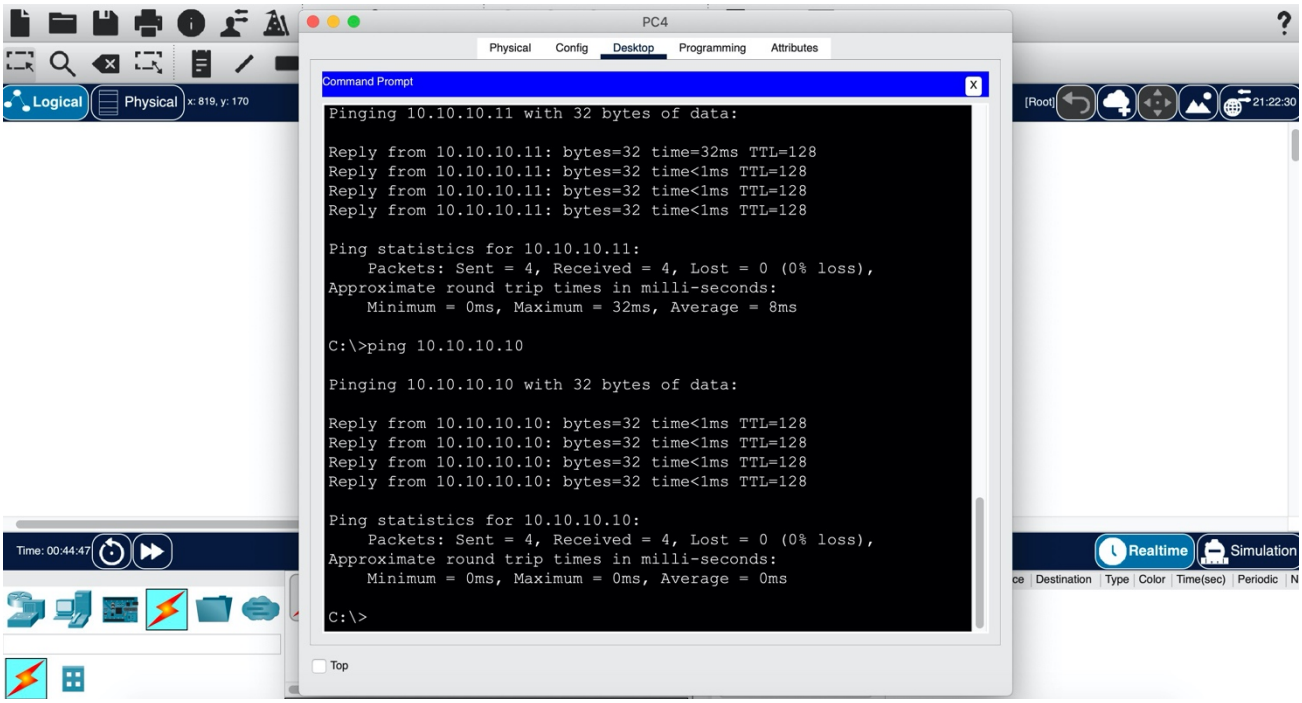
Unsuccessful Ping from PC2 (10.10.10.11)



Unsuccessful Ping from PC3 (10.10.10.12)



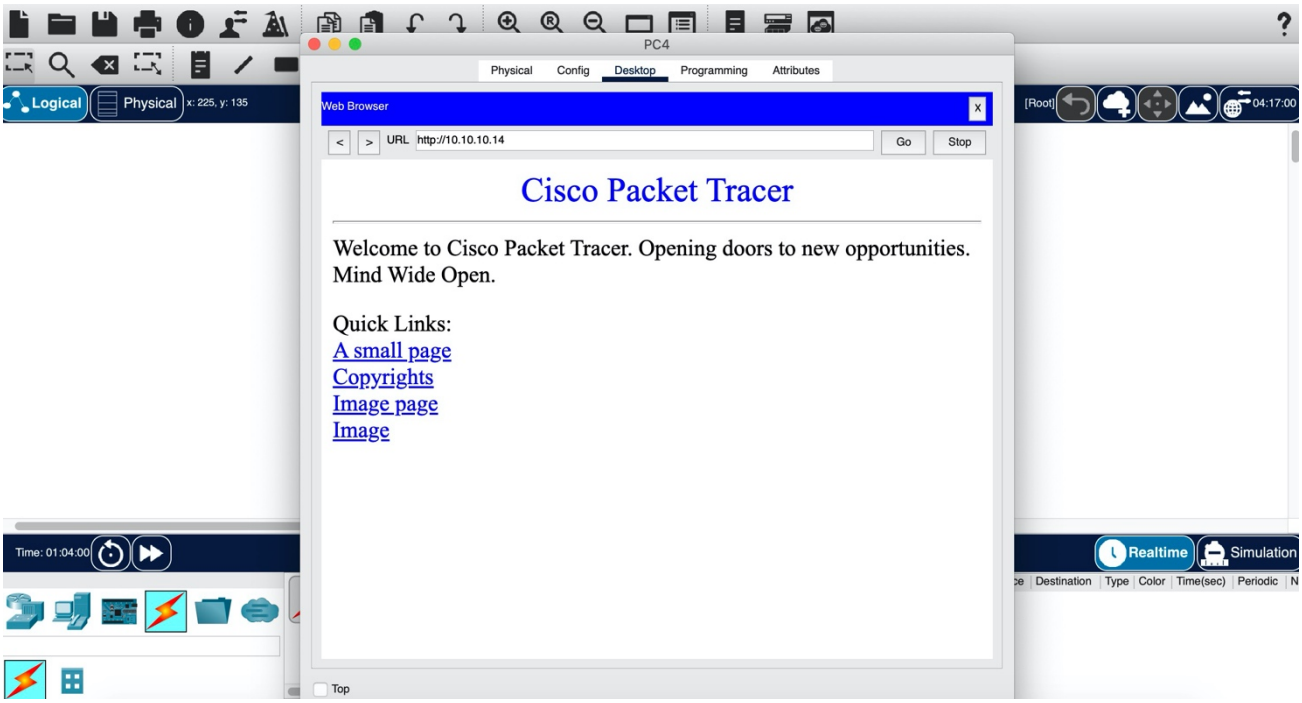
Successful Ping from PC4 (10.10.10.13)



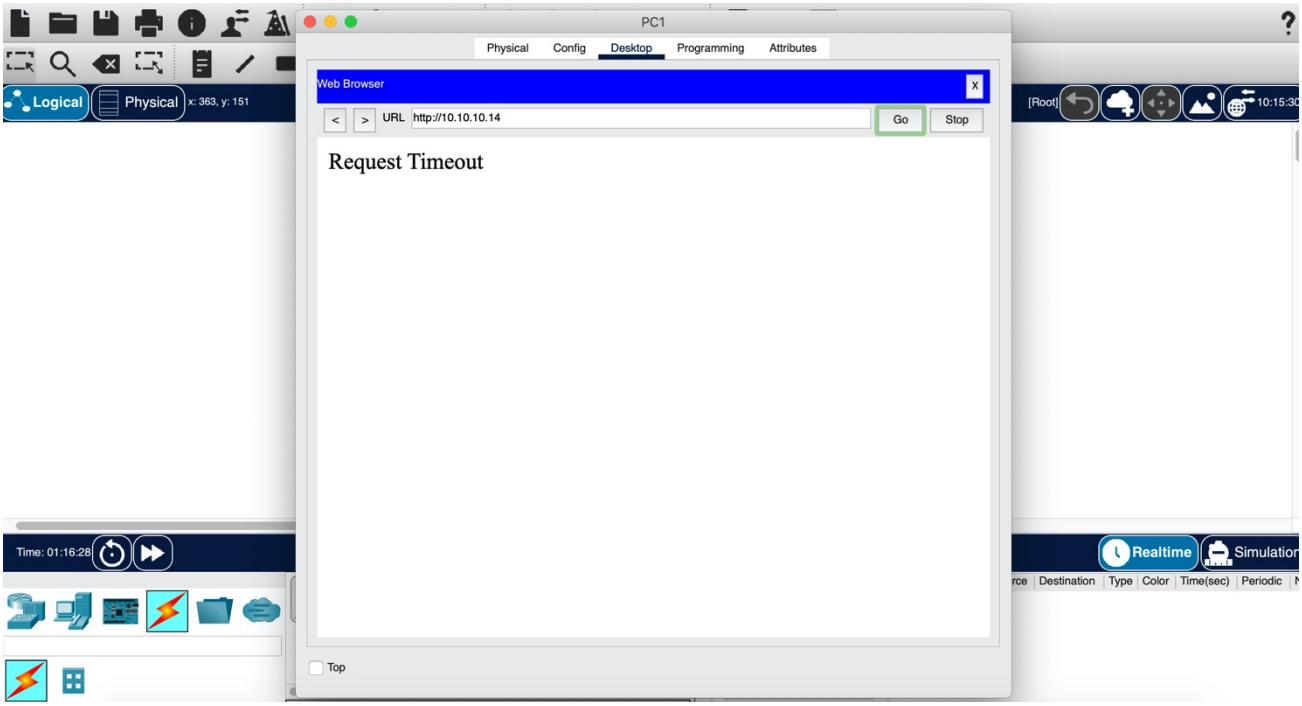
7 Filtering In-Bound Web Traffic

Now we are going to implement some firewall settings to allow or not allow in-bound web traffic from the server.

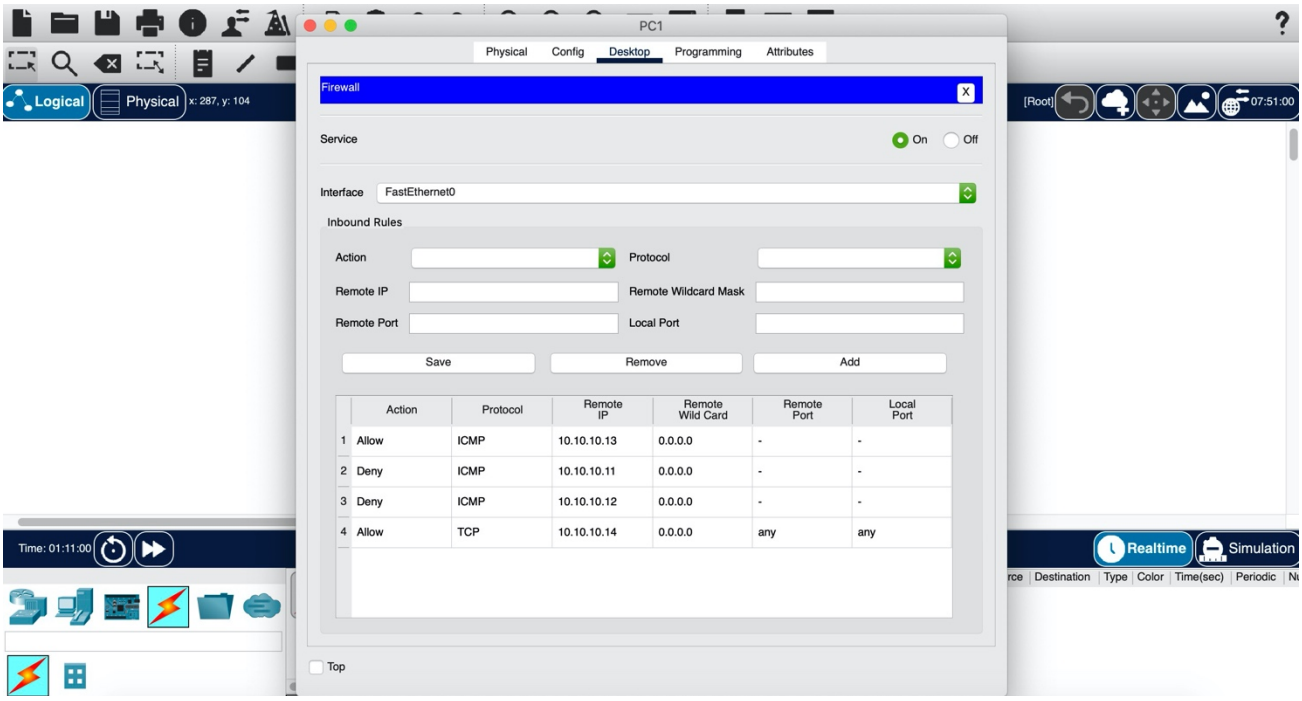
Go on to PC4, click on 'Web Browser' and enter the IP of the server (10.10.10.14). You should be able to connect to the internet and see the following:



However, if you do the same for PC1, this will not be the case. This is because we have set the firewall service to on, but in simplistic terms, we have not enabled (allowed) web traffic.

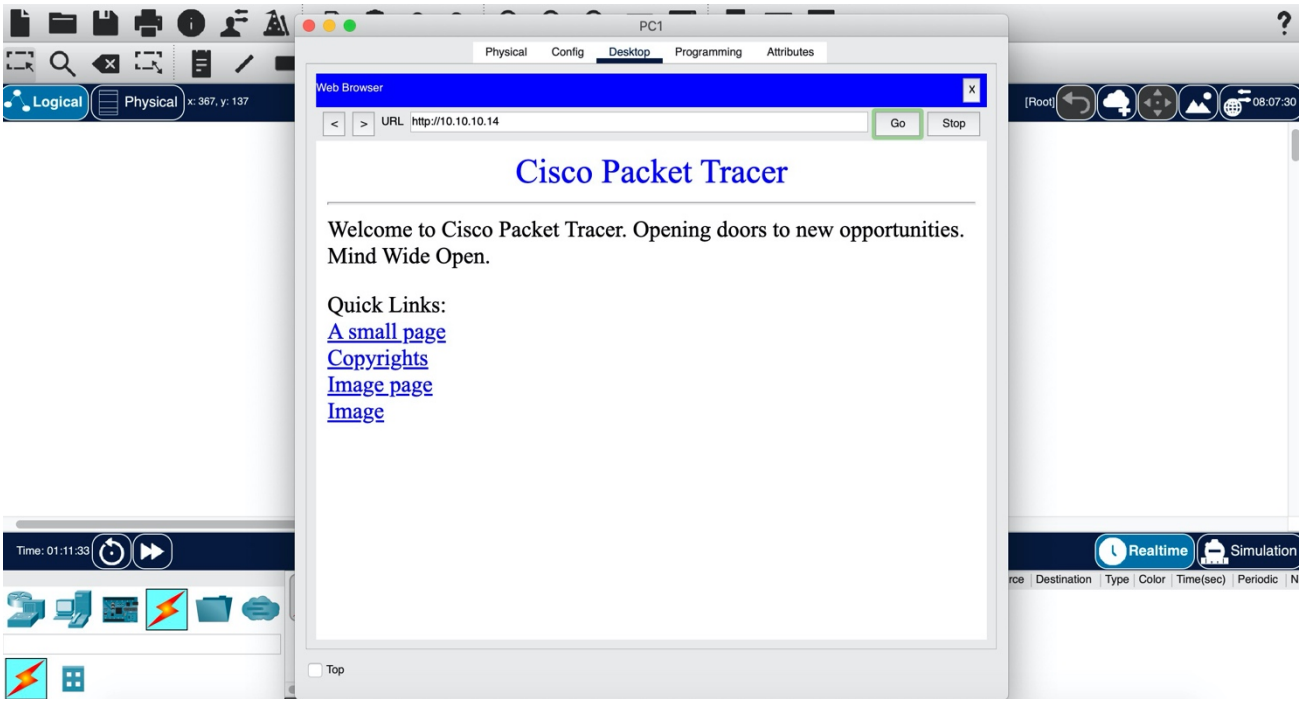


Hence, we need to go back to our firewall settings and do the following for PC1:

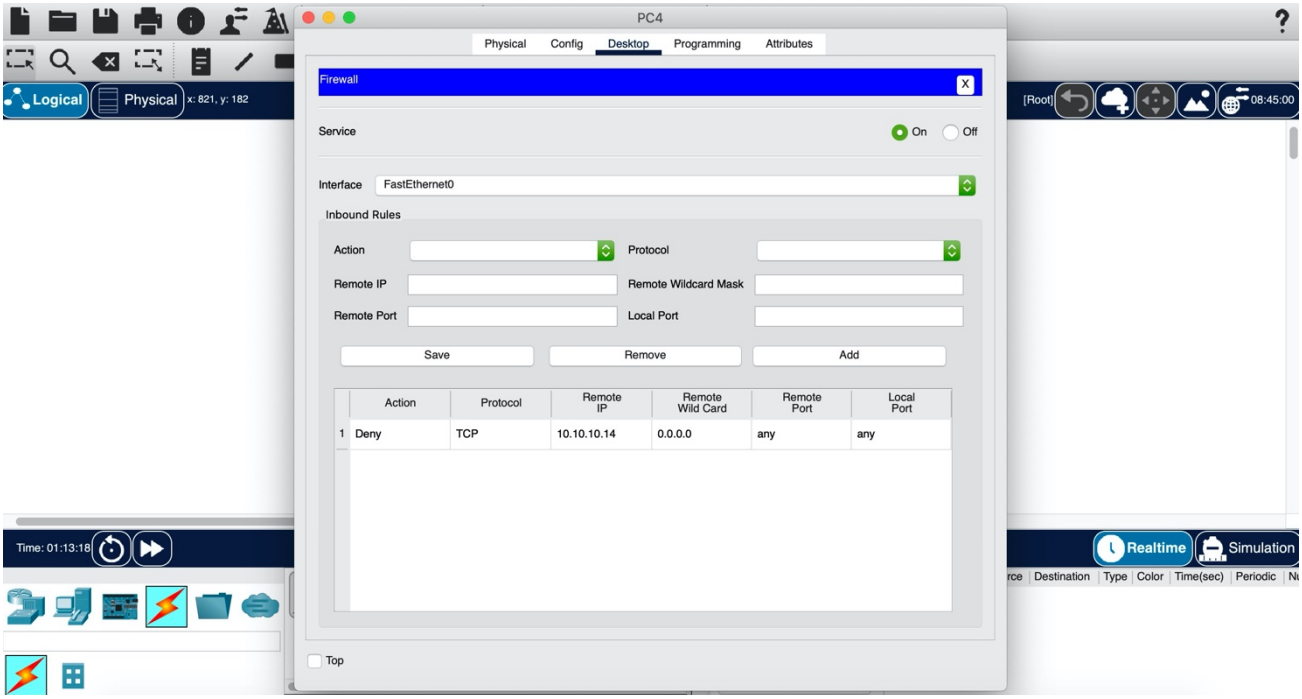


	Action	Protocol	Remote IP	Remote Wild Card	Remote Port	Local Port
1	Allow	ICMP	10.10.10.13	0.0.0.0	-	-
2	Deny	ICMP	10.10.10.11	0.0.0.0	-	-
3	Deny	ICMP	10.10.10.12	0.0.0.0	-	-
4	Allow	TCP	10.10.10.14	0.0.0.0	any	any

Now go back to the browser and enter the IP of the server, and we can now connect as seen below.



Finally, lets configure the firewall setting of PC4 to not allow access anymore:



As shown below, we can no longer connect since TCP traffic is denied and we receive a 'Request Timeout' message.

Practical Lab: Basic Firewall Implementation - JA