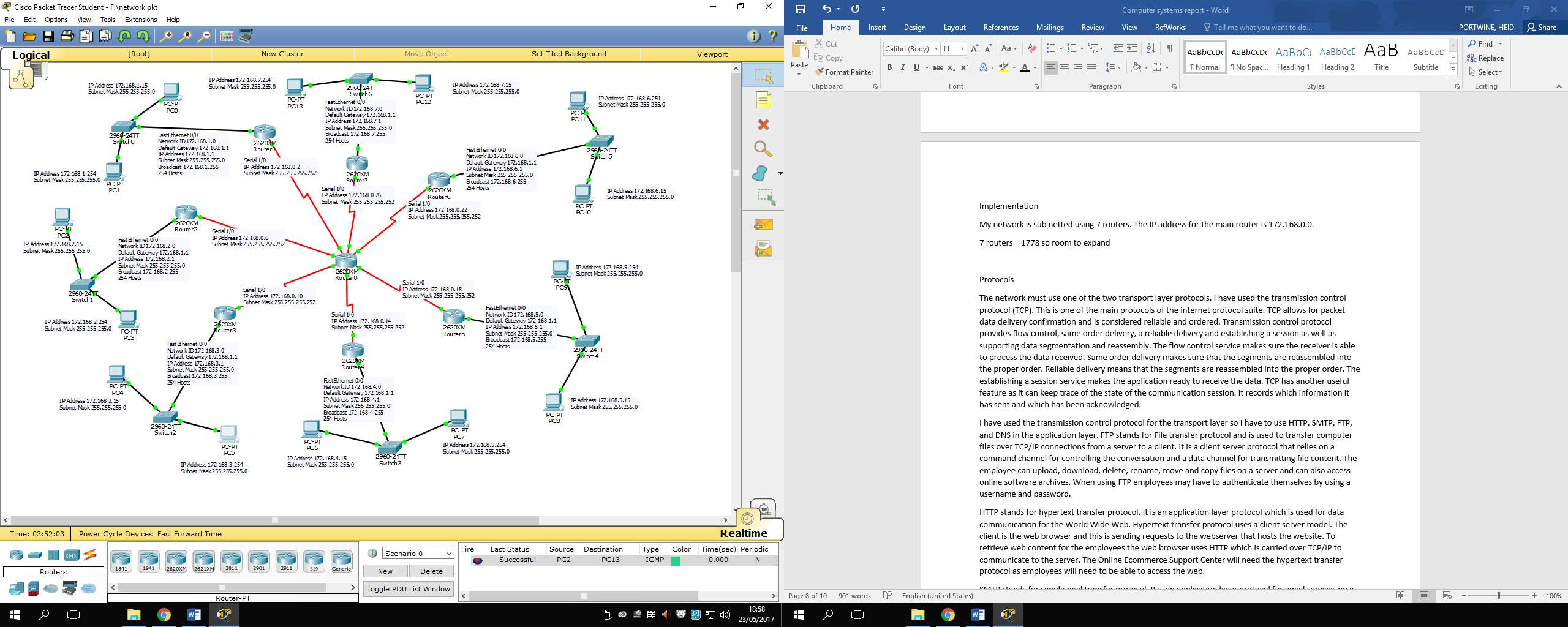
**Computer Systems Report**

This report will cover my design and implementation of a new network for the Online Ecommerce Support Center. I will include a diagram of my network, an addressing table for my IP addresses, my ping test results, the technologies I have used, the protocols I have used and the security, ethical and legal issues surrounding the network and the company.

**Annotated diagram of my network**



Above is an image of my network that I created on Cisco Packet Tracer. I have included labels for each of the connections, which describe the IP address, subnet mask, network ID, default gateway, broadcast and the number of hosts. I have laid it out like this, as it is easier to see which PC is connected to which switch. To connect the routers to each other I used the serial DCE cable and for the rest I used copper straight through.

**Addressing table**

**Router to switch**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Subnet ID | First Useable IP | Last Useable IP | Broadcast Address | Subnet Mask |
| 172.168.1.0 | 172.168.1.1 | 172.168.1.254 | 172.168.1.255 | 255.255.255.0 |
| 172.168.2.0 | 172.168.2.1 | 172.168.2.254 | 172.168.2.255 | 255.255.255.0 |
| 172.168.3.0 | 172.168.3.1 | 172.168.3.254 | 172.168.3.255 | 255.255.255.0 |
| 172.168.4.0 | 172.168.4.1 | 172.168.4.254 | 172.168.4.255 | 255.255.255.0 |
| 172.168.5.0 | 172.168.5.1 | 172.168.5.254 | 172.168.5.255 | 255.255.255.0 |
| 172.168.6.0 | 172.168.6.1 | 172.168.6.254 | 172.168.6.255 | 255.255.255.0 |
| 172.168.7.0 | 172.168.7.1 | 172.168.7.254 | 172.168.7.255 | 255.255.255.0 |

**Router to router**

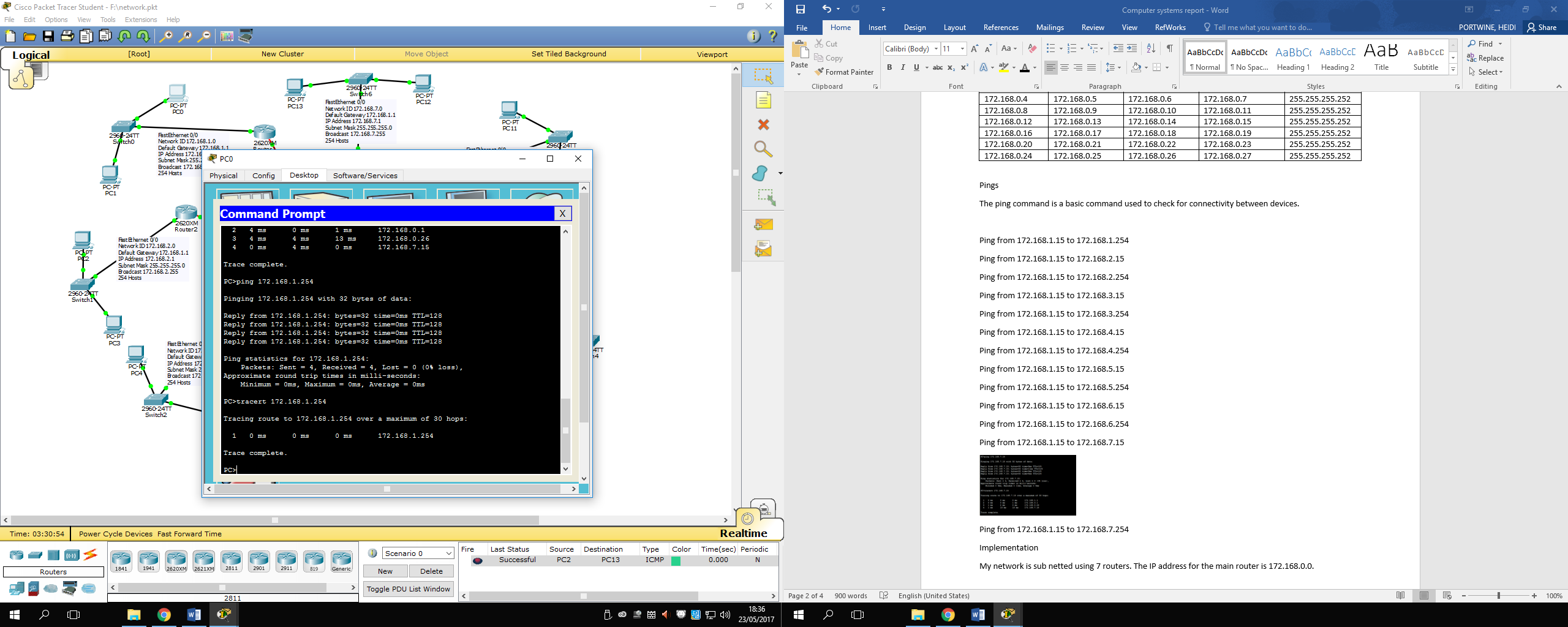
|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Subnet ID | First Useable IP | Last Useable IP | Broadcast Address | Subnet Mask |
| 172.168.0.0 | 172.168.0.1 | 172.168.0.2 | 172.168.0.3 | 255.255.255.252 |
| 172.168.0.4 | 172.168.0.5 | 172.168.0.6 | 172.168.0.7 | 255.255.255.252 |
| 172.168.0.8 | 172.168.0.9 | 172.168.0.10 | 172.168.0.11 | 255.255.255.252 |
| 172.168.0.12 | 172.168.0.13 | 172.168.0.14 | 172.168.0.15 | 255.255.255.252 |
| 172.168.0.16 | 172.168.0.17 | 172.168.0.18 | 172.168.0.19 | 255.255.255.252 |
| 172.168.0.20 | 172.168.0.21 | 172.168.0.22 | 172.168.0.23 | 255.255.255.252 |
| 172.168.0.24 | 172.168.0.25 | 172.168.0.26 | 172.168.0.27 | 255.255.255.252 |

These tables are my addressing tables for my router-to-switch connections and my router-to-router connections. As you can see, they include a subnet ID, first useable IP, Last useable IP, broadcast address and a subnet mask.

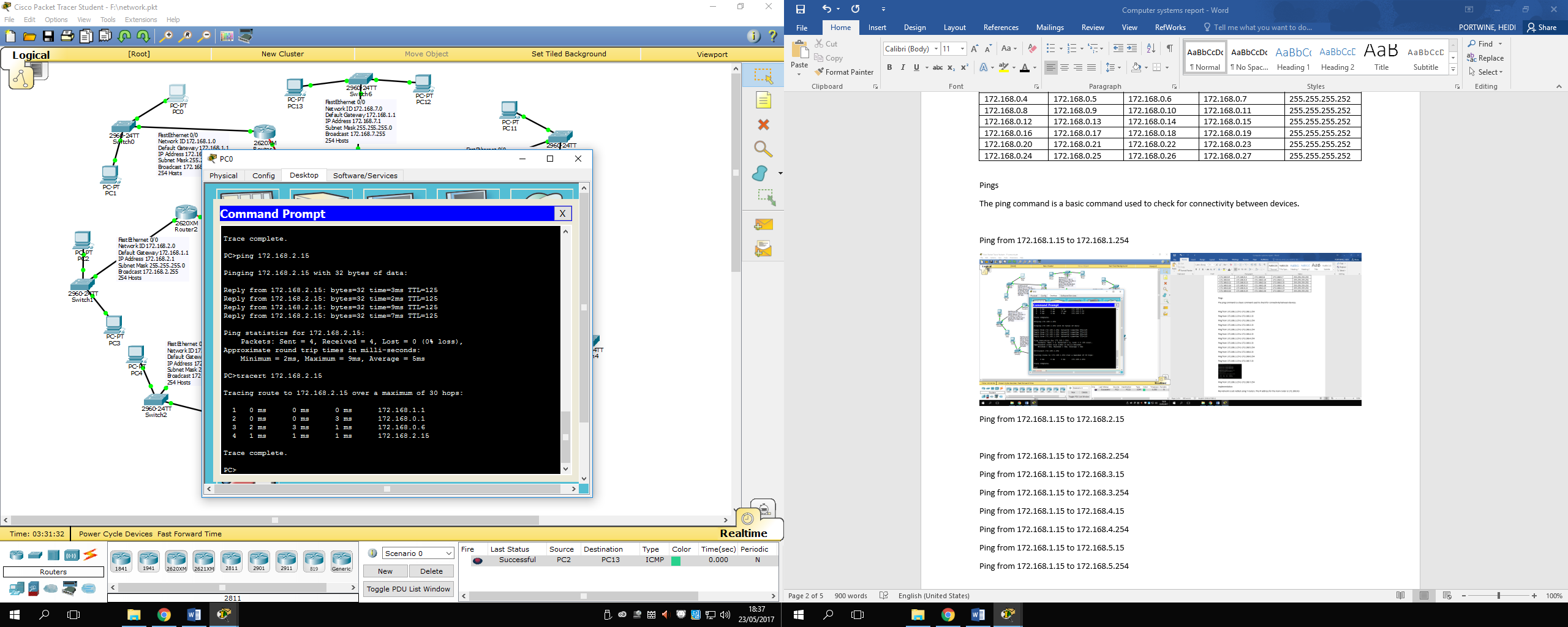
**Ping Tests**

The ping command is a basic command used to check for connectivity between devices. For each of these screen shots I have used the command prompt to ping from PC0 to each PC to show that my network is fully connected. I have also used the trace route command to show the route it took.

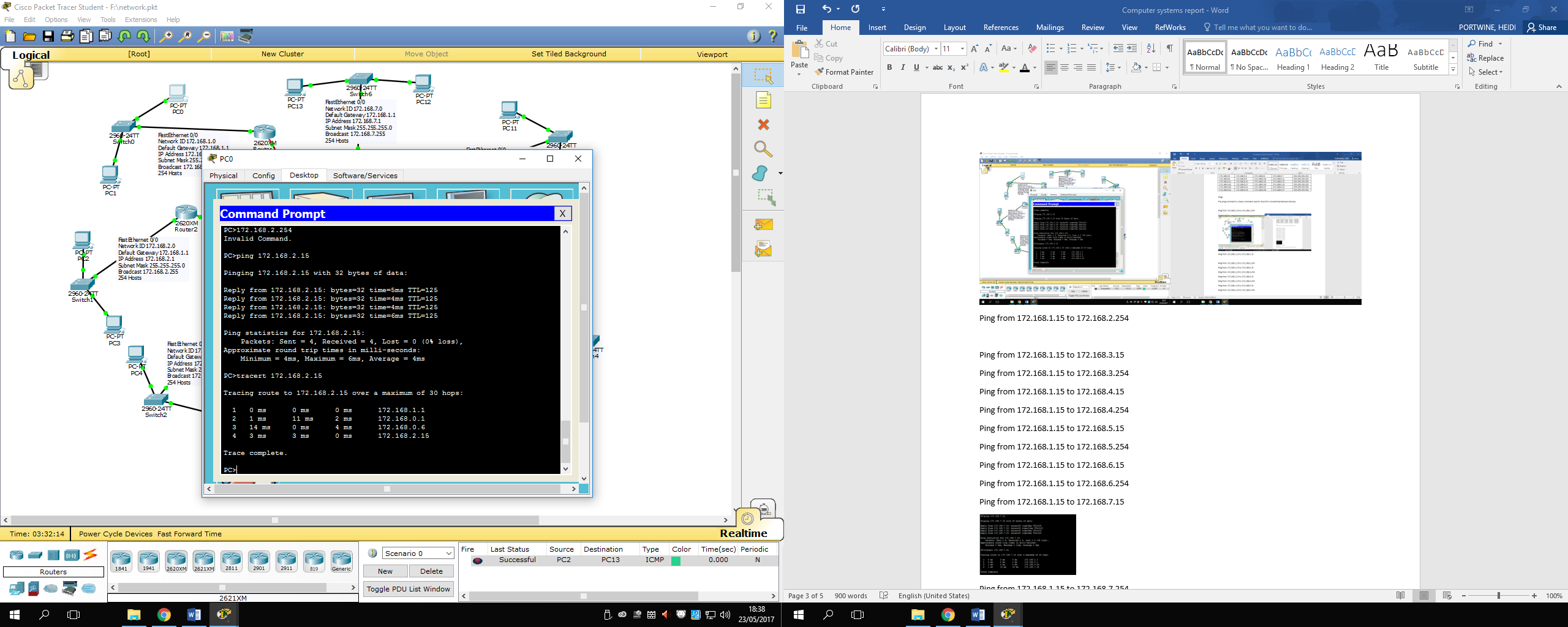
**Ping from 172.168.1.15 to 172.168.1.254**



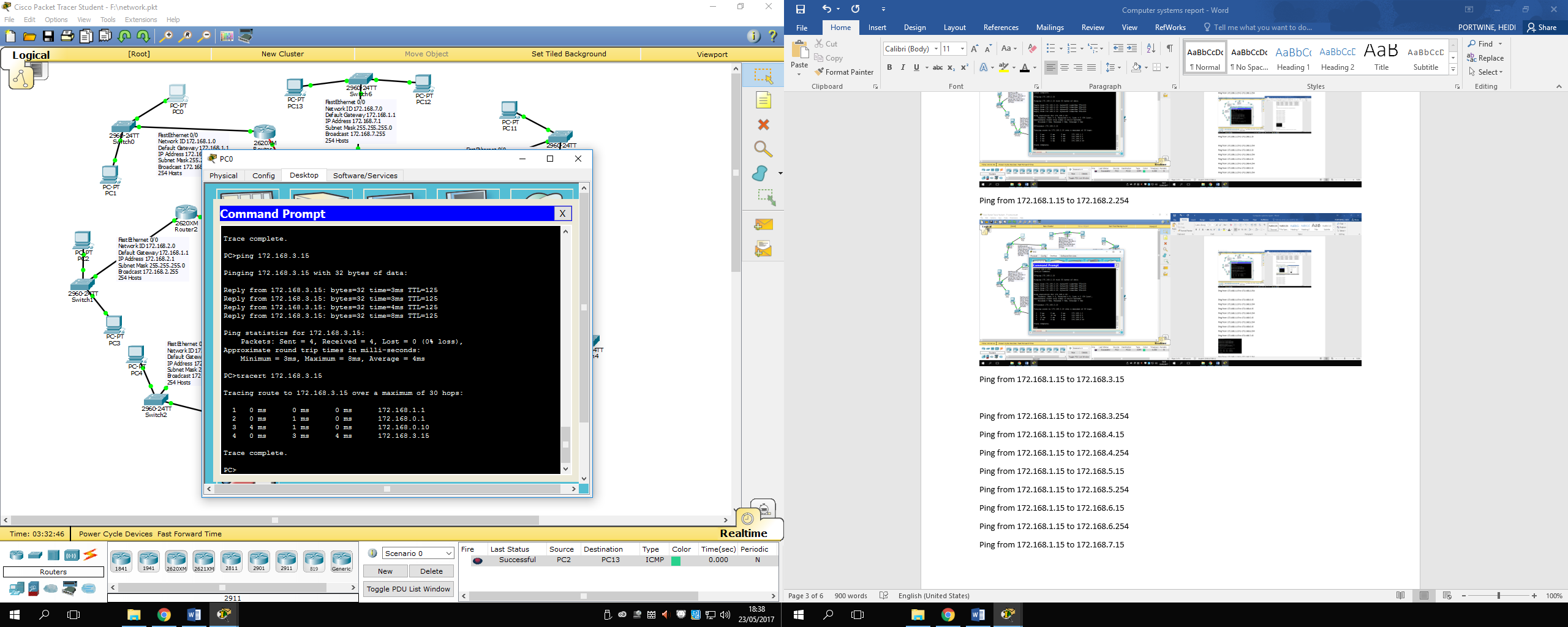
**Ping from 172.168.1.15 to 172.168.2.15**



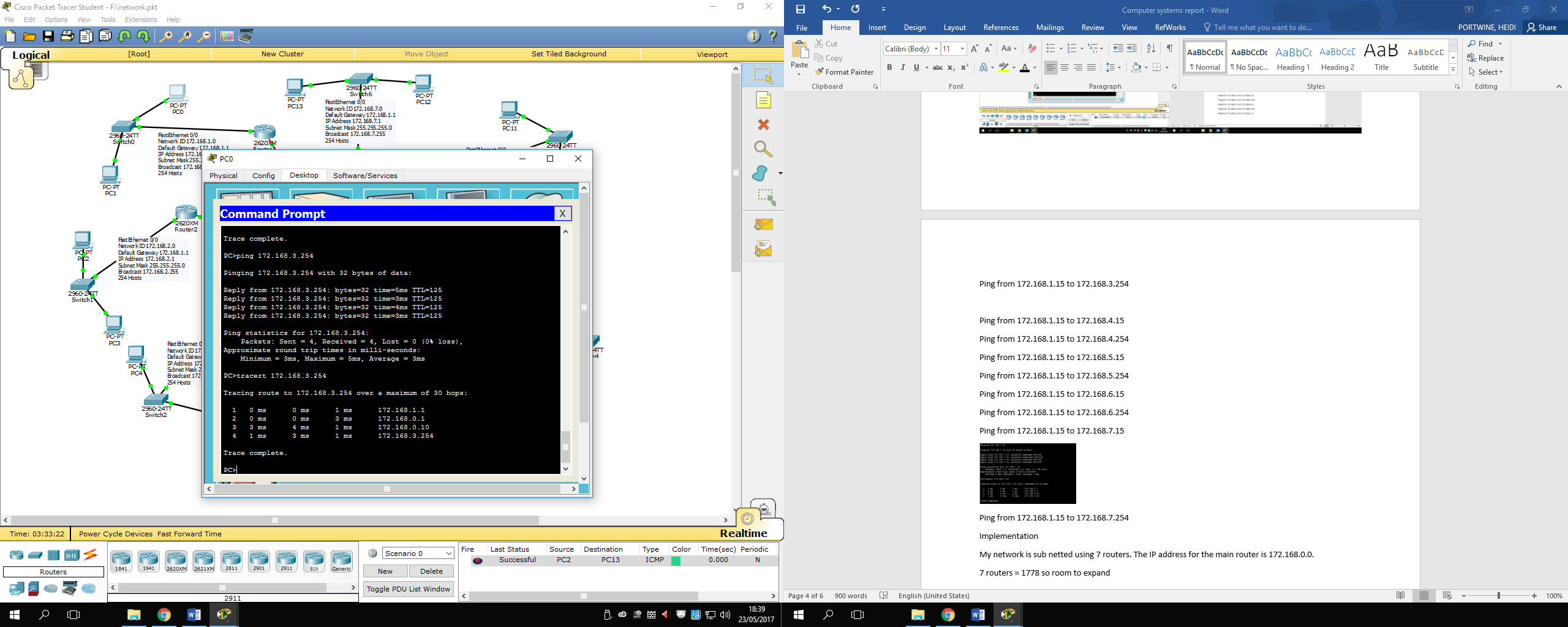
**Ping from 172.168.1.15 to 172.168.2.254**



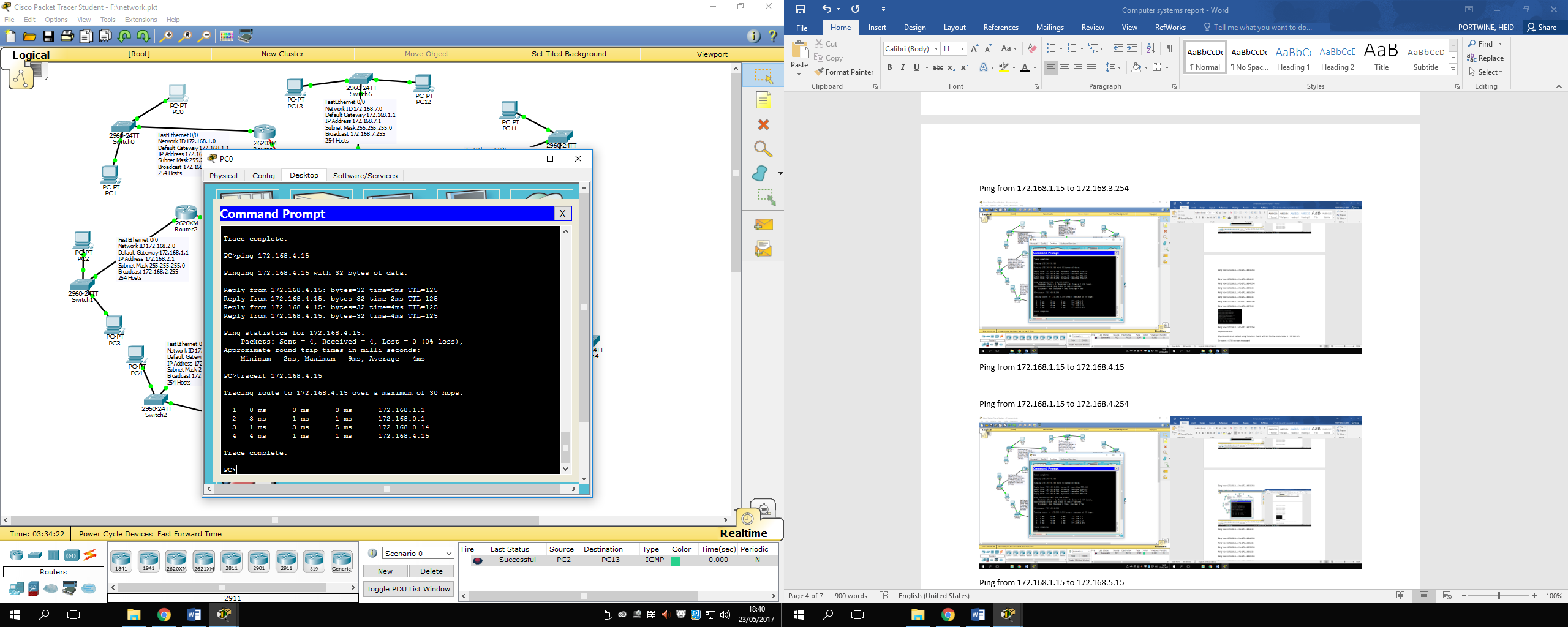
**Ping from 172.168.1.15 to 172.168.3.15**



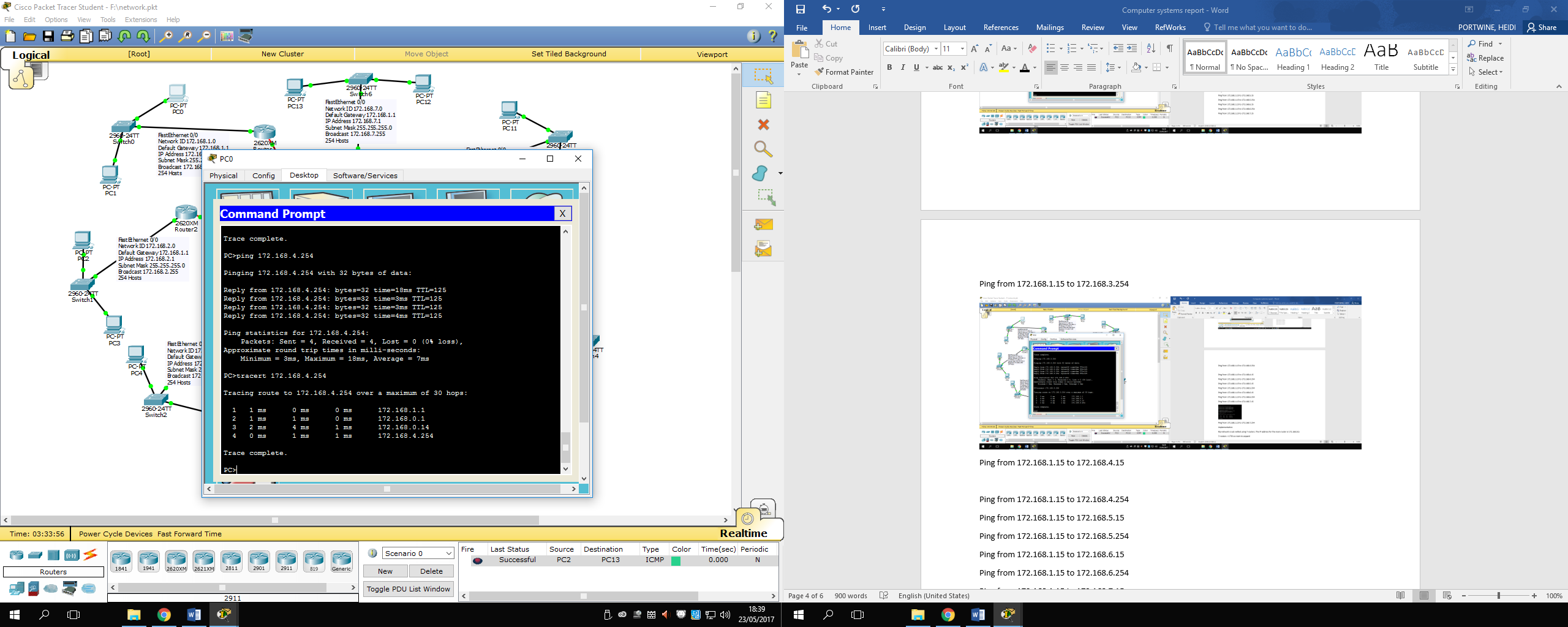
**Ping from 172.168.1.15 to 172.168.3.254**



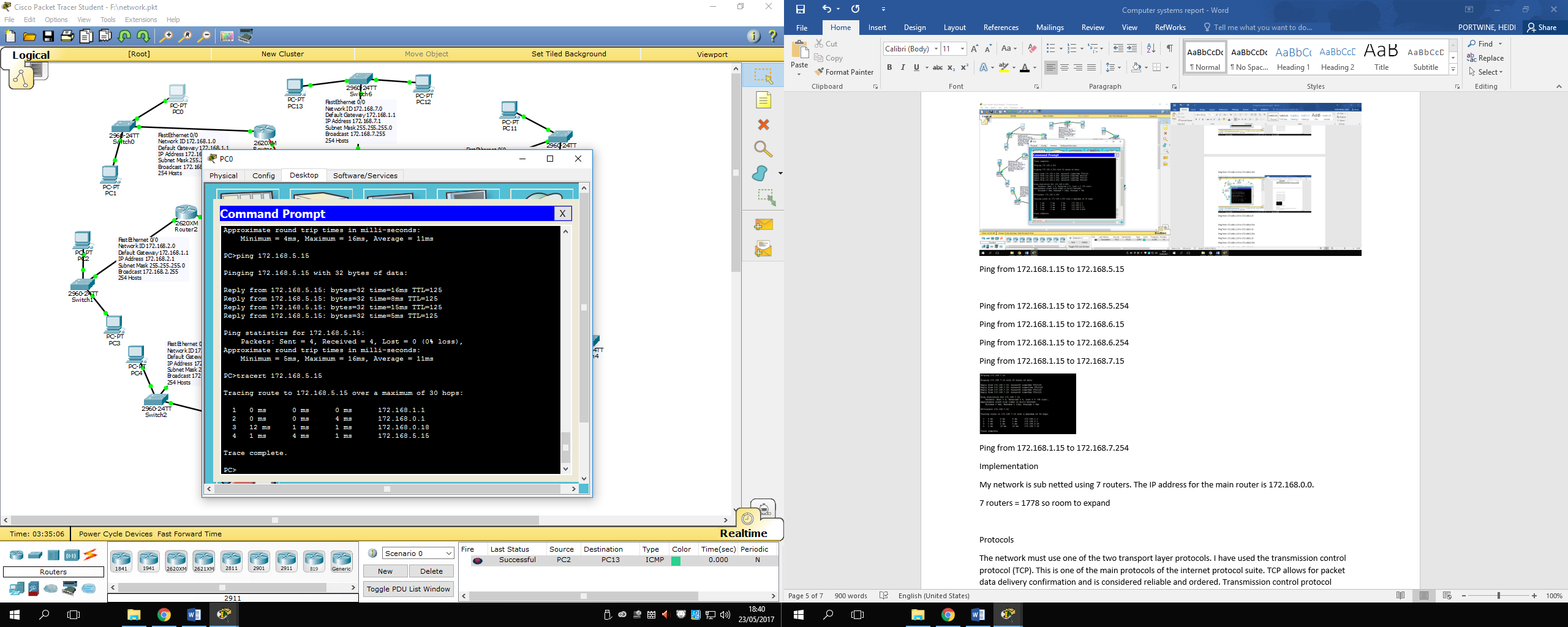
**Ping from 172.168.1.15 to 172.168.4.15**



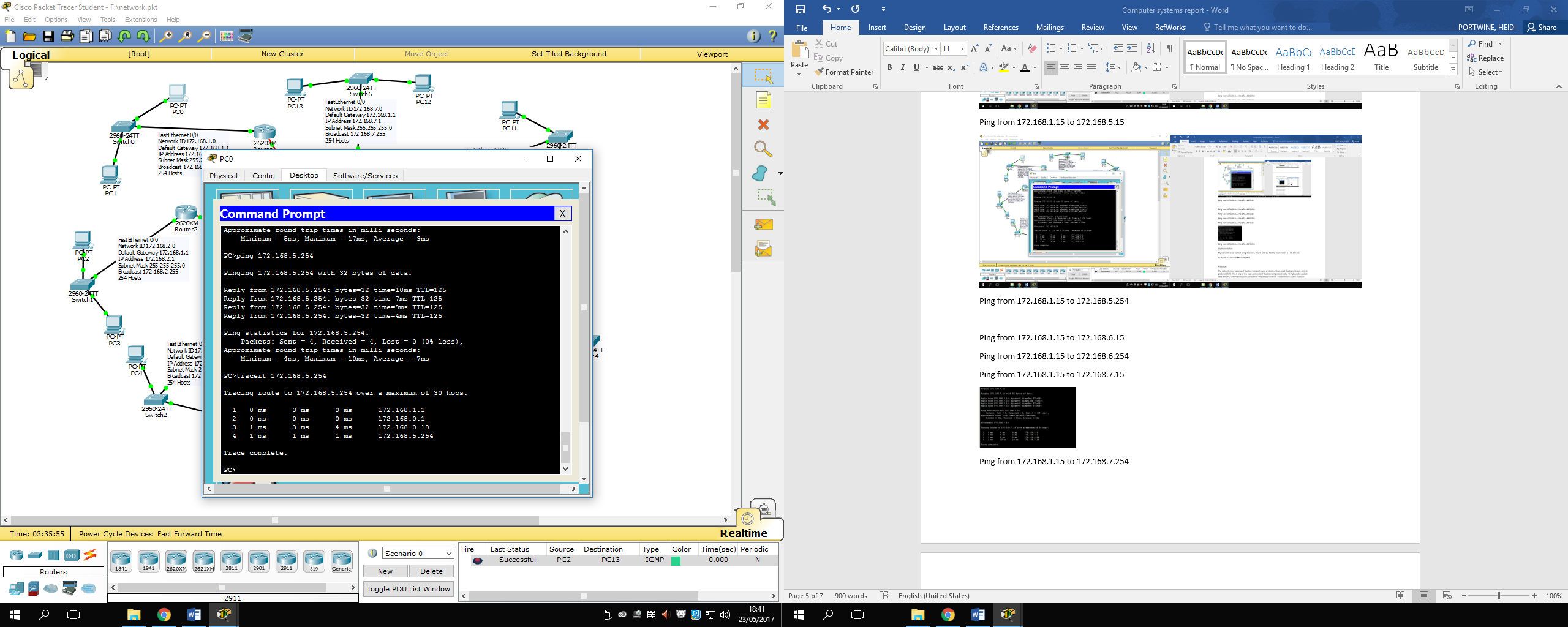
**Ping from 172.168.1.15 to 172.168.4.254**

****

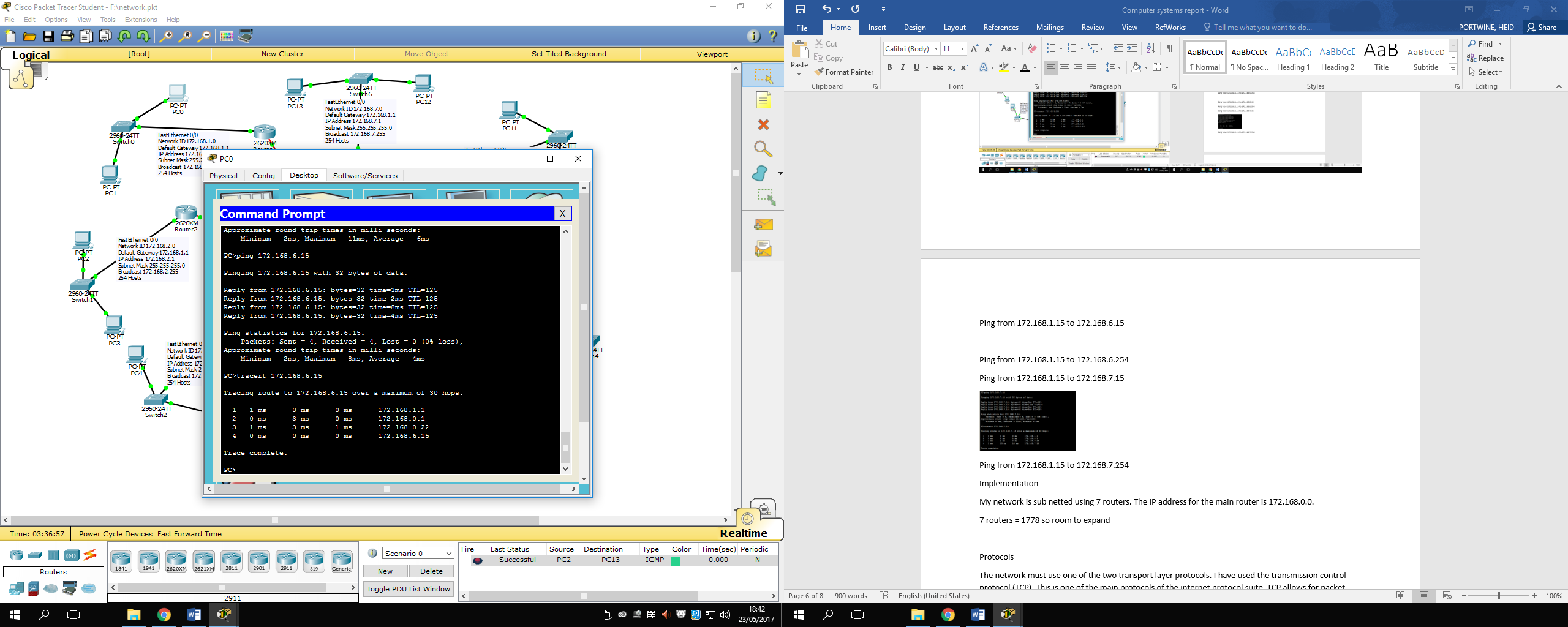
**Ping from 172.168.1.15 to 172.168.5.15**



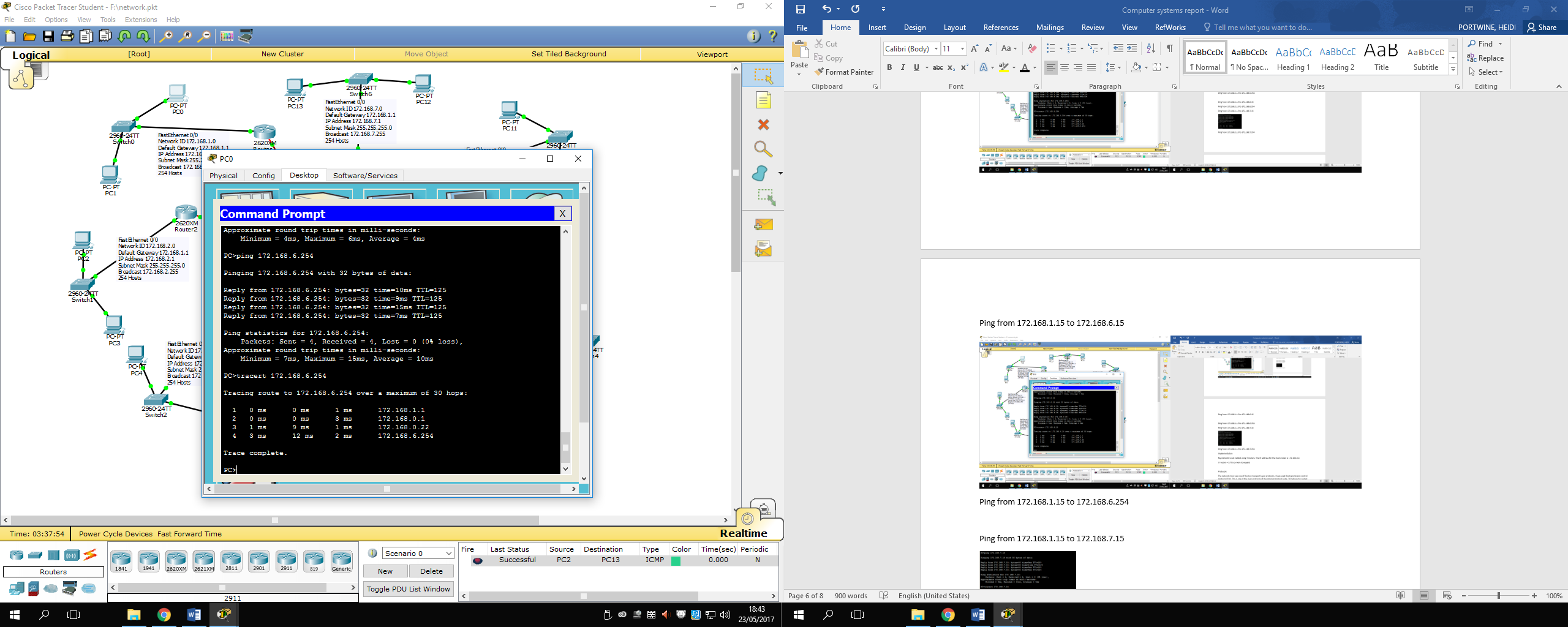
**Ping from 172.168.1.15 to 172.168.5.254**



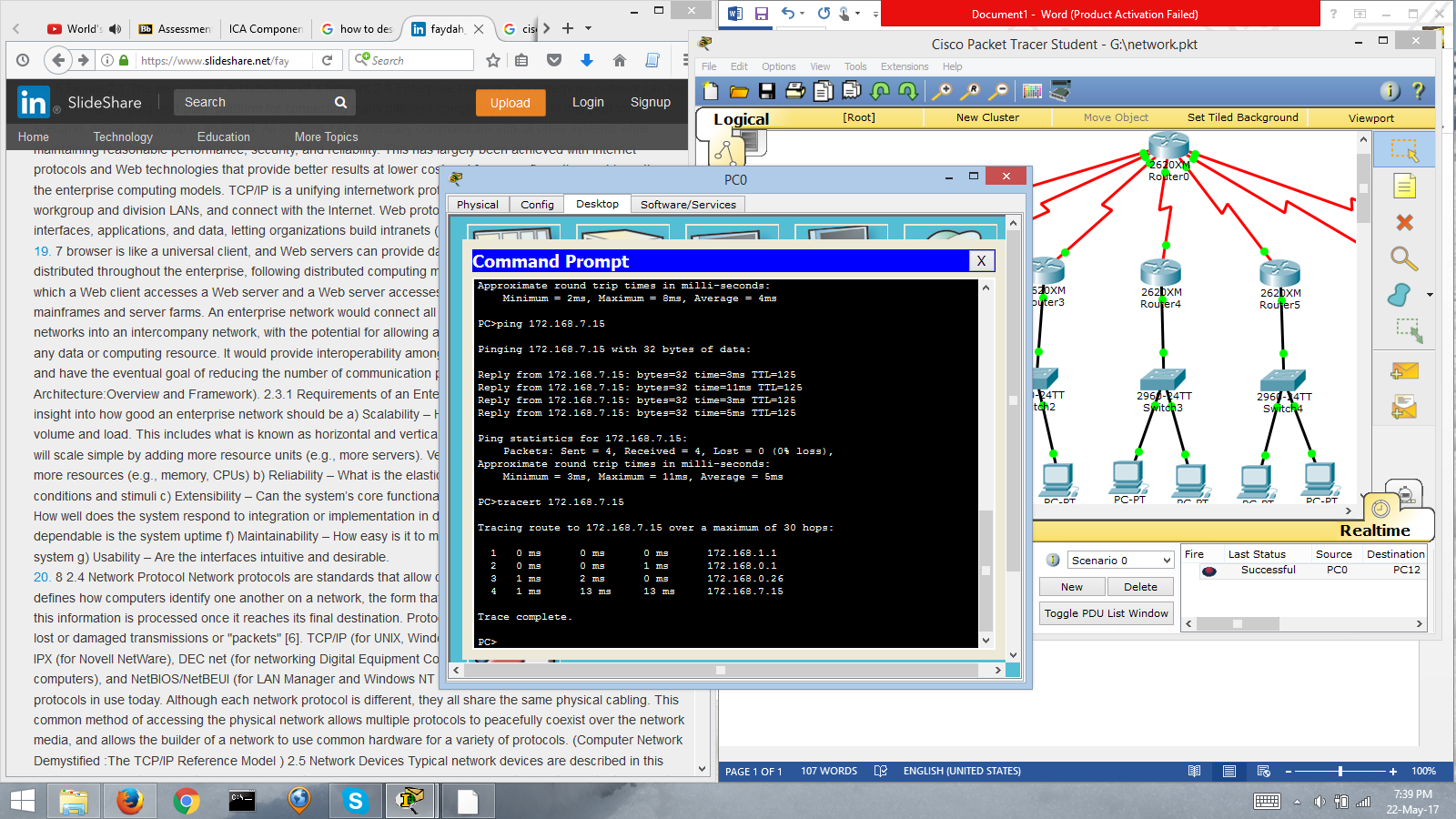
**Ping from 172.168.1.15 to 172.168.6.15**



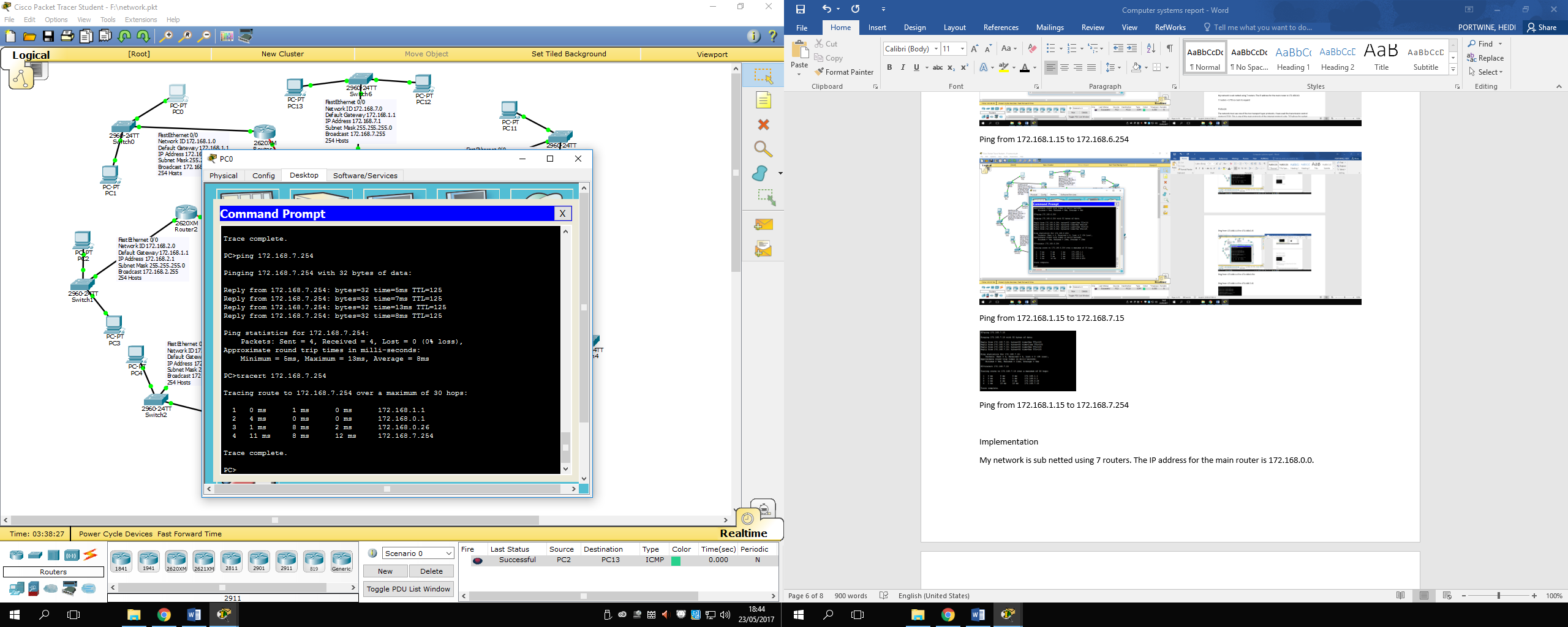
**Ping from 172.168.1.15 to 172.168.6.254**



**Ping from 172.168.1.15 to 172.168.7.15**



**Ping from 172.168.1.15 to 172.168.7.254**



**Technologies**

The technologies I used in cisco packet tracer to create my network were PCs, switches and routers. Overall, I used 14 PCs, 7 switches and 8 routers to connect everything together. My network is sub netted using seven routers, which are connected to a main router. This has an IP address of 172.168.0.0. I have used seven routers, as this would allow 1778 staff members to connect to the network. If I used six router then it there would not have been enough space. Having extra means that there is room for the company to expand if it so desires.

For each of my routers I added the eight-port Async/Sync Network Module (NM-8A/S) to the back. This gave me eight more ports to work with as for Router0 I have seven other routers connected to it. I added the NM-8A/S to the other routers just in case the company ever needed to connect any more switches to the routers if the company expanded. I have connected a switch to each of the seven routers and then two PCs to each switch. On the PCs, I could have included a firewall, which would prevent unauthorized access to the PC.

**Protocols**

The network must use one of the two transport layer protocols. I have used the transmission control protocol (TCP). This is one of the main protocols of the internet protocol suite. TCP allows for packet data delivery confirmation and is considered reliable and ordered. Transmission control protocol provides flow control, same order delivery, a reliable delivery and establishing a session as well as supporting data segmentation and reassembly. The flow control service makes sure the receiver is able to process the data received. Same order delivery makes sure that the segments are reassembled into the proper order. Reliable delivery means that the segments are reassembled into the proper order. The establishing a session service makes the application ready to receive the data. TCP has another useful feature as it can keep trace of the state of the communication session. It records which information it has sent and which has been acknowledged.

I have used the transmission control protocol for the transport layer so I have to use HTTP, SMTP, FTP, and DNS in the application layer. FTP stands for File transfer protocol and is used to transfer computer files over TCP/IP connections from a server to a client. It is a client server protocol that relies on a command channel for controlling the conversation and a data channel for transmitting file content. The employee can upload, download, delete, rename, move and copy files on a server and can also access online software archives. When using FTP employees may have to authenticate themselves by using a username and password.

HTTP stands for hypertext transfer protocol. It is an application layer protocol which is used for data communication for the World Wide Web. Hypertext transfer protocol uses a client server model. The client is the web browser and this is sending requests to the webserver that hosts the website. To retrieve web content for the employees the web browser uses HTTP which is carried over TCP/IP to communicate to the server. The Online Ecommerce Support Center will need the hypertext transfer protocol as employees will need to be able to access the web.

SMTP stands for simple mail transfer protocol. It is an application layer protocol for email services on a TCP/IP network. It allows the ability to send and receive email messages over the internet. SMTP provides intermediary network services between the remote email provider and the user accessing it. The Internet Engineering Task Force created and maintain the SMTP. The company will have to use SMTP as employees will need to be able to send emails to their clients and receive emails from their clients. The emails may also have important announcements so employees will need to be able to access them.

Domain Name System (DNS) is a ranked naming system which is built on a distributed database. DNS is the protocol that locates the internet domain names and translates them into IP addresses. When using the internet, web browsing relies on DNS to provide the information necessary to connect users to remote hosts.

**Security**

The Online Ecommerce Support Center will have to put in place a number of security measures to ensure that the network will be reliable and secure. Security breaches can happen. These could be viruses, hacks, phishing or blended attacks. Any one of these could do serious damage to the company and cause data loss.

To prevent a security breach to the network they could put in place antivirus/antimalware to catch viruses before they do any harm to the network. Firewalls are another measure that could be put in place. This would prevent unauthorized access by hackers and viruses from gaining entry. If the Online Ecommerce Support Centre want a secure private network then a VPN could be used. It would create a secure encrypted connection between the computer and server. A VPN would also enable the employees to securely access the company’s intranet while located outside the office. The company could encrypt their data so that if data is stolen by hackers then it wouldn’t be any use to them as they can’t read it. It would prevent personal information from been leaked out and used.

Usernames and passwords should be used in a company that employs 1580 staff members, as it would prevent unauthorized access to the computers. There could also be different levels of access like the department head could access more than a regular employee. Usernames and passwords would not only prevent outsiders from accessing the company network but from employees accessing information they shouldn’t. System logs could be recorded so that the company can see which employee accessed which file. This could then be traced back to them so if any data is loss they know who last accessed it and deleted it.

To prevent data loss the Online Ecommerce Support Center should make backups of their data regularly. These could be stored on an offsite storage for even better security. They should also train their employees so that they know all the legislation and rules of the work place. The training should be up to date and at least an induction is mandatory.

Online Ecommerce Support Center should also think about the physical security such as the hardware. The equipment could be stolen or vandalized so it should be kept lock away after hours and some protection should be in place such as cameras. They should have a risk assessment done so they know how to deal with each threat that appears. The assessment should include measures to solve it and protect the network better in the future.

**Ethical issues**

Many decisions when you are using computers can raise ethical questions. Lots of IT professional will use perform tasks but won’t think of how they can be misused. One of the major ethical issues when using computers is privacy. When is it ok to read someone’s email without them knowing? Is it ok to place key loggers on computers? Is it ok to routinely keep logs of visited sites?

Many companies such as the Online Ecommerce Support Center may have legal rights to monitor everything an employee does with the computer however is this ethical. Jobs such as network administration may raise ethical issues. They can access most of the data on the network and even read encrypted data if they have access to it. It is easy for people to read personal information, such as emails just for fun but this would be unethical as they are abusing their power. Before a person starts there job they should have the necessary training required and the company should send them on more training courses if they need to.

When looking at the ethical issues involved in the use of computers you need to consider a variety of things. If a security consultant works for different companies but learns something about one of your clients that any affect another client do you tell them or keep it a secret? Every action could develop into a much less justifiable action but it all depends on your opinion of what is ethical and unethical.

**Legal issues**

When operating with computers there are a number of legal issues that we need to be aware of. These are the laws that are in place to govern the use of computers and the internet. The first law is the Computer Misuse Act. It was introduced in 1990 to secure computer material against unauthorized access or modification.

The second law is the Data Protection act, which was introduced in 1998.This law controls how your personal information is used by organisations, businesses or the government.

The Data Protection Act has eight principles that must be followed:

* The data must be processed fairly and lawfully
* The data shall be obtained and processed for only its purpose
* The data must be adequate, relevant and not excessive
* The data should be accurate and up to date
* The data processed should not be kept for longer than necessary
* The data should be processed in accordance with the rights of the data subject
* The data must be kept safe and secure
* The data should not be transferred outside the European Economic Area without adequate protection

There is stronger legal protection for more sensitive information such as criminal records or religious beliefs but I do not think the Online Ecommerce Support Center will be handling this type of information. The Online Ecommerce Support Center may however be handling information about the customer such as name, address and telephone number or email address so they will still have to adhere to it.

Another law is the Copyright, Designs and Patents Act, which was introduced in 1988. This law protects the authors or creators of a piece of work and ensures that their investment of time, money and effort is recognized. The law means that the original work is protected and cannot be plagiarized. The copyright law extends to the items on a website like the images or photos.

**References**

<https://en.wikipedia.org/wiki/Transmission_Control_Protocol>

<https://en.wikipedia.org/wiki/File_Transfer_Protocol>

<http://searchenterprisewan.techtarget.com/definition/File-Transfer-Protocol>

<https://kb.iu.edu/d/aerg>

<https://www.techopedia.com/definition/2336/hypertext-transfer-protocol-http>

<https://www.techopedia.com/definition/1710/simple-mail-transfer-protocol-smtp>

<https://www.techopedia.com/definition/24201/domain-name-system-dns>

<http://searchnetworking.techtarget.com/definition/domain-name-system>

<http://www.computerworld.com/article/2557944/security0/ethical-issues-for-it-security-professionals.html>

<http://www.gre.ac.uk/it-and-library/about/policies-and-procedures/it-policies/computer-related-legislation>

<https://www.gov.uk/data-protection/the-data-protection-act>

<https://ico.org.uk/for-organisations/guide-to-data-protection/data-protection-principles/>

<https://www.sqa.org.uk/e-learning/ProfIssues02CD/page_09.htm>