**CIST 0165 Networking I**

**Quiz 1 and Mid-Term Study Guide**

Please familiarize yourself with the below guidelines and topics for the upcoming quiz and mid-term exams.

1. ***Guidelines***

* Lecture slides, notes, homework and reading assignments will be good reference material.
* Exams are open book, open notes but searching on web for answers and working with others on the exam questions are not allowed.
* Any act of academic dishonesty would directly lead to an F grade in the course.
* Exam questions would be a mix of multiple choice, matching, short answer/definition, and command execution (terminal, cisco packet tracer etc).

**Types of Computer Networks**

1. Local Area Network (LAN)
2. Office, School, Colleges
3. Wired or Wireless
4. Wide Area Network (WAN)
5. Connect the computers placed in one location to another location
6. Metropolitan Area Network (MAN)
7. Designed to be used in a city or a town through the wireless medium or using optical fiber cables
8. Campus Area Network (CAN)
9. Designed to be used by a particular campus or a military base with computers placed within a limited area
10. Home Area Network (HAN)
11. Connected within user home that connects various digital devices over a network for communicating with other devices
12. ***Key Concepts***

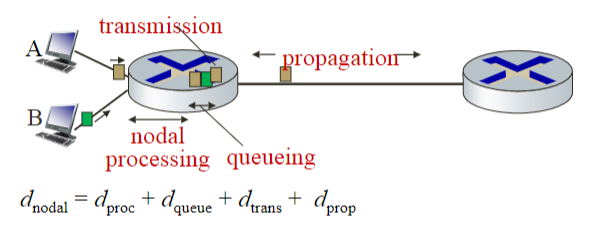
* **What is a network**

1. Infrastructure for computer devices to communicate with each other
2. Refers to the connection of two or more computers by some type of medium wired or wireless

* **Differences between internet, intranet, and extranet**

1. Intranet
2. Private network contained within an enterprise
3. Internet
4. Worldwide public internetwork
5. Uses protocols such as TCP/IP and HTTP to transfer and view information
6. Extranet
7. Allows limited and controlled access to internal resources by outside users

* Sources of packet delay

1. 

* **Malware, Denial of Service, Packet Sniffing, IP Spoofing**

1. Malware
2. Malware can get in host from:
3. Virus: self-replicating infection by receiving/executing object (e.g. e-mail attachment)
4. Worm: self-replicating infection by passively receiving object that gets itself executed
5. Spyware malware can record keystrokes, web sites visited, upload info to collection site
6. Infected host can be enrolled in botnet, used for spam or distributed denial of service (DDos) attacks

* **Classification of network media**

1. Diagram

   Description automatically generated

* **Common IEEE Ethernet Standards (lecture 3, slide 6)**

1. Table

   Description automatically generated with medium confidence
2. Table

   Description automatically generated

* Straight vs Crossover Cables

1. Diagram

   Description automatically generated
2. Table

   Description automatically generated
3. Table

   Description automatically generated

* **Copper cables vs fiber optic cables**

1. Copper cables can only carry signals about 100 meters, while some single-mode fiber optic cables can carry more data up to 25 miles. Fiber optic cable also carries data with less attenuation or signal loss—only about three percent every 100 meters—than copper, which loses over 90 percent over the same distance.

* **Usages of NIC, Repeater, Hub, Switch, Router, Modem, Firewall**

1. Network Interface card (NIC)
2. To create and mediated the connection between a computer and the networking medium
3. Date is represented as it signals that NIC transmits or receives
4. Contains electronic components needed to send and receive signals
5. Allows a PC to communicate with computer hardware
6. Uniquely identifies a computer
7. Networks won’t function correctly if duplicate MAC addresses exist
8. Most NICs are built into a computer’s motherboard
9. MAC address is stored in nonvolatile memory on the NIC
10. Repeater
11. The number of nodes on a network and the length of cable used to influence the quality of communication on the network
12. Attenuation
13. The degradation of signal clarity
14. Repeaters
15. Work against attenuation by repeating signals that they receive on a network
16. Typically cleaning and regenerating the digital transmission in the process
17. Amplifies or reshapes a weak signal into its original strength and form
18. Diagram

    Description automatically generated
19. Hub (Multiport Repeaters)
20. A multiport repeater is just a repeater with several ports to which you can connect cabling
21. Also referred to as a HUB
22. Receives bit signals generated from a connected computer on one of its ports
23. Cleans the signal by filtering out electrical noise
24. Regenerates the signal to full strength
25. Generic connection device used to tie several networking cables together to create a link between different stations on a network
26. Active hubs
27. Amplify or repeat signals that pass through them
28. Passive hub
29. Merely connects cables on a network and provides no signal regeneration
30. Network Bandwidth
31. Amount of data that can be transferred during a specific interval
32. Usually measured in bits per second (bps)
33. Networks operate from 10 million bps (10 Mbps) up to 10 gigabits per second (Gbps)
34. Hub share bandwidth with all other connected computers
35. Only one computer can successfully transmit data at a time
36. Switches
37. Filters and directs network traffic
38. Creates subnetworks from a larger network
39. A network switch looks just like a hub
40. However, a switch reads data in the message, determines which port the destination device is connected to, and forwards the message to only that port
41. Data is sent onto the medium one frame at a time
42. Each frame has the destination MAC address and the source computer’s MAC address
43. When the frame reaches a switch, the switch reads both addresses:
44. Keeps a record of which computer is on which port
45. Forwards the frame to the port where the destination MAC can be found
46. A switch maintains a switching table of MAC addresses that have been learned and their associated port numbers
47. Basic Switch Operation
48. The switch receives a frame.
49. The switch reads the source and destination MAC addresses.
50. The switch looks up the destination MAC address in its switching table.
51. The switch forwards the frame to the port where the computer owning the MAC address is found.
52. The switching table is updated with the source MAC address and port information.
53. Advantages
54. Switches increase available network bandwidth
55. Switches reduce the workload on individual computers
56. Switches increase network performance
57. Networks that include switches experience fewer frame collisions because switches create collision domains for each connection) a process called micro segmentations)
58. Switches connect directly to workstations
59. Disadvantages
60. Switches are significantly more expensive than bridges
61. Network connectivity problems can be difficult to trace through a switch
62. Broadcast traffic may be troublesome.
63. Switch remembers MAC addresses of recent senders on each port
64. If packet is addressed to an unknown address, broadcast to all ports
65. Routers
66. Routers connect LANs together to create an internetwork
67. Typically have two or more network ports to which switches or hubs are connected
68. Routers are devices that enable multiple LANs to communicate with one another by forwarding packets from one LAN to another
69. A picture containing microscope

    Description automatically generated
70. Default Routes
71. Default Routes tell the router where to send a packet when the router doesn’t have an entry in its routing table
72. Network Unreachable
73. Network unreachable is a message a router might send to the sending station when the network can’t be found
74. Navigates packets across large networks
75. Uses the most efficient route
76. Similar to switches in that they segment a network and filter traffic
77. Routers use the logical address
78. Routers use the IP address to route packets to the correct network segment
79. Diagram, map

    Description automatically generated
80. Advantages
81. Can connect different network architectures, such as Ethernet and Token Ring
82. Can choose the best path across the internetwork using dynamic routing techniques
83. Reduce network traffic by creating collision domains
84. Disadvantages
85. Routers work only with routable network protocols; most but not all protocols are routable
86. Routers are more expensive than other devices
87. Dynamic router communications (inter-router communication) cause additional network overhead, which results in less bandwidth for user data
88. Routers are slower than other devices because they must analyze a date transmission from the Physical through the Network layer
89. Modems
90. Digital to analog
91. Analog to digital
92. Internet reads analog
93. Computers use digital encoding
94. Router comes in after the modem
95. In a SOHO, a modem embedded in a router
96. Types of Modems
97. Cable
98. Connected using co-axial cable
99. Cable is typically provided by the same company that provides cable connection
100. Comcast
101. DSL
102. Connected using typical phone line
103. ATT
104. Lot of times when the service provider sends a modem – a combination of modem and router – wireless router
105. Firewall
106. Filters info that comes in from network/internet
107. Creates a safety barrier between a private network and the wider external internet
108. To avoid disruptions from unwanted elements
109. Especially imp for a large org that has lot of computer and servers
110. A picture containing chart

     Description automatically generated
111. Types of Firewalls
112. Host-based firewall
113. Software firewall that is installed on a computer
114. Protects only that computer
115. Ex: Microsoft windows firewall, anti-virus programs
116. Network-based firewall
117. Combination of hardware and software
118. Placed between a private network and the internet
119. Protects the entire network unlike the host based by following the management rules that ate applied to entire networks
120. Can be a standalone product – used by large organizations
121. Can also be built into routers – used by small organizations
122. Or deployed in the service provider’s cloud infrastructure – cloud firewall
123. Lot of organizations will use both network-based and host-based firewalls
124. Ensure maximum protection – 2-layer security

* **Source Address Table**

1. Ethernet switches give every conversation the full   
   bandwidth of the network
2. Maintains Source Address Table (SAT)
3. A switch copies the source MAC addresses and builds a table of MAC addresses of each connected computer

* **Wireless Ethernet Standards (lecture 3, slide 41)**

1. Table

   Description automatically generated

* **Client**

1. A client can be a workstation running a client OS or it can refer to the network software on a computer that requests network resources from a server

* **Server**

1. A computer becomes a server when software is installed on it that provides a network service to client computers

* **What is a peer-to-peer network**

1. Computers on a peer-to-peer network can take both a client and a server role
2. Any user can share resources on his/her computer with any other user’s computer
3. Every user must act as the administrator of his/her computer
4. Can give everyone else unlimited access to their resources or grant restricted access to other users
5. Usernames and passwords (credentials) are used to control that access
6. In a P2P network, no computer has more authority than another; each computer controls its own resources and communicates directly with other computers
7. Advantages
8. Simple configuration
9. Less expensive compared to other network models
10. Disadvantages
11. Must remember multiple sets of credentials to access resources on several computers
12. Desktop PCs and the OS installed on them aren’t made to provide network services as efficiently as dedicated network servers
13. Data organization
14. If every machine can be a server, how can users keep track of what information is stored on which machine?
15. Not scalable
16. Not necessarily secure
17. Not practical for large installations

* **What is the client/server network**

1. Severs hosts the resources for the clients to use and provide security
2. A Client is the computer that requests resources from the server
3. Diagram

   Description automatically generated
4. Client-Server applications
5. Network services are the resources a network makes available to its users
6. It includes applications and the data provided by these applications
7. In client-server applications
8. A client computer requests data or service from a second computer, called the server
9. Server/Domain-Based Model
10. Server-based networks allow centralized control over network resources
11. Users log on to the network with a single set of credentials maintained by one or more server OS
12. In most cases, servers are dedicated to running network services and should not be used to run user applications
13. Text

    Description automatically generated

* Network Topologies – Bus, ring, Star, Hybrid, Star

1. Every network provides a method of getting data from one system to another
2. Cabling
3. Wireless methods
4. Standards ensure networking equipment works well together
5. Topology describes how parts of a whole work together
6. Physical topology
7. Network’s hardware and how computers, other devices, and cables work together to form the physical network
8. Logical topology
9. Path data travels between computers on a network
10. Physical Bus Topology
11. A continuous length of cable connecting one computer to another in daisy chain fashion
12. The simplest and at one time the most common method for connecting computers
13. 
14. Bus Topology
15. Single bus cable
16. Connects all computers in a line
17. Data flows form each computer onto the bus
18. Termination required at end prevent signal from reflecting at the ends of the cable
19. Uses a single cable or conductor to connect all nodes
20. Used as a backbone to link other topologies
21. A picture containing stationary, table

    Description automatically generated
22. Ring Topology
23. Connects all computers on the network in ring
24. Data flows form one computer to next one in circle
25. No end of cable and no need for termination
26. Single cable
27. Runs continuously from node to node
28. Diagram

    Description automatically generated
29. One problem: Entire network stops working if the cable is broken at any point
30. Star Topology
31. One central connection for all computers
32. Diagram

    Description automatically generated
33. Uses a central device (hub or switch) to connect computers
34. Each computer has a single length of cable going from its NIC to the central device
35. Has fault tolerance
36. If one cable breaks, other computers can still communicate
37. Not successful early on
38. More expensive than bus and ring
39. Difficult to redesign early bus and ring hardware
40. Advantages
41. Much faster technologies than bus
42. Using a central device allows for monitoring and managing a network Hubs and switches can include software that collects statistics about network traffic patterns and detect errors
43. If cabling and NICs support it, a star network can be easily updated by replacing the central device
44. When the number of workstations you need exceed the number of ports on a central device you simply add another central device
45. The main disadvantage is that the central device represents a single point of failure
46. If the hub or switch fails or someone kick the power cord out of the outlet, the entire network goes down
47. Mesh Topology
48. Diagram

    Description automatically generated
49. Hybird Topology
50. A hybrid topology is mixture of topologies
51. Diagram

    Description automatically generated
52. Tree Topology
53. Two or more-star topologies connected by a common backbone
54. A picture containing antenna

    Description automatically generated

* **LAN vs WAN**

1. LAN
2. A LAN (local area network) is usually contained in a small space
3. This LAN has five computers, a network printer, a local printer, a scanner, and a switch, and uses a star topology
4. Diagram

   Description automatically generated
5. WAN
6. A WAN (wide area network) is a group of LANs that spread over a wide geographical area
7. Spans multiple geographic areas and is usually connected by common telecommunication carriers
8. Diagram

   Description automatically generated
9. LAN vs WANS
10. LANS
11. Your Control
12. Your Equipment
13. Your premises
14. WANS
15. Outside Control
16. Outside Entity’s Equipment
17. Outside your physical property

* **Root, top-level, authoritative, and subdomain name servers**

1. International Corporation for assigned names and number
2. These store IP addresses of the nameservers for all the top-level domains (TLDs): com, net, uk, edu, cn, etc
3. Map

   Description automatically generated

* Querying the DNS Hierarchy

1. Client wants IP address of cs.pitt.edu
2. Query iteratively, starting with the root server
3. Each server replies with an answer or the name of server to contact:
4. “I don’t know this name but ask this server.”
5. Performance problems?
6. Every request hits the root server
7. Common domains, like google.com are queried billions of tines per day!
8. Diagram

   Description automatically generated

* **Elements of network protocol**

1. Encoding – based on medium (wired or wireless)
2. Formatting and encapsulation – common format, identifying information
3. Timing – flow control, acknowledgement, and re-transmission
4. Size – fragmentation, numbering
5. Delivery options – unicast, multicast, broadcast

* Functionalities of OSI Model Layers

1. Diagram

   Description automatically generated
2. OSI Model
3. Used as a reference model by vendors
4. Introduced to enable communication between different computers
5. Implements all the elements of a network protocol
6. Modular design
7. Easy to troubleshoot
8. Graphical user interface, application

   Description automatically generated
9. A picture containing diagram

   Description automatically generated
10. Diagram

    Description automatically generated

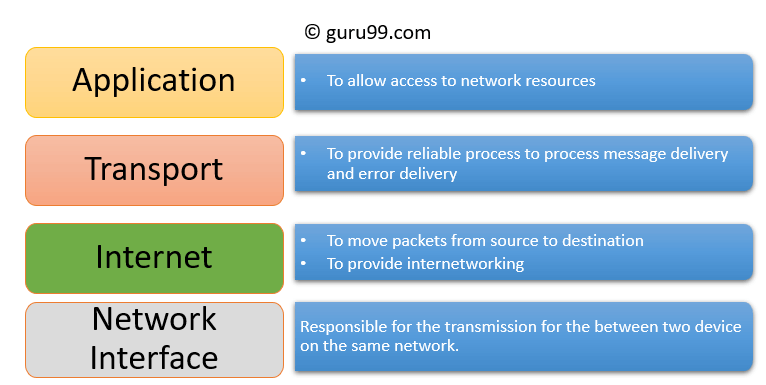
* **OSI layer 1, layer 2, layer 3 devices**

1. Graphical user interface

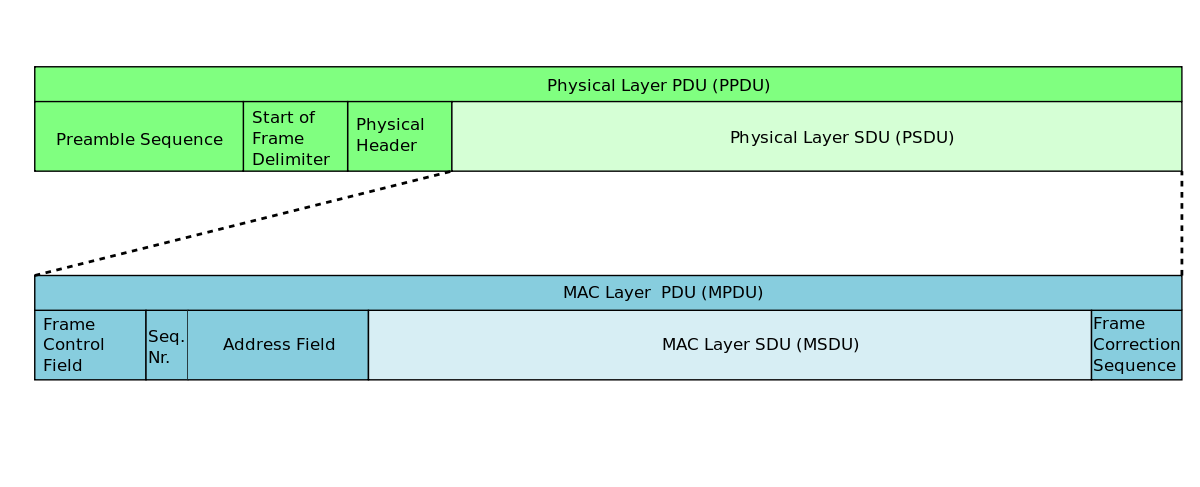
   Description automatically generated
2. Diagram

   Description automatically generated

* **TCP/IP Model Layers**

1. 

* **Understand protocol data units, segments, packets, frames**

1. Protocol data units is a single unit of information transmitted among peer entities of a computer network.
2. 
3. Packet is a small segment of a larger message
4. Frame is data that is transmitted between network points as a unit complete with addressing and necessary protocol control information.

* **MAC address vs IP Address**

1. MAC address
2. Found at the Data Link Layer of the OSI model
3. Used by bridges and switches to make forwarding decisions within a network or subnetwork
4. IP address
5. Logical address when TCP/IP is used on an internetwork
6. TCP Features

* **Multiplexing**

1. Feature of both TCP and UDP
2. Solution for handling traffic for multiple applications simultaneously
3. Utilizes ports for identifying traffic
4. Creates sockets to track traffic
5. Source Socket
6. Destination Socket
7. Text

   Description automatically generated with low confidence

* **End-to-end packet delivery**

1. Connections terminated on both sides to finish conversation
2. Introduces new Flag Bit of “FIN”
3. TCP conducts Four Way handshake
4. Text, letter

   Description automatically generated

* **Reliability**

1. TCP gives reliable data transfer
2. Utilizes Sequence and Acknowledge fields of TCP header
3. A picture containing timeline

   Description automatically generated
4. What happens on Error
5. A picture containing table

   Description automatically generated

* **Flow control**

1. Protocol to ensure that the sender does not send data faster than the receiver can receive it
2. Receiver sends window size in ACK
3. If window is small, sender waits
4. Control how much data can be sent before ACK
5. Allows Receiving Host to adjust window size up or down
6. Text

   Description automatically generated

* **Congestion control**

1. Diagram

   Description automatically generated
2. Text, letter

   Description automatically generated
3. Chart, diagram

   Description automatically generated
4. IP Addressing and Routing

* **Binary to decimal and vice versa**

1. Table

   Description automatically generated with medium confidence

* Different classes of IP Addresses

1. Class A
2. Reserved for governments and large corporations throughout the world
3. Each Class Address supports 16,777,214 hosts
4. Table

   Description automatically generated with medium confidence
5. Class B
6. Assigned to large and medium sized companies
7. Each Class B address supports 65,534
8. A picture containing diagram

   Description automatically generated
9. Class C
10. Addresses are assigned to groups that do not meet the qualifications to obtain Class A or B addresses
11. Each Class C address supports 254 hosts
12. Diagram

    Description automatically generated with medium confidence
13. Class D
14. Addresses (also known as multicast addresses) are reserved for multicasting
15. Multicasting is sending of steam of data (usually audio and video) to multiple computers simultaneously
16. Diagram

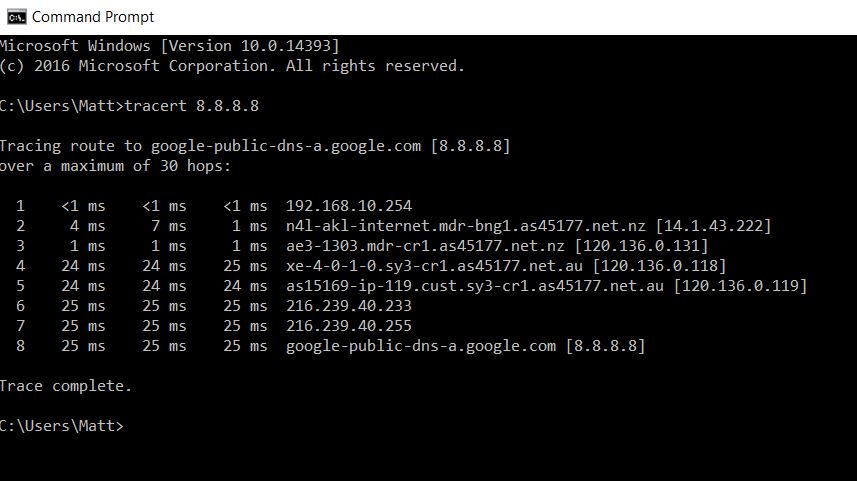
    Description automatically generated with medium confidence
17. Class E
18. Addresses are reserved for research, testing, and experimentation
19. The Class E range starts where Class D leaves off
20. Private IP ranges
21. Many companies use private IP addresses for their internal networks
22. Will not be routable on the internet
23. Gateway devices have network interface connections to the internal network and the internet
24. Route packets between them
25. IP Classes
26. Table

    Description automatically generated

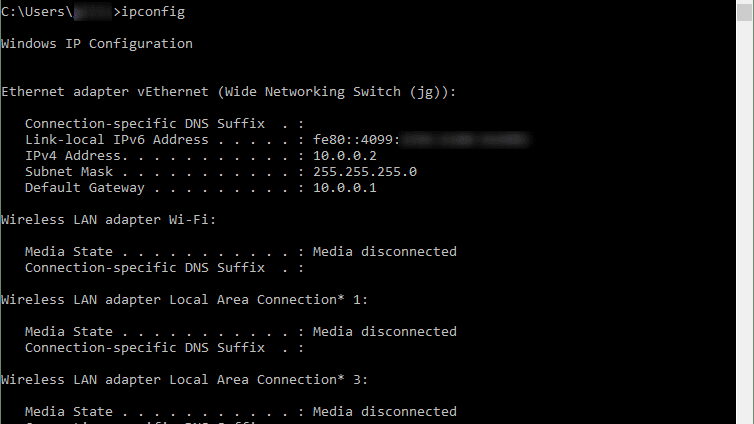
* Subnet Masks

1. Indicates how much of the IP address represents the network or subnet
2. Standard (default) subnet masks:
3. Class A subnet mask is 255.0.0.0
4. Class B subnet mask is 255.255.0.0
5. Class C subnet mask is 255.255.255.0
6. ***Understand the usage of the below commands and be able to explain the result:***

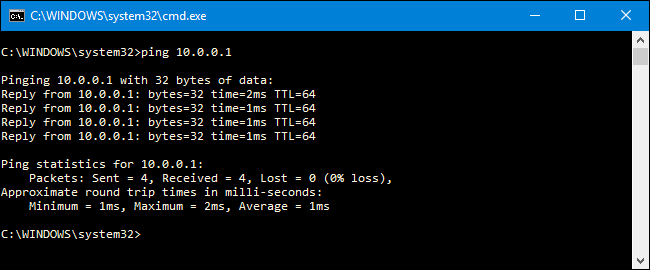
* traceroute or tracert

1. Command-line utility that you can use to trace the path that an Internet Protocol (IP) packet takes to its destination.
2. 

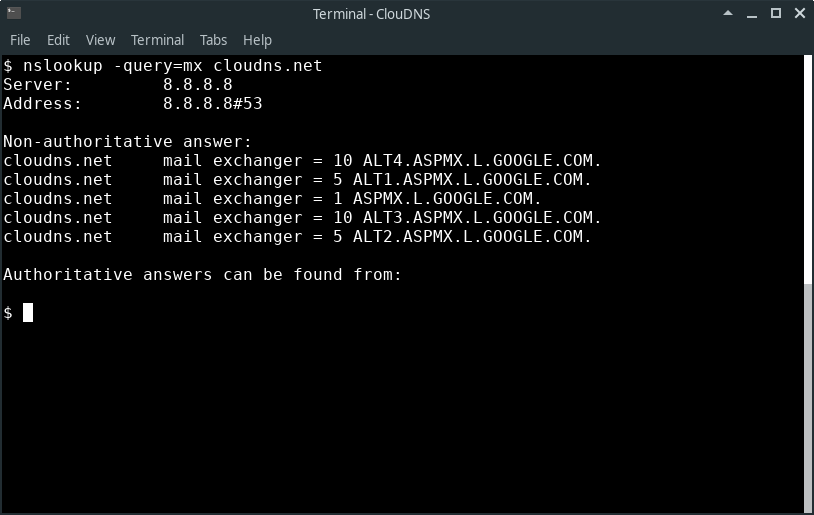
* ipconfig /all

1. Output of the default command contains the IP address, network mask, and gateway for all physical and virtual network adapters.
2. 

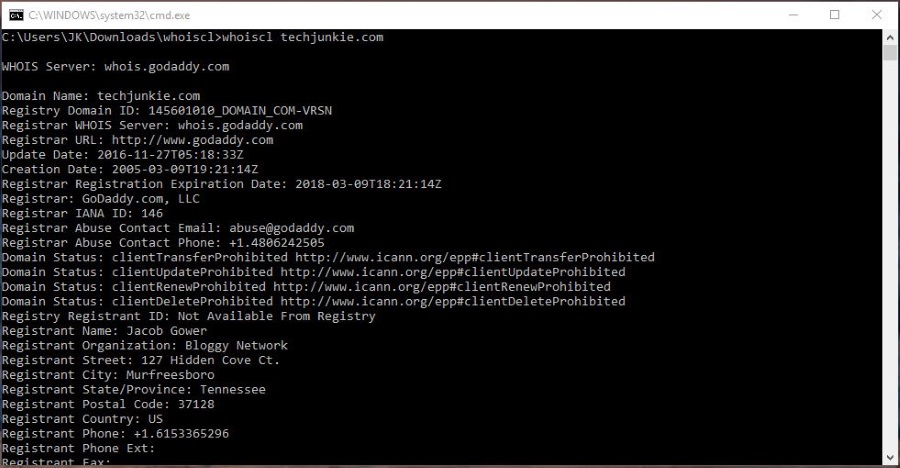
* Ping

1. Used to test the reachability of a host on an Internet Protocol network
2. 

* Nslookup

1. Cross-platform command for obtaining DNS records
2. 

* Whois

1. A query and response protocol that is widely used for querying databases that store the registered users or assignees of an Internet resource, such as a domain name, an IP address block or an autonomous system, but is also used for a wider range of other information.
2. 

* netstat

1. Text

   Description automatically generated
2. ***Cisco Packet Tracer***

* Basic commands and functionalities (to be explained in class)

\*\* Sections 2,3,4 would be covered in Quiz 1

\*\*\* Sections 2,3,4,5,6 would be covered in the mid-term