

Name \_\_\_\_\_

# Final Exam

## CIS 68C2

### Fall 2002

#### **Instructions**

- Write your name on your Scantron, and on a separate blank sheet of paper for short answers.
- Follow the instructions in each of the sections
- If you are unclear about something, raise your hand.
- Any form of cheating will result in an automatic F in the course.

#### **Hints for Success**

- Use your knowledge of the fundamentals, and draw conclusions from there.
- Read each problem carefully!
- Try to determine the skills or knowledge a question is attempting to assess.
- Decide if a general answer or specific answer is the best choice.

Name \_\_\_\_\_

### Multiple Choice (2 points each)

Select your answer to the problems below by filling-in the corresponding bubble on your Scantron sheet. Multiple selections will be marked as incorrect. There is no penalty for incorrect answers.

1. The maximum number of TCP/IP services is:
  - a. 1024
  - b. 2048
  - c. 4096
  - d. 65536
  - e. unlimited
  
2. UDP, TCP, ARP, and ICMP are all:
  - a. protocols
  - b. acronyms
  - c. a formal set of rules
  - d. all of the above
  - e. none of the above
  
3. A layer header and payload is called:
  - a. a frame
  - b. a segment
  - c. a datagram
  - d. depends on the layer
  - e. none of the above
  
4. After passing up through the Internet Layer, the headers that remain in a message are the:
  - a. application, IP, and transport headers
  - b. transport and IP headers
  - c. application and transport headers
  - d. application header
  - e. none of the above
  
5. If there is no response from **ping somehost.somedomain.com** it means: (NOTE: This question is unclear – credit will be given for any answer)
  - a. the host is down or is configured to not respond to pings
  - b. your network stack is not configured correctly
  - c. DNS is not working
  - d. either (a) or (b)
  - e. all of the above
  
6. The error message **sendto: Network is unreachable** implies:
  - a. the network is not functional
  - b. DNS is not functional
  - c. there is no route to the destination
  - d. the host table does not contain an entry
  - e. any of the above
  
7. Fragmentation and packet reassembly are defined by:
  - a. ICMP
  - b. IP
  - c. TCP
  - d. UDP
  - e. RARP
  
8. The value 00:0B:6F:57:4E:2D is:
  - a. an MCC address
  - b. a hexadecimal IP address
  - c. an Ethernet device address
  - d. an ARP response

Name \_\_\_\_\_

- e. an packet header
9. The dotted-decimal notation for the IP address 192.168.43.97 is:
- a. 11000001101010000010101101100000
  - b. 11000000101010000010101101100001
  - c. 11000011101010000010101101100000
  - d. 01000111101010000010101101100001
  - e. none of the above
10. The Ethernet MTU is:
- a. 512
  - b. 1500
  - c. 2400
  - d. 4500
  - e. 8002
11. MTU affects:
- a. segment size
  - b. maximum fiber length
  - c. fragmentation
  - d. positive acknowledgement and retransmission parameters
  - e. none of the above
12. What is the traditional IP Class of 11000000101010001010111100001:
- a. A
  - b. B
  - c. C
  - d. D
  - e. none of the above
13. OSPF is a:
- a. static routing protocol
  - b. interior routing protocol
  - c. exterior routing protocol
  - d. open source routing protocol
  - e. distance vector protocol
14. PAR is useful for:
- a. prioritized packet reassembly
  - b. ensuring correct data transmission
  - c. UDP reliability
  - d. performance and reliability
  - e. none of the above
15. The **domain** statement in /etc/resolv.conf:
- a. defines the DNS server to be authoritative
  - b. supplies a domain for BIND to append to non-FQDNs
  - c. instructs BIND to ignore other domains
  - d. defines the zone for the recursive server
16. An octet is:
- a. 1 byte
  - b. 4 bytes
  - c. 8 bytes
  - d. 32 bits
  - e. 128 bits
17. CIDR required:
- a. a network mask
  - b. routing protocol modifications

Name \_\_\_\_\_

- c. router modifications
  - d. all of the above
18. Multi-homing is
- a. a confused pigeon
  - b. enjoying a vacation home in the Bahamas
  - c. multiple routes to the same destination
  - d. a system with more than one operational TCP/IP network interfaces
  - e. the dynamically changing IP address for a mobile system on a wireless network
19. Complete the translation sequence: Hostname → IP Address → \_\_\_\_\_ :
- a. MAC address
  - b. route
  - c. ARP table entry
  - d. destination
  - e. broadcast
20. The IP addresses 200.198.254.9/22 belongs to:
- a. class A
  - b. class B
  - c. class C
  - d. none of the above
21. RIP is generally considered obsolete because it:
- a. is old and crusty
  - b. is no longer supported by LPD printers
  - c. does not support CIDR
  - d. is a simple distance vector protocol
  - e. is not implemented in gated
22. Supernetting is.
- a. aggregating consecutive IP addresses to create a network with more hosts than a traditional class allows
  - b. combining disparate networks to create a hybrid bridge
  - c. using the upper bits of the host part of an IP address to subdivide none of the above
  - d. achieving maximum performance through bandwidth combining
  - e. combing several class A addresses into a multicast address
23. The DHCP client/server message exchange typically looks like:
- a. DCHPWHOGOTTA, DHCPIGOTTA, DHCPIWANNA, DHCPYUOGOTTA
  - b. DHCPDISCOVER, DHCPOFFER, DHCPREQUEST, DHCPACK
  - c. DHCPREQUEST, DHCPDISCOVER, DHCPOFFER, DHCPACK
  - d. DHCPREQUEST, DHCPOFFER, DHCPDISCOVER, DHCPACK
  - e. DHCPDISCOVER, DHCPREQUEST, DHCPOFFER, DHCPACK
24. The command **netstat -r** shows:
- a. the routing table
  - b. the ARP table
  - c. the RARP table
  - d. various network statistics
25. To help resolve a duplicate IP addresses on your network, you would:
- a. examine the /etc/hosts file
  - b. use the ethers command
  - c. use the arp command
  - d. use the rpcinfo command
  - e. none of the above
26. Using nslookup with a non-authoritative server for a zone to uncover its MX record generally provides:
- a. a reliable answer
  - b. an inaccurate answer

Name \_\_\_\_\_

- c. an answer only if cached
  - d. an error
27. SMTP, daytime, whois, FTP, and telnet are:
- a. TCP/IP services
  - b. protocols
  - c. defined by RFCs
  - d. application layer services
  - e. all of the above
28. BOOTP:
- a. is the same as DHCP
  - b. provides more information than DHCP
  - c. is supported by the ISC implementation of DHCP
  - d. is obsolete and no longer used
  - e. none of the above
29. NFS runs over:
- a. TCP
  - b. UDP
  - c. RPC
  - d. none of the above
  - e. all of the above
30. The list of mounted NFS filesystems is contained the file :
- a. /etc/exports
  - b. /var/lib/nfs/xtab
  - c. /etc/fstab
  - d. /etc/hosts
  - e. none of the above
31. The command **umount /mnt/floppy** :
- a. un-mounts the floppy device mounted on /mnt/floppy
  - b. un-mounts the floppy device /mnt/floppy
  - c. un-mounts the filesystem mounted at /mnt/floppy
  - d. un-mounts the filesystem device /mnt/floppy
  - e. none of the above
32. The **nfsstat** command is used to:
- a. examine NFS client statistics
  - b. examine NFS server statistics
  - c. examine RPC statistics
  - d. both (a) and (b)
  - e. all of the above
33. Key, map, direct, indirect and executable all refer to:
- a. NFS
  - b. automounter
  - c. DBM databases
  - d. filesystems
  - e. routing protocols
34. Recursive DNS servers:
- a. follow referrals to provide an answer to a query, or return an error
  - b. answer a query if the answer is known, or return an error
  - c. return referrals, or return an error
  - d. are only necessary for stub servers
35. A **bounce attack** is:
- a. a security issue with proxy FTP servers

Name \_\_\_\_\_

- b. a form of IP spoofing
  - c. a security issue also known as DNS hijacking
  - d. not really much of a threat
36. A name server is authoritative:
- a. if it gives accurate responses to queries
  - b. **only for its own zone**
  - c. if an ISP has an entry for it in its DNS tables
  - d. if configured as such for the domain
  - e. none of the above
37. The yppush command:
- a. is run periodically by cron on NIS slaves
  - b. pushes the NIS DBM databases to NIS slaves
  - c. follows a ypxfer
  - d. is run periodically by cron on NIS clients
  - e. **none of the above**
38. DNS defines:
- a. local hostname translation
  - b. **a hierarchical namespace of domains**
  - c. email priorities
  - d. IP addresses
  - e. none of the above
39. Version, TTL, protocol, source and destination address are all fields in the:
- a. **IP datagram header**
  - b. routing table
  - c. ARP table
  - d. traceroute packet
  - e. ICMP response
40. Running **named** as a caching-only server requires:
- a. /etc/resolv.conf
  - b. /etc/named.conf
  - c. /etc/named.conf and a hints file
  - d. **/etc/named.conf, a hints file, and possibly localhost zone files**
  - e. /etc/named.conf and zone files
41. The TTL field of the SOA record in BIND 9 is used for:
- a. **negative caching**
  - b. dead slave server retries
  - c. the duration in a cache of records returned from a query
  - d. the number of hops a resolver is willing to allow a RR query to travel
  - e. none of the above
42. A CNAME is:
- a. **an alias to a host's canonical name**
  - b. a common name for a domain
  - c. a shortcut in a zone file
  - d. a list of nameservers
43. To delegate a sub-domain, the domain's owner must:
- a. gain permission from the upstream ISP
  - b. **create an NS record and an A record glue entry referring to the sub-domain's nameserver**
  - c. remove the domain's zone files
  - d. disable the DNS server
44. FTP facilitates access through firewalls via the command:
- a. PORT

Name \_\_\_\_\_

- b. **PASV**
  - c. OPEN
  - d. TRAN
45. The **ypbind** daemon, when bound to an NIS domain, provides NIS:
- a. **client queries**
  - b. server queries
  - c. client responses
  - d. server responses
46. An FTP proxy transfer occurs by opening:
- a. two data channels
  - b. **two command channels**
  - c. one data channel and one command channel to each server
  - d. one command channel, and instructing the server to open its own command channel
  - e. none of the above
47. The **chroot** system call or command:
- a. provides minimal extra security
  - b. **redefines the root of the filesystem for a process**
  - c. changes a process' root UID into another UID
  - d. allows anonymous users to become real users in FTP
  - e. none of the above
48. The disable-until-needed philosophy helps:
- a. increase reliability
  - b. reduce network traffic
  - c. increase security
  - d. decrease system maintenance
  - e. **all of the above**
49. RSA provides
- a. authentication
  - b. encryption
  - c. **authentication and encryption**
  - d. intrusion detection
  - e. packet filters
50. The RSA public/private key mechanism is:
- a. a DSA implementation
  - b. **asymmetric**
  - c. symmetric
  - d. a digital certificate
  - e. none of the above

### Short Answer (5 points each)

Answer / respond to the problems below, being as specific, clear, and complete as possible. Use correct terminology. Partial credit will be given for good and reasonable attempts, however, no credit will be given for clearly nonsensical responses.

51. Explain subnetting.

Subnetting is internally subdividing a larger network into several smaller networks by using some upper host bits as part of the network address, thus reducing the amount of hosts/network. This is accomplished by using a subnet mask.

52. Describe the difference between routing and routing protocols.

Routing is the forwarding of packets from network to network. Routing protocols exchange routing information amongst routers in support of dynamic routing.

53. Compare and contrast UDP vs TCP.

Both UDP and TCP are TCP/IP transport level protocols. UDP is a lightweight, efficient, connectionless protocol. The protocol is reliable, but packet delivery not guaranteed. TCP is a connection-oriented protocol and though Positive Acknowledgement and Retransmission (PAR), packet delivery is guaranteed. Because a connection is required, TCP is initially more expensive.

54. Explain and describe unicast, broadcast, and multicast addressing.

All three are IP addressing modes. A packet addressed to a single, specific host is a unicast packet. Broadcast packets are addressed to all hosts on the directly attached network, and multicast packets are delivered, through routers, to all subscribed hosts.

55. The 144.133.0.0/16 network has been subdivided into /18 networks. What is the broadcast address for each network?

Since two bits have been used for the subnet, there are four possible subnets. The broadcast address for each subnet is the subnet's network address with all the host bits set to 1. The network addresses of these subnets are: 144.133.0.0, 144.133.64.0, 144.133.128.0, 144.133.192.0. Thus, the broadcast addresses would be: 144.133.63.255, 144.133.127.255, 144.133.191.255, 144.133.255.255.

56. Explain the necessity of the yppasswdd daemon.

The yppasswdd daemon is necessary when the password database (/etc/passwd) is shared via NIS, and you want users to be able to change their passwords from NIS clients. The normal passwd command is not NIS aware, and as such, would attempt to change the local /etc/passwd file. Users must use yppasswd to change NIS passwords. And yppasswd contacts yppasswdd on the server to change the master /etc/passwd file. Without yppasswd/yppasswdd, users must log into the master NIS server to change passwords (and this is typically discouraged or disallowed).

57. Since IP can only deliver packets to hosts directly connected on the physical network, explain how a packet ultimately reaches its destination on other physical networks.

Packets reach other networks through routers which are connected to two or more physical networks. Packets that are destined for hosts on the local network are addressed to those hosts directly. Packets for hosts on remote networks are directed to a local router for forwarding. This is accomplished by IP which leaves the destination IP address to that of the remote destination host, and sets the destination MAC address to that of the router. The router picks up the packet, and forwards if it contains an appropriate route.

58. Explain the issue(s) regarding DHCP and DNS.

DNS translates hostnames to IP addresses and vice versa. This translation is essentially static, and is a table driven process (via zone files). DHCP is typically used for assigning dynamically generated IP addresses to hosts. Since a DHCP client's IP address may change, but its hostname does not, there is no way to use DNS to lookup a hostname and obtain the DHCP-generated IP address. It is only with the extension to DNS called DDNS, and with modifications to DHCP, that DHCP could notify a DDNS server of a host's hostname/IP address pairs.

Name \_\_\_\_\_

59. What security risk is posed by ICMP redirects?

ICMP redirects are messages sent by routing systems to clients to update their routing tables with more direct routes. A trusting host blindly installs the new route. A malicious routing system could send an ICMP redirect request to a host, redirecting the host's traffic through itself for nefarious or illegitimate purposes.

60. Explain the reverse branch of DNS.

The reverse branch in the DNS namespace tree is used for IP address to hostname lookups. This form of reverse lookup is used by software such as sendmail to assist in the prevention of IP spoofing. The branch is organized with arpa as the TLD, in-addr.arpa as the domain, and the byte-oriented network numbers as sub-domains. The most significant portion of the network address is at the top of the tree, while the least significant portion is towards the bottom. For example, the class C network address 200.100.50.0 would be in the 50.100.200.in-addr.arpa.