ProProfs Comptia Network+ Cram Sheets

Sneak Peek: Network+ Cram Notes & Guide

Welcome to Network+ Cram Notes! This brief guide should assist you in your path to Network+ certification, offering insight into the kind of key points frequently tested on the exam. Many obscure facts show up time and time again, and though they will seldom be found useful “in real life,” CompTIA continues to test on these points. Therefore, you should have a strong, working knowledge of the information in this Sneak Peek guide; the information in here can be considered as a “cram” guide and not a complete study guide, so it is still recommended that you read our study guide before reading this Sneak Peek.

The best way to utilize these Network+ cram notes is to read it several times, especially right before the exam itself. It is definite that you will find questions on the exam that cover points found only in the cram notes, so make sure you can understand and comprehend each individual point – it could be the one that makes the difference between a passing and failing score (but let's hope not).

Topologies

- Associate easy management, centralization, and Ethernet (802.3) with the Star topology (each node has a media connection to a hub).
- Associate fail/chokepoints, terminating ends (terminators), and tokens with the Token Bus and Token Ring topologies.
- Remember that the Mesh topology provides the most redundancy because every node has a direct connection to every other node. Ad-hoc mode in Wireless networks features this kind of topology, though it is not physical per se.
- Another name for a Mesh network is a "peer-to-peer network;" this terminology is not exclusive to file sharing, either.
- 10Base2 is usually a kind of Token Bus network, while 10BaseT is usually in the form of a Star network.
- On Token networks, data is passed from each node physically connected between two communicating hosts. Therefore, a break in a token bus or ring network could lead to total network failure. In comparison, a break in a Star network media would only lead to the lack of availability of the host connected to the hub.

Media

- Plenum grade cabling provides protection from the elements, and in particular, fire. Non-plenum-cabling (i.e. most cabling) does not provide such protection. Plenum cabling is usually employed in places where the risk of fire hazard is more common, such as the ceiling or between stories in a building. It is also used in mission-critical applications.
- Normal 10/100/1000BaseT or TX cable has a maximum length of 100 meters, but this can be extended with the use of a powered hub or a simple repeater.
- EMI : Electromagnetic interference also called RFI, can be radiated or conducted. It is any electromagnetic energy released by an electronic device that disrupts the operation or performance of another device. EMI is produced by many sources commonly found in an office environment, including fluorescent lights, photocopiers, and motors such as those used in elevators. EMI is also produced by natural atmospheric or solar activity, which can interfere with satellites, GPS devices and radio transmissions. Fiber optic cabling does not experience EMI because fiber optic cabling uses light rather than electrical current to send a signal.
- Category 5 UTP cable

"Patch" cable is used to connect a node to a router, switch or hub.

Crossover, or XO, cables allow for a direct node-to-node connection without the use of a hub or switch.

XO and patch cables look similar, but if you look closely at the RJ45 plugs, the wires on a patch cable are in the same order at both ends, whereas with a XO cable the wires on pins 1,2 and 3,6 will swap. When looking at the RJ45 from the top (so that your looking at the gold contacts, not the plastic tab or the end), pin 1 is on the left.

Equipment

- Modems are typically designated V.XX, and most modern modems are V.90 or higher
- A Hardware Loop allows for network card diagnostics on a PC
- Active hubs act as repeaters (are powered) and can strengthen a signal "on the wire" so the signal can continue further. Passive hubs, in contrast, are not powered and thus cannot strengthen a signal.
- Servers provide resources for users. Workstations, or PC's, allow users to access servers.
- Static routing requires the most administrative overhead because it requires that administrators constantly update the routing tables.
- Every NIC has a unique physical MAC address.
- Modems and CSU/DSU can provide hardware loopback capability.

TCP/IP and Related Technologies

- Remember your common ports! In particular, you should know that:
  - Trojan horses (backdoors) tend to use uncommon, high-range TCP/UDP ports like TCP 27374 or UDP 12345. Therefore an open connection to such a port usually indicates that a Trojan horse or backdoor is connected through that port.
  - Port numbers are specific to their respective protocols; for example, TCP and UDP port 21 offer different services on many servers.
  - If a service isn't working and the server is behind a NAT, it is likely that the NAT is blocking requests on the service port.
- IPv4 addresses are 32 bits, or four 8-bit octets, in the form X.X.X.X. IPv6 addresses are 128 bits and utilize hexadecimal numbering.
- IP addresses can be automatically assigned with a DHCP server. Windows 2000, Mac OS X, and most Linux distributions include such a server.
- Subnets allow a single physical network segment to be sub-networked into multiple logical network segments. For example, a subnet mask of 255.255.255.142 could create two segments, one from 192.168.1.1 to 192.168.1.142 and the other from 192.168.1.143 to 192.168.1.254. In other words, Subnetting changes the configuration of an IP network so that it treats the node and network number differently.
- A private IP address is an IP address used only within a LAN. It cannot be used to identify a unique node on the wider Internet or WAN. A public IP address can be used to identify such a node. In many network setups, private IP addresses are employed “behind the NAT” while the gateway connected to the NAT owns the public IP address for the whole network.
- ARP maps Layer 3 Network IP addresses to Layer 2 Data Link MAC addresses. RARP does the opposite.

- Note that to establish a connection to or from a specific service or server, such as a file server or a web server, a “port” for communication must necessarily be opened on the server so that outside nodes can connect and communicate with the server. So, for example: Assume you have an existing, working web server and add HTTP over SSL (HTTPS) capacity. If your clients cannot connect via HTTPS, the port for communication (TCP 443) is probably being blocked by your router to the Internet or some other firewall.

- DHCP is the service that allows for automatic IP address and IP information assignment. If you do not have a DHCP server, you would configure the IP address information on each node manually.

- UDP and IP are connectionless protocols. TCP is connection-oriented.

- The broadcast address, so that a node can send a packet to all other nodes on the network, is 255.255.255.255.

Tools

- A wire media tester can test the integrity of media that utilizes any kind of electronic signal. Optical media testers (fiber media testers), in contrast, can test the integrity of media that uses an optical signal.

- Crimpers can be used to crimp or attach connectors to media; for example, a network administrator might use a crimper to attach a standard RJ-45 connector to CAT5 media.

- Anytime the word “loopback tester” is employed, it refers to the testing of the output of a network device. For example, a hardware loopback tester tests the output of a NIC.

- Punch-down tools are used to attach media to outlets or patch panels.

- A Reflectometer can be used to find kinks or breaks in media.

- Tone generators can be used to identify media by tone as well as verify the integrity of a connection.

WAN

- High-speed WAN connections that use fiber-optic cabling are least vulnerable to "vampire" tapping (packet sniffing) and are considered highly secure.

- An ISDN connection has two 64 Kbps. channels for a total connection speed of 128 Kbps.

- The IANA determines the ownership and usage of Public Network (Internet) IP addresses.

- POTS, or dialup, utilizes a modem for an easily available, affordable, but slow connection to the Internet.

Redundancy and Fault Tolerance

- Remember that fault tolerance refers to the ability of the network/system to maintain availability and service even when some components of the network fail.

- Redundancy typically comes in the form of multiple servers that perform the same basic function. In other words, a redundant email system might feature two servers both running the same email software so that if one fails, the other one remains running.

- RAID can be used to ensure redundancy and fault tolerance. RAID 0 provides no such services, RAID 1 provides disk mirroring and fault tolerance, and RAID 5 provides disk striping.
- Disk striping is a feature that allows a disk drive to span across multiple physical or logical disks for increased redundancy.
- Disk mirroring is a feature that allows for a disk drive to have an exact replica in the form of another logical or physical disk drive.

Remote Access and Tunneling

- Kerebos is a security suite that utilizes “tickets” for authentication. It is best known for its role in UNIX authentication though it is oftentimes used in Windows-based authentication these days as well.
- PPP is used in the majority of home dial-up connections as it provides easy remote access over TCP/IP, which allows for home access to the resources of the Internet.
- PPTP is a tunneling version of PPP.
- IPSec is a standardized framework for securing Internet Protocol (IP) communications by encrypting and/or authenticating each IP packet in the data stream. It is a Network layer feature that allows for encryption between remote hosts. It is used in L2TP. IPsec is an obligatory part of IPv6, and is optional for use with IPv4.
- SSL, or Secure Sockets Layer, allows for the encryption of data between remote hosts on the Internet and is commonly employed with HTTP, where it is known as HTTP over SSL with the common prefix “https”

Operating Systems and Networking

- Remember that Microsoft Windows networking tends to support the TCP/IP suite as well as NetBIOS (and therefore NetBEUI)
- Active Directory is Microsoft's version of LDAP
- Novell tends to support IPX/SPX, though they are moving away from this
- Nix operating systems (Unix and Linux) tend to support TCP/IP
- Unix operating systems support NetBIOS and the Windows Browser Service through an open source suite known as SAMBA
- RAS is an almost Microsoft-exclusive remote access (dial-in networking) service
- Newer versions of Windows (including XP) have a built-in Firewall suite that mainly works to block traffic on certain ports rather than analyze actual traffic

Review Tables

Review Table: Media Information

Media Name	Cable Type	Max Length	Speed	Connector
10Base2	Coaxial	185m.	10 Mbps.	BNC
10BaseT	CAT 3+ Twisted pair	100 m.	10 Mbps	RJ45
10BaseFL	Fiber optic	2000 m.	10 Mbps	ST
100BaseTX	CAT5 Twisted pair	100 m.	100 Mbps	RJ45
100BaseFX	Fiber optic	2000 m.	100 Mbps	ST or SC
1000BaseT AKA "Gigabit Ethernet"	CAT5 Twisted pair	100 m.	1000 Mbps	RJ45
X GBase (etc.)	Fiber optic or laser	2000 - 5000 m.	Variable	SC

ProProfs Comptia Network+ Cram Sheets

Review Table: OSI Model

Name of Layer	Associate With	Examples
1 Physical	Media, topologies	Repeaters or wires and cabling
2 Data Link	802.3 Ethernet, MAC sublayer	NIC, Switch, ARP protocol
3 Network	Routing, Internetworking, Subnetting, connection-less	IP protocol, router
4 Transport	End-to-end connection, connection-oriented	TCP protocol, tunneling
5 Session	Connection management, quality of service	Encrypted tunneling, Duplex
6 Presentation	Translation from "networking" packets to computer-understandable data	Encryption, compression, character conversion
7 Application	Everything else, including most human applications and readable formats	HTTP, FTP, POP3 protocols; database, flow control, etc.

Review Table: Frame Type Numbers

Standard Number	Association	Examples
802.1	Internetworking	General standard that covers other ones
802.2	LLC (sub-layer of Layer 2 Data Link)	Acts as translator between higher-layer and physical layer
802.3	Ethernet CSMA/CD	Allows multiple access and automatic collision detection, key features of a standard Ethernet network
802.4	Token Bus LAN	Defines standards for a token bus topology network
802.5	Token Ring LAN	Defines standards for a token ring topology network
802.6	MAN (Metropolitan Area Network)	Wide-scale network over a large metropolitan area, between LAN and WAN, limited geographically
802.7	Broadband technology	Standards for WAN via high-speed broadband
802.8	Fiber Optic technology	Defines standards for connections via fiber optic media
802.9	Voice and Data	Standards for Voice over IP
802.10	Security	Largely unused standards defining network security options
802.11	Wireless	Defines standards for connecting via wireless; includes 802.11a, b, g, and now n

Review Table: Common Port Numbers

Port Number	Name and/or Use
TCP 20-21	FTP
TCP 22	SSH
TCP 23	Telnet
TCP 25	SMTP (Sendmail)
UDP 69	TFTP
TCP 80	HTTP
TCP 110	POP3
TCP 443	SSL

ProProfs Comptia Network+ Cram Sheets

Review Table: IP Addressing

Type	Range	Default Subnet	Reserved Range
Class A	1.0.0.0 - 126.254.254.254	255.0.0.0	10.0.0.0 - 10.254.254.254
Loopback	127.0.0.0 - 127.254.254.254	N/A	127.0.0.0 - 127.254.254.254 (All reserved)
Class B	128.0.0.0 - 191.254.254.254	255.255.0.0	172.16.0.0 - 172.31.254.254
Class C	192.0.0.0 - 223.254.254.254	255.255.255.0	192.168.0.0 - 192.168.254.254

Review Table: 10 protocols to remember of the TCP/IP suite

Name	Layer	Function
TCP	4 Transport	Connection-oriented, guaranteed delivery
IP	3 Network	Connectionless, unreliable delivery; used to establish TCP connections and for addressing
ARP	2 Data Link	Translates IP addresses into MAC physical addresses
FTP	7 Application	Transferring files
RIP	3 Network	Used for routing between different inter-networks
HTTP	7 Application	Web pages and web sites
UDP	4 Transport	Connectionless, unreliable, quick, best-effort delivery
ICMP	3 Network	Networking troubleshooting with tools like PING, TRACERT
POP3	7 Application	Used to receive Email
SMTP	7 Application	Used to send Email