How does traceroute work?
It works with UDP, ICMP echo requests, and TTL. Packets are sent with headers that contain information such as SRC and DST for IP and port. Whenever a router forwards a packet to the next hop, it decrements the TTL value of the packet (this prevents infinite routing loops). Whenever a packet has its TTL field decremented to 0 and is thus dropped for good, the router that does that action also communicates back to where it received the packet from, and says "I dropped this packet" -- and of course that reply back has header information in it that describes the router. So traceroute first sends a packet with TTL 1; then it sends a packet with TTL 2; then TTL 3; and etcetera. This is how traceroute crawls through router after router to get the info of each router. Certain networks and routers may be configured to not respond to ICMP. But when and where it works, traceroute tells you the path to get to the final host or IP in question, the names and identities of routers and devices along the path, and network latency between each hop.

What are some different kinds of ICMP packets?
ECHO
REDIRECT
DEST_UNREACH
TIME_EXCEEDED

Those are good to know. REDIRECT is a good one to block in firewall configurations. Other ICMP packets include router advertisements/solicitations, address mask request/reply, ...

Name some tools useful for troubleshooting when another host goes down?
Ping, traceroute, arp, nslookup, dig, ifconfig, ethtool, host, route, netstat, mtr, tcpdump, wireshark,

What packets involved in establishing a TCP session, with "the handshake"?
SYN, SYN+ACK, ACK
There will also be TCP sequence numbers.

What packets involved with closing a TCP session?
FIN, FIN+ACK, ACK
There will also be TCP sequence numbers.

What about for UDP?
Trick question -- there are no stages for this, because it is unreliable.

Where do DNS client settings for a linux host reside?
/etc/hosts
/etc/resolv.conf
nsswitch.conf
/etc/named.conf (old, redhat 5)

What's the difference between nslookup, host, and dig?
dig uses the OS resolver libraries. *nslookup* uses its own internal libraries.
Both commands do basically the same thing, but they have different formatting for the output.
dig, nslookup, and *host* are very similar to what they do.

What is the arp command?
Address Resolution Protocol. Display/modify the ARP cache. An ARP cache is a mapping of IP addresses to MAC addresses.

How would you exclude SSH traffic from a tcpdump output?
"not port 22"
"tcpdump -i eth1 port not 22 and host 1.2.3.4"

In wireshark, if you wanted to filter out netbios or dns protocols, you could have… *!(netbios or dns)*

What's the difference between OSPF and RIP?
RIP == Routing Information Protocol. OSPF == Open Shortest Path First. RIP builds a routing table using hops and metrics from one specific (neighboring) router, while OSPF has routers advertising themselves and their adjacent routers, and so it offers a more complete topological database. OSPF is more scalable and mitigates the risk of "hop loops", but RIP is more efficient. RIP is a "distance vector routing protocol", and OSPF is a "link state routing protocol". RIP is ok for small networks; OSPF is better for larger networks (more than 5 routers, for example).

What are some load balancing techniques?
Round robin
Least-connection
Weighted round robin
Weighted least connection
Bandwidth and load based
Random
Least traffic
Least latency

If you manage hardware, let's say a server crashes and reboots; how do you determine what happened?
Check logs…
/var/log/messages or /var/log/kernel
last log (it could show if anyone logged in at the time, or show if there was a OS-handled reboot)
Check disk space if it's full
Check dmesg if it returns hardware errors at last boot time
Check if there are any crash dump files
Check application logs
Try a fsck
If server has a RAID array, do the RAID diagnostics find anything?
Check with the NOC or other teams?

If you were to make a basic monitoring system for a multi-tier web application, what are some things you'd choose to monitor?
Per node disk space, CPU, per process CPU usage (for critical processes), per process memory usage, swap usage, node and cluster disk I/O, power and cooling traps on servers, per node and interface NIC throughput, number of active TCP connections, network connectivity between tiers, application-specific connectivity between tiers, database connections and pooling, error and warning messages in logs, SSL certificate expirations, ……

How would you add a user for sudo access?
adduser michaelscott

(ubuntu way)

usermod -aG sudo michaelscott

another way, if you want to grant it with specific group (wheel group)
visudo
%wheel ALL=(ALL) ALL
usermod -Ag wheel michaelscott

sudo whoami

How would you debug a broken cron job?
crontab -l
crontab -e
check /var/spool/cron
run the script manually, check the crontab for any custom env settings, run the cron with output saved to a file (instead of the default of email, which might also be broken)

Time management behavioral questions:

- Was there ever a time where you needed to pick up the pace? What was going on at the time?
- Was there a time when you worked against deadlines and you didn't have time to consider all options before making decisions? What was the result of your actions?
- Can you describe a time when you had to think through several different options to a problem? How did you arrive to your preferred solution?

How do you approach a new project?

- Outline the scope and timeline
- Outline stakeholders and communicate with them
- Draft a plan and share it, requesting feedback
- Communicate early, communicate often
- Schedule meetings (kick off, milestone, sprint planning, kaizen explorations) to set expectations and be in the loop on progress and to find opportunities for improvement
- Always take detailed notes about everything and share them
- Organize in JIRA -- tags, "Fixed Version", sprint version, kanban, is related to, time spent on, story points, priority, planned to be finished on, …

What is your style for every day on the job work?
I ask for clarification when needed. I take a logical approach to things. I take care to reduce impact to customers. I experiment on a small scale before going large-scale. I always have an "undo" plan, a rollback plan. I communicate about changes or happenstances, especially to affected parties. I seek review from peers. I don't make it a habit to always ask permission for things, but I also do not make knee-jerk reactions.

What happens when you connect to a website from your web browser?

- Resolve IP for www.google.com
- ARP broadcast query from your host to resolve the ethernet address for the configured name server
- Name server responds with its ethernet address
- Host then sends a DNS query to the NS, to resolve hostname
    - port 53 UDP for DNS; the query is of type "A" (host address)
- Get a response to the host address query, and that the response was authoritative

- Send a HTTP request for a document, to the server IP address that was retrieved from the DNS response
    - Do TCP handshake to establish connection
        - First, send SYN packet with a sequence number and 0 bytes in the data segment; also has another field for an acknowledgement number
        - Get back an acknowledgement number, and ack back -- handshake complete
- HTTP request and HTTP response!
- Browser then parses HTML, CSS, JavaScript, and downloads images from cross-origin and CDN sources

What are load balancers?
Load balancers help you scale out horizontally. For example, you can spin up a dozen worker nodes

How many hosts can you have in a /23 network?
Twenty-three 1s in the netmask: 11111111.11111111.11111110.00000000
It is two class C networks. A class C network, a common one, is /24, which is 2^8 = 256; but you typically subtract two for the broadcast address and network address which are reserved (or subtract 5 for an AWS subnet!). So 2 * 255 = 510 host addresses available in a /23. You could also simplify this to 32 - 23 = 9, and 2^9 = 512.

What is a hypervisor?
Examples: Xen, VMWare, VirtualBox. Hypervisors are a privileged abstraction layer between hardware and OS. They…:

- Define virtual machines with virtual hardware
- Grant portions of physical resources to each guest VM
- Export simplified devices to guests
- Enforce isolation among guests

A weakness with traditional hypervisors is that they require a full-blown OS installation in each guest VM, whereas containerization tools like Docker and Kubernetes can squeeze more compute density out of a physical server, because its guests (containers) do not need full operating systems installed in each container.

What is the OSI networking model?

1. Physical
2. Data link
3. Network
4. Transport
5. Session
6. Presentation
7. Application

What is noatime in Linux?
If a filesystem is mounted with ‘noatime’, such as can be described in */etc/fstab* , then Linux will not record access time or when files in that system were created/modified. Because of this, performance is improved. Use this for filesystems where files are frequently accessed and changed.
You can also set ‘noatime’ for a specific directory tree:
chattr -R +A /var/spool

What is the sync command in Linux?

Synchronize data on disk with memory; write out any data buffered in memory out to the disk. This is good to do before you do something that might cause the system to crash. When you issue a shutdown or reboot, part of the subcommands that the OS will run include the sync command.

What does the 'count' entry in an inode track?
How many times has the file been opened without closed (how many references still active?)
What if you try to truncate a big log file to try reclaim disk space, but the space doesn't reappear? A way to debug is to see what process might have the data part still open -- if so, then the OS won't release the space until the process closes it. So look at the count entry in an inode and look at lsof

What is umask in Linux?
umask dictates what is a user's default permissions when creating files. Use the umask command to set the default mode for newly created files. It takes as argument a 3-digit code to represent the access to be inhibited (masked out). If you want all new files to automatically have the permission mode 751, then set umask to 026 (because 777 - 751 = 026).

You can put a umask command in the system init file to set a default for all users. You can also set your own umask in your shell setup files to override defaults.

What is setuid?
Some executable files can have an *s* instead of an *x* in the permission listing, which would indicate that the setuid is set. This flag makes it so that the file is run as the owner, instead of you. A program might use this setuid bit to run as root, in order to always have special privileges. The setuid bit is aka mode 4000.
chmod u+s /home/dgibney/myscript.sh
chmod 4755 /home/dgibney/myscript.sh
chmod u-s /home/dgibney/myscript.sh

What is setgid?
AKA mode 2000. This sets the group ID. When a file is created, it normally belongs to the primary group of the user that created it; however, if the setgid bit is set on the directory in which a file is to be created, then new files created will have their group ownership set to the same group as the directory's owner. This allows a level of access to group members while allowing different access to non-group members.
chmod 2755 /home/share -- sets the SGID flag
chmod g-s /home/share -- removes the SGID flag

What is Sticky Bit?
AKA mode 1000. Set the sticky bit to prevent users from deleting others' files, even if they might have full access to the directory. The owner of a directory should set its sticky bit; this way, only the owner and superuser can rename/remove files in that directory.

chmod o+t /home/share