

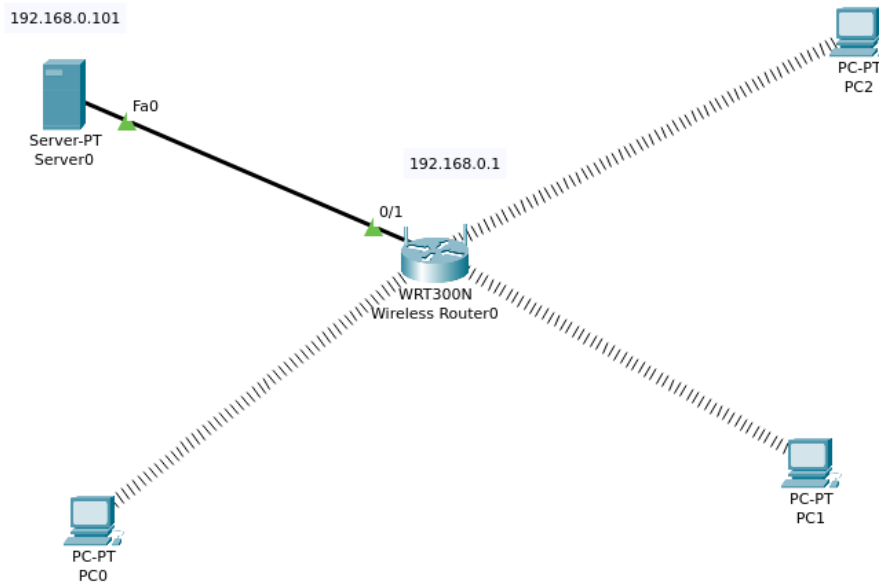
Practical 4

Aim: Planning Network-based Firewalls

Components:

- Server-PT
- WRT300N (Wireless Router)
- PC-PT - 3

Configure the system



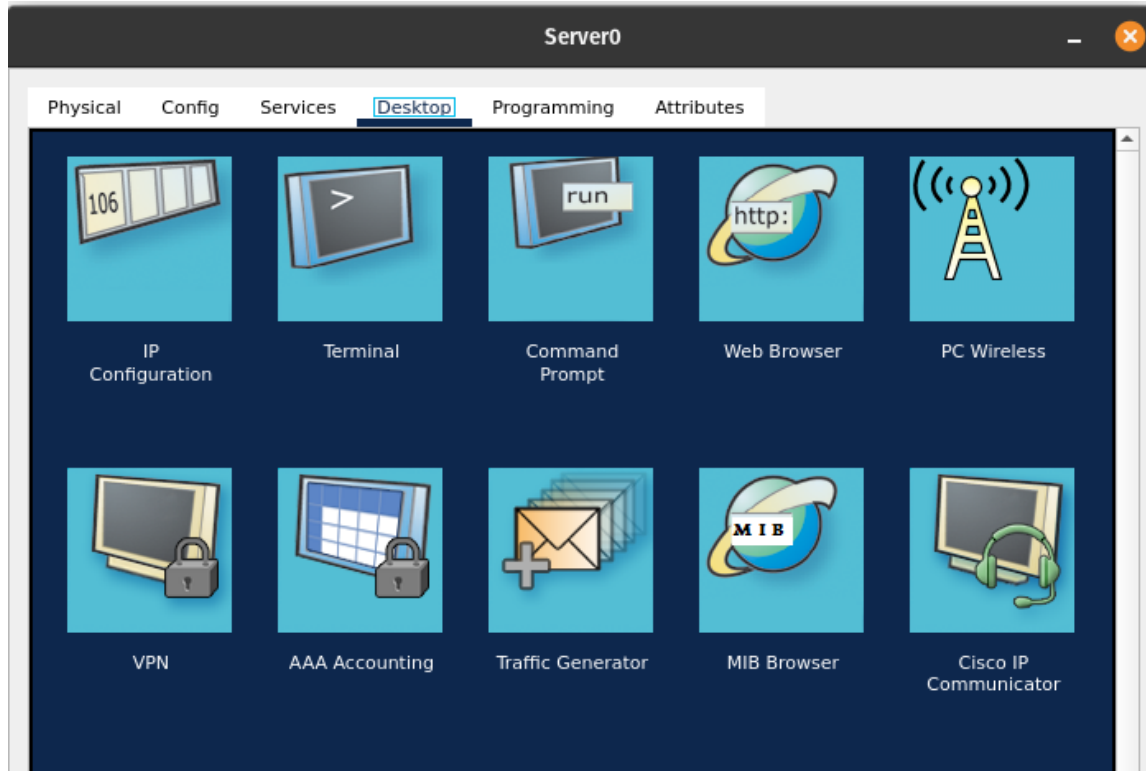
Wireless Router Configurations (Let it be default no change)

The screenshot shows the configuration interface for the Wireless Router0. The 'Setup' tab is active, displaying the following settings:

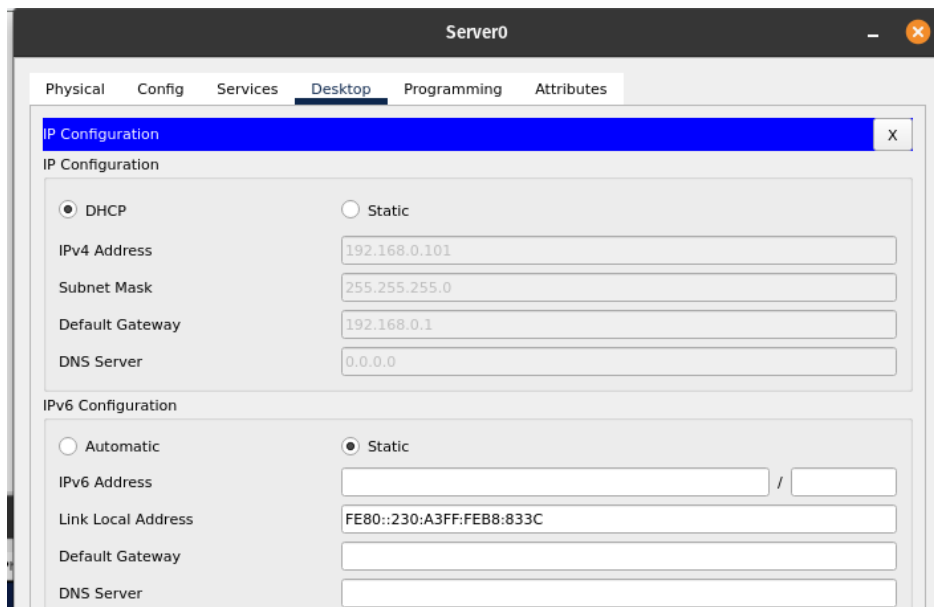
- Internet Setup:**
 - Internet Connection type: Automatic Configuration - DHCP
 - Optional Settings (required by some internet service providers):
 - Host Name: []
 - Domain Name: []
 - MTU: [] Size: 1500
- Network Setup:**
 - Router IP:
 - IP Address: 192 . 168 . 0 . 1
 - Subnet Mask: 255.255.255.0
 - DHCP Server Settings:
 - DHCP Server: Enabled Disabled
 - DHCP Reservation: []
 - Start IP Address: 192.168.0. 100
 - Maximum number of Users: 50
 - IP Address Range: 192.168.0. 100 - 149
 - Client Lease Time: 0 minutes (0 means one day)
 - Static DNS 1: 0 . 0 . 0 . 0

Configure the Server0

1. Click Server0 > Desktop > IP Configuration

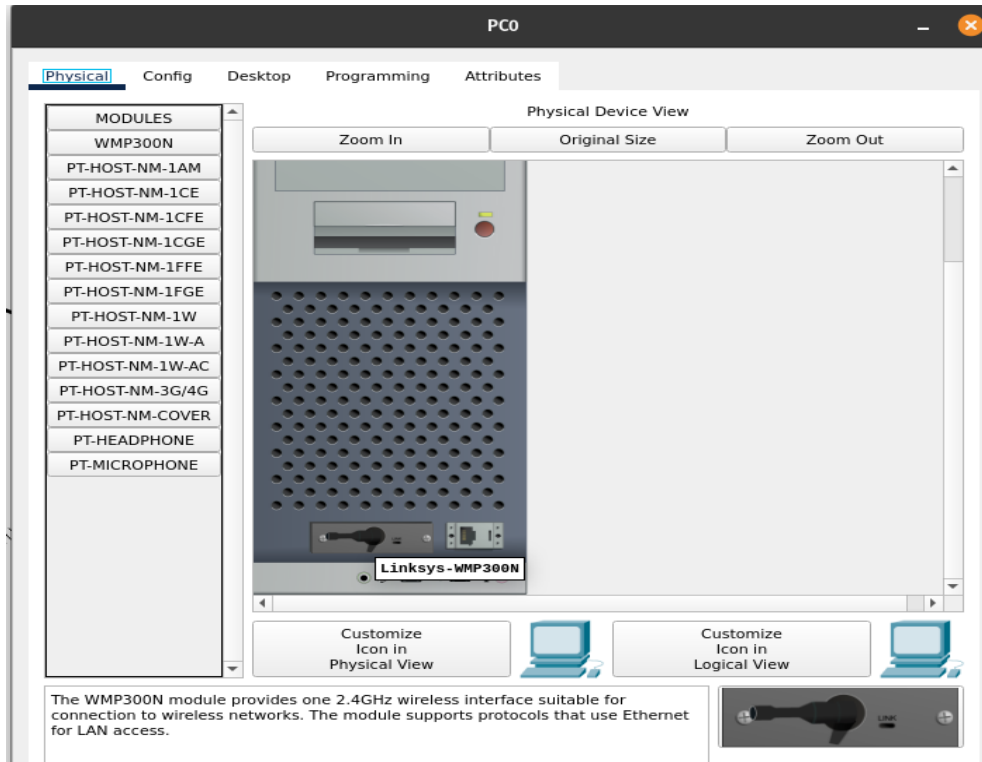


Set IP Configuration to DHCP



Configure the PC

1. Add the wireless interface after removing wired interface from it (turn OFF the PC before and turn back ON once done)



Check Connectivity between server and any PC

1. Open PC CMD



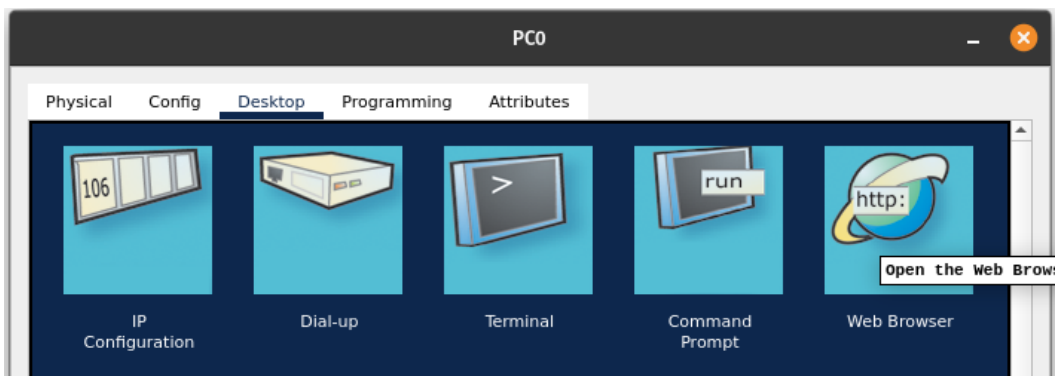
```
Cisco Packet Tracer PC Command Line 1.0
C:\>
ping 192.168.0.101

Pinging 192.168.0.101 with 32 bytes of data:

Reply from 192.168.0.101: bytes=32 time=27ms TTL=128
Reply from 192.168.0.101: bytes=32 time=11ms TTL=128
Reply from 192.168.0.101: bytes=32 time=12ms TTL=128
Reply from 192.168.0.101: bytes=32 time=18ms TTL=128

Ping statistics for 192.168.0.101:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 11ms, Maximum = 27ms, Average = 17ms
```

2. Open Web Browser



Enter the IP address of the server

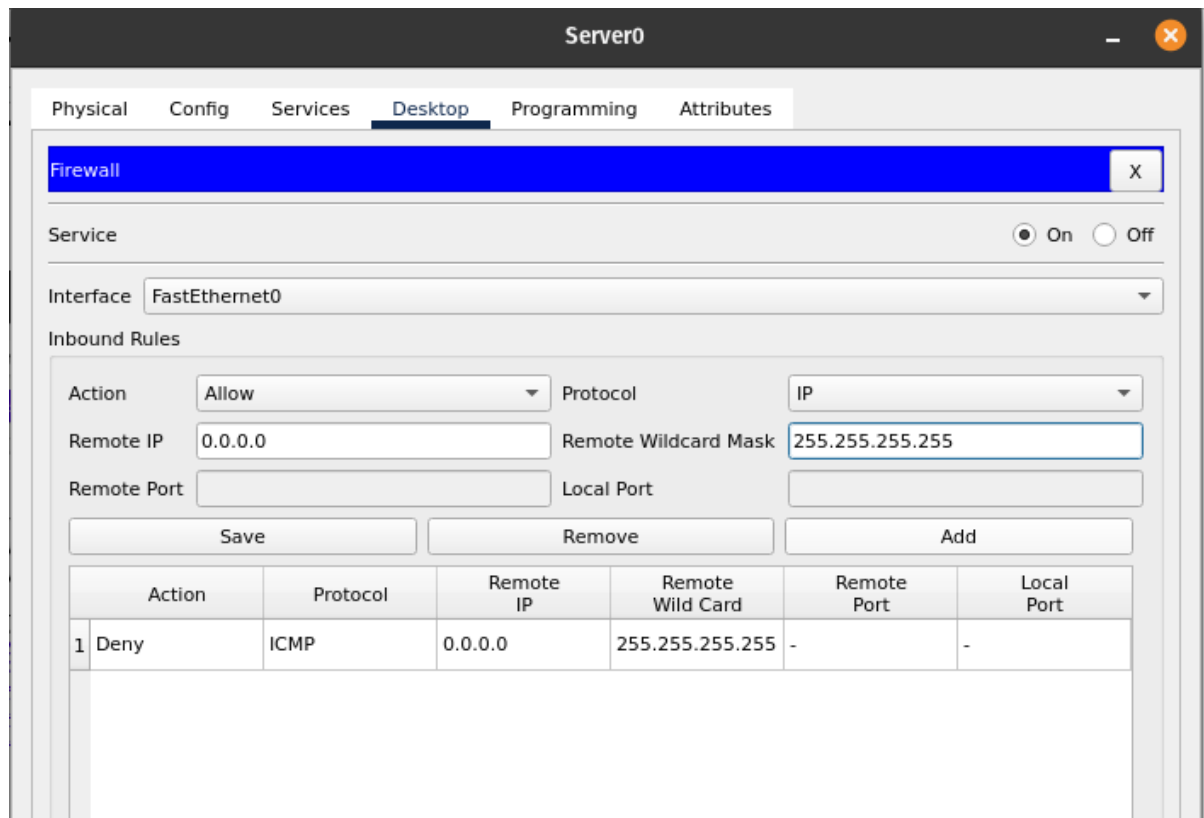


Currently Both IP and ICMP protocol are enabled by the Server, Next we will deny the ICMP and allow IP protocol to work as it is.

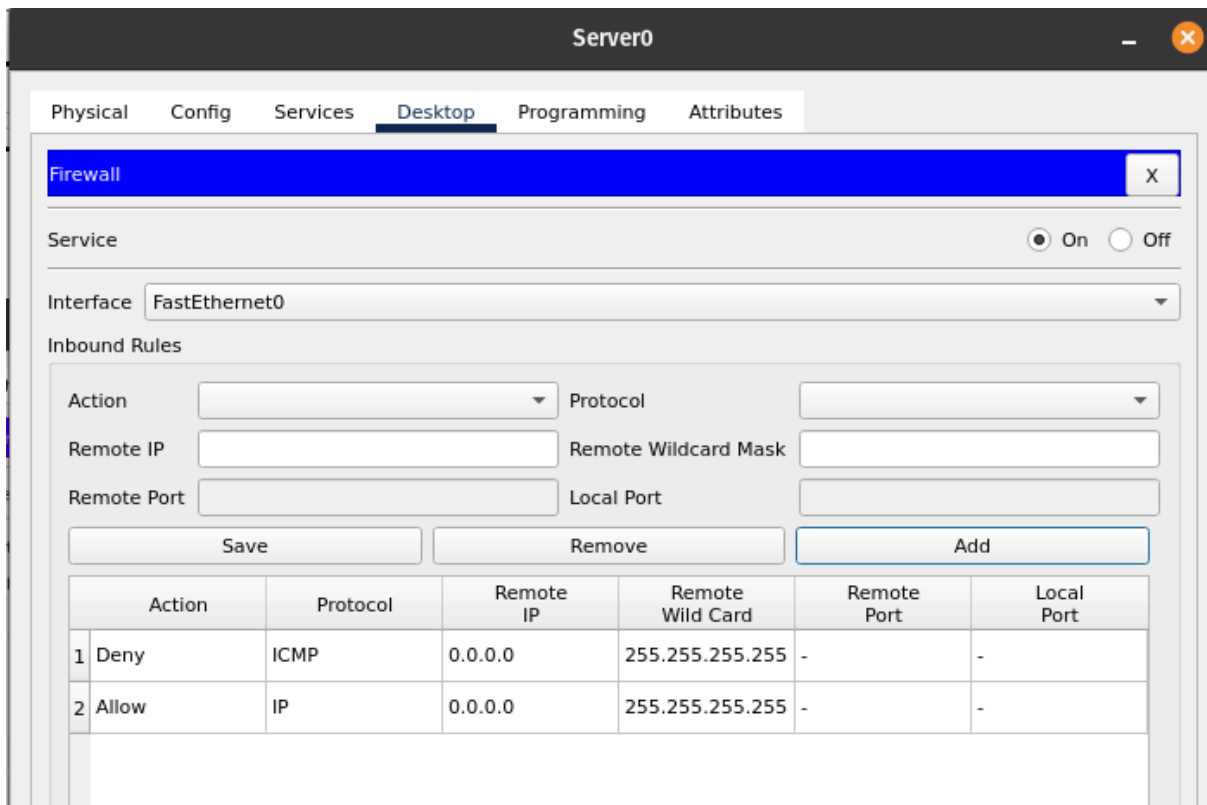
Configure the Server Firewall rule



1. Add a rule to deny the ICMP protocol

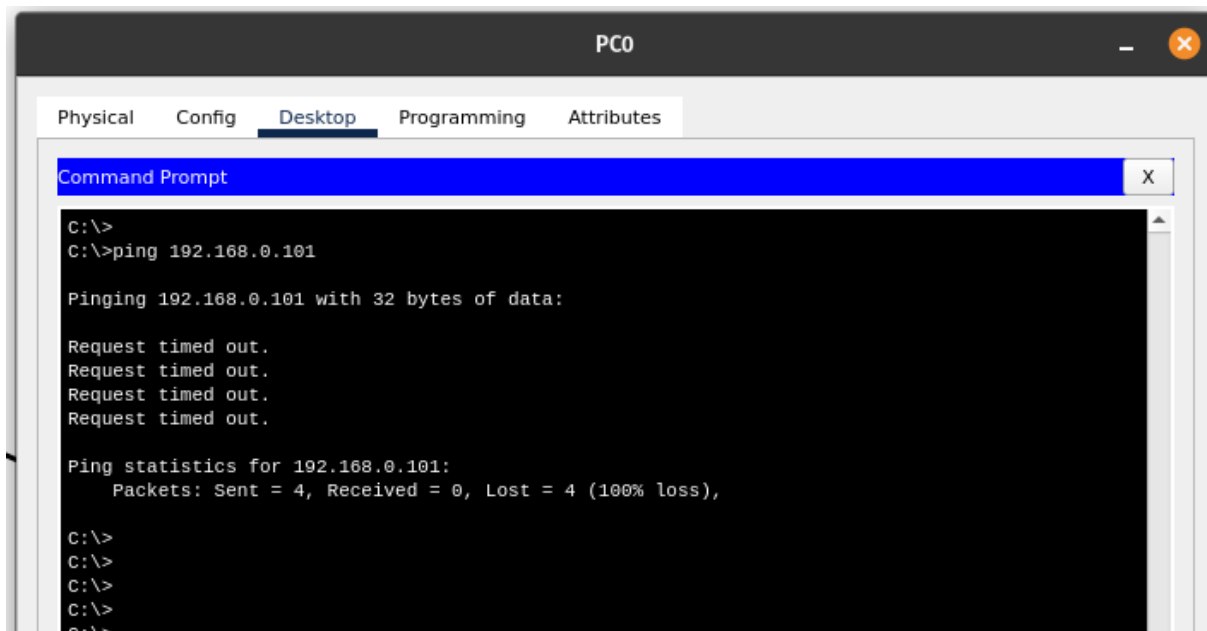


2. Add rule to allow IP protocol



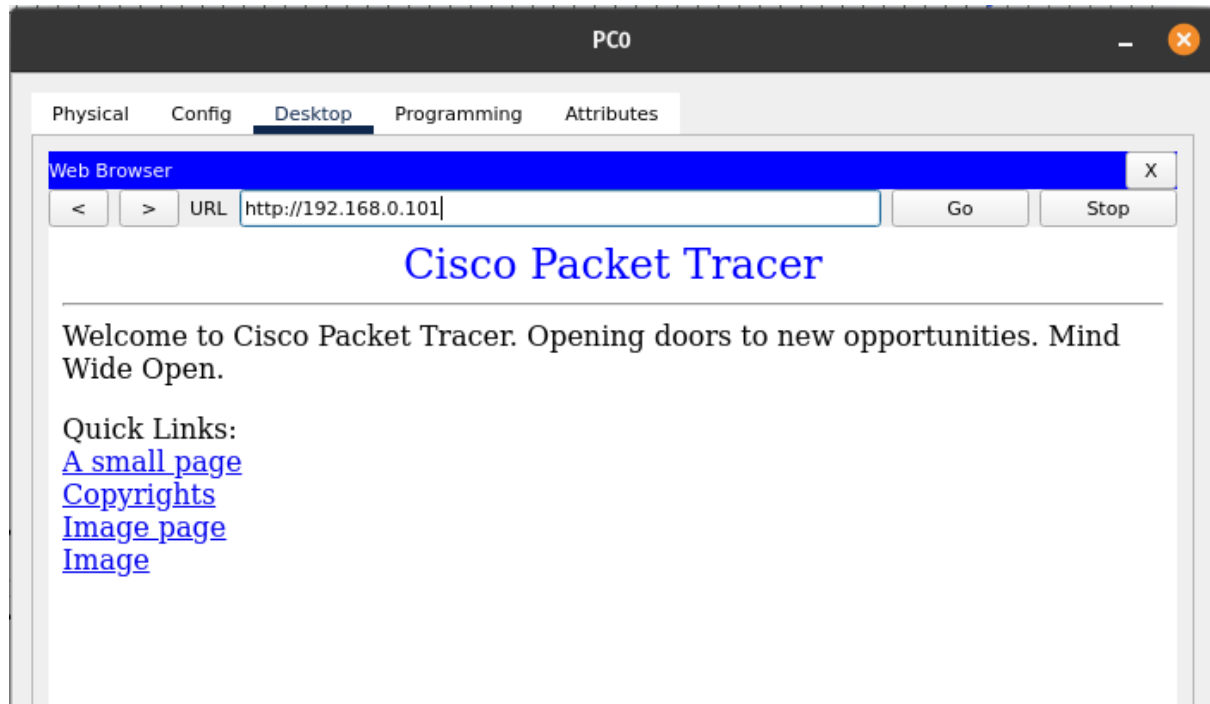
Check the output

1. Ping the server again



ICMP protocol is disabled as you can see

2. Visit server IP in PC web Browser again



IP protocol is still allowed as Expected, you can try to ping the server from the other 2 PC as well it will result the same output.