NETWORKING ESSENTIALS WORKBOOK 2

Name: Lidia Pascu
Course Date: 30/06/2025
Programme:

Contents

BUILD A HOME NETWORK

Task 12a:

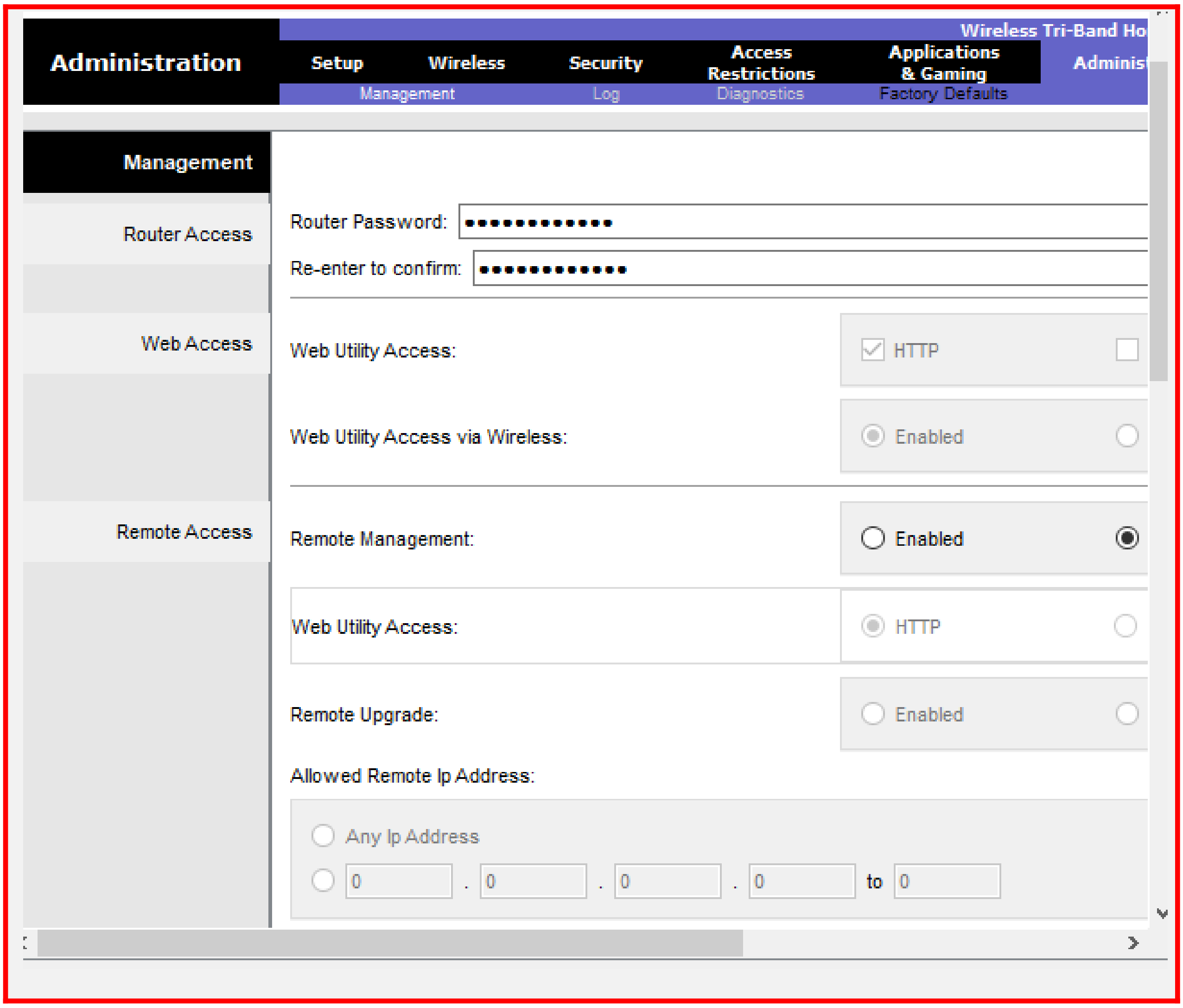
Define the following network terminologies by using statements from the below.

Terminology	Definition
Ethernet port	● Usually labeled "Ethernet" or "LAN", these ports connect to the internal switch portion of the router
Internet Port	● Used to connect the device to another network, such as the internet, through a cable or DSL modem
Network Name (SSID)	● Used to identify the WLAN. All devices that wish to participate in the WLAN must have the same SSID
SSID Broadcast	● Determines if the SSID will be broadcast to all devices within range. By default, set to Enabled.

Task 12b:

Once you have completed Packet Tracer – ***Configure a Wireless Router and Client***,, paste the following evidence in the boxes below.

Wireless SSID changed



Router Password: ••••••••••••

Re-enter to confirm: ••••••••••••

Web Utility Access: ☑ HTTP □

Web Utility Access via Wireless: ● Enabled ○

Remote Management: ○ Enabled ●

Web Utility Access: ● HTTP ○

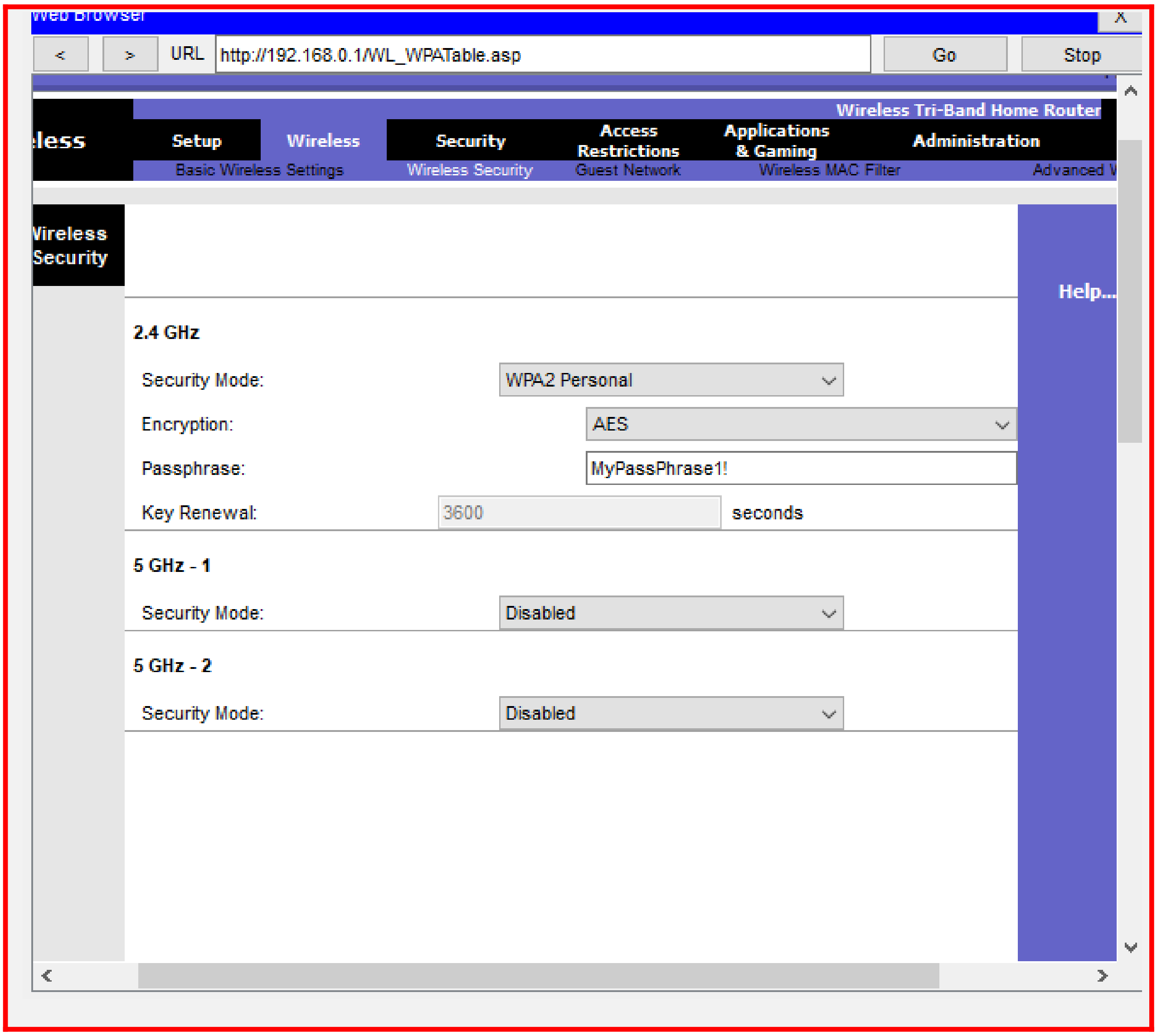
Remote Upgrade: ○ Enabled ○

Allowed Remote Ip Address:

○ Any Ip Address

○ 0 . 0 . 0 . 0 to 0

Security mode set to WPA2 Personal with a Passphrase



2.4 GHz

Security Mode: WPA2 Personal

Encryption: AES

Passphrase: MyPassPhrase1!

Key Renewal: 3600 seconds

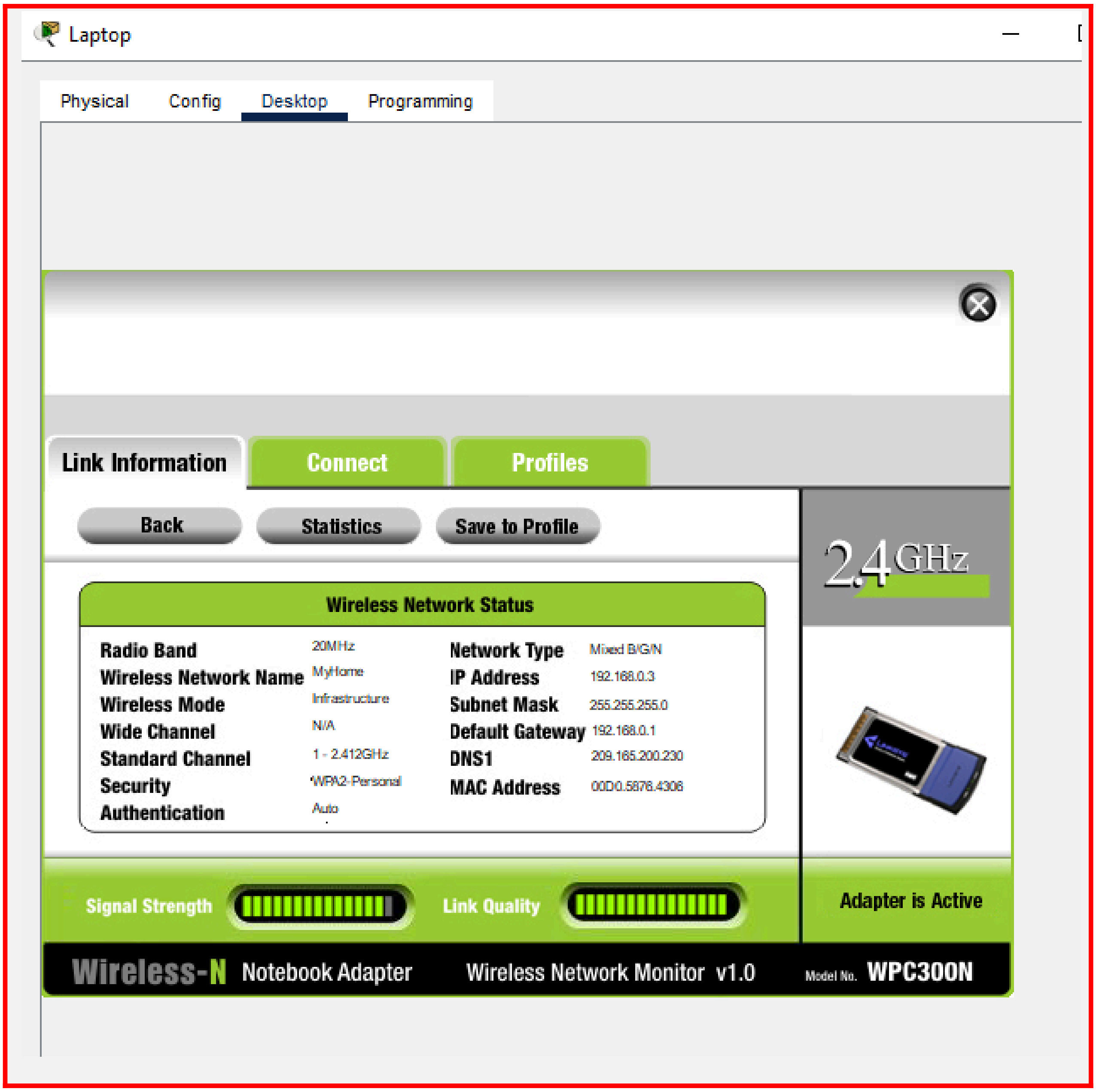
5 GHz - 1

Security Mode: Disabled

5 GHz - 2

Security Mode: Disabled

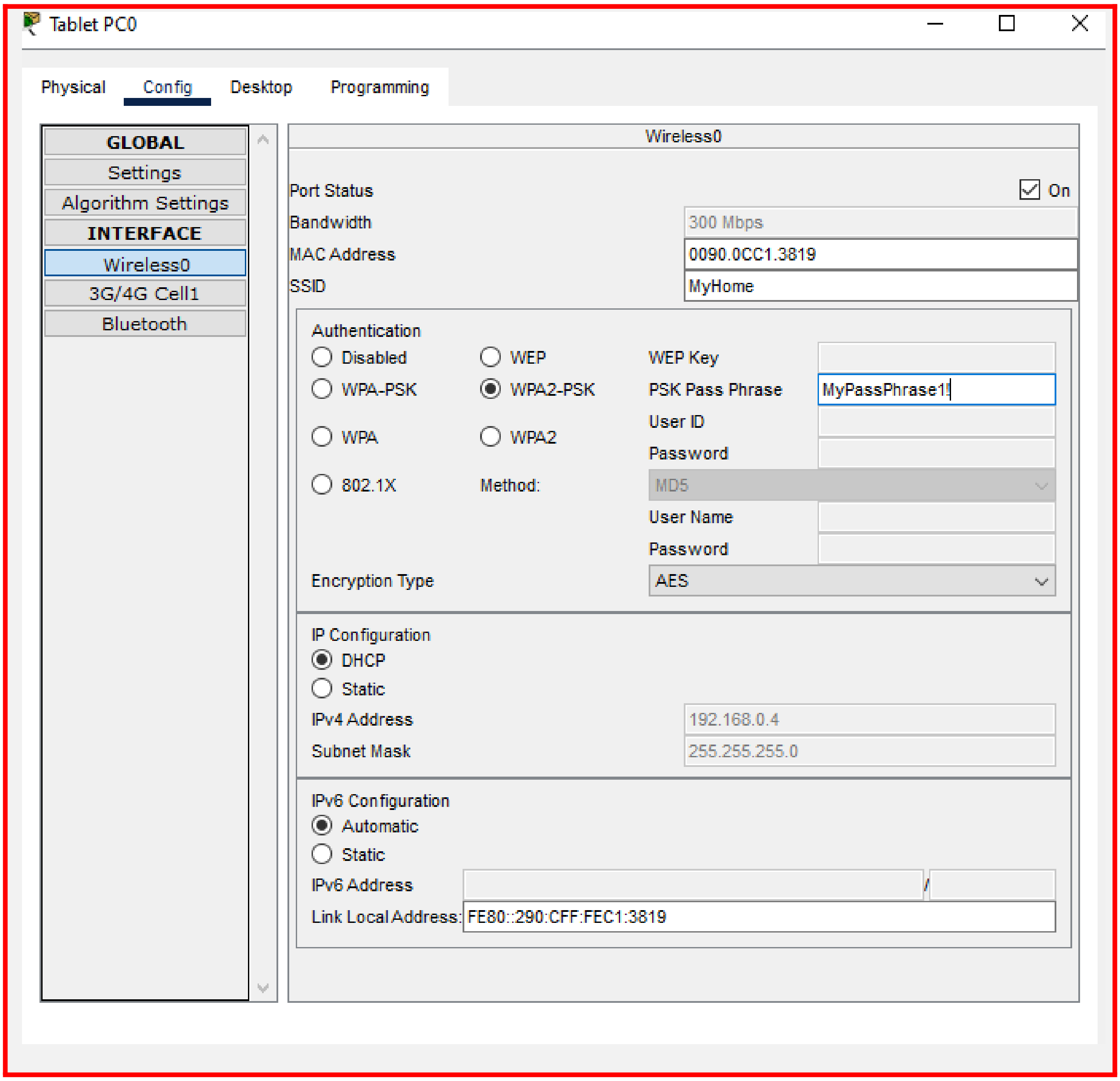
SSID and Passphrase setting on a laptop



Wireless Network Status

Radio Band	20MHz	Network Type	Mixed B/G/N
Wireless Network Name	MyHome	IP Address	192.168.0.3
Wireless Mode	Infrastructure	Subnet Mask	255.255.255.0
Wide Channel	N/A	Default Gateway	192.168.0.1
Standard Channel	1 - 2.412GHz	DNS1	209.165.200.230
Security	'WPA2-Personal	MAC Address	00D0.5876.4306
Authentication	Auto		

SSID and Passphrase setting on a tablet



Port Status ☑ On

Bandwidth 300 Mbps

MAC Address 0090.0CC1.3819

SSID MyHome

Authentication

○ Disabled ○ WEP WEP Key

○ WPA-PSK ● WPA2-PSK PSK Pass Phrase MyPassPhrase1!

User ID

○ WPA ○ WPA2 Password

○ 802.1X Method: MD5

User Name

Password

Encryption Type AES

IP Configuration

● DHCP

○ Static

IPv4 Address 192.168.0.4

Subnet Mask 255.255.255.0

IPv6 Configuration

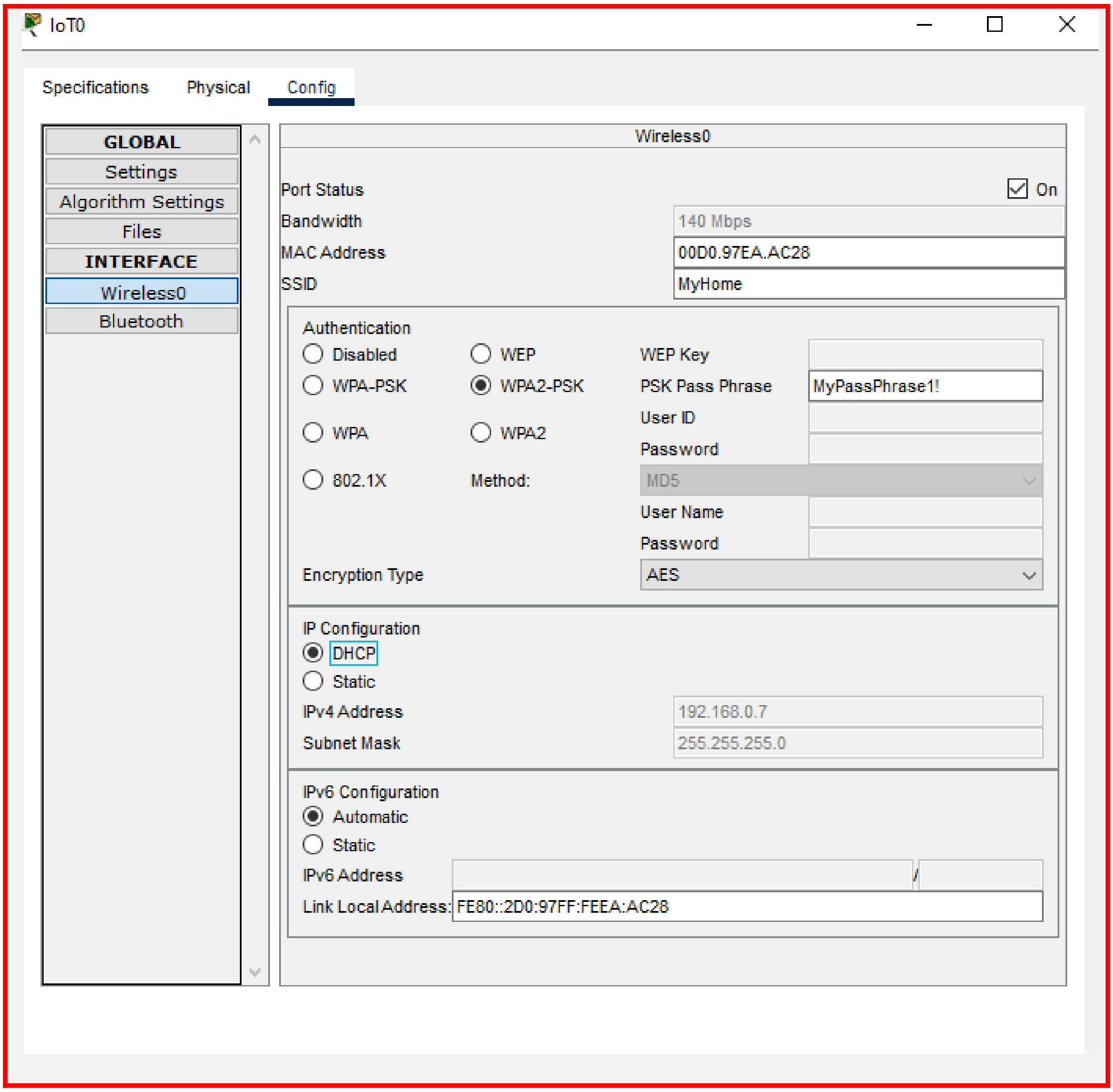
● Automatic

○ Static

IPv6 Address /

Link Local Address: FE80::290:CFF:FEC1:3819

SSID and Passphrase setting on a IoT device



Wireless0

Port Status ☑ On

Bandwidth: 140 Mbps

MAC Address: 00D0.97EA.AC28

SSID: MyHome

Authentication

○ Disabled ○ WEP WEP Key:

○ WPA-PSK ● WPA2-PSK PSK Pass Phrase: MyPassPhrase1!

User ID:

○ WPA ○ WPA2 Password:

○ 802.1X Method: MD5

User Name:

Password:

Encryption Type: AES

IP Configuration

● DHCP

○ Static

IPv4 Address: 192.168.0.7

Subnet Mask: 255.255.255.0

IPv6 Configuration

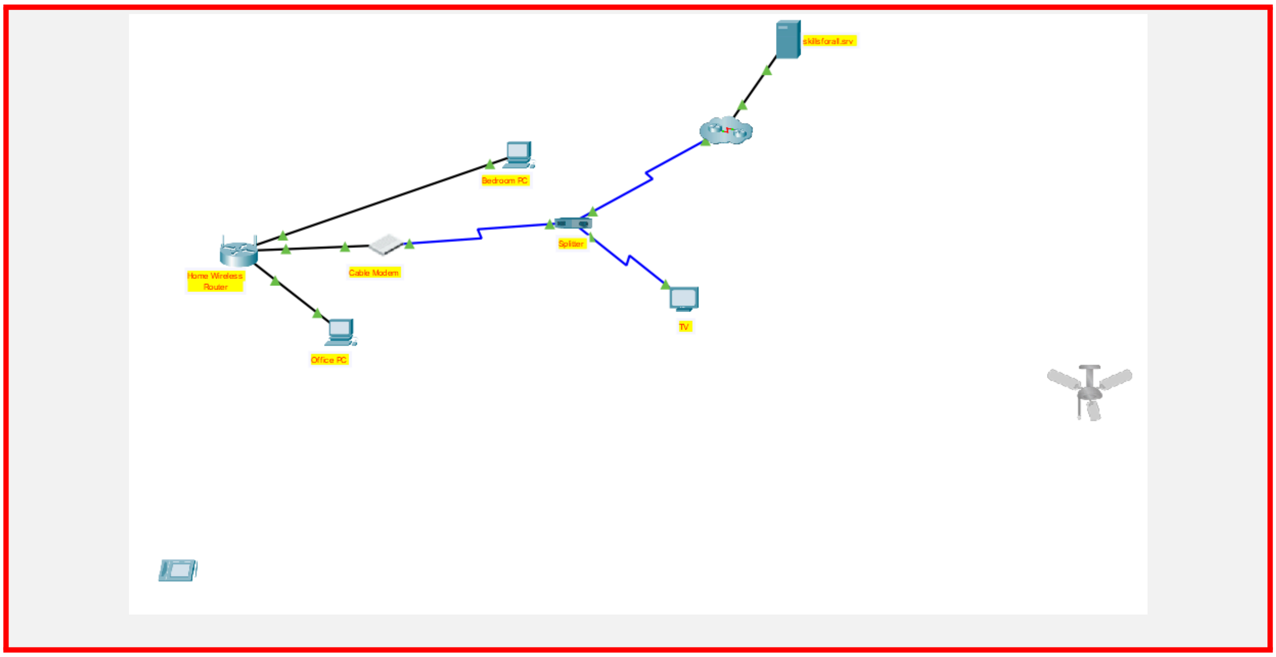
● Automatic

○ Static

IPv6 Address: /

Link Local Address: FE80::2D0:97FF:FEEA:AC28

Logical wireless router and client network



CONNECT TO THE INTERNET

Task 13a:

Match the following descriptions to the correct terminology from the list below.

Cable	Satellite	ISP	Cellular	DSL	Dial-up

Description	Terminology
Provides a high bandwidth, always on, connection to the internet. It runs over a telephone line, with the line split into three channels. One channel is for voice and the other two channels are for data downloading and uploading.	DSL

Provides the link between the home network and the internet	ISP
Uses a cell phone network to connect. Performance will be limited by the capabilities of the phone and the cell tower to which it is connected.	Cellular
Typically offered by television service providers, the internet data signal is carried on the same coaxial cable that delivers the services. A special cable modem separates the internet data signal from the other signals carried on the cable	Cable
An inexpensive option that uses any phone line and a modem. To connect to the ISP, a user calls the ISP access phone number. The low bandwidth provided by a modem connection is usually not sufficient for large data transfer.	Dial-up
Is a good option for homes or offices that do not have access to DSL or cable. A dish requires a clear line of sight to the satellite and so might be difficult in heavily wooded areas or places with other overhead obstructions.	Satellite

Task 13b:

Read the statement carefully and then fill in the missing words.

Applications and services offered in a public cloud are available to the general population. Services may be free or are offered on a pay-per-use model.

A community cloud is created for exclusive use by a specific community. The functional needs have been customized for the community. For example, healthcare organizations.

A hybrid cloud is made up of two or more clouds (example: part private, part public), where each part remains a separate object, but both are connected using a single architecture.

Applications and services offered in a private cloud are intended for a specific organization or entity, such as the government.

Task 13c:

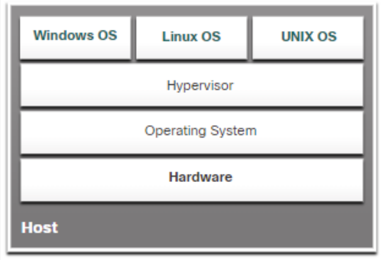
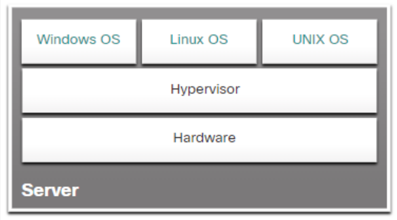
In your own words, describe the following cloud *services*.

Cloud Service	Description
Software-as-a-Service	This is when you use software over the internet without needing to install it. Everything is managed for you, just log in and use it. Examples include Gmail, Microsoft 365, and Zoom.
Platform-as-a-Service	This gives developers a place to build, test, and deploy apps without managing the underlying hardware or software. It provides the tools and environment needed to create software. Examples include Google App Engine and Microsoft Azure App Services.
Infrastructure-as-a-Service	This provides basic computing resources like servers, storage, and networking. You rent these resources and control the operating systems and applications yourself. Examples include Amazon Web Services (AWS) and Microsoft Azure.

Task 13d:

Using the images in the table, state which hypervisor it is, and then provide short description of it.

Image	Hypervisor Type	Description

 Windows OS Linux OS UNIX OS Hypervisor Operating System Hardware Host	Type 2 Hypervisor - "Hosted" Approach	A Type 2 hypervisor is software that creates and runs VM instances on a host computer. A Type 2 hypervisor is installed on top of the existing OS on the host. One or more additional OS instances are installed on top of the hypervisor.
 Windows OS Linux OS UNIX OS Hypervisor Hardware Server	Type 1 Hypervisor - "Bare Metal" Approach	Type 1 hypervisor is installed directly on the server or networking hardware. Type 1 hypervisor have direct access to the hardware resources. They are more efficient than hosted architectures. Instances of an OS are installed on the hypervisor.

SECURITY CONSIDERATIONS

Task 14a:

Match the correct security threat to its description.

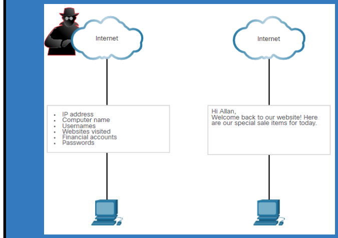
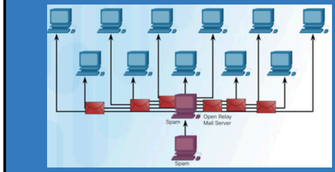
External	Internal	Information theft	Data loss	Disruption of service	Identity theft

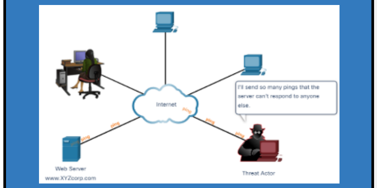
Description	Security Threat
It occurs when someone has authorized access to the network through a user account or has physical access to the network equipment.	Internal
Breaking into a computer to obtain confidential information.	Information theft
Form of information theft where personal information is stolen for the purpose of taking over the identity of someone.	Identity theft
Arise from individuals outside of an organization who do not have authorized access to the computer systems or network.	External
Breaking into a computer to destroy or alter data records.	Data loss

Preventing legitimate users from accessing services to which they are entitled.	Disruption of service

Task 14b:

Using the images from the table below, identify what malware it is and then provide a description of it.

Image	Malware	Description
	Viruses	Attaches itself to legitimate programs or files and replicates when the host is executed, often causing harm such as corrupting data, slowing system performance, or spreading to other systems. - Requires human action to activate (e.g., opening an infected file). - Can spread through email attachments, USB drives, or downloads. - Often used to steal information, disrupt operations, or damage systems.
	Trojan Horse	**Malware disguised as legitimate software.** Once installed, it gives attackers access to your system or steals data without your knowledge.
	Worms	**A self-replicating program that spreads through networks without human interaction.** Worms often consume bandwidth or overload systems, leading to denial of service.
 - IP address - Computer name - Usernames - Websites visited - Financial accounts - Passwords Hi Allan, Welcome back to our website! Here are our special sale items for today.	Spyware	**Secretly gathers user information (like keystrokes, passwords, or browsing habits)** and sends it to third parties without consent.
	Botnets and Zombies	**Botnets** - A **network of compromised computers or devices ("bots") controlled remotely by a cybercriminal**, usually without the users' knowledge. They are commonly used to: - Launch **Distributed Denial of Service (DDoS)** attacks - **Send spam emails** - **Steal data** - Spread **malware** to other devices **Zombies** - A **single compromised computer or device** in a botnet that is **under the control of a hacker (botmaster)**. It performs malicious tasks like: - Participating in DDoS attacks - Sending spam - Logging keystrokes or stealing information - Spreading malware to others

 Internet ping I'll send so many pings that the server can't respond to anyone else. Web Server www.XYZcorp.com Threat Actor	Denial of Service	**Distributed Denial of Service (DDoS)** - Comes from multiple systems (often a **botnet** of zombie computers), making it harder to block. - Flooding a website with fake traffic until it crashes. - Sending malformed packets to exploit a vulnerability and cause system failure. A **Brute Force Attack** is a **trial-and-error method** used by attackers to **crack passwords, encryption keys, or login credentials** by systematically trying all possible combinations until the correct one is found. **SYN flooding** is a type of **Denial of Service (DoS)** attack that **exploits the TCP handshake process** to **overload a target server with half-open connections**, making it unable to handle legitimate traffic. The **Ping of Death (PoD)** is a type of **Denial of Service (DoS) attack** that involves **sending malformed or oversized ping (ICMP) packets** to a target device, causing it to crash, freeze, or reboot.

Task 14c:

Complete the table below by inserting the correct security tool in its description.

Virus protection	Popup blocker	Firewall	Spam blocker	Spyware protection	Patches and updates

Security Tool or Application	Description
Firewall	A security tool that controls traffic to and from a network.
Patches and updates	Software that is applied to an OS or application to correct a known security vulnerability or add functionality.
Virus protection	Antivirus software is installed on an end-user workstation or server to detect and remove viruses, worms, and Trojan horses from files and email.
Spyware protection	Antispyware software is installed on an end-user workstation to detect and remove spyware and adware.
Spam blocker	Software is installed on an end-user workstation or server to identify and remove unwanted emails.
Popup blocker	Software is installed on an end-user workstation to prevent popup and pop-under advertisement windows from displaying.

CONFIGURE NETWORK AND DEVICE SECURITY

Task 15a:

Complete the table below by identifying correct authentication protocol.

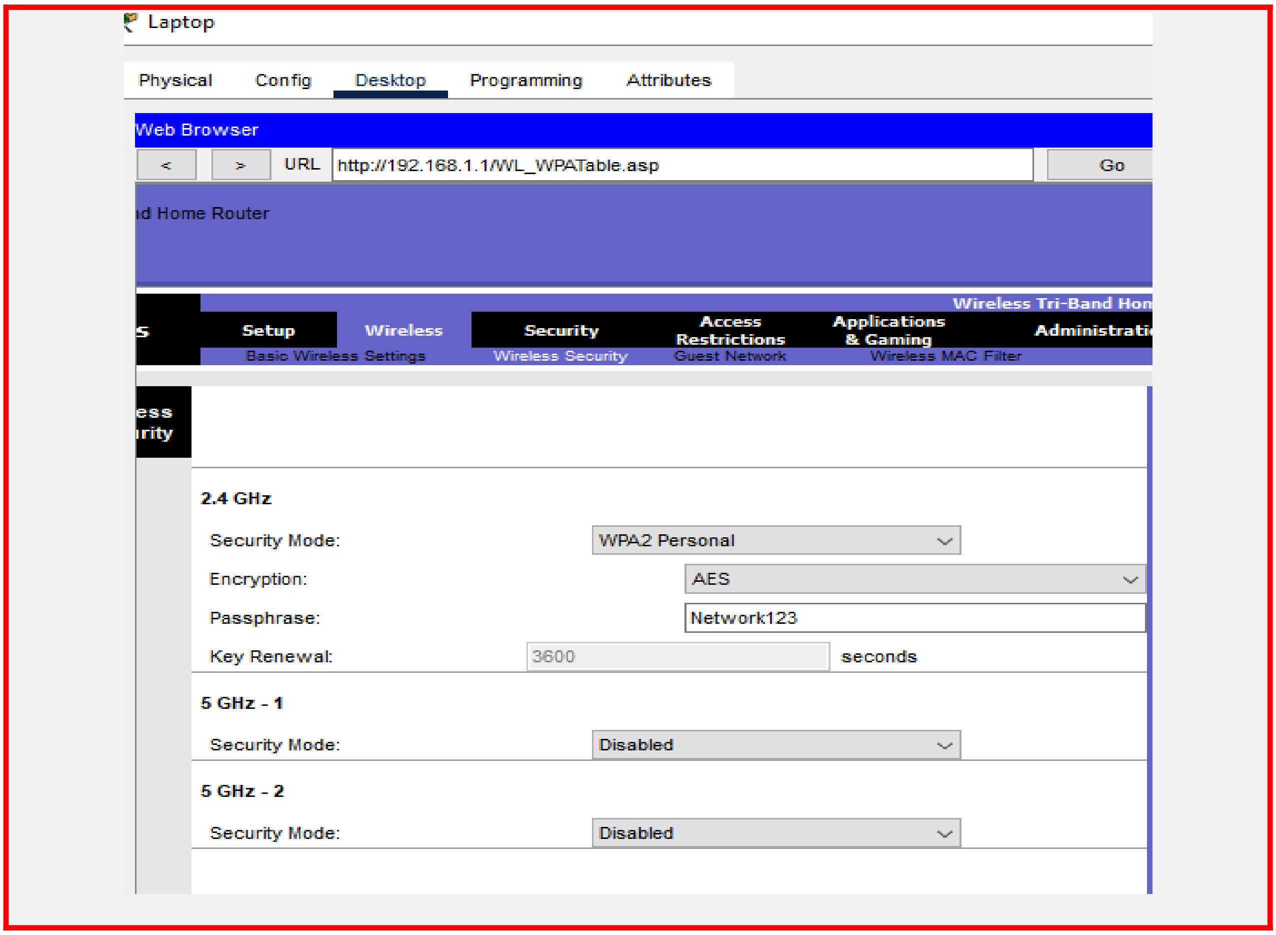
Uses pre-configured key	Generates new key each time connection is made	Weakness can include the use of static key	Uses TKIP or AES encryption protocol

WEP	WPA
Uses pre-configured key	Generates new key each time connection is made
Weakness can include the use of static key	Uses TKIP or AES encryption protocol

Task 15b:

Once you have completed Packet Tracer – Configure Basic Wireless Security, paste the evidence in the appropriate boxes below.

Wireless configuration on the router via a laptop



URL: http://192.168.1.1/WL_WPATable.asp

2.4 GHz

Security Mode: WPA2 Personal

Encryption: AES

Passphrase: Network123

Key Renewal: 3600 seconds

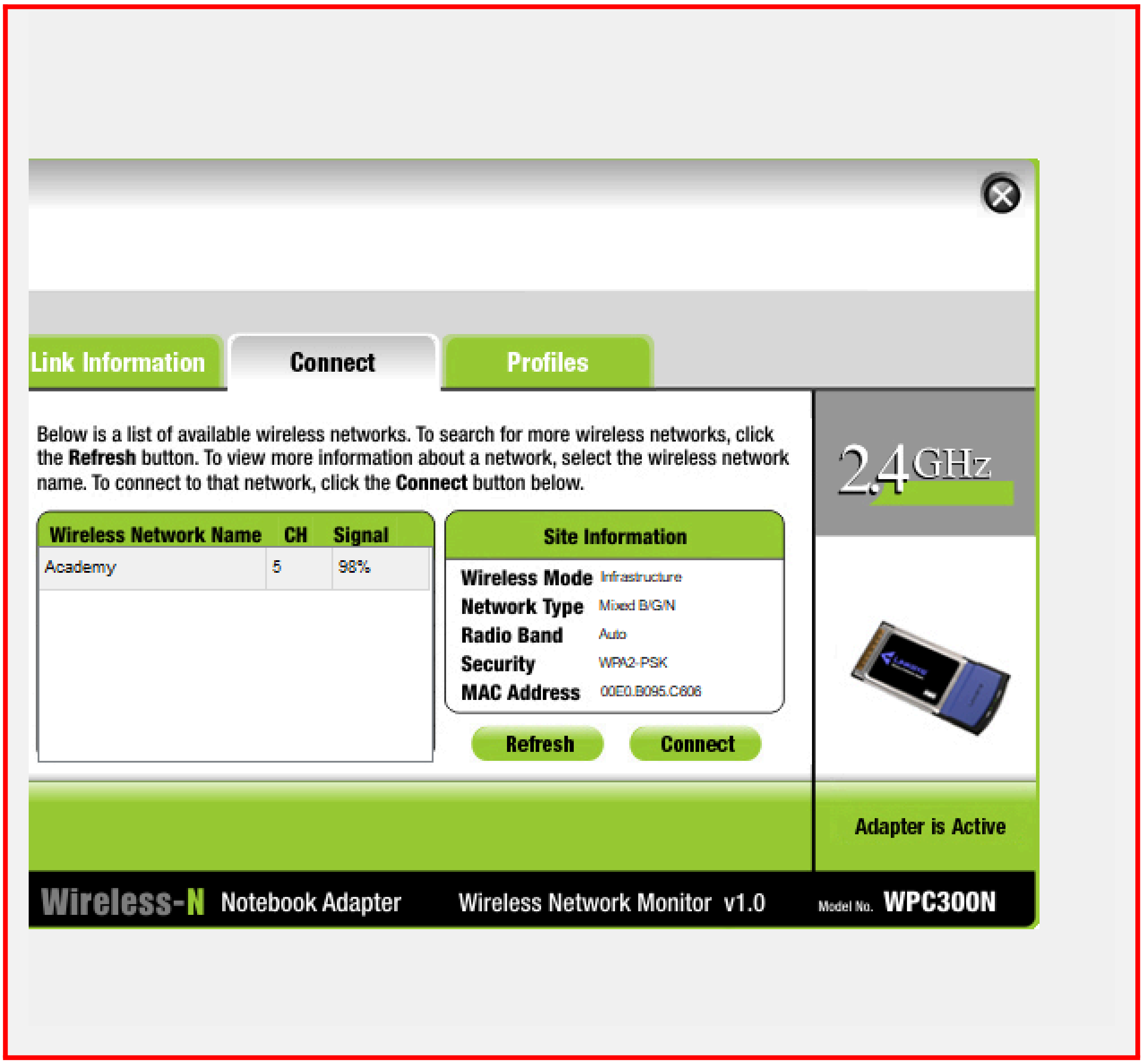
5 GHz - 1

Security Mode: Disabled

5 GHz - 2

Security Mode: Disabled

PC (laptop) Wireless Connectivity



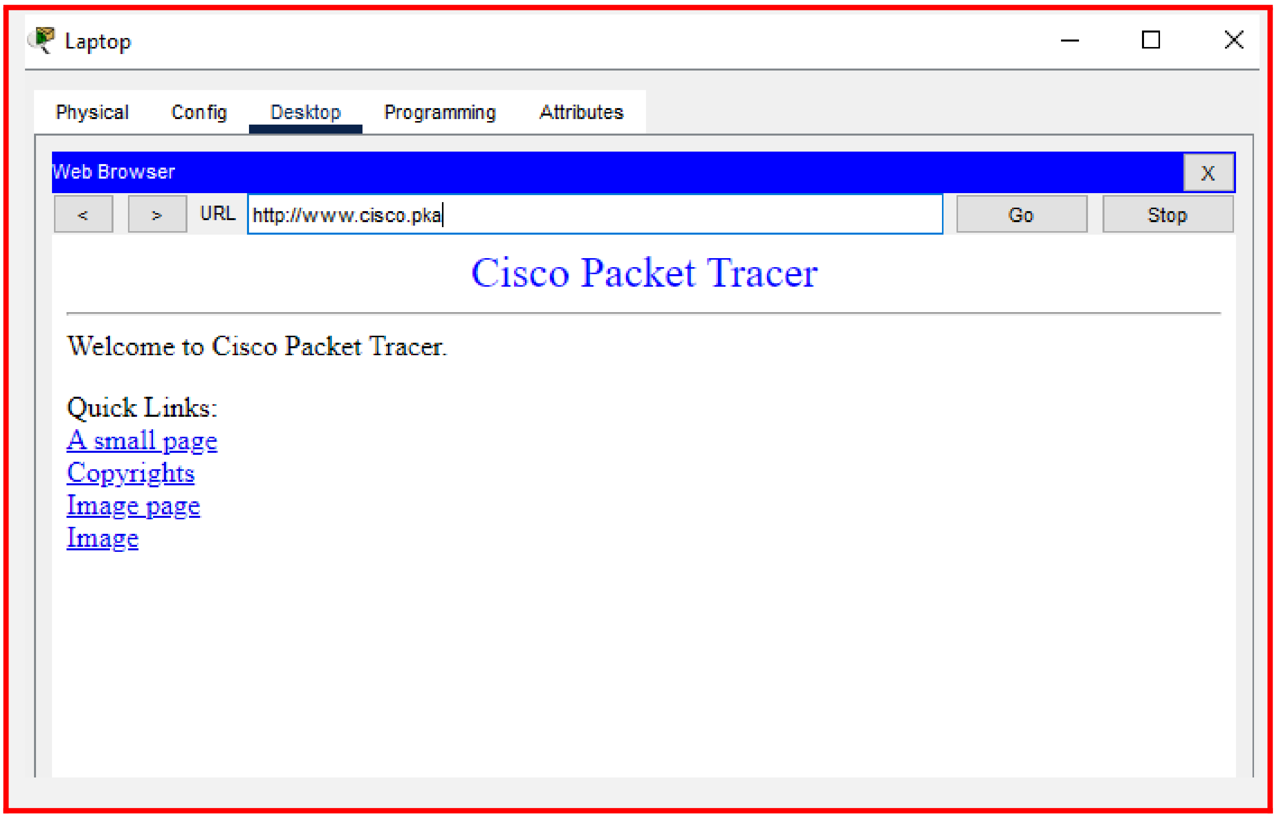
Below is a list of available wireless networks. To search for more wireless networks, click the **Refresh** button. To view more information about a network, select the wireless network name. To connect to that network, click the **Connect** button below.

Wireless Network Name	CH	Signal
Academy	5	98%

Site Information

Wireless Mode	Infrastructure
Network Type	Mixed B/G/N
Radio Band	Auto
Security	WPA2-PSK
MAC Address	00E0.B095.C606

Verifying wireless connectivity



http://www.cisco.pka

Cisco Packet Tracer

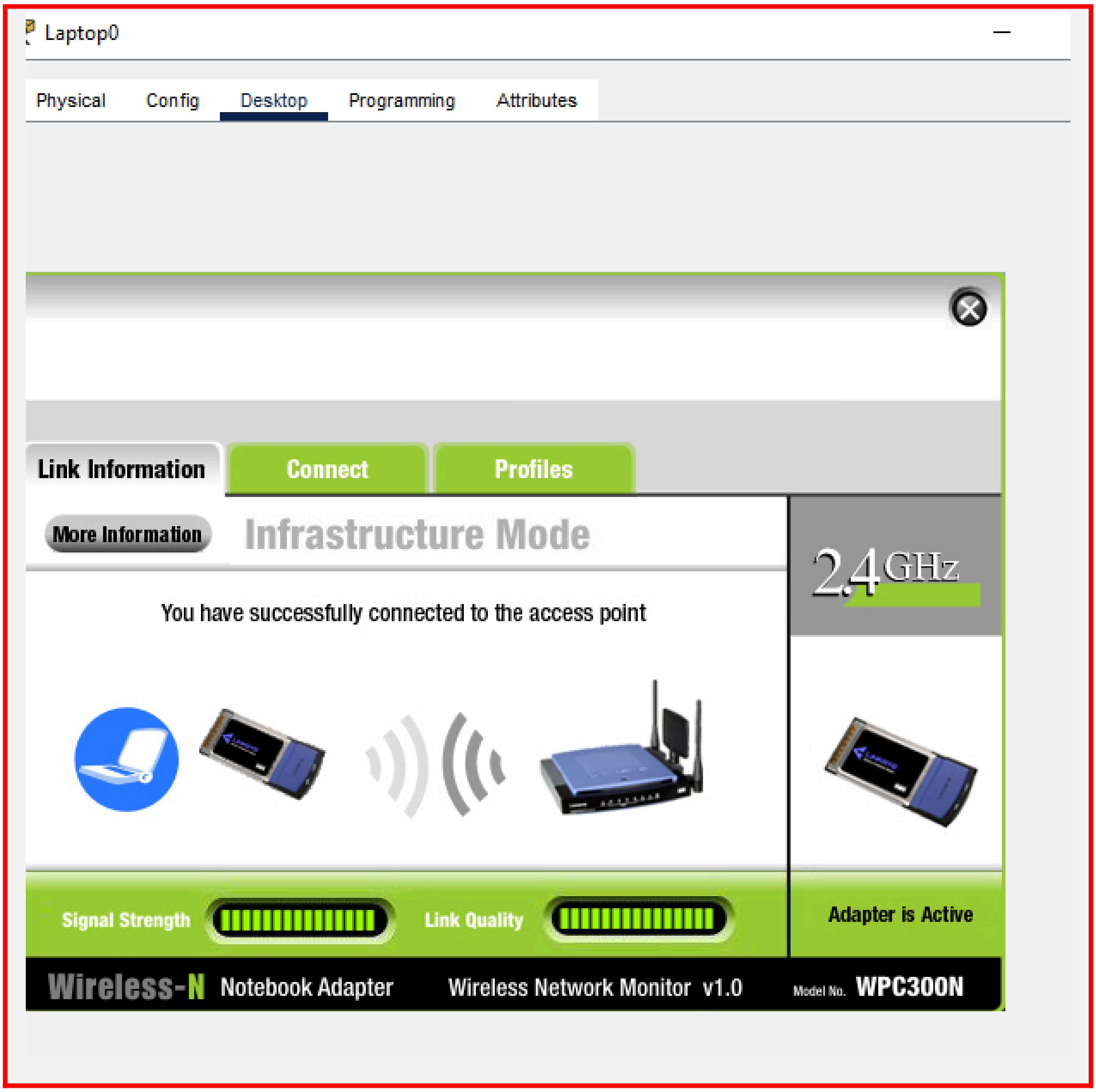
Welcome to Cisco Packet Tracer.

Quick Links:
A small page
Copyrights
Image page
Image

Task 15c:

Once you have completed Packet Tracer – ***Configure Firewall Settings***, paste the evidence in the appropriate boxes below.

Laptop0 wireless connectivity via PC Wireless (should show Adapter is Active)



Infrastructure Mode

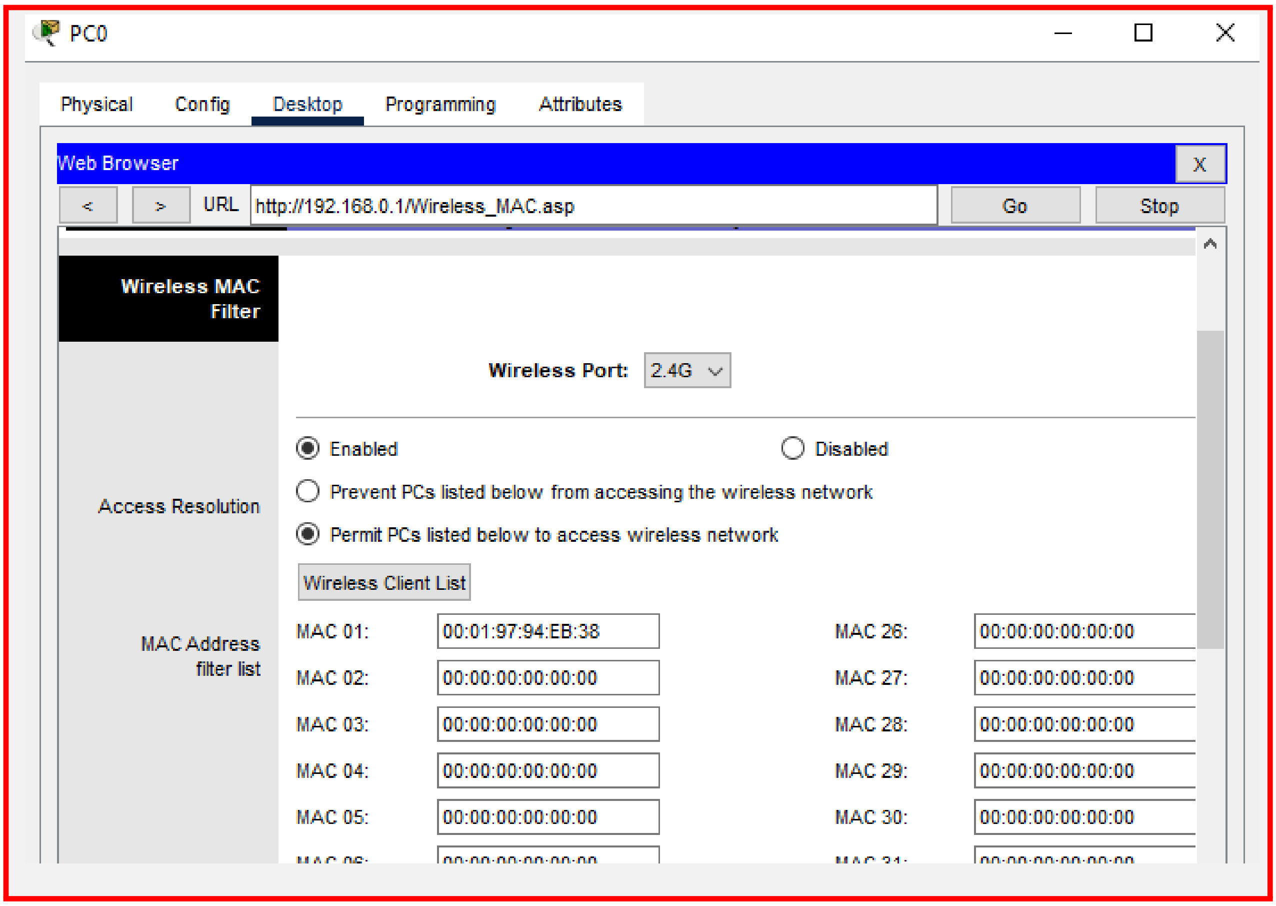
You have successfully connected to the access point

Adapter is Active

List laptop0 IP details

IP address	192.168.0.101
MAC address	0001.9794.EB38

MAC address filtering for laptop0



URL http://192.168.0.1/Wireless_MAC.asp

Wireless MAC Filter

Wireless Port: 2.4G

Access Resolution

● Enabled ○ Disabled

○ Prevent PCs listed below from accessing the wireless network

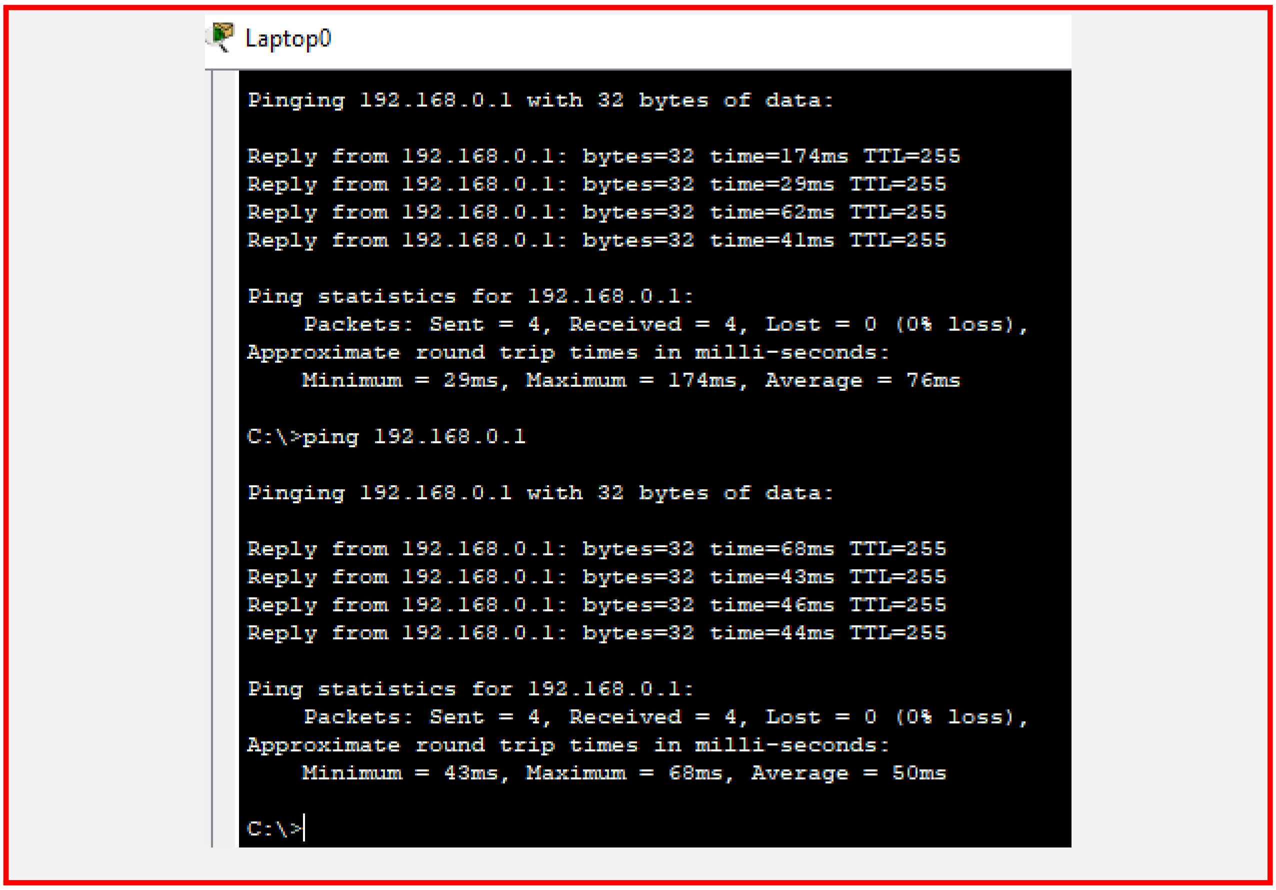
● Permit PCs listed below to access wireless network

Wireless Client List

MAC Address filter list

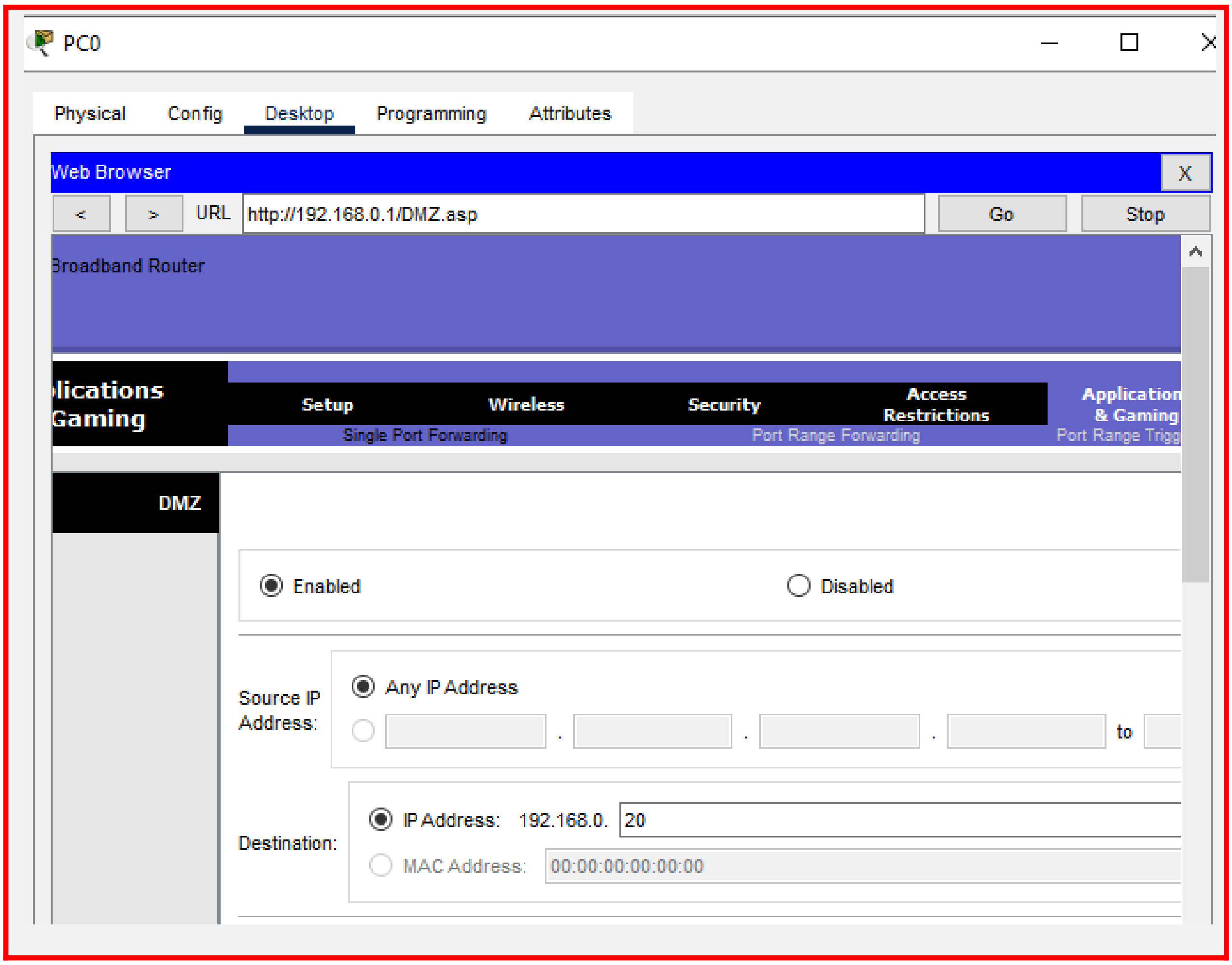
MAC 01:	00:01:97:94:EB:38	MAC 26:	00:00:00:00:00:00
MAC 02:	00:00:00:00:00:00	MAC 27:	00:00:00:00:00:00
MAC 03:	00:00:00:00:00:00	MAC 28:	00:00:00:00:00:00
MAC 04:	00:00:00:00:00:00	MAC 29:	00:00:00:00:00:00
MAC 05:	00:00:00:00:00:00	MAC 30:	00:00:00:00:00:00

Verify that laptop0 MAC filtering works via ping command to the Remote PC.



```
Pinging 192.168.0.1 with 32 bytes of data:

Reply from 192.168.0.1: bytes=32 time=174ms TTL=255
Reply from 192.168.0.1: bytes=32 time=29ms TTL=255
Reply from 192.168.0.1: bytes=32 time=62ms TTL=255
Reply from 192.168.0.1: bytes=32 time=41ms TTL=255

Ping statistics for 192.168.0.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 29ms, Maximum = 174ms, Average = 76ms

C:\>ping 192.168.0.1

Pinging 192.168.0.1 with 32 bytes of data:

Reply from 192.168.0.1: bytes=32 time=68ms TTL=255
Reply from 192.168.0.1: bytes=32 time=43ms TTL=255
Reply from 192.168.0.1: bytes=32 time=46ms TTL=255
Reply from 192.168.0.1: bytes=32 time=44ms TTL=255

Ping statistics for 192.168.0.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 43ms, Maximum = 68ms, Average = 50ms

C:\>
```

Show that you have enabled DMZ on wireless router via PC0.



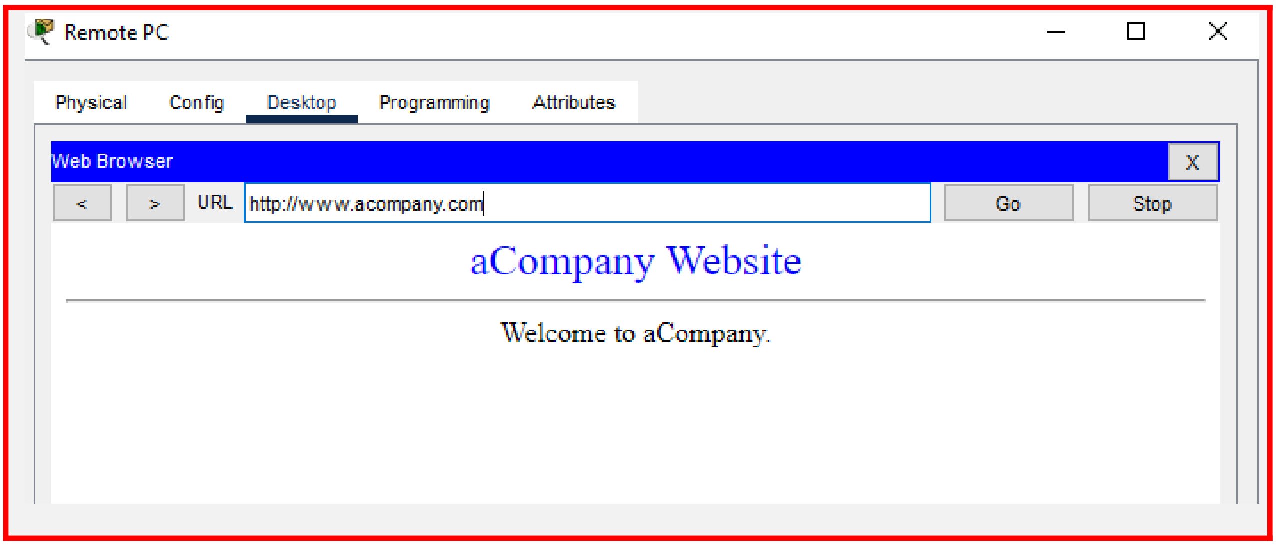
URL: http://192.168.0.1/DMZ.asp

● Enabled ○ Disabled

Source IP Address: ● Any IP Address
○ . . . to

Destination: ● IP Address: 192.168.0. 20
○ MAC Address: 00:00:00:00:00:00

Verify connection to Server0 from Remote PC via web browser

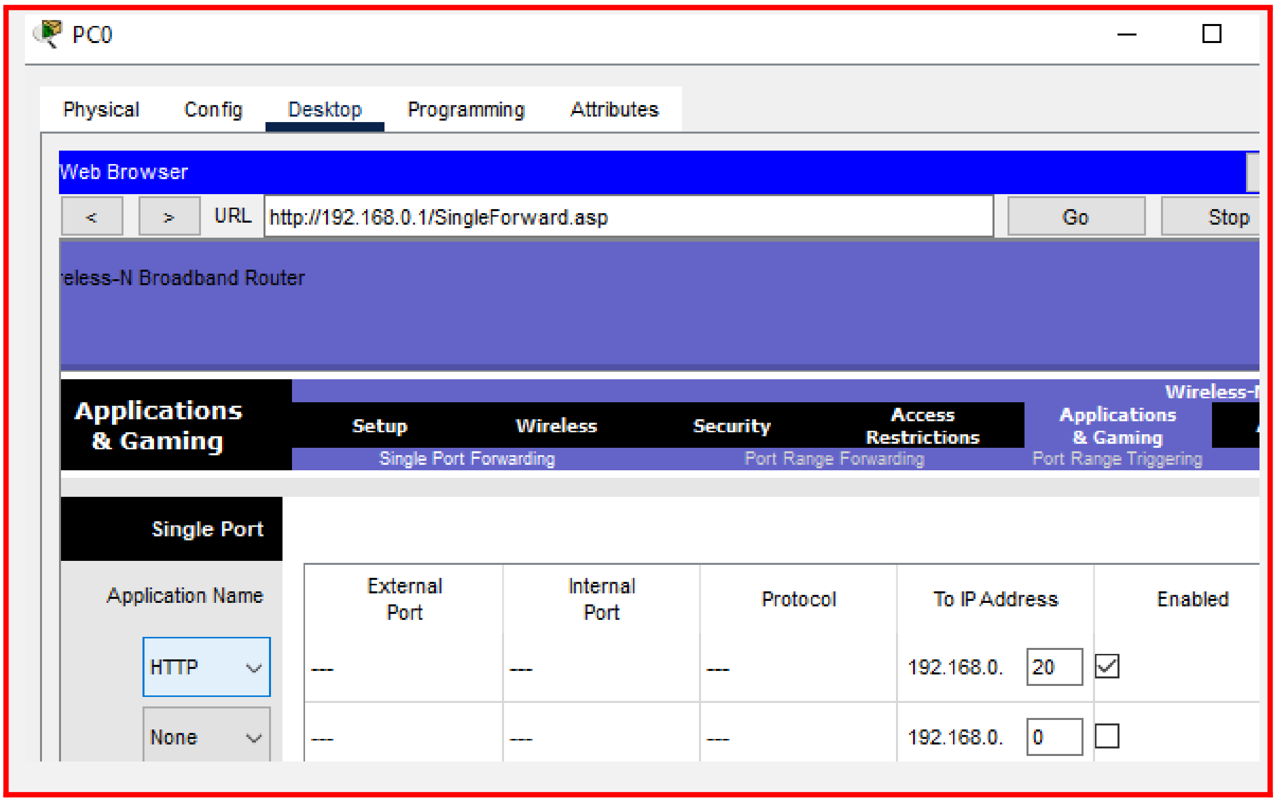


URL: http://www.acompany.com

aCompany Website

Welcome to aCompany.

Show that you have set up Port Forwarding on the router via PC0



URL http://192.168.0.1/SingleForward.asp

Application Name	External Port	Internal Port	Protocol	To IP Address	Enabled
HTTP	---	---	---	192.168.0. 20	☑
None	---	---	---	192.168.0. 0	□

CISCO SWITCHES AND ROUTERS

Task 16a:

Using the words from the list below, match then to their correct description.

Power switch	SFP-based Port	Management Interface	Power input	RJ-45 Ports
2 Gigabit Ethernet Ports	Auxiliary Port and Console Ports	USB Port		

Interface Ports	Description/Function
2 Gigabit Ethernet Ports	One port can be used for the Wide Area Network (WAN) connection to your internet service provider, while the other can be used for Local Area Network (LAN) connections to your devices
Auxiliary Port and Console Ports	This port is mainly used to remote management. This can include backup console access, out-of-band management, and dial-up connections.
Power switch	Turn the device on and off.
RJ-45 Ports	These ports are primarily used for Ethernet connections, allowing the router to connect to other network devices such as switches, computers, and other routers
USB Port	You can use this port to connect external storage devices. This allows you to store configuration files, backup router settings, and even save logs
SFP-based Port	These ports on routers and switches provide flexible, high-speed data transmission over long distances using hot-swappable transceivers. They support various data rates and interfaces, making them ideal for scalable and evolving network needs
Power input	This port is used to connect the router to its power source, typically through an AC or DC power adapter.

Management Interface	This port on a router allows administrators to access, configure, and troubleshoot the router without affecting regular network traffic. It's often used for out-of-band management, providing a dedicated path for these tasks even if the main network is down.

CISCO IOS COMMAND LINES

Task 17a:

Decide whether the following statements belong to the User Exec Mode or Privilege EXEC Mode.

User Exec Mode	Privilege EXEC Mode
● Mode allows access to only a limited number of basic monitoring commands.	● Mode allows access to all commands and features.
● It is often referred to as "view-only" mode.	● The user can use any monitoring commands and execute configuration and management commands.
● Defines by Switch> / Router>	● Defined by Switch# / Router#

Task 17b:

Using the syntax ***Switch>show ip protocols***, decide which part of the syntax represents the **Prompt**, the **Command** and the **Key/Argument**

Command Structure	**Privilege EXEC Mode**
Switch>.	Prompt
show	Command

ip protocols	Key/Argument

Task 17c:

Using the descriptions in the table, decide which missing key stroke should be used.

Enter	Ctrl-Z		Ctrl-C	Ctrl+K	Ctrl+W

Key Stroke	Description
Up Arrow or Ctrl+P	Recalls the previous command in the history buffer, beginning with the most recent command.
Ctrl+R or Ctrl+I or Ctrl+L	Redisplays the system prompt and command line after a console message is received.
Enter	Displays the next line.
Space	Displays the next screen.
Ctrl-C	When in any configuration mode, ends the configuration mode and returns to privileged EXEC mode. When in setup mode, aborts back to the command prompt.
Ctrl-Z	When in any configuration mode, ends the configuration mode and returns to privileged EXEC mode.
Ctrl+K	Erases all characters from the cursor to the end of the command line.
Ctrl+U or Ctrl+X	Erases all characters from the cursor back to the beginning of the command line.
Ctrl+W	Erases the word to the left of the cursor.

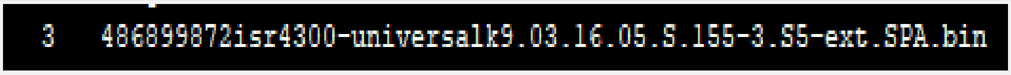
Task 17d:

Whilst completing the ***Packet Tracer – Use Cisco IOS Show Commands***, answer the questions below.

Record the ***MAC address*** and the ***IP address*** listed

IP	209.165.201.1	**MAC**	0001.96CD.2501

Record the ***IOS image*** listed (use copy/paste). ***Hint***: *begins with 486...*



```
3   486899872isr4300-universalk9.03.16.05.S.155-3.S5-ext.SPA.bin
```

How many ***routes*** are listed in the table?

2

Which **interface** is up and running? Complete the table.

Interface	Status	Protocol
GigabitEthernet 0/0/0	Up	Up
GigabitEthernet 0/0/1	Down	Down
Serial0/1/0	Down	Down
Serial0/1/1	Down	Down

According to the **show ip interface** output, which interface is connected?

GigabitEthernet 0/0/0

What **technology package** is enabled currently on the router?

ipbasek9	securityk9

Which **protocols** are enabled currently on the router?

Internet Protocol routing is enabled	GigabitEthernet0/0/0

What is the output when you enter ***show running-config*** command?

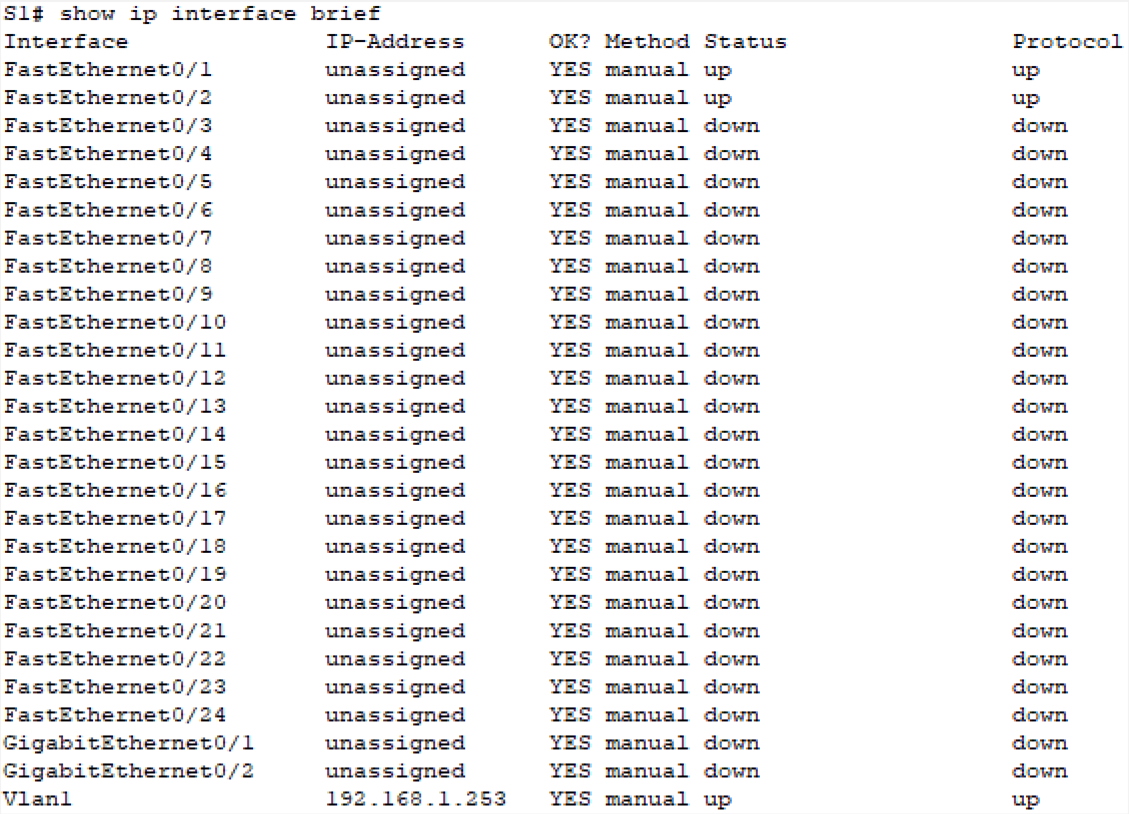
% Invalid input detected at '^' marker.

BUILD A SMALL CISCO NETWORK

Task 18a:

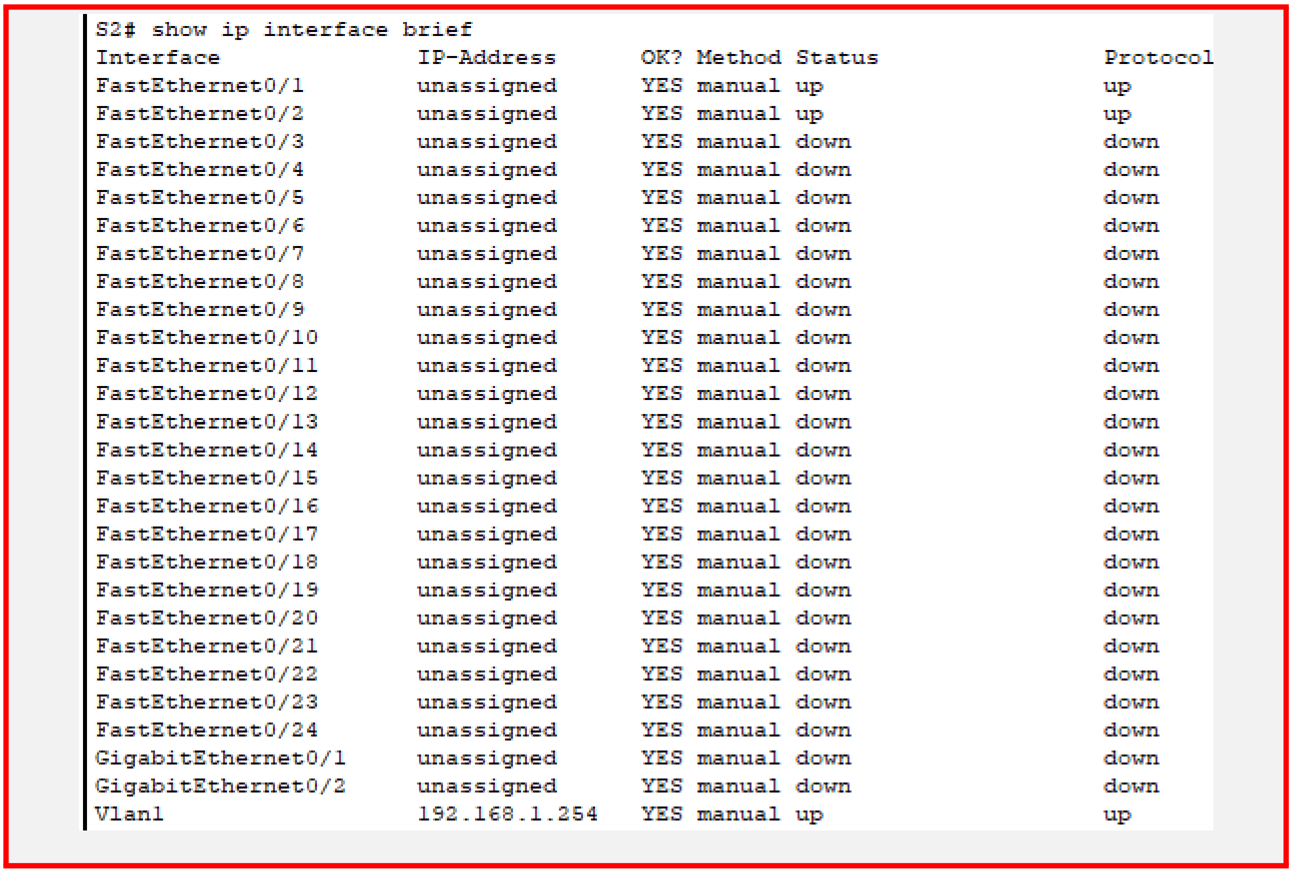
Once you have completed Packet Tracer – ***Implement Basic Connectivity***, paste your evidence in the appropriate boxes below.

Show ***IP address of VLAN 1*** on **switch 1**



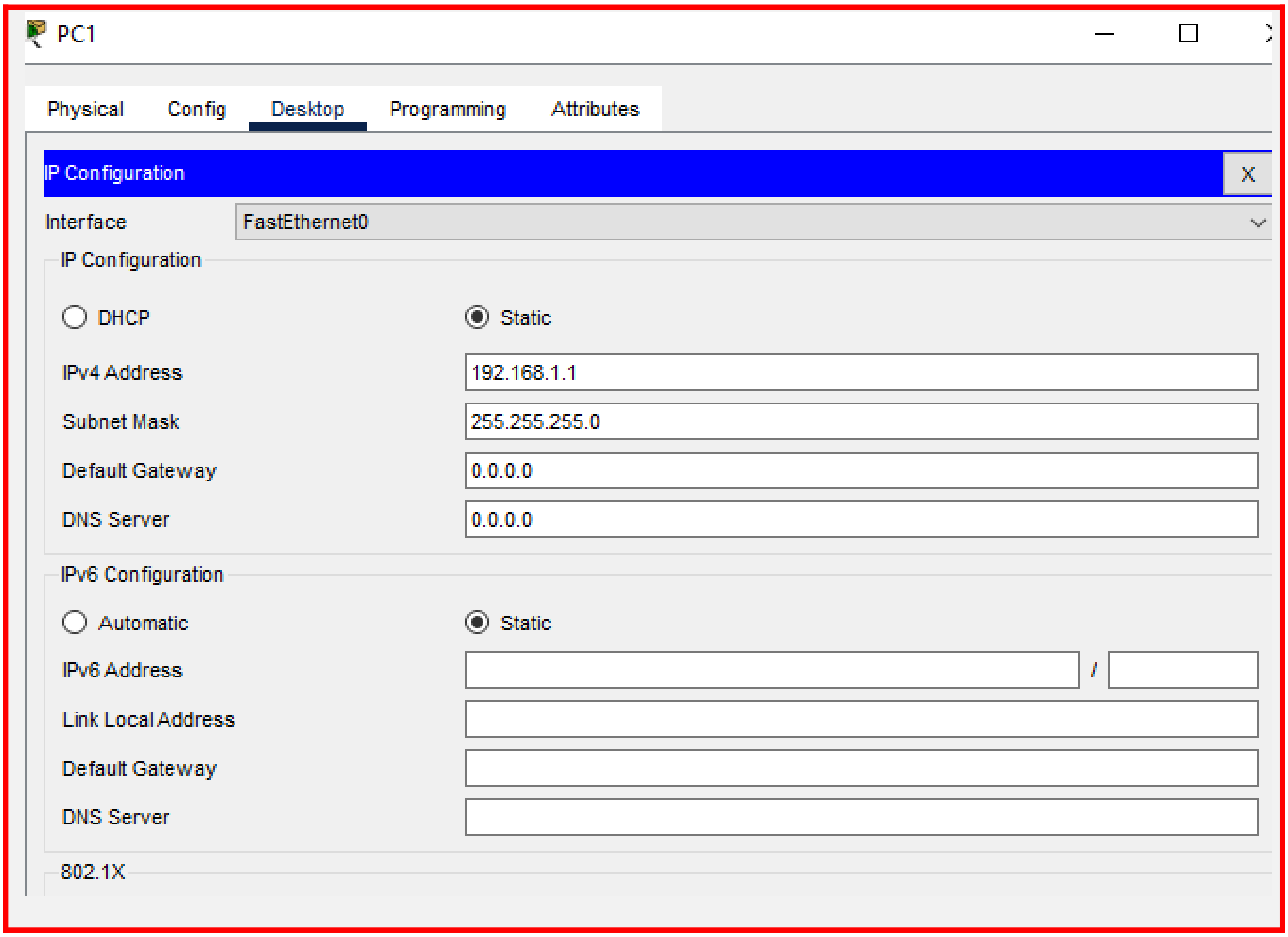
```
S1# show ip interface brief
Interface              IP-Address      OK? Method Status                Protocol
FastEthernet0/1        unassigned      YES manual up                    up
FastEthernet0/2        unassigned      YES manual up                    up
FastEthernet0/3        unassigned      YES manual down                  down
FastEthernet0/4        unassigned      YES manual down                  down
FastEthernet0/5        unassigned      YES manual down                  down
FastEthernet0/6        unassigned      YES manual down                  down
FastEthernet0/7        unassigned      YES manual down                  down
FastEthernet0/8        unassigned      YES manual down                  down
FastEthernet0/9        unassigned      YES manual down                  down
FastEthernet0/10       unassigned      YES manual down                  down
FastEthernet0/11       unassigned      YES manual down                  down
FastEthernet0/12       unassigned      YES manual down                  down
FastEthernet0/13       unassigned      YES manual down                  down
FastEthernet0/14       unassigned      YES manual down                  down
FastEthernet0/15       unassigned      YES manual down                  down
FastEthernet0/16       unassigned      YES manual down                  down
FastEthernet0/17       unassigned      YES manual down                  down
FastEthernet0/18       unassigned      YES manual down                  down
FastEthernet0/19       unassigned      YES manual down                  down
FastEthernet0/20       unassigned      YES manual down                  down
FastEthernet0/21       unassigned      YES manual down                  down
FastEthernet0/22       unassigned      YES manual down                  down
FastEthernet0/23       unassigned      YES manual down                  down
FastEthernet0/24       unassigned      YES manual down                  down
GigabitEthernet0/1     unassigned      YES manual down                  down
GigabitEthernet0/2     unassigned      YES manual down                  down
Vlan1                  192.168.1.253   YES manual up                    up
```

Show ***IP address of VLAN 1*** on **switch 2**



```
S2# show ip interface brief
Interface              IP-Address      OK? Method Status                Protocol
FastEthernet0/1        unassigned      YES manual up                    up
FastEthernet0/2        unassigned      YES manual up                    up
FastEthernet0/3        unassigned      YES manual down                  down
FastEthernet0/4        unassigned      YES manual down                  down
FastEthernet0/5        unassigned      YES manual down                  down
FastEthernet0/6        unassigned      YES manual down                  down
FastEthernet0/7        unassigned      YES manual down                  down
FastEthernet0/8        unassigned      YES manual down                  down
FastEthernet0/9        unassigned      YES manual down                  down
FastEthernet0/10       unassigned      YES manual down                  down
FastEthernet0/11       unassigned      YES manual down                  down
FastEthernet0/12       unassigned      YES manual down                  down
FastEthernet0/13       unassigned      YES manual down                  down
FastEthernet0/14       unassigned      YES manual down                  down
FastEthernet0/15       unassigned      YES manual down                  down
FastEthernet0/16       unassigned      YES manual down                  down
FastEthernet0/17       unassigned      YES manual down                  down
FastEthernet0/18       unassigned      YES manual down                  down
FastEthernet0/19       unassigned      YES manual down                  down
FastEthernet0/20       unassigned      YES manual down                  down
FastEthernet0/21       unassigned      YES manual down                  down
FastEthernet0/22       unassigned      YES manual down                  down
FastEthernet0/23       unassigned      YES manual down                  down
FastEthernet0/24       unassigned      YES manual down                  down
GigabitEthernet0/1     unassigned      YES manual down                  down
GigabitEthernet0/2     unassigned      YES manual down                  down
Vlan1                  192.168.1.254   YES manual up                    up
```

Show *IP address configuration* of **PC1**



Interface: FastEthernet0

IP Configuration

○ DHCP ● Static

IPv4 Address: 192.168.1.1

Subnet Mask: 255.255.255.0

Default Gateway: 0.0.0.0

DNS Server: 0.0.0.0

IPv6 Configuration

○ Automatic ● Static

IPv6 Address: /

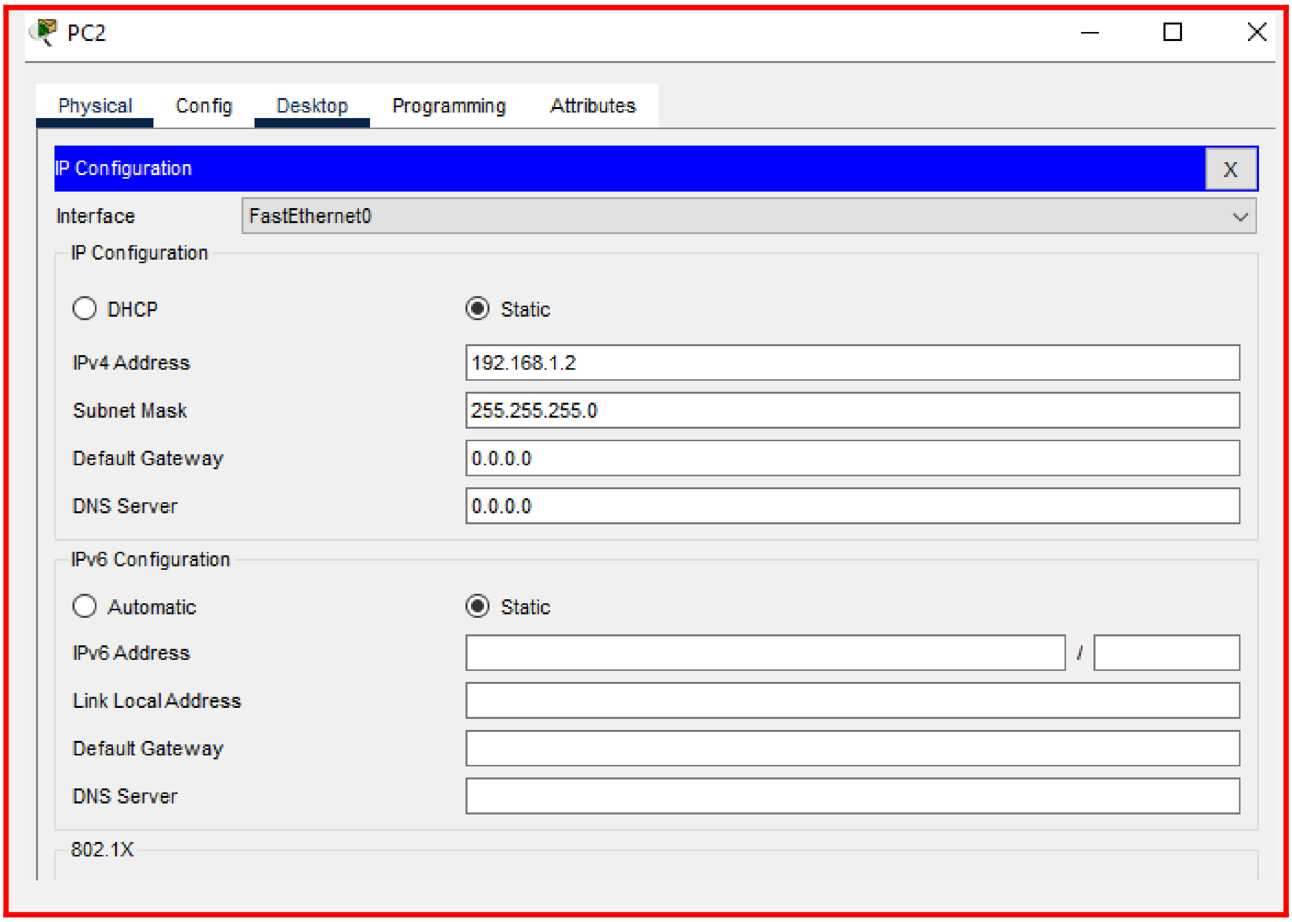
Link Local Address:

Default Gateway:

DNS Server:

802.1X

Show ***IP address configuration*** of **PC2**



PC2

IP Configuration

Interface: FastEthernet0

IP Configuration

○ DHCP ● Static

IPv4 Address: 192.168.1.2

Subnet Mask: 255.255.255.0

Default Gateway: 0.0.0.0

DNS Server: 0.0.0.0

IPv6 Configuration

○ Automatic ● Static

IPv6 Address: /

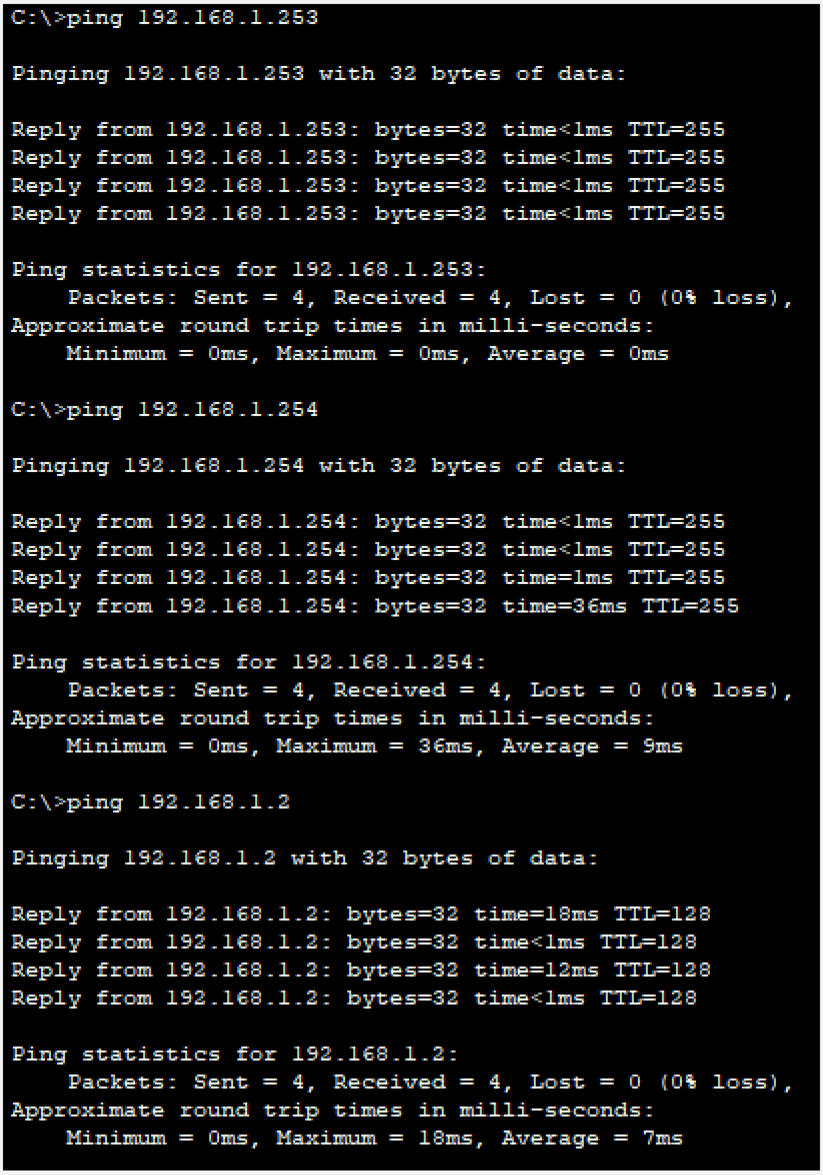
Link Local Address:

Default Gateway:

DNS Server:

802.1X

Show ***PING*** test from **PC1** to **Switch 1, Switch 2, and PC2** *(you should have 3 ping tests in your screenshot)*



```
C:\>ping 192.168.1.253

Pinging 192.168.1.253 with 32 bytes of data:

Reply from 192.168.1.253: bytes=32 time<1ms TTL=255
Reply from 192.168.1.253: bytes=32 time<1ms TTL=255
Reply from 192.168.1.253: bytes=32 time<1ms TTL=255
Reply from 192.168.1.253: bytes=32 time<1ms TTL=255

Ping statistics for 192.168.1.253:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\>ping 192.168.1.254

Pinging 192.168.1.254 with 32 bytes of data:

Reply from 192.168.1.254: bytes=32 time<1ms TTL=255
Reply from 192.168.1.254: bytes=32 time<1ms TTL=255
Reply from 192.168.1.254: bytes=32 time=1ms TTL=255
Reply from 192.168.1.254: bytes=32 time=36ms TTL=255

Ping statistics for 192.168.1.254:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 36ms, Average = 9ms

C:\>ping 192.168.1.2

Pinging 192.168.1.2 with 32 bytes of data:

Reply from 192.168.1.2: bytes=32 time=18ms TTL=128
Reply from 192.168.1.2: bytes=32 time<1ms TTL=128
Reply from 192.168.1.2: bytes=32 time=12ms TTL=128
Reply from 192.168.1.2: bytes=32 time<1ms TTL=128

Ping statistics for 192.168.1.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 18ms, Average = 7ms
```

Task 18b:

Whilst completing the Packet Tracer – ***Configure Initial Router Settings***, paste your evidence in the appropriate boxes below and answer the questions as you go along.

What is the router's **hostname**?

Router

How many **Fast Ethernet interfaces** does the Router have?

None

How many **Gigabit Ethernet** interfaces does the Router have?

Two

How many **Serial interfaces** does the router have?

Two

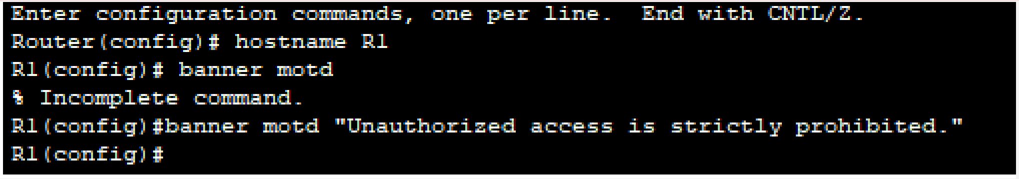
What is the range of values shown for the **vty** lines?

0 4

Why does the router respond with the **startup-config is not present** message?

Probably because the router doesn’t have prior configuration, or it wasn’t previously saved.

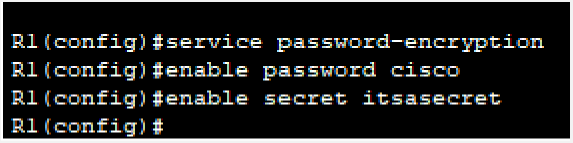
Use the ***banner motd*** command to set ‘*Unauthorized access is strictly prohibited*’. *(Note: you will need to exist completely in order to view the message.)*



```
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)# hostname R1
R1(config)# banner motd
% Incomplete command.
R1(config)#banner motd "Unauthorized access is strictly prohibited."
R1(config)#
```

Privilege Password

From the R1(Config) use ***enable secret*** ‘*Itsasecret*’ command to set Privilege EXEC Mode password. Then exit to R1> and type R1> **enable** to test the password.

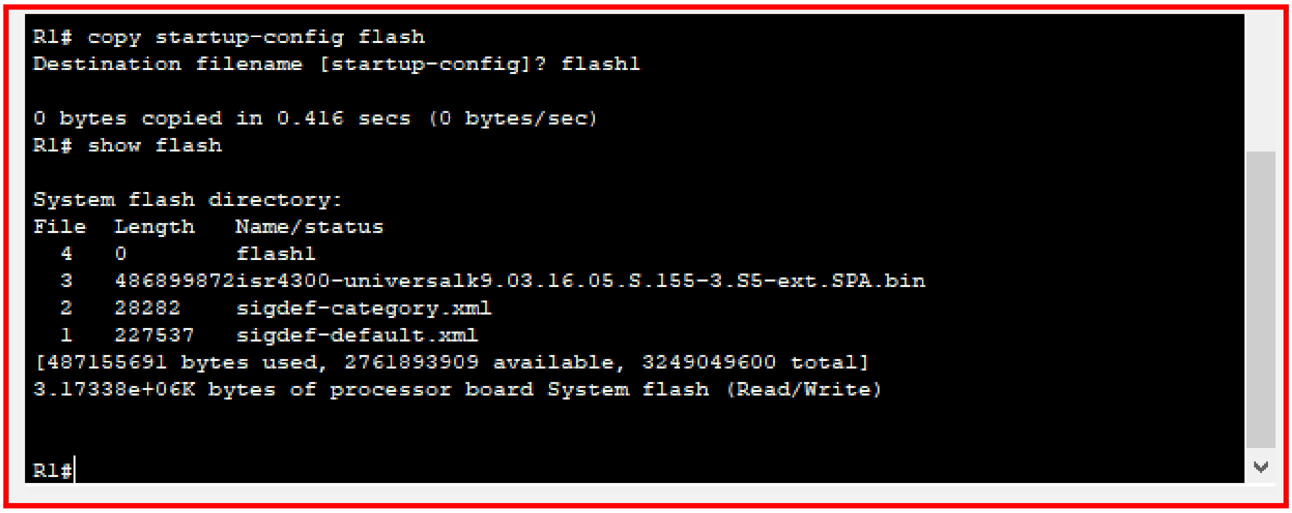


```
R1(config)#service password-encryption
R1(config)#enable password cisco
R1(config)#enable secret itsasecret
R1(config)#
```

Console Password

From the *R1(Config)* use ***con 0*** command to enter the Console 0 line. Then type *R1(Config)* ***password*** *‘letmein’* (enter). Then type *R1(config)* ***login*** (enter). Return back to beginning by typing exit several times to test the password.

What **command** did you use to **verify the contents of NVRAM** (memory)



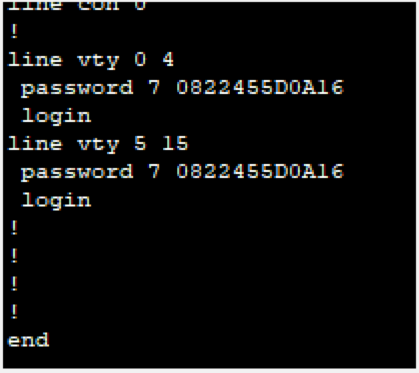
```
R1# copy startup-config flash
Destination filename [startup-config]? flash1

0 bytes copied in 0.416 secs (0 bytes/sec)
R1# show flash

System flash directory:
File  Length   Name/status
  4   0        flash1
  3   486899872isr4300-universalk9.03.16.05.S.155-3.S5-ext.SPA.bin
  2   28282    sigdef-category.xml
  1   227537   sigdef-default.xml
[487155691 bytes used, 2761893909 available, 3249049600 total]
3.17338e+06K bytes of processor board System flash (Read/Write)


R1#
```

Task 18c:

Whilst completing the Packet Tracer – ***Configure SSH***, paste your evidence in the appropriate boxes below as you go along.

Encrypting passwords

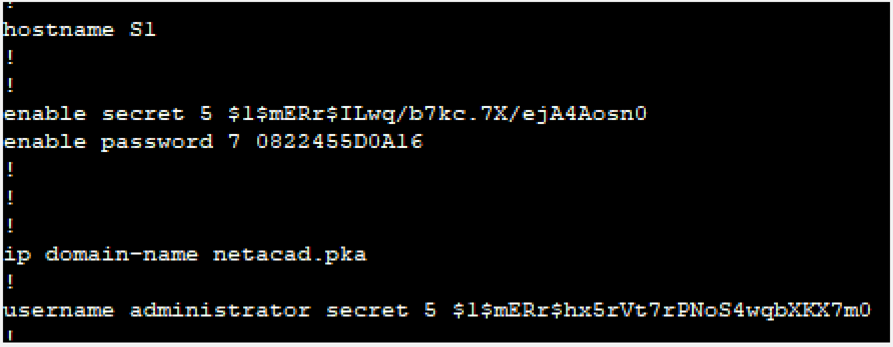
Show that your **passwords are encrypted.**



```
line con 0
!
line vty 0 4
 password 7 0822455D0A16
 login
line vty 5 15
 password 7 0822455D0A16
 login
!
!
!
!
end
```

Create Domain and Generate Encryption Keys

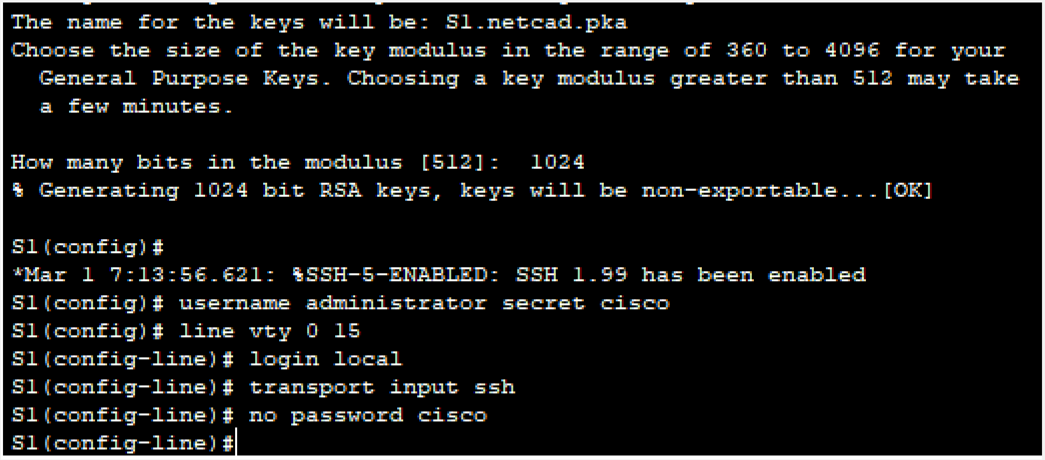
Show that you have **created a domain-name** and **generated encryption keys**



```
hostname S1
!
!
enable secret 5 $1$mERr$ILwq/b7kc.7X/ejA4Aosn0
enable password 7 0822455D0A16
!
!
!
ip domain-name netacad.pka
!
username administrator secret 5 $1$mERr$hx5rVt7rPNoS4wqbXKX7m0
!
```

Create SSH User and Reconfigure VTY lines

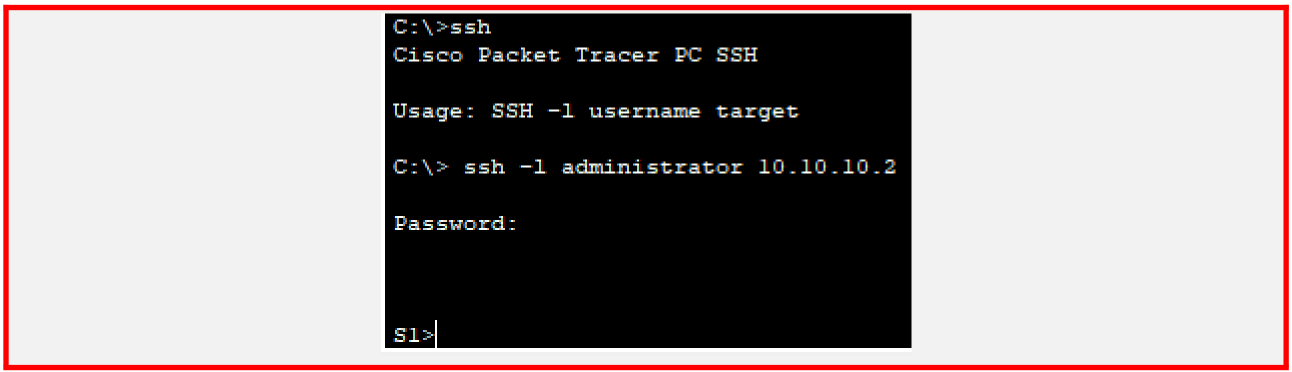
Show that you have **created an SSH user** and **reconfigured the VTY lines for SSH-only access**.



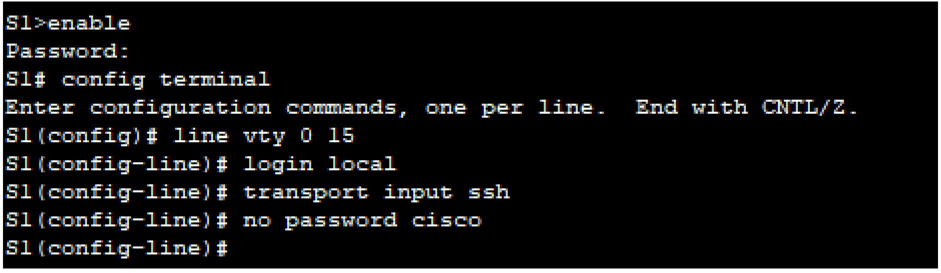
```
The name for the keys will be: S1.netcad.pka
Choose the size of the key modulus in the range of 360 to 4096 for your
  General Purpose Keys. Choosing a key modulus greater than 512 may take
  a few minutes.

How many bits in the modulus [512]:  1024
% Generating 1024 bit RSA keys, keys will be non-exportable...[OK]

S1(config)#
*Mar 1 7:13:56.621: %SSH-5-ENABLED: SSH 1.99 has been enabled
S1(config)# username administrator secret cisco
S1(config)# line vty 0 15
S1(config-line)# login local
S1(config-line)# transport input ssh
S1(config-line)# no password cisco
S1(config-line)#
```

Check verification

Verify that SSH implementation. Use C:\>***ssh -l administrator 10.10.10.2*** command.



```
C:\>ssh
Cisco Packet Tracer PC SSH

Usage: SSH -l username target

C:\> ssh -l administrator 10.10.10.2

Password:


S1>
```



```
S1>enable
Password:
S1# config terminal
Enter configuration commands, one per line.  End with CNTL/Z.
S1(config)# line vty 0 15
S1(config-line)# login local
S1(config-line)# transport input ssh
S1(config-line)# no password cisco
S1(config-line)#
```

TROUBLESHOOTING COMMON NETWORK PROBLEMS

Task 19a:

Using the statements from the list, decide which troubleshooting step they belong in.

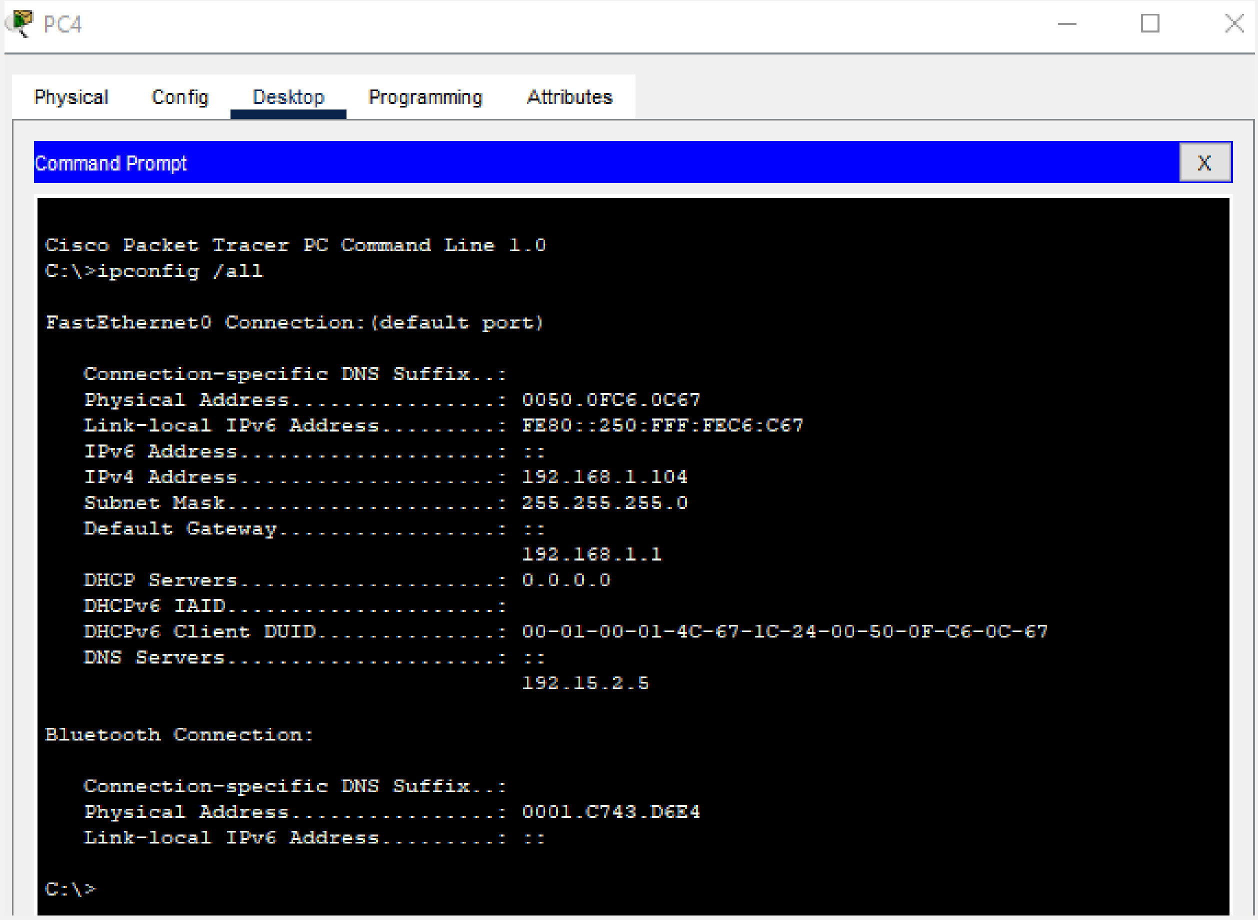
Troubleshooting Step	Statement
Gather Information	● Talk to the user and try to determine how much of the network is affected by the issue
Bottom-Up	● Start with the physical layer and the physical components of the network and move up through the layers of the OSI model until the cause of the problem is identified.
Top-Down	● Start with the end-user applications and move down through the OSI layers.
Divide-and-Conquer	● Select a layer and test in both directions.
Follow-the-path	● First discover the traffic path all the way from source to destination
Substitution	● Also called swap-the-component because you physically swap the problematic device with a known, working one

Task 19b:

Once you have completed Packet Tracer – ***Use the ipconfig Command***, paste your evidence in the appropriate boxes below.

Verify the connections

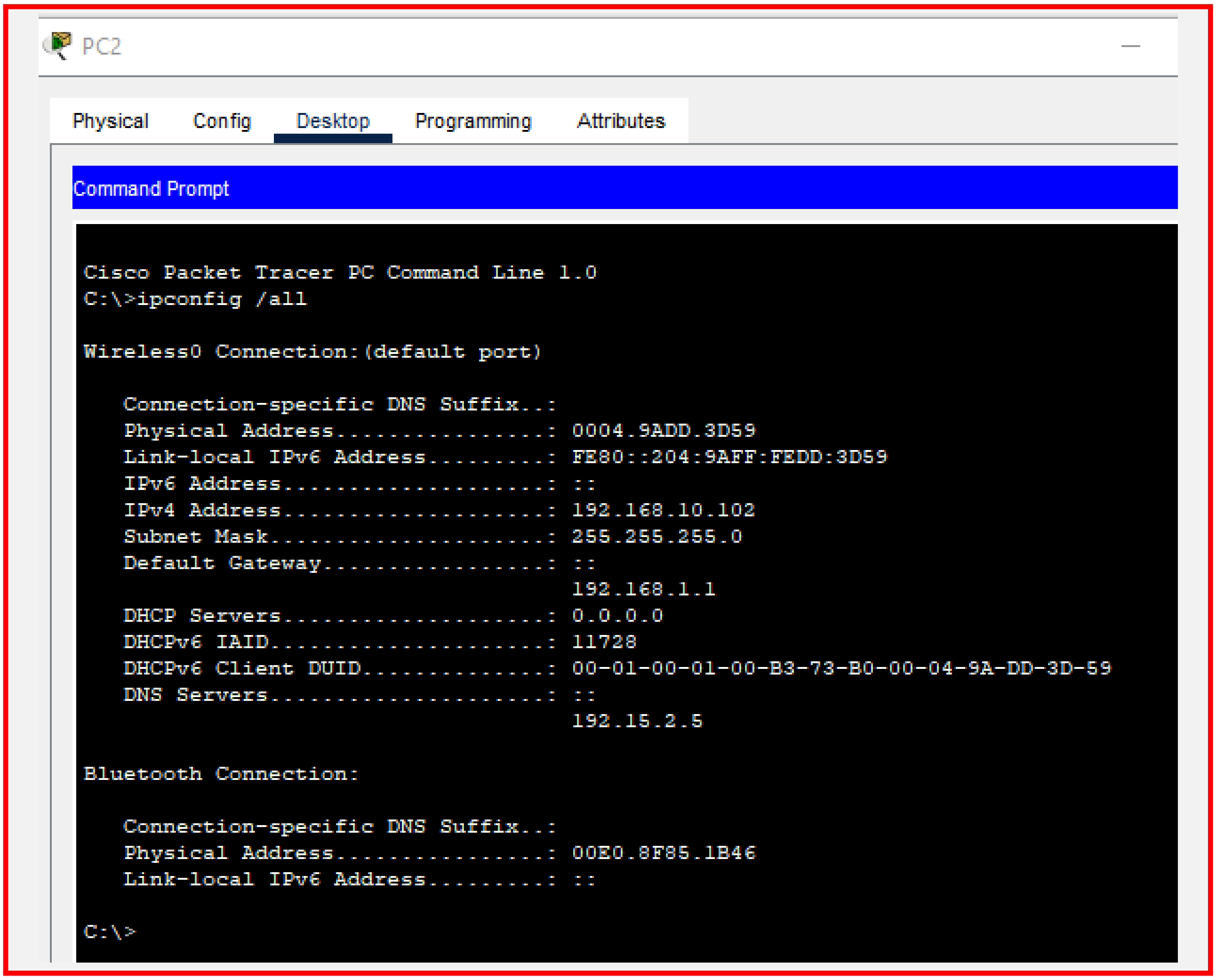
Show that you have used ipconfig /all command on any PC.



```
Cisco Packet Tracer PC Command Line 1.0
C:\>ipconfig /all

FastEthernet0 Connection:(default port)

   Connection-specific DNS Suffix..:
   Physical Address................: 0050.0FC6.0C67
   Link-local IPv6 Address.........: FE80::250:FFF:FEC6:C67
   IPv6 Address....................: ::
   IPv4 Address....................: 192.168.1.104
   Subnet Mask.....................: 255.255.255.0
   Default Gateway.................: ::
                                     192.168.1.1
   DHCP Servers....................: 0.0.0.0
   DHCPv6 IAID.....................:
   DHCPv6 Client DUID..............: 00-01-00-01-4C-67-1C-24-00-50-0F-C6-0C-67
   DNS Servers.....................: ::
                                     192.15.2.5

Bluetooth Connection:

   Connection-specific DNS Suffix..:
   Physical Address................: 0001.C743.D6E4
   Link-local IPv6 Address.........: ::

C:\>
```

Identify Problem

View all PCs IP details and identify the PC that is not on the same network.

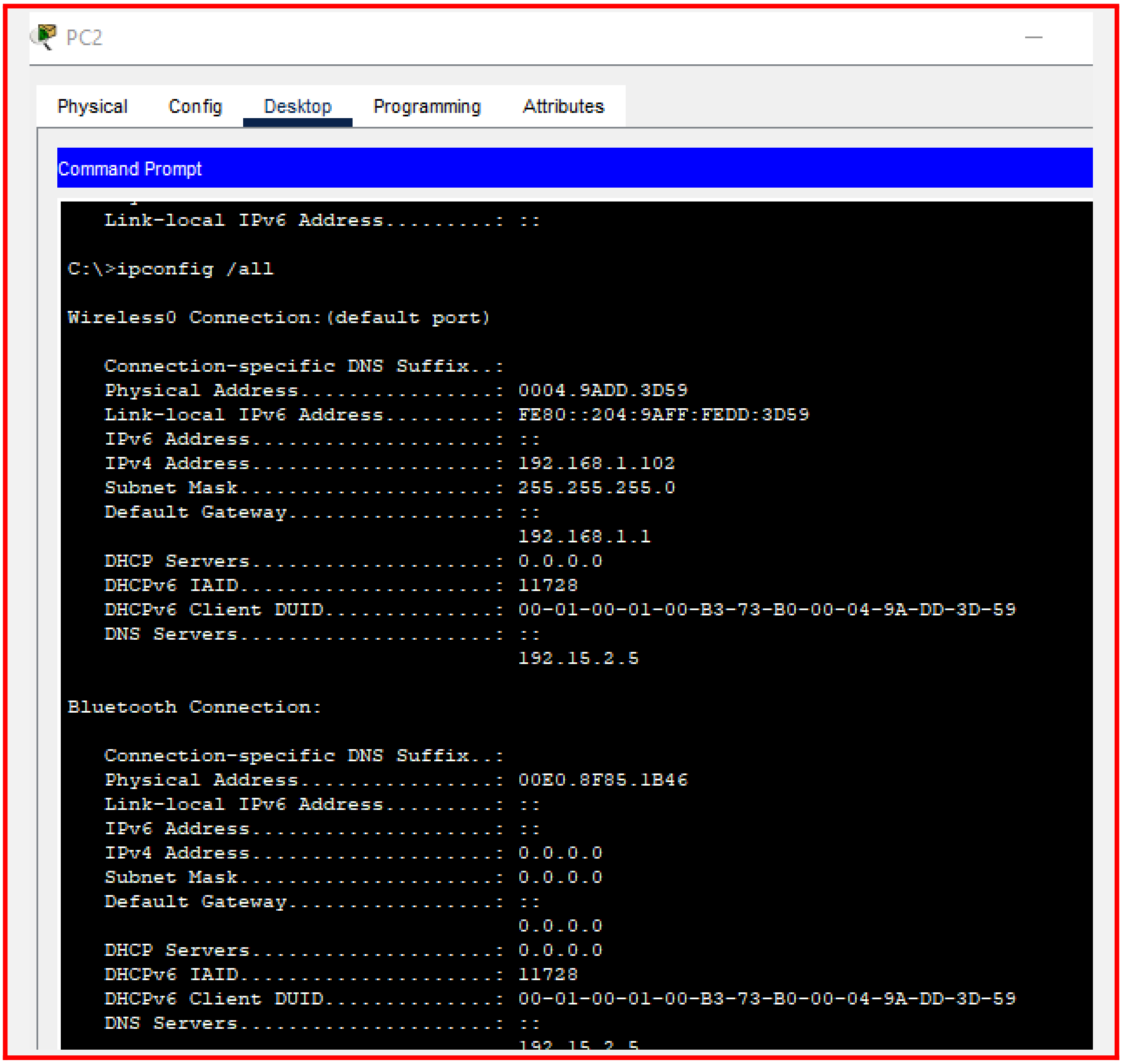


```
Cisco Packet Tracer PC Command Line 1.0
C:\>ipconfig /all

Wireless0 Connection:(default port)

   Connection-specific DNS Suffix..:
   Physical Address................: 0004.9ADD.3D59
   Link-local IPv6 Address.........: FE80::204:9AFF:FEDD:3D59
   IPv6 Address....................: ::
   IPv4 Address....................: 192.168.10.102
   Subnet Mask.....................: 255.255.255.0
   Default Gateway.................: ::
                                     192.168.1.1
   DHCP Servers....................: 0.0.0.0
   DHCPv6 IAID.....................: 11728
   DHCPv6 Client DUID..............: 00-01-00-01-00-B3-73-B0-00-04-9A-DD-3D-59
   DNS Servers.....................: ::
                                     192.15.2.5

Bluetooth Connection:

   Connection-specific DNS Suffix..:
   Physical Address................: 00E0.8F85.1B46
   Link-local IPv6 Address.........: ::

C:\>
```

Which PC is on a wrong network, and why?

PC 2 is on the wrong network IP address 192.168.10.0 and the other PC's are on the 192.168.1 network.

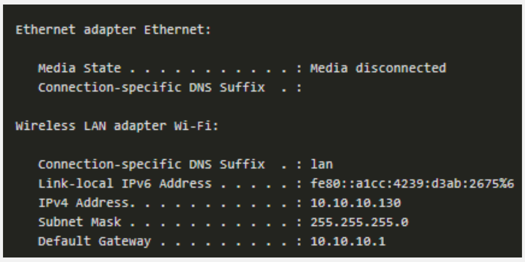
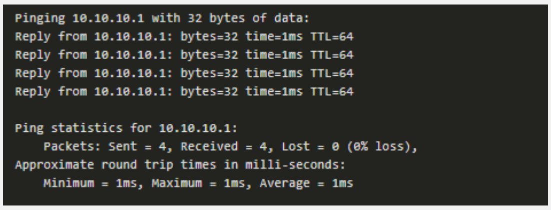
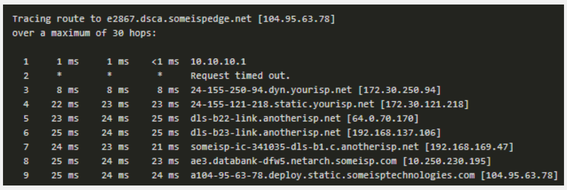
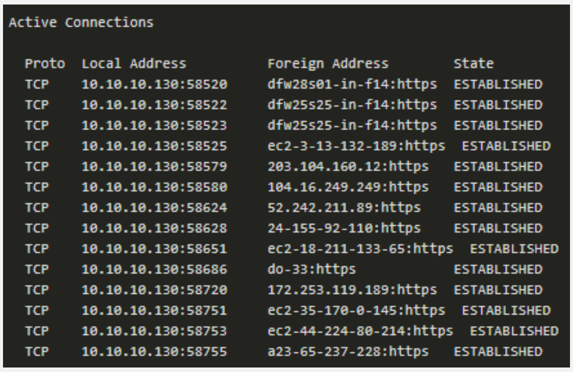
Correct any misconfiguration



```
   Link-local IPv6 Address.........: ::

C:\>ipconfig /all

Wireless0 Connection:(default port)

   Connection-specific DNS Suffix..:
   Physical Address................: 0004.9ADD.3D59
   Link-local IPv6 Address.........: FE80::204:9AFF:FEDD:3D59
   IPv6 Address....................: ::
   IPv4 Address....................: 192.168.1.102
   Subnet Mask.....................: 255.255.255.0
   Default Gateway.................: ::
                                     192.168.1.1
   DHCP Servers....................: 0.0.0.0
   DHCPv6 IAID.....................: 11728
   DHCPv6 Client DUID..............: 00-01-00-01-00-B3-73-B0-00-04-9A-DD-3D-59
   DNS Servers.....................: ::
                                     192.15.2.5

Bluetooth Connection:

   Connection-specific DNS Suffix..:
   Physical Address................: 00E0.8F85.1B46
   Link-local IPv6 Address.........: ::
   IPv6 Address....................: ::
   IPv4 Address....................: 0.0.0.0
   Subnet Mask.....................: 0.0.0.0
   Default Gateway.................: ::
                                     0.0.0.0
   DHCP Servers....................: 0.0.0.0
   DHCPv6 IAID.....................: 11728
   DHCPv6 Client DUID..............: 00-01-00-01-00-B3-73-B0-00-04-9A-DD-3D-59
   DNS Servers.....................: ::
                                     192.15.2.5
```

Task 19c:

Using the images below, decide which troubleshooting command is being used.

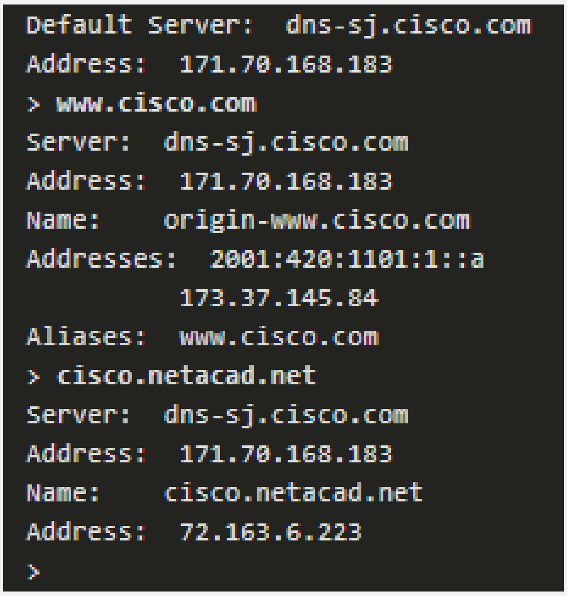
Image	Troubleshooting
	Basic network information
	ping command
	tracert command
	netstat command

```
Ethernet adapter Ethernet:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :

Wireless LAN adapter Wi-Fi:

   Connection-specific DNS Suffix  . : lan
   Link-local IPv6 Address . . . . . : fe80::a1cc:4239:d3ab:2675%6
   IPv4 Address. . . . . . . . . . . : 10.10.10.130
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 10.10.10.1
```

```
Pinging 10.10.10.1 with 32 bytes of data:
Reply from 10.10.10.1: bytes=32 time=1ms TTL=64
Reply from 10.10.10.1: bytes=32 time=1ms TTL=64
Reply from 10.10.10.1: bytes=32 time=1ms TTL=64
Reply from 10.10.10.1: bytes=32 time=1ms TTL=64

Ping statistics for 10.10.10.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 1ms, Maximum = 1ms, Average = 1ms
```

```
Tracing route to e2867.dsca.someispedge.net [104.95.63.78]
over a maximum of 30 hops:

  1     1 ms     1 ms    <1 ms  10.10.10.1
  2     *        *        *     Request timed out.
  3     8 ms     8 ms     8 ms  24-155-250-94.dyn.yourisp.net [172.30.250.94]
  4    22 ms    23 ms    23 ms  24-155-121-218.static.yourisp.net [172.30.121.218]
  5    23 ms    24 ms    25 ms  dls-b22-link.anotherisp.net [64.0.70.170]
  6    25 ms    24 ms    25 ms  dls-b23-link.anotherisp.net [192.168.137.106]
  7    24 ms    23 ms    21 ms  someisp-ic-341035-dls-b1.c.anotherisp.net [192.168.169.47]
  8    25 ms    24 ms    23 ms  ae3.databank-dfw5.netarch.someisp.com [10.250.230.195]
  9    25 ms    24 ms    24 ms  a104-95-63-78.deploy.static.someisptechnologies.com [104.95.63.78]
```

```
Active Connections

  Proto  Local Address          Foreign Address        State
  TCP    10.10.10.130:58520     dfw28s01-in-f14:https  ESTABLISHED
  TCP    10.10.10.130:58522     dfw25s25-in-f14:https  ESTABLISHED
  TCP    10.10.10.130:58523     dfw25s25-in-f14:https  ESTABLISHED
  TCP    10.10.10.130:58525     ec2-3-13-132-189:https  ESTABLISHED
  TCP    10.10.10.130:58579     203.104.160.12:https   ESTABLISHED
  TCP    10.10.10.130:58580     104.16.249.249:https   ESTABLISHED
  TCP    10.10.10.130:58624     52.242.211.89:https    ESTABLISHED
  TCP    10.10.10.130:58628     24-155-92-110:https    ESTABLISHED
  TCP    10.10.10.130:58651     ec2-18-211-133-65:https  ESTABLISHED
  TCP    10.10.10.130:58686     do-33:https            ESTABLISHED
  TCP    10.10.10.130:58720     172.253.119.189:https  ESTABLISHED
  TCP    10.10.10.130:58751     ec2-35-170-0-145:https  ESTABLISHED
  TCP    10.10.10.130:58753     ec2-44-224-80-214:https  ESTABLISHED
  TCP    10.10.10.130:58755     a23-65-237-228:https   ESTABLISHED
```



```
Default Server:  dns-sj.cisco.com
Address:  171.70.168.183
> www.cisco.com
Server:  dns-sj.cisco.com
Address:  171.70.168.183
Name:    origin-www.cisco.com
Addresses:  2001:420:1101:1::a
          173.37.145.84
Aliases:  www.cisco.com
> cisco.netacad.net
Server:  dns-sj.cisco.com
Address:  171.70.168.183
Name:    cisco.netacad.net
Address:  72.163.6.223
>
```

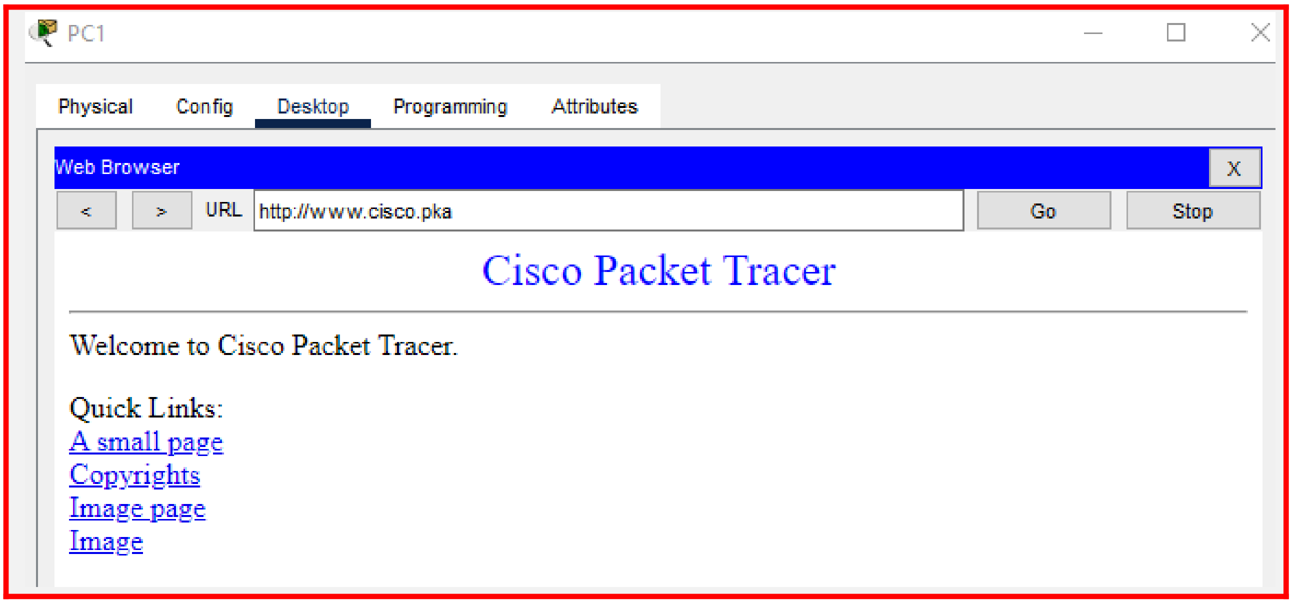
nslookup command

Task 19d:

Once you have completed Packet Tracer – ***Use the ping Command***, paste your evidence in the appropriate boxes below.

Verify connectivity

Show that you have accesses the **www.cisco.pka** via a Web Browser.



URL http://www.cisco.pka

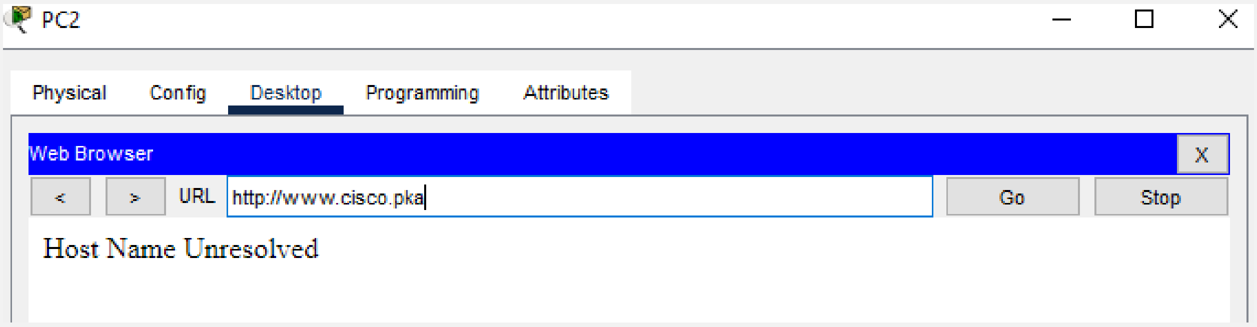
Cisco Packet Tracer

Welcome to Cisco Packet Tracer.

Quick Links:
A small page
Copyrights
Image page
Image

Identify Problem

Identify the PC that is unable to connect to www.cisco.pka.



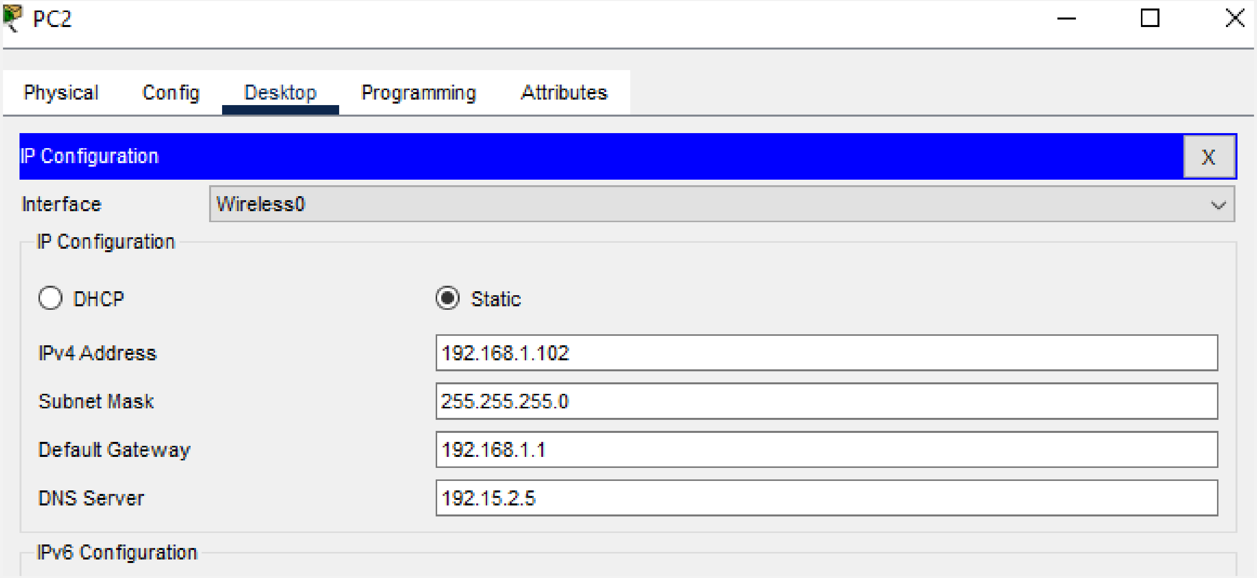
URL http://www.cisco.pka

Host Name Unresolved

Why is above PC unable to connect to www.cisco.pka?

Ping request could not find host www.cisco.pka because the DNS Server on PC 2 was incorrectly configured.

Correct any misconfiguration



Interface: Wireless0

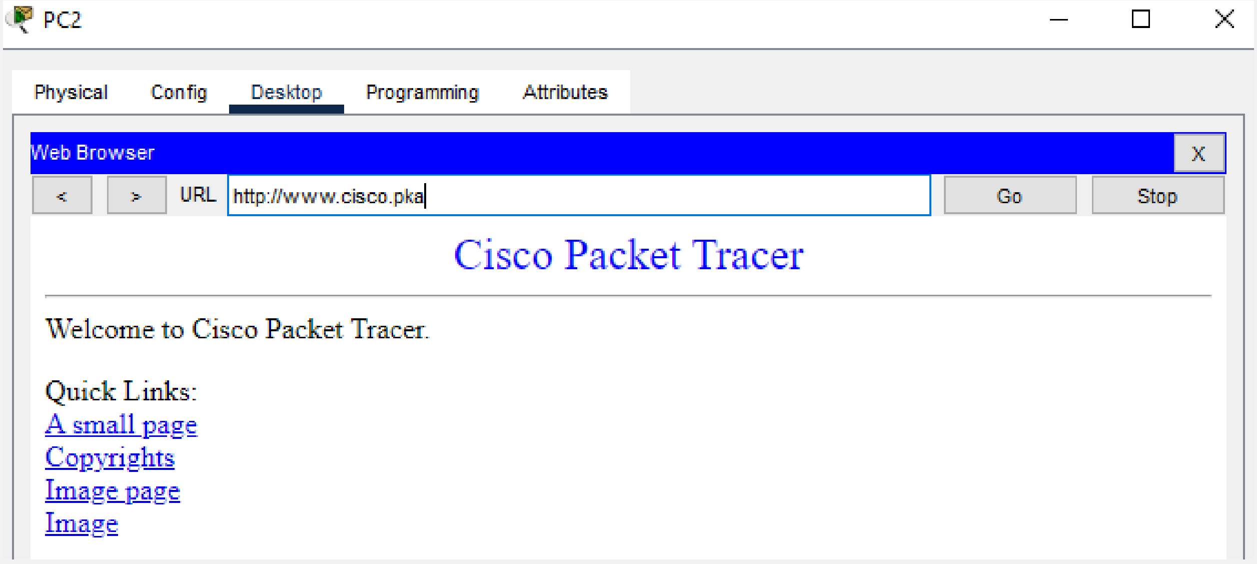
○ DHCP ● Static

IPv4 Address: 192.168.1.102

Subnet Mask: 255.255.255.0

Default Gateway: 192.168.1.1

DNS Server: 192.15.2.5



URL http://www.cisco.pka

Cisco Packet Tracer

Welcome to Cisco Packet Tracer.

Quick Links:
A small page
Copyrights
Image page
Image

Task 19e:

Once you have completed Packet Tracer – ***Skills Integrated Challenge***, paste your evidence in the appropriate boxes below.

Router 1/Switch 1

What command did you use to change the hostname?

The command I used to change the hostname is: Router(config)# hostname R1

What command did you use to add banner?

I used the configure terminal : R1(config)# banner motd #Unauthorized access is prohibited. Warning!#

What command did you use to set Privilege EXEC password?

I used configure line : R1(config)# line console 0

What commands did you use to set Console Password? Enter line in each box.

R1(config-line)# password cisco

R1(config-line)#login

What command did you use to encrypt all plaintext passwords?

R1(config-line)# enable secret class
R1(config)#service password-encryption

What commands did you use to configure Domain. Enter line in each box.

ip domain-name networking.pka

crypto key generate rsa

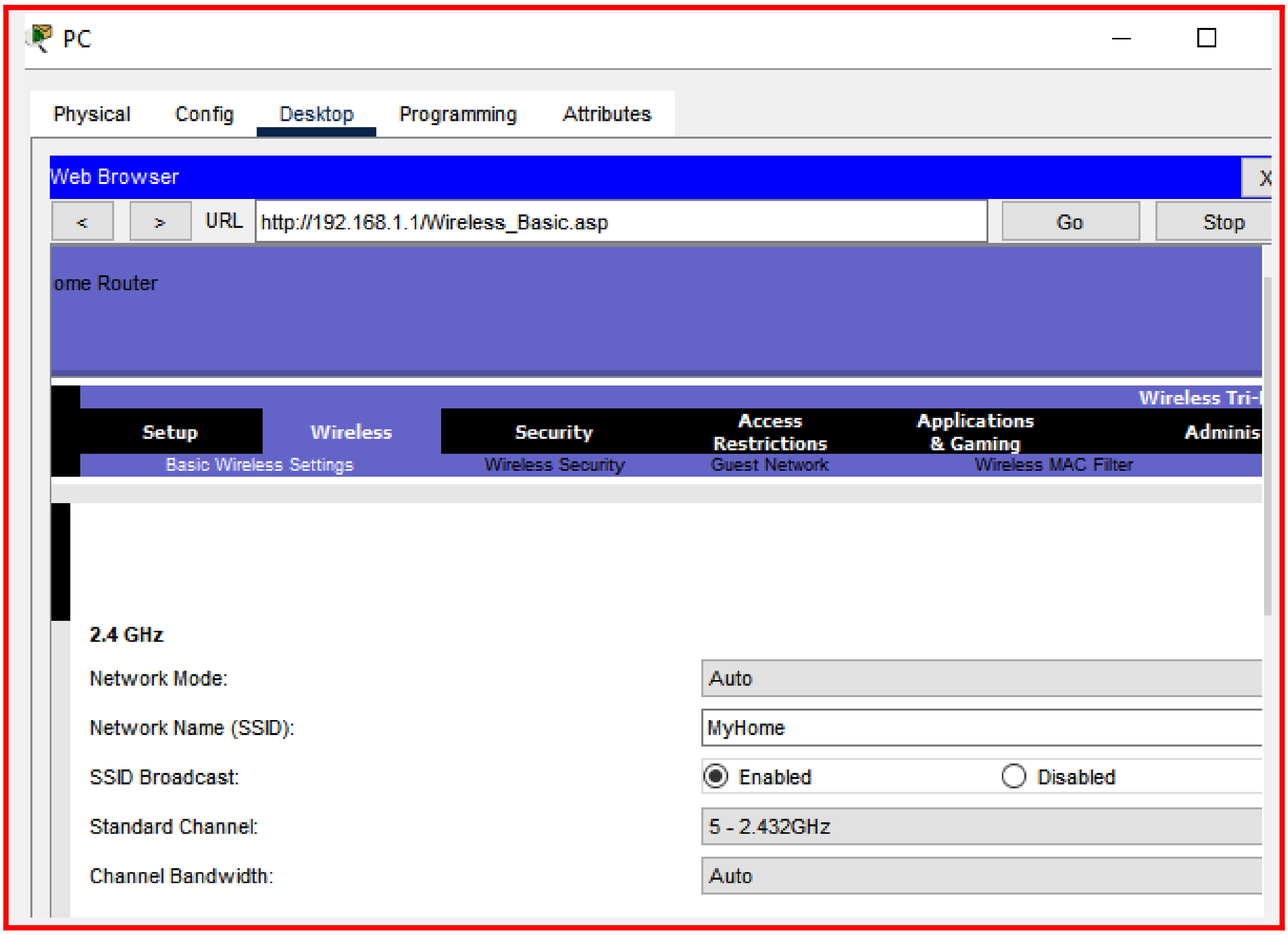
modulus 1024

What commands did you use to configure SSH access. Enter line in each box.

username	*admin*	secret	*cisco*

```
line vty 0 4
transport input ssh
login local
```

Wireless Router
Show screenshot that you have changed SSID to 'MyHome' on the Wireless Router.



URL http://192.168.1.1/Wireless_Basic.asp

2.4 GHz

Network Mode: Auto

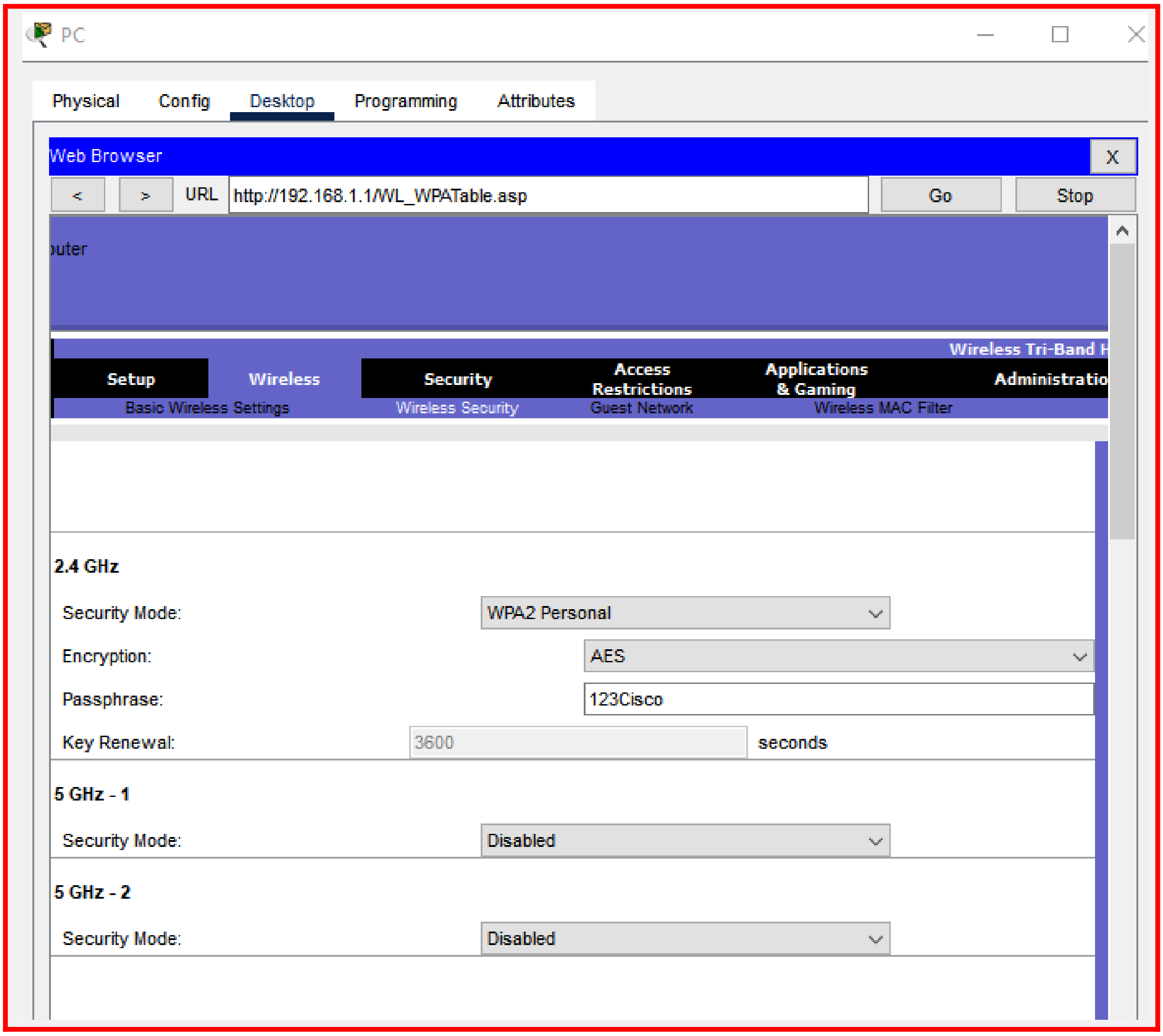
Network Name (SSID): MyHome

SSID Broadcast: ● Enabled ○ Disabled

Standard Channel: 5 - 2.432GHz

Channel Bandwidth: Auto

Show screenshot that you have changed set ***Security Mode for 2.4GHz*** to **WPA2 Personal** and used ***123Cisco as the Passphrase***



URL http://192.168.1.1/WL_WPATable.asp

2.4 GHz

Security Mode: WPA2 Personal

Encryption: AES

Passphrase: 123Cisco

Key Renewal: 3600 seconds

5 GHz - 1

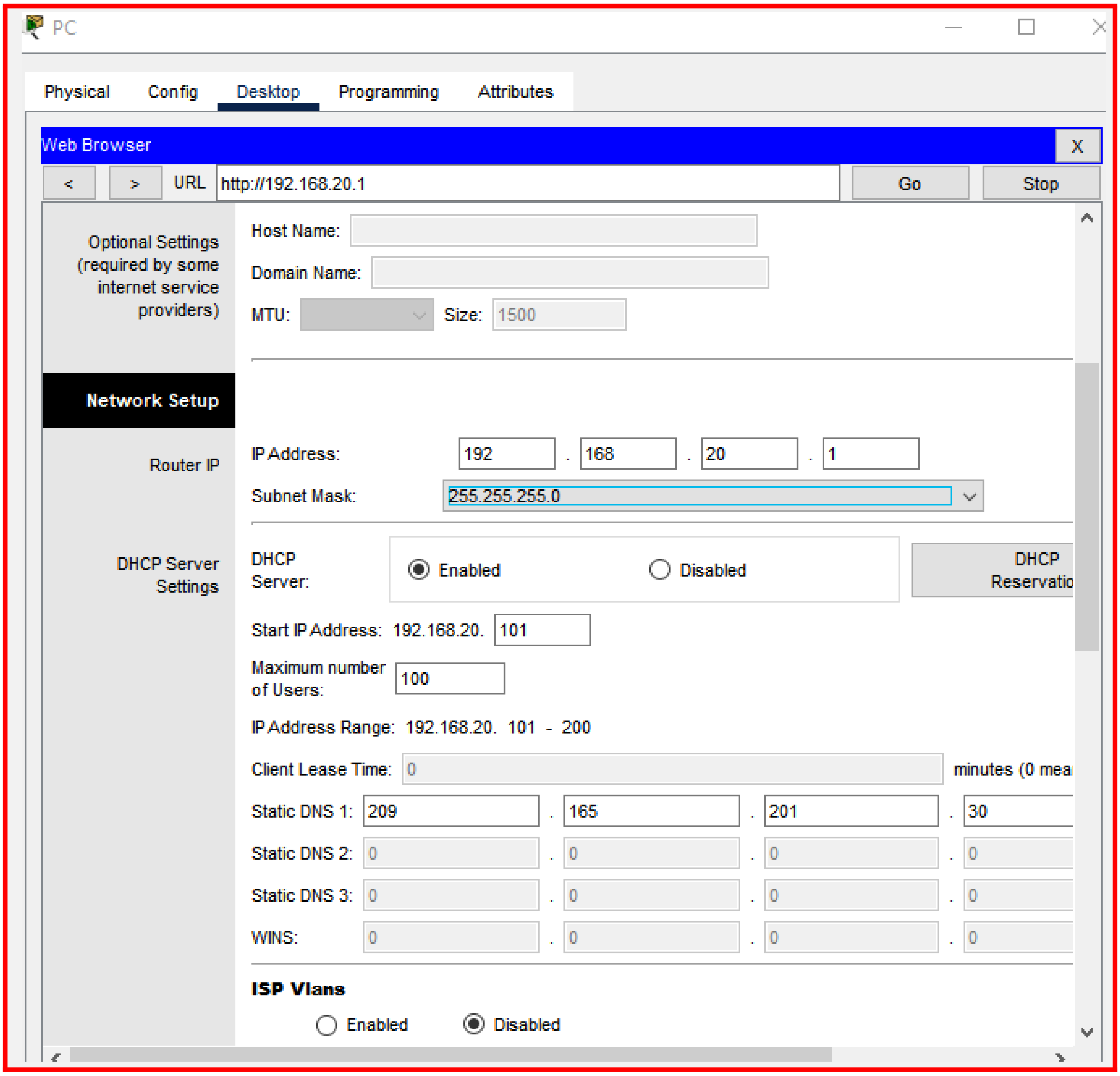
Security Mode: Disabled

5 GHz - 2

Security Mode: Disabled

Show screenshot that you have **configured DHCP** according to the following instructions:

Wireless Router IP Address:	**192.168.20.1**
Starting IP Address:	**192.168.20.101**
Maximum Number:	**100**
DNS 1:	**209.165.201.30**



URL http://192.168.20.1

Optional Settings (required by some internet service providers)

Host Name:

Domain Name:

MTU: Size: 1500

Router IP

IP Address: 192 . 168 . 20 . 1

Subnet Mask: 255.255.255.0

DHCP Server Settings

DHCP Server: ● Enabled ○ Disabled

Start IP Address: 192.168.20. 101

Maximum number of Users: 100

IP Address Range: 192.168.20. 101 - 200

Client Lease Time: 0 minutes (0 mea

Static DNS 1: 209 . 165 . 201 . 30

Static DNS 2: 0 . 0 . 0 . 0

Static DNS 3: 0 . 0 . 0 . 0

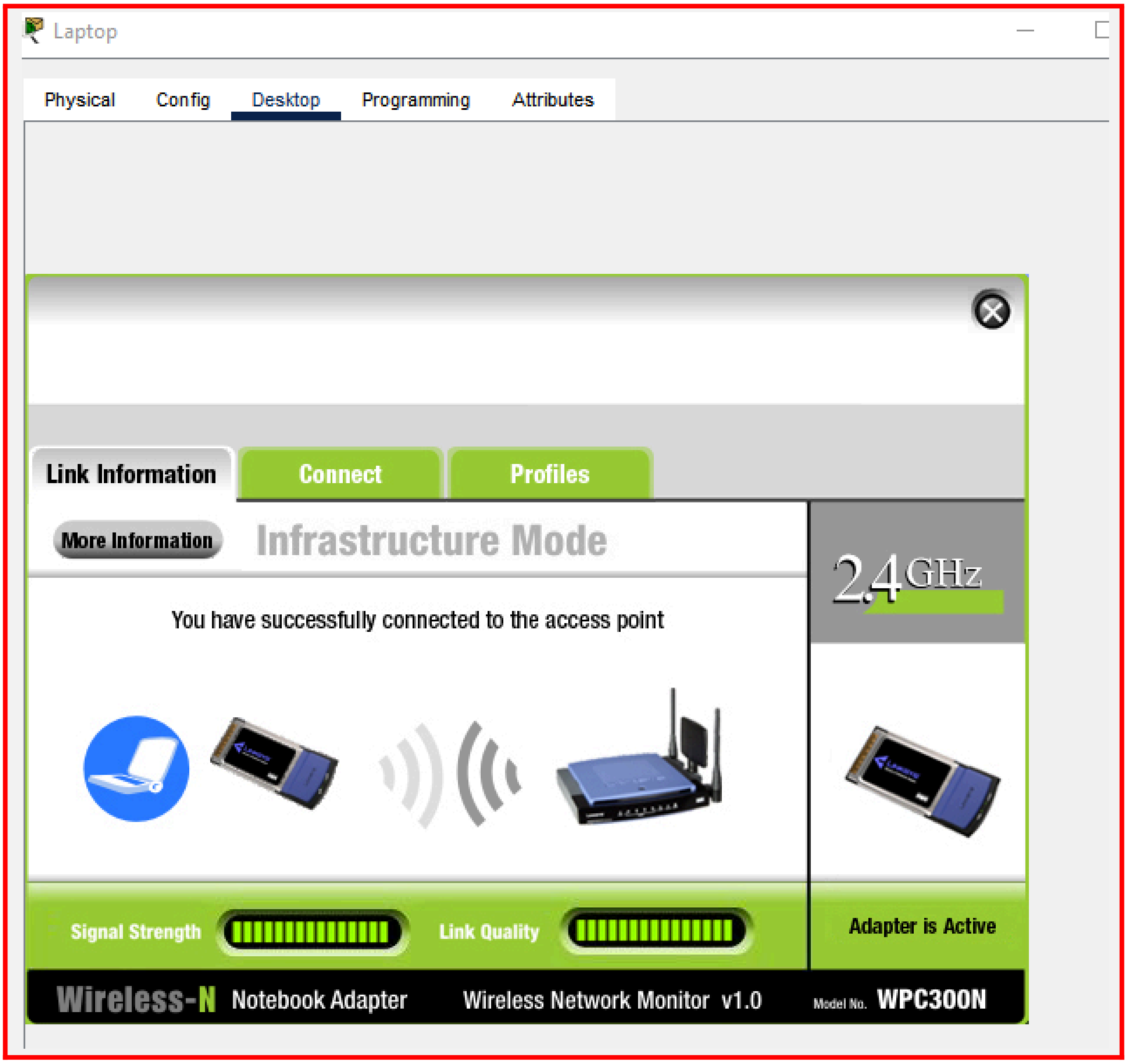
WINS: 0 . 0 . 0 . 0

ISP Vlans

○ Enabled ● Disabled

End Devices

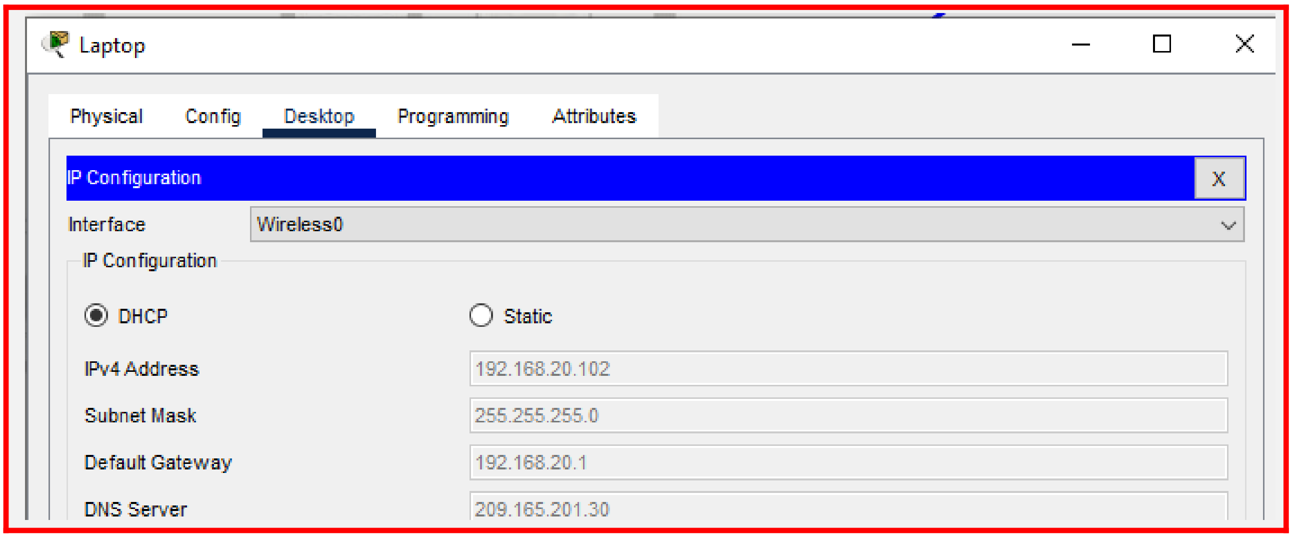
Show screenshot that you have **configured End Devices**. One screenshot is needed!



You have successfully connected to the access point

Verify Connectivity

Show screenshot that **verifies that IP addresses are in the correct networks**. All the end devices should be in 192.168.20.0/24 network.



Interface: Wireless0

IP Configuration

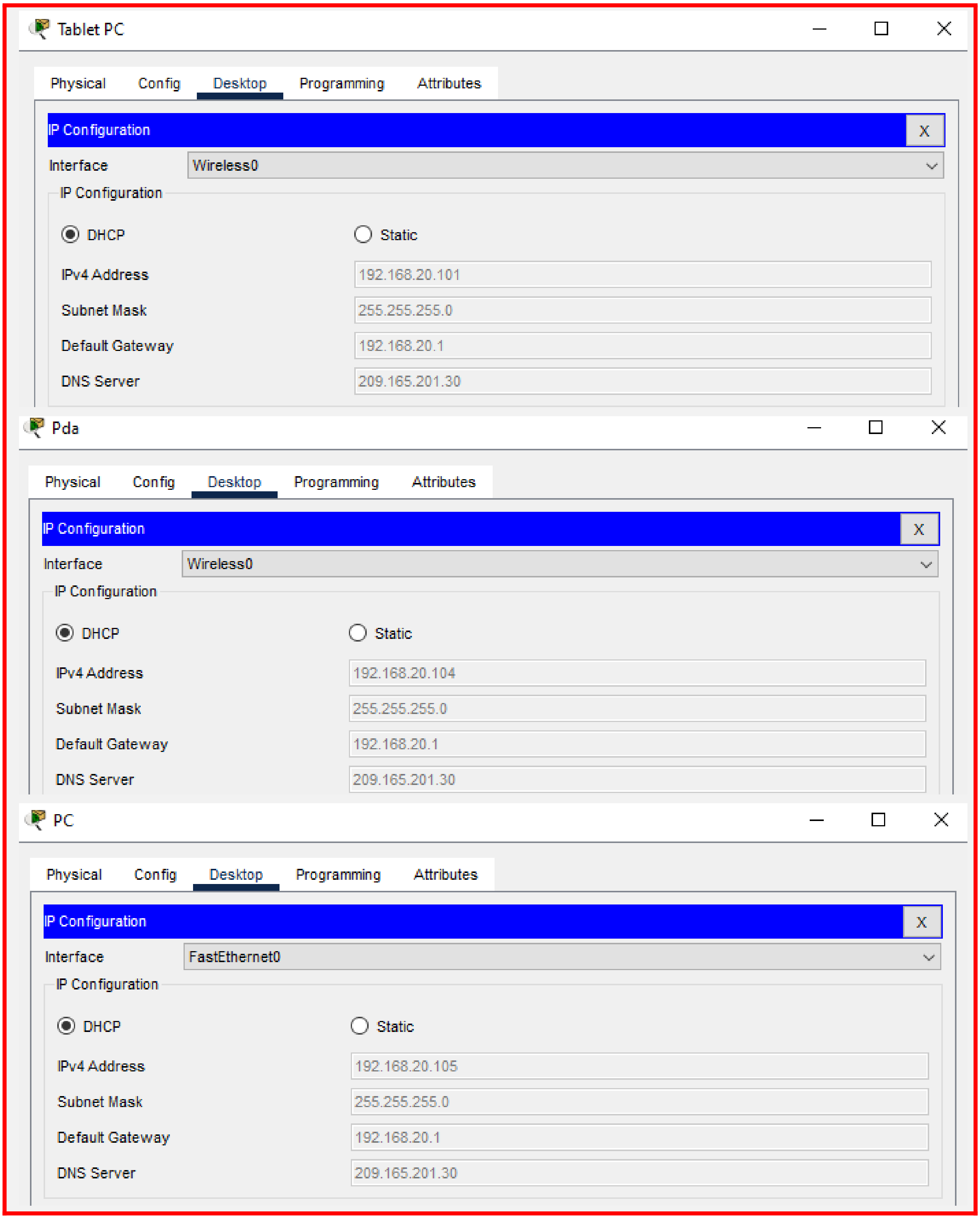
● DHCP ○ Static

IPv4 Address: 192.168.20.102

Subnet Mask: 255.255.255.0

Default Gateway: 192.168.20.1

DNS Server: 209.165.201.30



Tablet PC

IP Configuration

Interface: Wireless0

IP Configuration

● DHCP ○ Static

IPv4 Address: 192.168.20.101

Subnet Mask: 255.255.255.0

Default Gateway: 192.168.20.1

DNS Server: 209.165.201.30

Pda

IP Configuration

Interface: Wireless0

IP Configuration

● DHCP ○ Static

IPv4 Address: 192.168.20.104

Subnet Mask: 255.255.255.0

Default Gateway: 192.168.20.1

DNS Server: 209.165.201.30

PC

IP Configuration

Interface: FastEthernet0

IP Configuration

● DHCP ○ Static

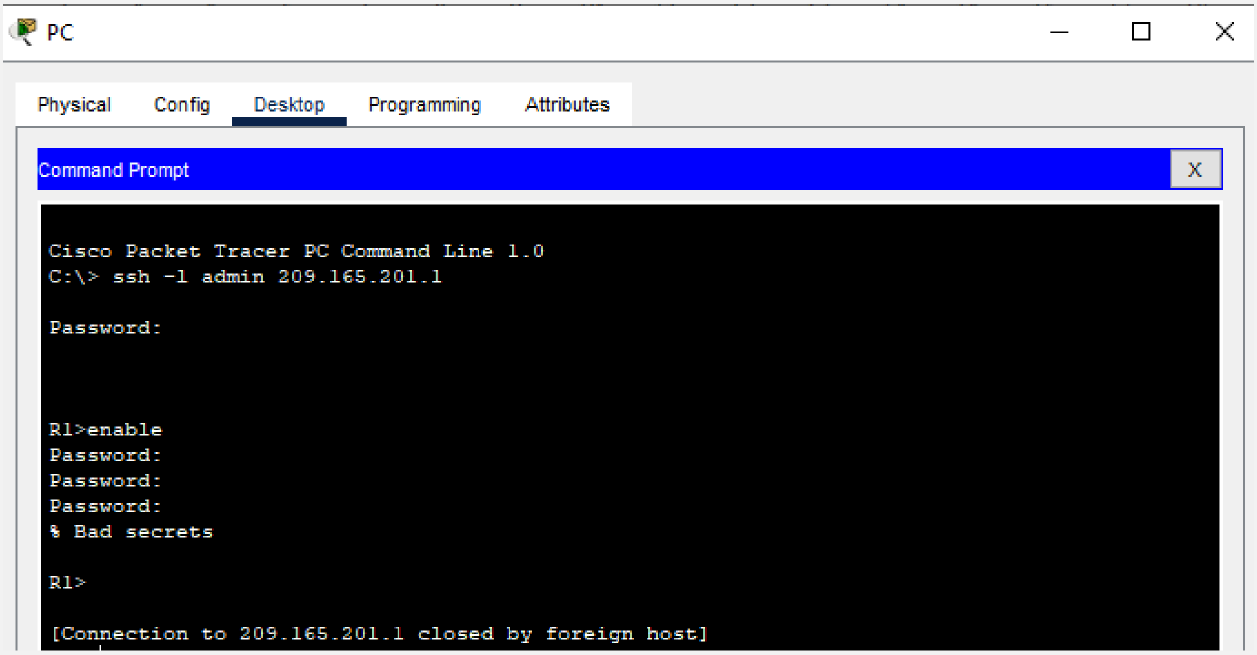
IPv4 Address: 192.168.20.105

Subnet Mask: 255.255.255.0

Default Gateway: 192.168.20.1

DNS Server: 209.165.201.30

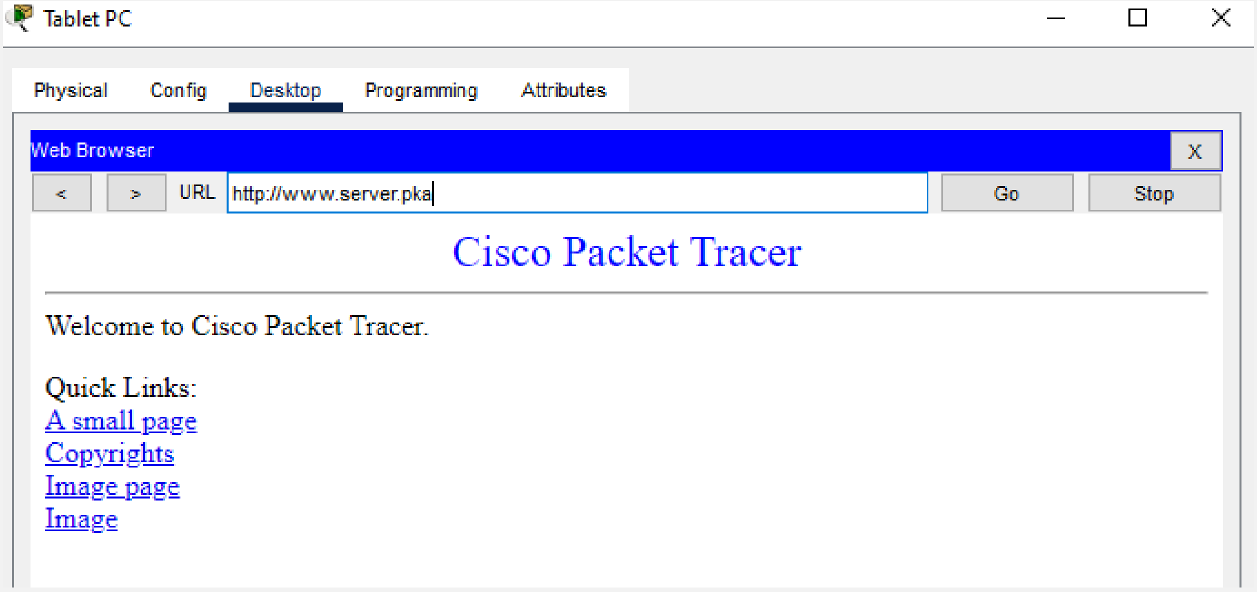
Show screenshot that **verifies you can login to R1 via SSH from a PC from Home**.



```
Cisco Packet Tracer PC Command Line 1.0
C:\> ssh -l admin 209.165.201.1

Password:



R1>enable
Password:
Password:
Password:
% Bad secrets

R1>

[Connection to 209.165.201.1 closed by foreign host]
```

I've tried several times, reset it as well and had the same problem. Tried different passwords too.

Show screenshot that **verifies** you can access **www.server.pka** from **tablet**



URL http://www.server.pka

Cisco Packet Tracer

Welcome to Cisco Packet Tracer.

Quick Links:
A small page
Copyrights
Image page
Image

END OF WORKBOOK

Please check through your work thoroughly before submitting and update the table of contents.