CSE 3501

INFORMATION SECURITY ANALYSIS & AUDIT

Theory DA – 1

F2 | SJT403

FALL SEMESTER 2021-22

by

SHARADINDU ADHIKARI

19BCE2105

  sharadindu.adhikari2019@vitstudent.ac.in

Question-1:

Access security risks, threats and vulnerabilities to an organisation of your choice and design appropriate information security protection mechanisms by analysing requirements, plans and IT security policies. Write a report which can evaluate the risk levels and the potential impact of threats and vulnerabilities on a hypothetical organisation.

Solution:

For the hypothetical organisation, I'm going to go ahead with an University setting. First, let's focus on different parameters:

Risks

1. Spam
2. pharming
3. Phishing
4. Ransomware
5. Computer worm
6. Insider threat
7. Data leakage
8. Hacking
9. Lack of coherent strategies
10. Regulatory compliance

Threats

1. Malware
2. Spear phishing
3. "Man in the Middle" Attack (MitM)
4. Denial of Service Attack
5. Attacks on IOT devices

Vulnerabilities

1. SQL Injections:
   a. prepared statements
   b. stored procedures
   c. Input validation
2. Phishing
   a. Email filters
   b. Training & Awareness Campaigns

  sharadindu.adhikari2019@vitstudent.ac.in

Risk levels and the potential impact of threats & vulnerabilities:

The first step in a risk management program is a threat assessment. A threat assessment considers the full spectrum of threats (i.e., natural, criminal, terrorist, accidental, etc.) for a given facility / location.

Specific definitions are important to quantify the level of each threat. The more specific the definition, the more consistent the assessments will be, especially if the assessments are being performed by a large number of accessors. Example:

- **Defined:** Man-made: There are aggressors who utilize this tactic, who are known to target this type of facility. There is a history of this type of activity in the area & this facility is a known target. Specific threats have been received or identified by law enforcement agencies.

  Natural: Events of this nature occur in the immediate vicinity periodically (i.e., once every 10 years).

- **Credible:** Man-made: There's a common history: no specific threat has been received or identified by law enforcement agencies.

  Natural: Events of this nature occur in immediate vicinity periodically (i.e. once every few decades or so)

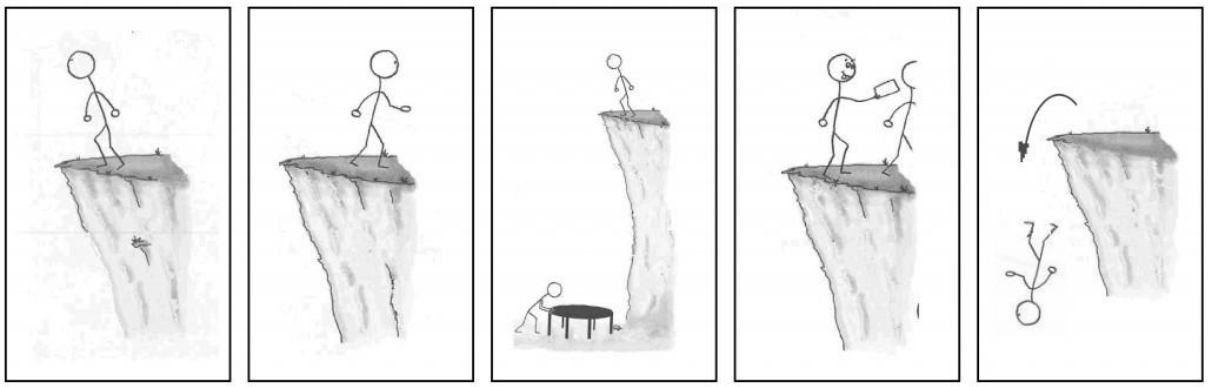
- **Potential**: Man-made: Throughout history this facility has not been a target.

  Natural: Events of this nature occur in the region on a sporadic basis.

- **Minimal**: Man-made: No aggrenors who utilise this tactic are identified for this facility and there is no history of this type of activity in the area, but this facility has not been a target.

  Natural: There is no history of this type of event in the area.

Having said all these, not all risks are negative though. Some events (like finding an easier way to do an activity) or conditions (like lower prices for certain materials) can help. When this happens, we call it an opportunity; but it's still handled just like a risk.



Your project | Avoid | Mitigate | Transfer | Accept

  sharadindu.adhikari2019@vitstudent.ac.in

When we're planning, risks are still uncertain: they haven't happened yet. But eventually some of the risks I've planned for do happen, and that's when we've to deal with them.

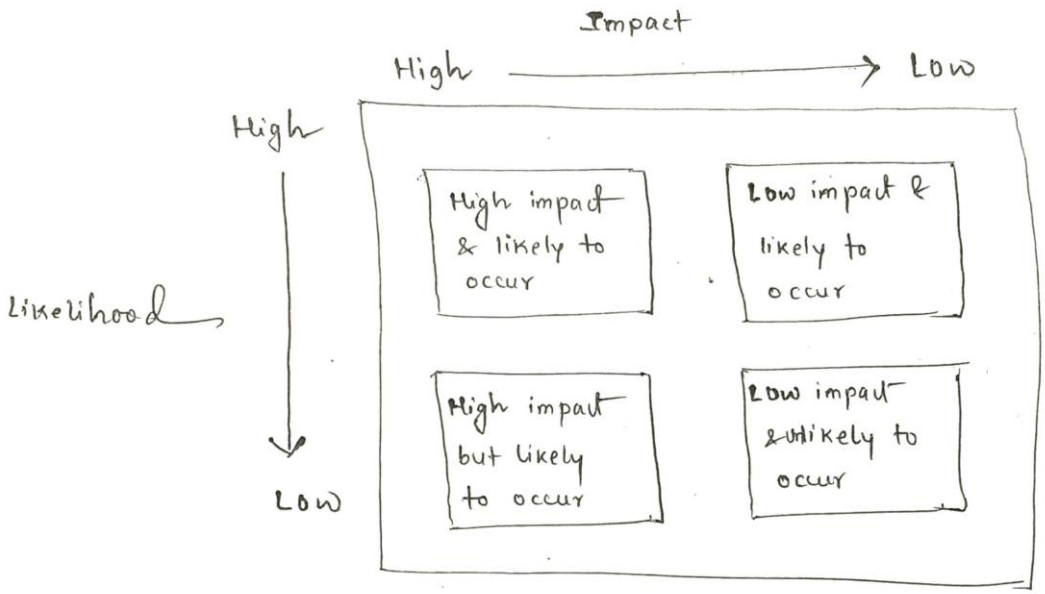
There are 4 basic ways to handle a risk:

- Avoid: The best thing we can do with a risk is avoid it. If we can prevent it from happening, it'll be great. The easiest way is to walk away from the cliff, ~~ma~~ but may not always be an option.
- Mitigate: If we can't avoid, we have to mitigate it. This means taking some sort of action that will cause it to do as little damage to the project as possible.
- Transfer: One effective way to deal with a risk is to pay someone else to accept it for us. The most common way to do this is to buy insurance.
- Accept: When we can't avoid, mitigate, or transfer a risk, then we've to accept it. But even when we accept a risk, at least we would have looked at the alternatives & we'd know what will happen if it works. If we can't avoid the risk, and there's nothing we can do to reduce its impact, then accepting it is the only choice.

- Risk management Process (Identification).

  - Technical
  - Cost
  - Schedule

- Client
- Contractual
- Weather
- Financial
- Political
- Environmental
- People



Once the plausible threats are identified, a vulnerability assessment must be performed. The vulnerability assessment considers the potential impact of loss from a successful attack, as well as the vulnerability of the facility / location to an attack. Impact of loss is the degree to which the mission of the legacy / agency is impaired by a successful attack from the given threat. A key component of the vulnerability assessment is properly defining the ratings for impact of loss & vulnerability. These definitions may vary greatly from facility to facility. For example, the amount of time that mission capability is impaired is an important part of impact of loss. If the facility being assessed

is an Air Traffic Control Tower, a downtime of a few minutes may become a serious impact of loss, while for a social security office, a downtime of a few minutes would be minor.

A sample set of definitions of impact of loss is described below. These definitions are for an organization that generates revenue by serving the public :-

- Devastating: The facility is damaged/contaminated beyond habital use. Most items/assets are lost, destroyed, or damaged beyond repair/restoration. The number of visitors to other facilities in the organization may be reduced by upto 75% for a limited period of time.

- Severe: The facility is partially damaged/contaminated. Examples include partial structure breach resulting in weather/water, smoke, impact, or fire damage to some areas. Some items/assets in the facility are damaged beyond repair, but the facility remains mostly intact. The entire facility may be closed for a period of upto 2 weeks and a portion of the facility may be closed for an extended period of time (more than 1 month). Some assets may need to be moved to remote locations to protect them from environmental damage. The number of visitors to this and other facilities in the organization may be reduced by upto 50% for a limited period of time.

  sharadindu.adhikari2019@vitstudent.ac.in

- **Noticeable:** The facility is temporarily closed or unable to operate, but can continue without an interruption of more than one day. A limited number of assets may be damaged, but the majority of the facility is not affected. The number of visitors to this and other facilities in the organization may be reduced by upto 25% for a limited period of time.

- **Minor:** The facility experiences no significant impact on operations (downtime is less than 4 hours) and there is no loss of major assets.

Vulnerability is defined to be a combination of the attractiveness of a facility as a target and the level of deterrence and/or defense provided by the existing countermeasures. Target attractiveness is a measure of the asset or facility in the eyes of an aggressor and is influenced by the function and/or symbolic importance of the facility. (Sample) definitions for vulnerability ratings are as follows :-

- **Very High:** This is a high profile facility that provides a very attractive target for potential adversaries, and the level of deterrence and/or defense provided by the existing countermeasures is inadequate.

  sharadindu.adhikari2019@vitstudent.ac.in

- **High**: This is a very high profile regional facility or a moderate national facility that provides an attractive target and/or the level of detterence and/or defense provided by the existing countermeasures is inadequate.

- **Moderate**: This is a moderate profile facility (not well known outside the local area or region) that provides a potential target and/or the level of deterrence and/or defense provided by the existing countermeasures is marginally adequate.

- **Low**: This is not a high profile facility and provides a possible target and/or the level of deterrence and/or defense provided by the existing countermeasures is adequate.

The vulnerability assessment may also include detailed analysis of the potential impact of loss from an explosive, chemical or biological attack. Professionals with specific training and experience in these areas are required to perform these detailed analyses.

Question 2:

Do a study on Network Connecting Devices.

a) Passive Hubs
b) Repeaters
c) Active Hubs
d) Bridges
e) Transparent Bridges
f) Switches
g) Routers
h) Gateway

Implement a Network with connecting devices (at least any two) in Cisco Packet Tracer.

Solution:

Solution:

a) Passive Hubs: Passive Hubs connects nodes in a star configuration by collecting wiring from nodes. They broadcast signals onto the network without amplifying or regenerating them. As they cannot extend the distance between nodes, they limit the size of the lan.

b) Repeaters; Repeaters are electronic devices that receives a signal and retransmits it. They are used to extend transmissions so that the signal can cover longer distances or be received on the other side of an obstruction. Some types of repeaters broadcast an identical signal, but alter its method of transmission, for example, on another frequency or baud rate.

c) **Active Hubs:** Active Hubs amplify and regenerate the incoming electrical signals before broadcasting them. They have their own power supply and serves both as a repeater as well as connecting centre. Due to their regenerating capabilities, they can extend the maximum distance between nodes, thus increasing the size of LAN.

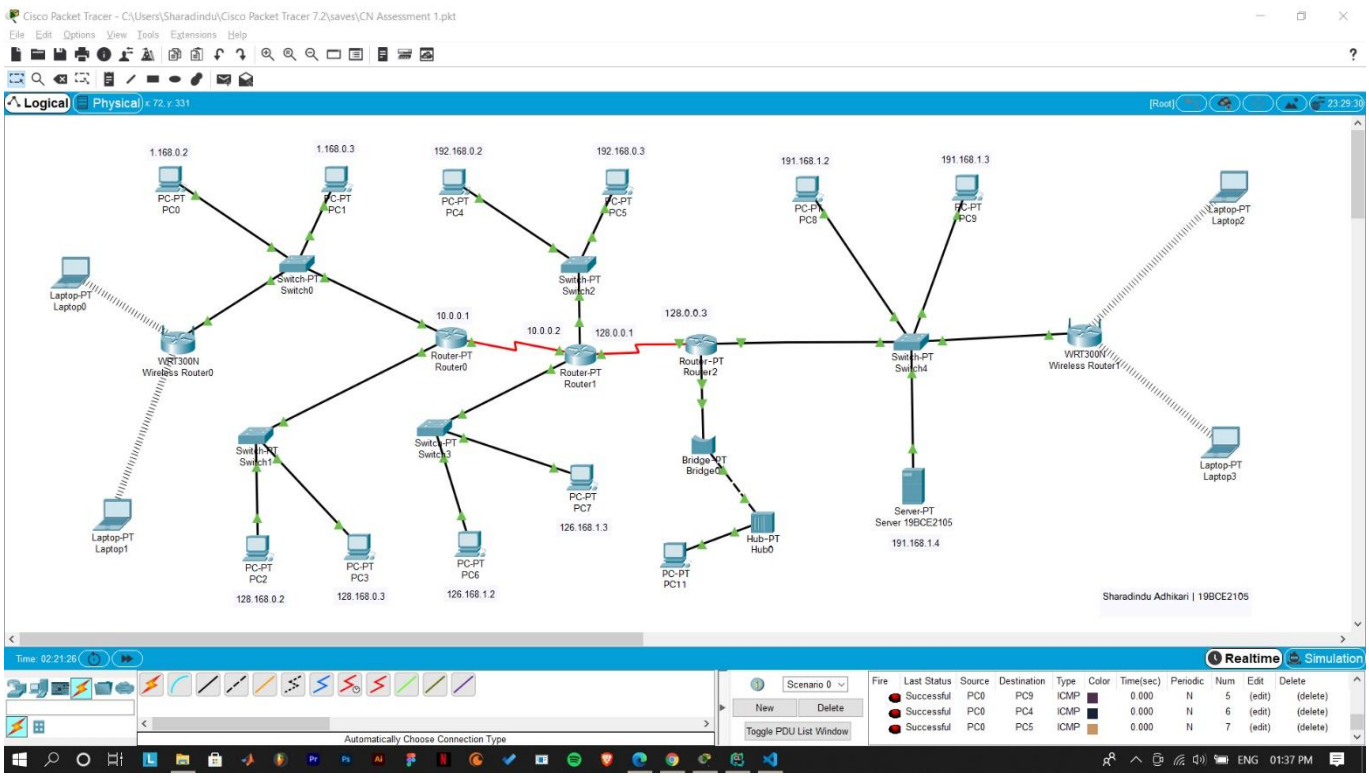
d) **Bridges:** Network bridges are computer networking devices that creates a single, aggregate network from multiple communication networks or network segments (e.g. LANs). The process of aggregating networks is called network bridging. Bridges operate at the data link layer of the OSI model and hence also referred to as Layer 2 switches.

e) **Transparent Bridges:** Transparent bridges are common type of bridges that observe incoming network traffic to identify media access control (MAC) addresses. These bridges operate in a way that is transparent to all the network's connected hosts. It records MAC addresses in a table that is much like a routing table and evaluates that information whenever a packet is routed toward its location. It may also combine several different bridges to better inspect incoming traffic. These bridges are implemented primarily in Ethernet networks.

f) Switches: Network switches are networking hardwares that connects devices on a computer network by using packet switching to receive & forward data to the destination device. It is a multiport network bridge that uses MAC addresses to forward data at the data link layer of the OSI model.

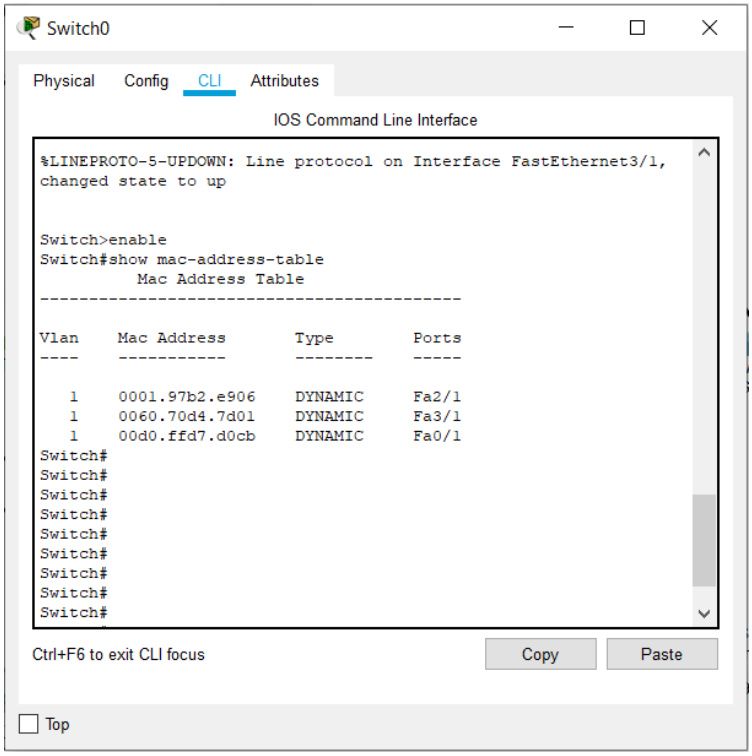
g) Routers: Routers are networking devices that forward data packets between computer networks. They perform the traffic directing functions on the internet. It is connected to two or more data lines from different IP networks. Routers can combine the functions of different components, like hubs, modems, switches, & connect with these devices as well.

h) Gateways: Gateways are network nodes used in telecommunications that connects two networks with different transmission protocols together. They serve as an entry and exit point for a network as all data must pass through or communicate with the gateway prior to being routed.



Since for all routers, switches, PCs, Hubs, servers and bridges, the input IPs and processes are similar, snaps of one from each category are enclosed:

(a) MAC address table (for Switch 0)



(b) Ping command (for PC 0)

PC0

Physical Config Desktop Programming Attributes

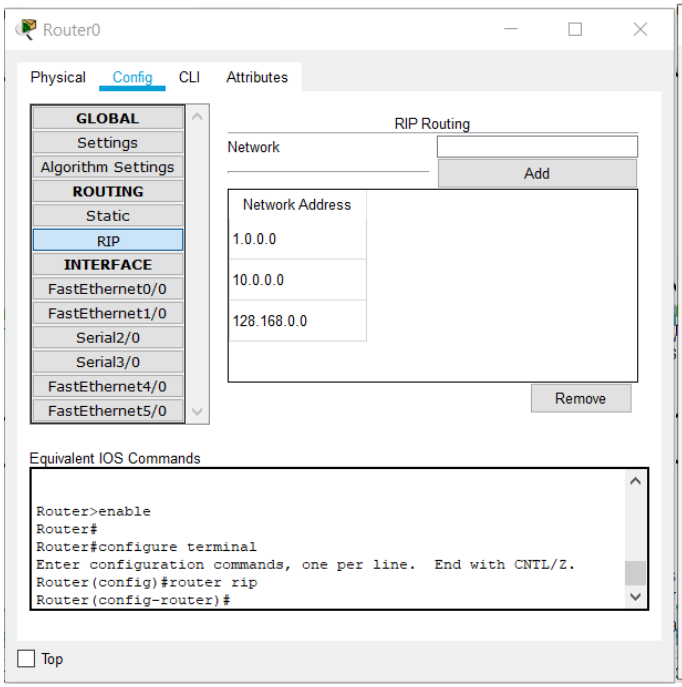
Command Prompt

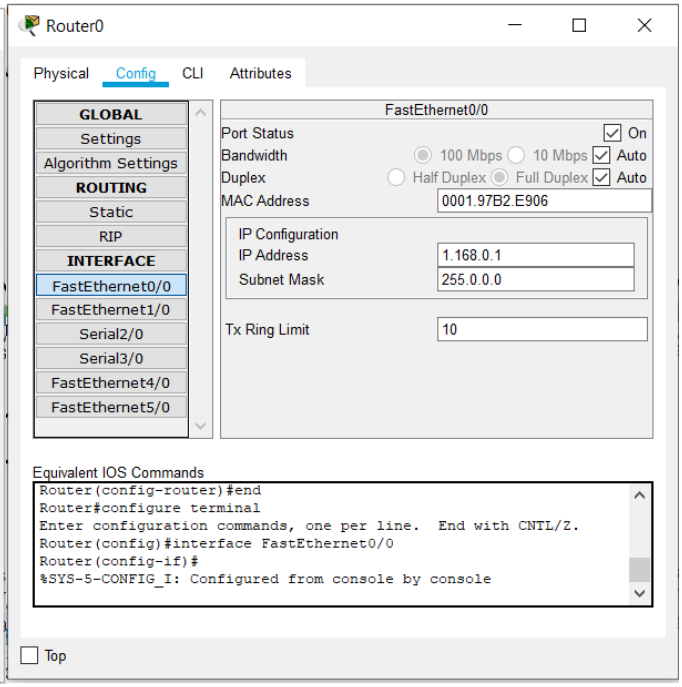
```
Packet Tracer PC Command Line 1.0
C:\>ping 128.168.0.2

Pinging 128.168.0.2 with 32 bytes of data:

Request timed out.
Reply from 128.168.0.2: bytes=32 time<1ms TTL=127
Reply from 128.168.0.2: bytes=32 time<1ms TTL=127
Reply from 128.168.0.2: bytes=32 time=1ms TTL=127

Ping statistics for 128.168.0.2:
    Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 1ms, Average = 0ms

C:\>ping 128.168.0.3

Pinging 128.168.0.3 with 32 bytes of data:

Request timed out.
Reply from 128.168.0.3: bytes=32 time=1ms TTL=127
Reply from 128.168.0.3: bytes=32 time<1ms TTL=127
Reply from 128.168.0.3: bytes=32 time<1ms TTL=127

Ping statistics for 128.168.0.3:
    Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 1ms, Average = 0ms

C:\>ping 192.168.0.2

Pinging 192.168.0.2 with 32 bytes of data:

Request timed out.
Reply from 192.168.0.2: bytes=32 time=5ms TTL=126
Reply from 192.168.0.2: bytes=32 time=1ms TTL=126
Reply from 192.168.0.2: bytes=32 time=1ms TTL=126

Ping statistics for 192.168.0.2:
    Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
Approximate round trip times in milli-seconds:
    Minimum = 1ms, Maximum = 5ms, Average = 2ms

C:\>ping 192.168.0.3

Pinging 192.168.0.3 with 32 bytes of data:

Request timed out.
Reply from 192.168.0.3: bytes=32 time=2ms TTL=126
Reply from 192.168.0.3: bytes=32 time=1ms TTL=126
Reply from 192.168.0.3: bytes=32 time=1ms TTL=126

Ping statistics for 192.168.0.3:
    Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
Approximate round trip times in milli-seconds:
    Minimum = 1ms, Maximum = 2ms, Average = 1ms

C:\>ping 126.168.1.2

Pinging 126.168.1.2 with 32 bytes of data:

Request timed out.
Reply from 126.168.1.2: bytes=32 time=2ms TTL=126
Reply from 126.168.1.2: bytes=32 time=1ms TTL=126
Reply from 126.168.1.2: bytes=32 time=1ms TTL=126

Ping statistics for 126.168.1.2:
    Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
Approximate round trip times in milli-seconds:
    Minimum = 1ms, Maximum = 2ms, Average = 1ms

C:\>ping 126.168.1.3

Pinging 126.168.1.3 with 32 bytes of data:

Request timed out.
Reply from 126.168.1.3: bytes=32 time=2ms TTL=126
Reply from 126.168.1.3: bytes=32 time=1ms TTL=126
Reply from 126.168.1.3: bytes=32 time=1ms TTL=126

Ping statistics for 126.168.1.3:
    Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
Approximate round trip times in milli-seconds:
    Minimum = 1ms, Maximum = 2ms, Average = 1ms

C:\>ping 191.168.1.2

Pinging 191.168.1.2 with 32 bytes of data:

Request timed out.
Reply from 191.168.1.2: bytes=32 time=4ms TTL=125
Reply from 191.168.1.2: bytes=32 time=15ms TTL=125
Reply from 191.168.1.2: bytes=32 time=3ms TTL=125

Ping statistics for 191.168.1.2:
    Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
Approximate round trip times in milli-seconds:
    Minimum = 3ms, Maximum = 15ms, Average = 7ms

C:\>ping 191.168.1.3

Pinging 191.168.1.3 with 32 bytes of data:

Request timed out.
Reply from 191.168.1.3: bytes=32 time=3ms TTL=125
Reply from 191.168.1.3: bytes=32 time=5ms TTL=125
Reply from 191.168.1.3: bytes=32 time=2ms TTL=125

Ping statistics for 191.168.1.3:
    Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
Approximate round trip times in milli-seconds:
    Minimum = 2ms, Maximum = 5ms, Average = 3ms

C:\>
```

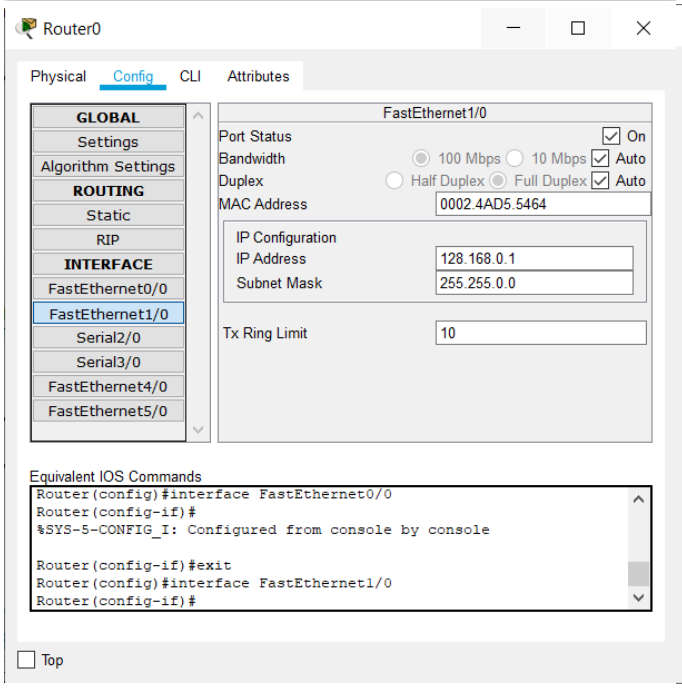
Top

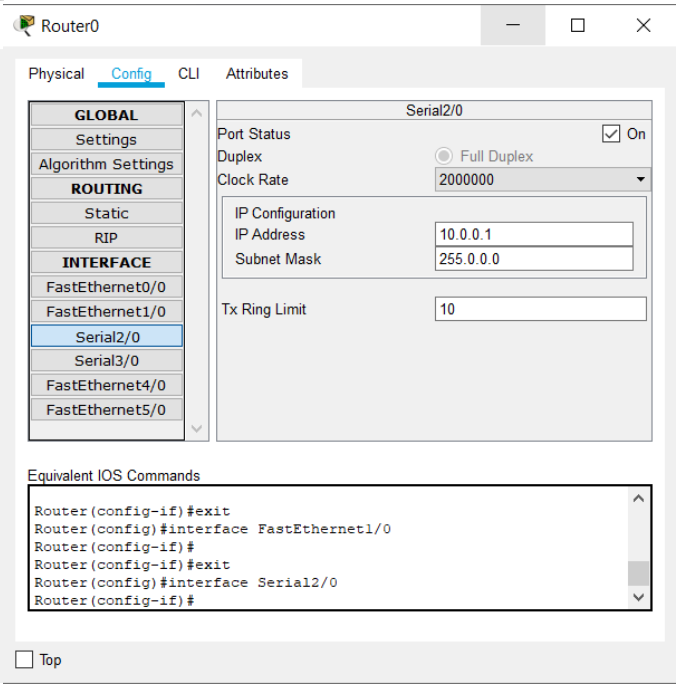
ENG 01:41 PM

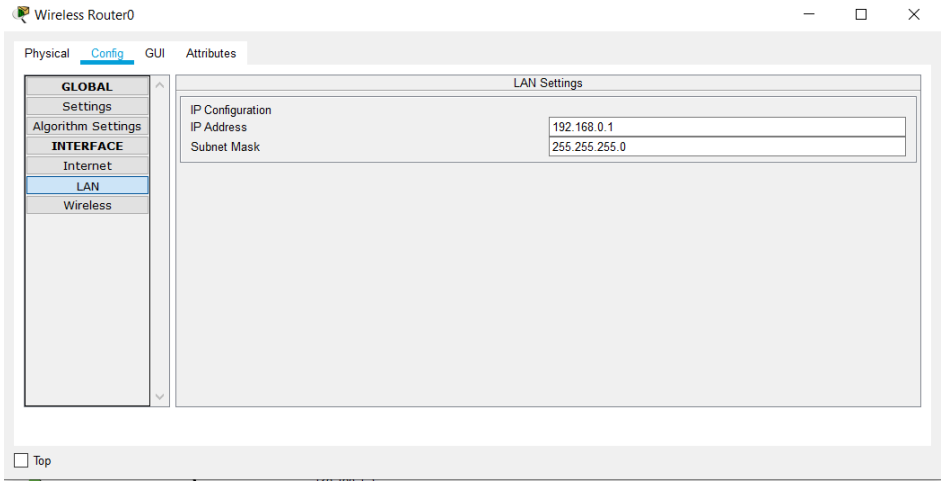
(c) IP config command (for Router 0 and Wireless Router 0)

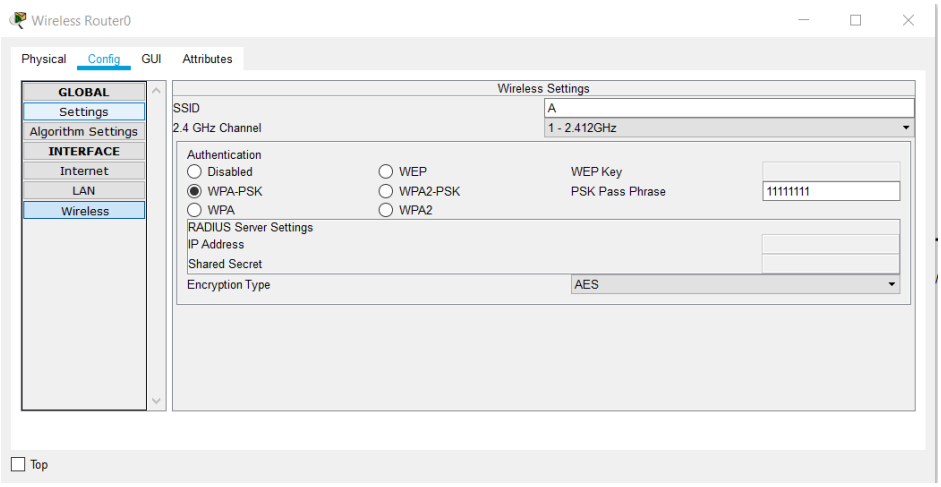












(d) **Simple PDUs** (from PC 0 through other PCs)