SRM

INSTITUTE OF SCIENCE & TECHNOLOGY

(Deemed to be University u/s 3 of UGC Act, 1956)

18CSS202J- Computer Communications

Project Report

Topic: Home Wireless Network Design

Team Members:

1.Aryan Gupta (RA2011003010351)
2.Keshav Agarwal (RA2011003010357)

Semester / Year: 4th / 2nd

Department: Networking and Communications

Abstract

A wireless network has to be designed at home with remote access from the office. There are 3 users at home. Two users have a desktop and the third user has a laptop. A high-speed cable internet connection is available at home and a serial port printer is available for printing. The (false) assumption is that the network is always available, that bandwidth is unlimited and that congestion and delays do not occur. As such, even though the applications and the network are tightly coupled, they are typically developed and deployed as independent components. It is exactly this decoupling that creates the burden of carefully planning a WLAN for successful support of the extension of applications to the wireless environment. Hence, start with the premise that the average application is not aware of the transport medium it is using. They treat the network—wired or wireless—identically. The challenge of applications not being aware of the network is compounded with WLANs. Indeed, most applications are developed for wired environments; however, they will likely be developed specifically for the one-to-one initiatives in the education sector. Specific characteristics of WLANs are their lower throughput and higher latency than their wired equivalents. This is typically not a problem for burst applications. However, WLAN can cause additional challenges for applications that demand high data rates or deterministic behavior. The interaction between applications and the network is only one of the challenges that must be tackled when 38defining WLAN architecture. Wireless networks can transfer data anywhere from 10-600 megabytes per second (Mbps) depending on the type of wireless standard that your modem uses. You can often improve the wireless signal by using a wireless repeater. Wireless repeaters pick up a signal, and if the signal has degraded, the repeater can rebroadcast it again at full strength. However, Wireless technology is often slower than wired technologies. Wireless technology can be affected by interference from walls, large metal objects, and pipes. Also, many cordless phones and microwave ovens can interfere with wireless networks when in use. Wireless networks are frequently about half as fast as their rated speed. Hence there lies a need for it to be investigated. The primary methods being used in the project   are installing of a Wireless Router, installing of a Wireless Access Point, configuring of the Wireless Adapters, configuring of an Ad-Hoc Home WLAN, configuring of Software Internet Connection Sharing and so on. Ensuring all the users share the internet connection, the laptop has a secure wireless access to the internet, the desktop users are able to access the internet through the LAN, the users are transparent to the IP addressing system and are not required to configure the same manually, making sure that one of the routers at home can be accessed from the office and that all the Users are able to use the Printer are the major results of this project. In conclusion we can say that a wireless home network with 3 users and a serial port printer has been successfully set up and all the objectives that were set have been fulfilled.

Objective of the Project

The objective of this project is to create a home wireless network that has remote access from the home office. Given that the three users have a high speed cable internet connection available at home, each user should be able to access the serial port printer for printing purposes.

Introduction

Wireless Networks:

Wireless networks can transfer data anywhere from 10-600 megabytes per second (Mbps)depending on the type of wireless standard that your modem uses.

Advantages-

- You can easily move devices because there are no cables.
- Wireless networks are cheaper to install than wired networks.
- You can often improve the wireless signal by using a wireless repeater. Wireless repeaters pick up a signal, and if the signal has degraded, the repeater can rebroadcast it again at fullstrength.

Drawbacks-

- Wireless technology is often slower than wired technologies.
- Wireless technology can be affected by interference from walls, large metal objects, and pipes. Also, many cordless phones and microwave ovens can interfere with wireless networks when in use.
- Wireless networks are frequently about half as fast as their rated speed.

Home Wireless Network Design

Project Scope:

A wireless network has to be designed at home with remote access from the office. There are 3 users at home. Two users have a desktop and the third user has a laptop. A high-speed cable internet connection is available at home. A serial port printer is available for printing.

Network requirements:

Home Office devices can connect as follows:

1. Laptops and tablets connect wirelessly to a home router.
2. A network printer connects using an Ethernet cable to the switch port on the home router.
3. The home router connects to the service provider's cable modem using an Ethernet cable.
4. The cable modem connects to the Internet service provider (ISP) network.

Application characteristics must be analyzed if this traffic flows over the WLAN. It is essential to outline this in the policy to protect and ensure scalability as planned. Performance is not limited to the 36 throughputs that a client can achieve. It is also directly related to the client keeping its network connection and communication session intact. When roaming from one AP to another, there is a small amount of time during either authentication or association during which the client will effectively be without a link. The duration of the lost link will determine if and how applications will be impacted. Note that last roaming was specifically conceived to make this link loss during authentication almost unnoticeable to end-users. Applications exhibit a distinctive sensitivity to the duration of a lost link. Transactional applications such as e-mail and web browsing are relatively insensitive, whereas real-time applications such as voice and video are susceptible. Ensure that fast roaming is enabled to make authentication occur promptly enough to not affect the core WLAN the application suite. Application bandwidth requirements can be analyzed by the software vendor's specifications or manuals. A common issue with network applications is that they are developed with little or no consideration for the resources they require from the communications infrastructure. Application developers take into consideration the notion of the network but typically fail to consider bandwidth and latency implications. The (false) assumption is that the network is always available, that bandwidth is unlimited and that congestion and delays do not occur. As such, even though the applications and the network are tightly coupled, they are typically developed and deployed as independent components. It is exactly this decoupling that creates the burden of carefully planning a WLAN for successful support of the extension of applications to the wireless environment. Hence, start

with the premise that the average application is not aware of the transport medium it is using. They treat the network—wired or wireless—identically. The challenge of applications not being aware of the network is compounded with WLANs. Indeed, most applications are developed for wired environments; however, they will likely be developed specifically for the one-to-one initiatives in the education sector. Specific characteristics of WLANs are their lower throughput and higher latency than their wired equivalents. This is typically not a problem for burst applications. However, WLAN can cause additional challenges for applications that demand high data rates or deterministic behaviour. The interaction between applications and the network is only one of the challenges that must be tackled when
38defining WLAN architecture. Defining a wireless architecture to support voice and video also introduces specific problems that must be considered. The considerations include provisioning sufficient bandwidth for latency-sensitive applications, implementing a quality of service (QoS) solution, and ensuring fast-roaming capabilities between cells. Perhaps today's students will be in one classroom and it is unlikely that they will be roaming between APs, which sounds like a rational and fair statement. However, recall that this WLANinvestment is meant to last districts up to five years. In the world of technology, five years is a very long time, and it may very well be that a district will want to implement other applications and devices to run over the WLAN. One such example, which could be used by students more likely teachers, is that of Voice over WLAN handsets.

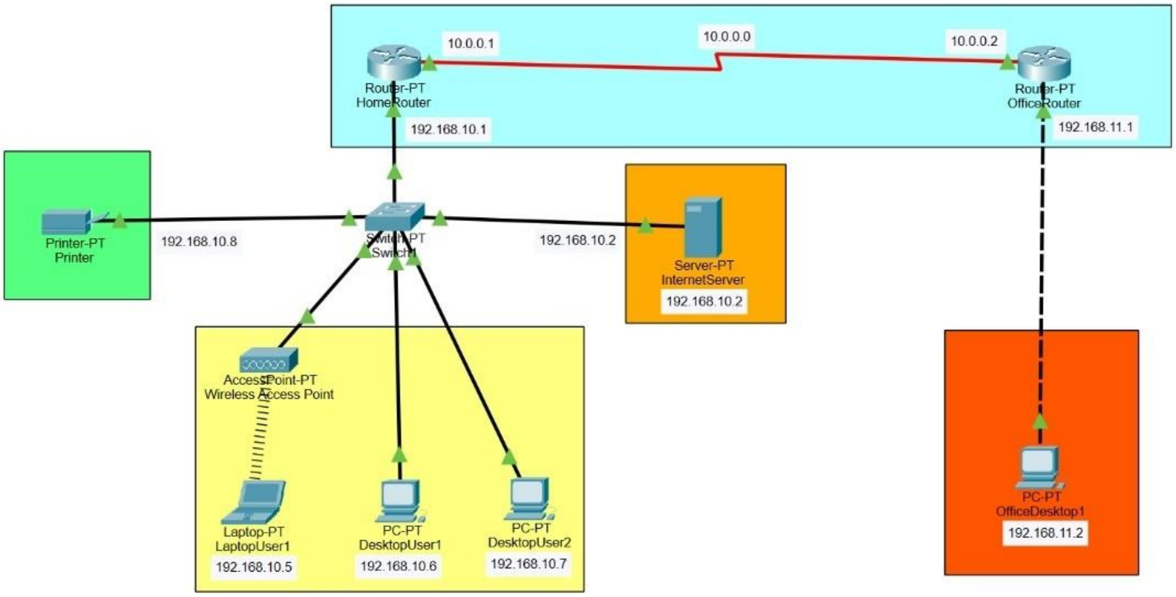
Hardware Requirements Analysis:

Hardware points to consider include:

- May require switch standards applicable for VLAN which support PoE, VLAN or capacity.
- Older hardware is incompatible with new security standards;
- Can older hardware support the new wireless cards?
- Is there room for them?

1. Wireless Network Adapters
   Wireless network adapters (also known as wireless NICs or wireless network cards) are required for each device on a wireless network.
2. Wireless Routers and Access Points
   Wireless routers are the heart of a wireless network. These routers function comparable to routers for wired Ethernet networks.
3. Wireless Antennas
   Access points and routers can use a Wi-Fi wireless antenna to increase the communication range of the wireless radio signal.
4. Wireless Repeaters
   A wireless repeater connects to a router or access point to extend the reach of the network.

Network Topology Diagram:



Identifying which services and applications the WLAN must support is a key to building a robust, relevant, scalable and sustainable architecture.
It is strongly urged to consider the following elements of any one-to-one initiative:
- Number of NOUN SST staff using the WLAN.
- Types of application(s) being utilized
- Total bandwidth requirements
- Throughput requirements
- Security for laptops
- Special attention should be considered for NOUN SST staff taking their laptops home to access the Internet or other resources.

- Obtain floor plans for the office and home to assist in setup.
- Determine how many Access Points. It will take to provide a signal to the desired coverage area.
- Physical Access Points placement map- Identify signal trouble areas and physical construction or environmental challenges. Determine user policies for the wireless network.
- Diagram channel layout of Access Points.
- Confirm hardware compatibility (include desired legacy hardware, new hardware and current or future for staff-owned device standards)
  Verify that each Access Points location is physically secure.
- Verify that there is a power source near the intended location for each Access Point or Power over Ethernet Compatibility.
- Confirm there is a way to run a patch cable between your wired network and each AP and/or APs to be used as repeaters. List specialized antennae requirements.
- Determine AP network cabling distances and are within CAT-5 or 6 limits (~100m)

Network implementation plan

- Install a Wireless Router
  - ❖ One wireless router supports one WLAN. Install the wireless router in a central location within the home. The way Wi-Fi networking works, computers closer to the router (generally in the same room or in line of sight) get better network speed than computers farther away.
  - ❖ Connect the wireless router to a power outlet and optionally to a source of internet connectivity. All modern wireless routers support broadband modems. Additionally, because wireless routers contain a built-in access point, you can also connect a wired router, switch, or hub.

    - ❖ Choose your network name. In Wi-Fi networking, the network name is often called the SSID. Although routers ship with a default name, it's best to change it for security reasons. Consult product documentation to find the network name for your wireless router.
    - ❖ Follow the router documentation to enable WEP security, turn on firewall features, and set any other recommended

- Install a Wireless Access Point
    - ❖ One wireless access point supports one WLAN. Install your access point in a central location, if possible. Connect power and cable the access point to your LAN router, switch, or hub.
    - ❖ You won't have a firewall to configure, but you still must set a network name and enable WEP on the access point at this stage.
- Configure the Wireless Adapters
    - ❖ Configure the adapters after setting up the wireless router or access point (if you have one). Insert the adapters into your computers as explained in the product documentation. Wi-Fi adapters require that you install TCP/IP on the host computer.
    - ❖ Manufacturers provide configuration utilities for their adapters. For example, on the Windows operating system, adapters generally have a graphic user interface (GUI) accessible from the Start Menu or taskbar after you install the hardware. The GUI is where you set the network name (SSID) and turn on WEP. You can also set a few other parameters.
    - ❖ All wireless adapters must use the same parameter settings for your WLAN to function properly.

- Configure an Ad-Hoc Home WLAN
    - ❖ Every Wi-Fi adapter requires you to choose between infrastructure mode (called access point mode in some configuration tools) and ad-hoc wireless (peer-to-peer) mode. Set every wireless adapter for infrastructure mode. In this mode, wireless adapters automatically detect and set their WLAN channel number to match the access point (router).
    - ❖ Alternatively, set all wireless adapters to use ad hoc mode. When you enable this mode, you see a separate setting for channel number.
    - ❖ All adapters on your ad hoc wireless LAN need matching channel numbers.
    - ❖ Ad-hoc home WLAN configurations work fine in homes with only a few computers situated fairly close to each other. You can also use this configuration as a fallback option if your access point or router breaks.
- Configure Software Internet Connection Sharing

    - ❖ You can share an internet connection across an ad hoc wireless network. To do this, designate one of your computers as the host (effectively a substitute for a router). That computer keeps the modem connection and must be on when you use the network. Microsoft Windows offers a feature called Internet Connection Sharing (ICS) that works with ad-hoc WLANs.

- Wireless Signal Interference within the Home
    - ❖ When installing a Wi-Fi router or access point, beware of signal interference from other home appliances. In particular, do not install the unit within 3 to 10 feet (about 1 to 3 m) from a microwave oven. Other common wireless interference sources are 2.4 GHz cordless phones, baby monitors, garage door openers, and some home automation devices.

- Wireless Routers and Access Point Interference from Outside
    - ❖ In densely populated areas, it's not uncommon for wireless signals from one person's home network to penetrate a neighbouring home and create interference. This problem usually happens when both households set conflicting communication channels. When configuring a router (access point), you can (except in a few locales) change the channel number your devices use.

- MAC Address Filtering
    - ❖ Newer wireless routers (access points) support a security feature called Media Access Control (MAC for short) address filtering. This feature allows you to register wireless adapters with your router (access point) and force the unit to reject communications from any wireless device that isn't on the list. MAC address filtering combined with strong Wi-Fi encryption (ideally WPA2 or better) affords good security protection.

- Wireless Security
    - ❖ Among the options you'll see for activating wireless security on home networks, WPA3 is considered the best. Some gear might not support this higher level of protection, though. Ordinary WPA works well on most networks and is a suitable fallback alternative to WPA3.
    - ❖ Avoid using older WEP technologies, when possible, except as a last resort. WEP helps prevent people from casually logging in to your network but offers minimal protection against attackers.

- To set up wireless security, choose a method and assign a long code number called a key or passphrase to the router and all devices. You must configure matching security settings on both the router and the client device for the wireless connection to work. Keep your passphrase secret, as others can join your network if they know the code.

Requirement Analysis and Solutions:

Given Requirements-

1) <u>All the users should share the internet connection.</u>

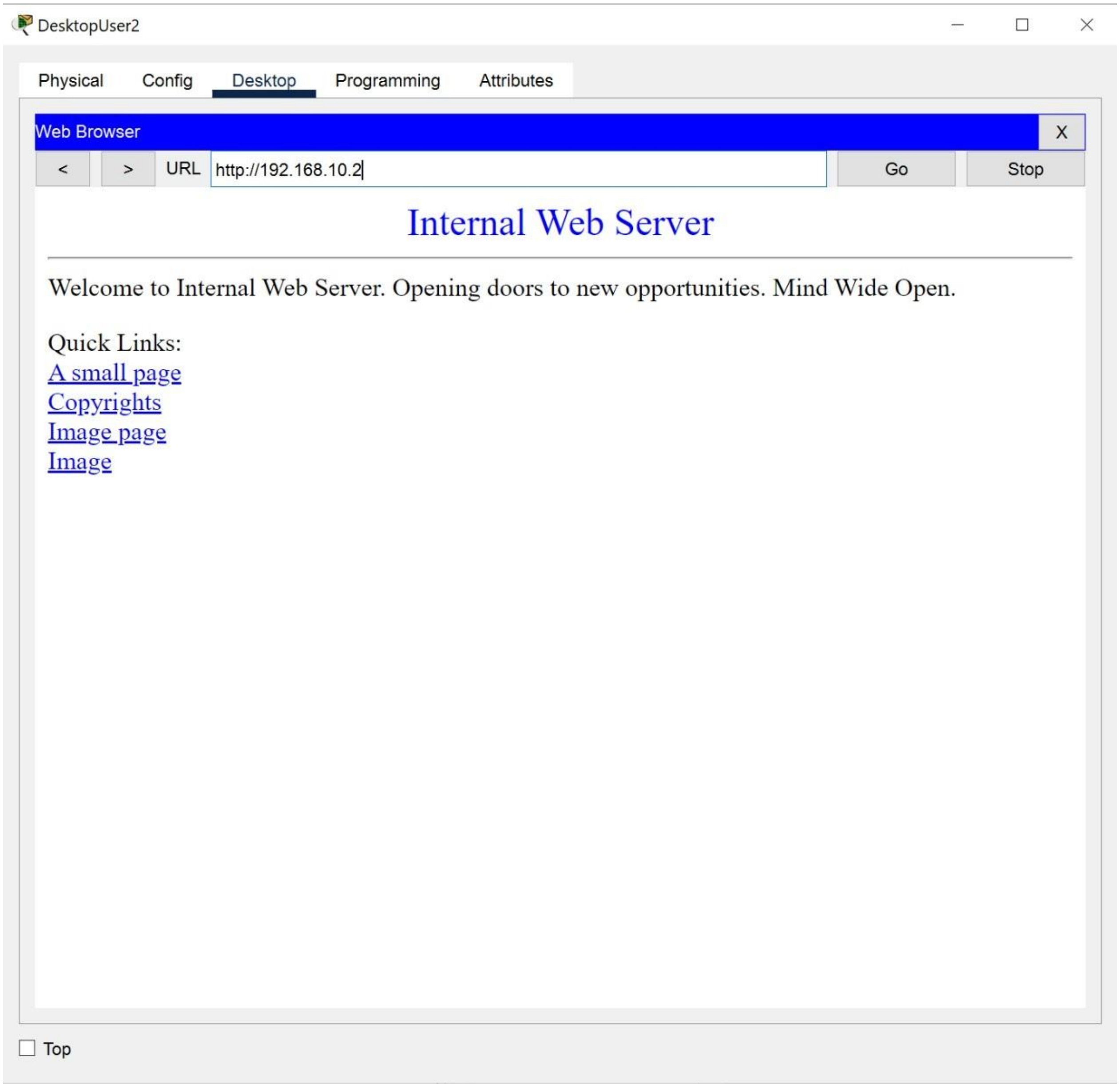
Solution - Steps

A. Configure your devices on the network
B. Open the Network Connections window on the host computer.
C. Right-click on the adapter that is connected to the internet source.
D. Select "Properties" and click the .Sharing tab.
E. Check the "Allow other network users to connect through this computer's Internet connection" box
F. Click the .Settings... button to enable specific services
G. Open your wireless router's configuration page. Open the Internet Settings page on the router.
H. Ensure that the "IP Address" section is set to "Get Automatically". Connect your other computers and devices to the router or hub.

2) <u>The laptop should have secure wireless access to the internet</u>

Solution - Steps

A. Change default username and password
B. Turn on Wireless Network Encryption, Use a VPN (Virtual Private Network).
C. Use Firewalls, Enable MAC Address Filtering
D. Disable Remote Administration.



URL: http://192.168.10.2

Internal Web Server

Welcome to Internal Web Server. Opening doors to new opportunities. Mind Wide Open.

Quick Links:
A small page
Copyrights
Image page
Image

Remote Access to the Internet

3) <u>The desktop users should be able to access the internet through the LAN</u>

A. On the other PC, if you want to join the network, select “My Network Places” properties.
B. Right-click on your LAN connection and select properties. A LAN Properties dialogue box should appear.
C. Select “Internet Protocol (TCP/IP)” as you did when you assigned the IP address.
D. Click the Properties button. An "Internet Protocol (TCP/IP) Properties” dialogue box should appear.

E. Enter the “Default Gateway” and “DNS Server” IP as shown in the image below. Repeat this step on other PCs too.
F. Connect to the Internet on the server PC, the one actually attached to the Internet, then try to access the Internet on the other PC(s).

4) <u>The users should be transparent to the IP addressing system and should not be required to configure the same manually</u>

Using NAT in transparent mode eliminates the need for the upstream or downstream routers to perform NAT for their networks. It can perform a similar function within a bridge group in routed mode.

NAT in transparent mode, or in routed mode between members of the same bridge group, has the following requirements and limitations:

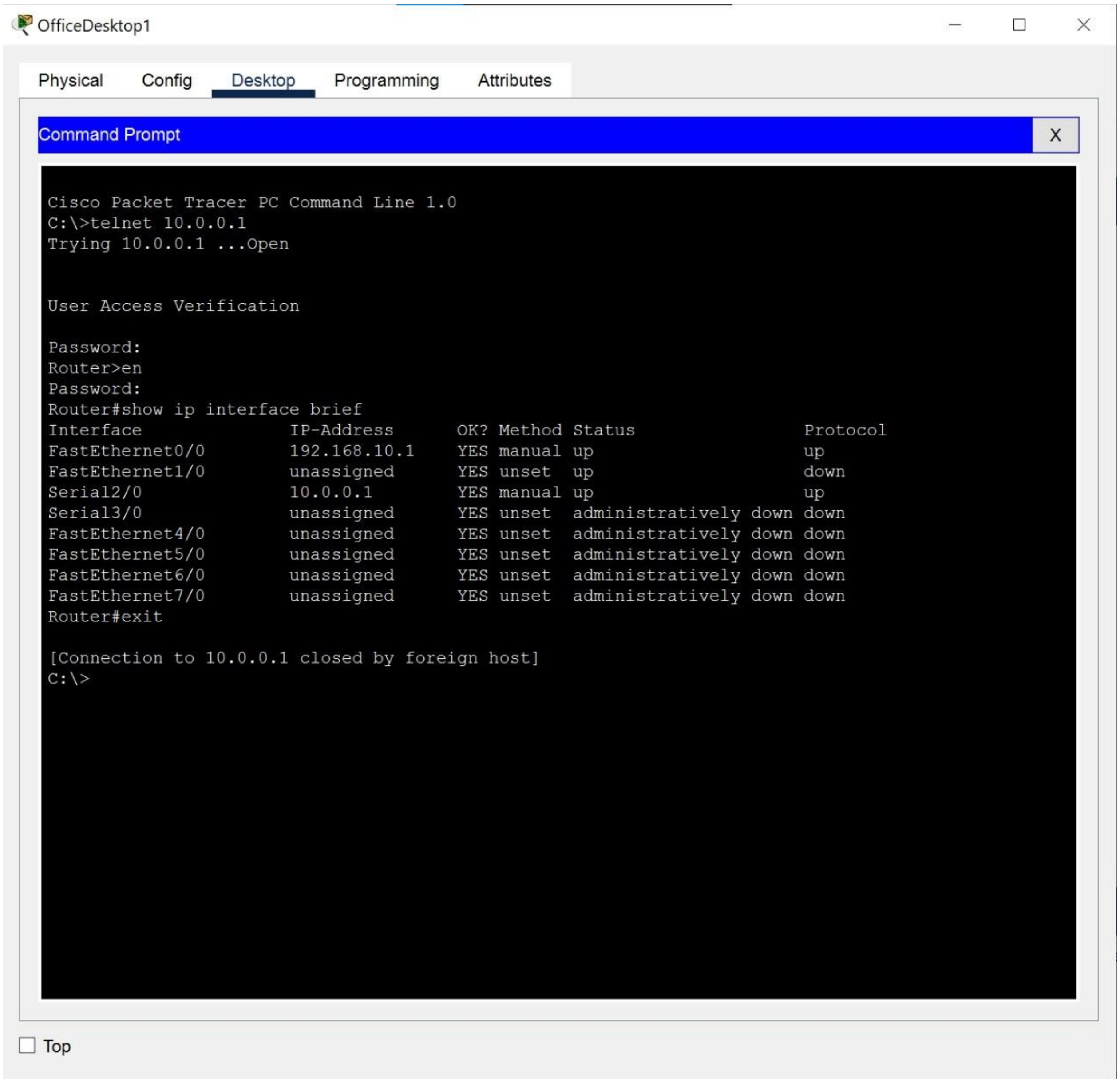
- You cannot configure interface PAT when the mapped address is a bridge group member interface, because there is no IP address attached to the interface.
- ARP inspection is not supported. Moreover, if for some reason a host on one side of the Firepower Threat Defense device sends an ARP request to a host on the other side of the Firepower Threat Defense device, and the initiating host's real address is mapped to a different address on the same subnet, then the real address remains visible in the ARP request.
- Translating between IPv4 and IPv6 networks is not supported. Translating between two IPv6 networks, or between two IPv4 networks is supported.

5) <u>One of the routers at home needs to be accessed from the office</u>.

REMOTE DESKTOP PROTOCOL (RDP)

Finally, there is the RDP, which is very similar to the Independent Computing Architecture (ICA) protocol used by Citrix products. RDP is utilized to access Windows Terminal Services, which is a close relative of the product line provided by Citrix WinFrame.

RDP offers the same core functions as ICA, although there are some limitations. RDP provides remote access for Windows clients only, while ICA can provide access for numerous platforms. ICA also offers support for automatic client updates, publishing an app to a web browser, and more.



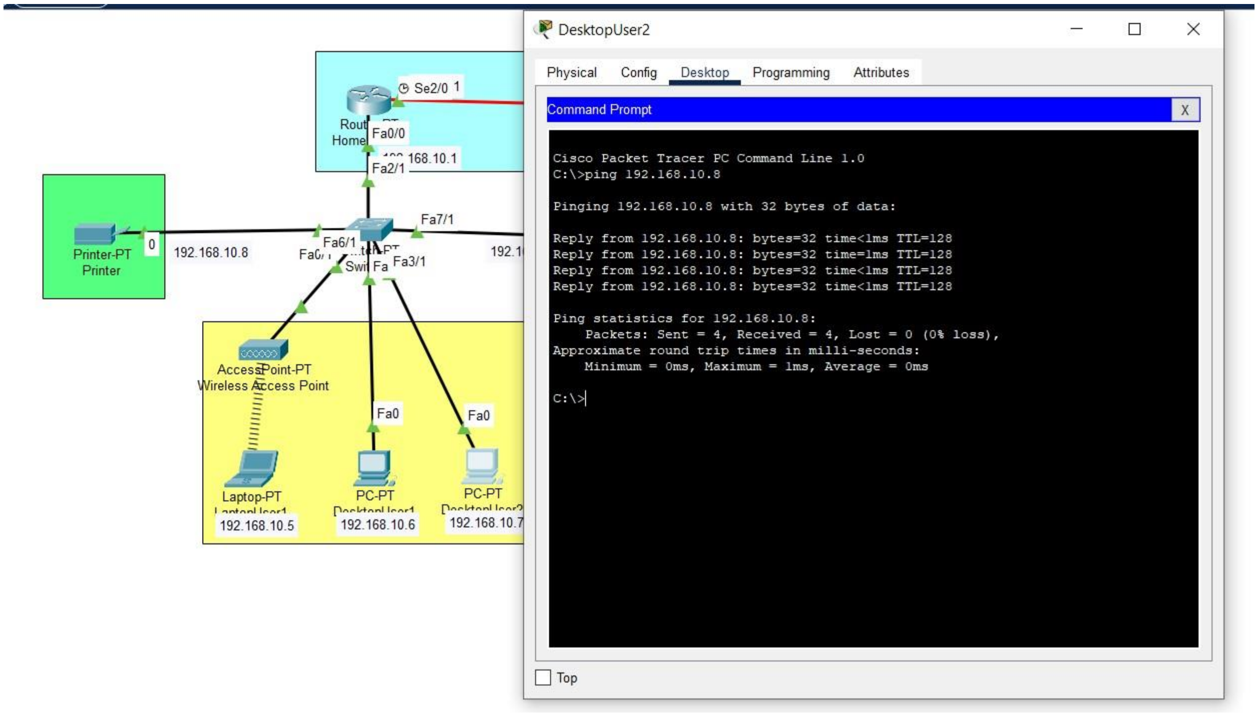
```
Cisco Packet Tracer PC Command Line 1.0
C:\>telnet 10.0.0.1
Trying 10.0.0.1 ...Open


User Access Verification

Password:
Router>en
Password:
Router#show ip interface brief
Interface              IP-Address      OK? Method Status                Protocol
FastEthernet0/0        192.168.10.1    YES manual up                    up
FastEthernet1/0        unassigned      YES unset  up                    down
Serial2/0              10.0.0.1        YES manual up                    up
Serial3/0              unassigned      YES unset  administratively down down
FastEthernet4/0        unassigned      YES unset  administratively down down
FastEthernet5/0        unassigned      YES unset  administratively down down
FastEthernet6/0        unassigned      YES unset  administratively down down
FastEthernet7/0        unassigned      YES unset  administratively down down
Router#exit

[Connection to 10.0.0.1 closed by foreign host]
C:\>
```

Remote Access to Router

6) <u>All the Users Should be Able to use the Printer</u>

A. Select your Wi-Fi network on your wireless-capable printer. Most Wi-Fi printers automatically display a message on their displays when a compatible wireless network is available. Follow the printer’s prompts to confirm that you wish to join the network. Enter your company’s Wi-Fi password when prompted. Consult your printer’s manual for more detailed instructions, as they vary depending on the printer you are using.

B. Click the “Start” button on a computer connected to your Wi-Fi network. Select "Control Panel | Hardware and Sound | Printers | Add a Printer | Add a network, wireless or Bluetooth printer.”
C. Select your Wi-Fi printer, and then click “Next.” Click “Install Driver” if you are prompted to install updated drivers for your printer.
D. Click “Finish.” Your printer is now available to all devices that share your Wi-Fi network.



```
Cisco Packet Tracer PC Command Line 1.0
C:\>ping 192.168.10.8

Pinging 192.168.10.8 with 32 bytes of data:

Reply from 192.168.10.8: bytes=32 time<1ms TTL=128
Reply from 192.168.10.8: bytes=32 time=1ms TTL=128
Reply from 192.168.10.8: bytes=32 time<1ms TTL=128
Reply from 192.168.10.8: bytes=32 time<1ms TTL=128

Ping statistics for 192.168.10.8:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 1ms, Average = 0ms

C:\>
```

Access to Printer

Recommended Products:

- Wireless Access Point:
  NETGEAR Wireless Access Point
  Ubiquiti Networks Wireless Access Point
  Zyxel True WiFi6 Wireless Access Point
  JOOWIN AC1200 High Wireless Access Point

- Network Switches:
  TP-Link TL-SG108 (Unmanaged)
  TP-Link TL-SG105-M2

Ubiquiti Unifi USW-Flex
Zyxel XGS1010-12 (Unmanaged)
TP-Link TL-SG116

- Power Over Ethernet:

  TP-Link AV600 Powerline Ethernet Adapter
  Actiontec by Screenbeam MoCA 2.5 Network Adapter
  Netgear Powerline adapter kit
  ScreenBeam MoCA 2.5 Network Adapter
  Tenda AV1000 1-Port Gigabit Powerline Adapter
  goCoax MoCA 2.5 Adapter
  Motorola MoCA Adapter for Ethernet

- Firewall:

  Bitdefender Box
  CUJO AI Smart Internet Security
  Firewalla.
  FortiGate Next Generation
  SonicWall TZ400
  SonicWall SOHO

- Internet Service Providers:

  Excitel Broadband Plans
  MTNL Broadband Plans
  SITI Cable Broadband Plans
  BSNL Broadband Plans
  ACT Fibernet Broadband Plans

Inferences from the Project

The PC's were connected to each other virtually and logically and was verified with the ping command. Routers are connected to the devices successfully. Laptop connected to the network successfully. Printer connected to the network successfully. The simulation check returns successfully when parsing between two devices.

References

1) http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.857.5409&rep=rep1&type=pdf

2) **https://ieeexplore.ieee.org/abstract/document/5455031**

3) https://www.cisco.com/c/en/us/products/collateral/wireless/nb-06-preparing-for-wifi-6-ebook-cte-en.html

4) https://www.cisco.com/c/en/us/td/docs/solutions/CVD/Campus/cisco-campus-lan-wlan-design-guide.html

5) https://www.cisco.com/c/en_id/products/wireless/technology.html

6) https://link.springer.com/chapter/10.1007/978-3-319-15509-8_23

7) https://pdfs.semanticscholar.org/aae9/6baababdbe75d0ad49bfd8738016cbac20c3.pdf

8) https://www.proquest.com/docview/220959194?pq-origsite=gscholar&fromopenview=true