* What is HTTP?

The Hypertext Transfer Protocol (HTTP) is an application protocol for distributed, collaborative, hypermedia information systems.[1] HTTP is the foundation of data communication for the World Wide Web.

Hypertext is structured text that uses logical links (hyperlinks) between nodes containing text. HTTP is the protocol to exchange or transfer hypertext.

[Read More](https://en.wikipedia.org/wiki/Hypertext_Transfer_Protocol)

* What is an HTTP proxy and how does it work?
* Describe briefly how HTTPS works.
* What is SMTP? Give the basic scenario of how a mail message is delivered via SMTP.
* What is RAID? What is RAID0, RAID1, RAID5, RAID10?
* What is a level 0 backup? What is an incremental backup?
* Describe the general file system hierarchy of a Linux system.

**[[⬆]]Simple Linux Questions:**

* What is the name and the UID of the administrator user?

Name - root

UID - 0

Can check with command:

$ id root

uid=0(root) gid=0(root) groups=0(root)

* How to list all files, including hidden one, in a directory?

ls - command ti list directory contents

a - argument show hidden files in a directory

Full command:

$ ls -a ./

* What is the Unix/Linux command to remove a directory and its contents?

rm - command to remove files or directories

r - argument tp remove directories and their contents recursively

Full command:

$ rm -r ./somedir

* Which command will show you free/used memory? Does free memory exist on Linux?

free - command to display amount of free and used memory in the system

Full command:

$ free

total used free shared buffers cached

Mem: 1551836 1048324 503512 0 324244 518224

-/+ buffers/cache: 205856 1345980

Swap: 731132 0 731132

* How to search for the string “my konfi is the best” in files of a directory recursively?

You can use find and grep command.

Full command:

$ find ./\* -type f -exec grep -H 'my konfi is the best' {} \;

$ grep -r 'my konfi is the best' ./\*

[Read More](https://stackoverflow.com/questions/16956810/finding-all-files-containing-a-text-string-on-linux)

* How to connect to a remote server or what is SSH?

Secure Shell, or SSH, is a cryptographic (encrypted) network protocol to allow remote login and other network services to operate securely over an unsecured network.

To connect to remote server we can use command ssh

Full command:

$ ssh login@remote\_server\_ip

[Read More](https://en.wikipedia.org/wiki/Secure_Shell)

* How to get all environment variables and how can you use them?

All UNIX-like operating systems such as OpenBSD, Linux, Redhat, CentOS, Debian allows you to set environment variables. When you log in on UNIX, your current shell (login shell) sets a unique working environment for you which is maintained until you log out.

printenv\env - command to print all or part of environment

Full command:

$ printenv PATH HOME

$PATH - Display lists directories the shell searches, for the commands.

$HOME - User's home directory to store files.

All environment variables you can use in scripts.

[Read More](http://www.tutorialspoint.com/unix/unix-environment.htm)

* I get “command not found” when I run ifconfig -a. What can be wrong?

Possible causes:

1. net-tools package is not installed in your system.

2. you don`t have "/sbin" directory in your $PATH, so just write full path for command - /sbin/ifconfig -a

* What happens if I type TAB-TAB?

It depends where you are type this.

If we are talking about shells like bash\zsh, so you type TAB-TAB it will enable built in "completion" function.

Most shells allow command completion, typically bound to the TAB key, which allow you to complete the names of commands stored upon your PATH, file names, or directory names. This is typically used like so:

$ ls /bo[TAB]

When you press the TAB key the argument /bo is automatically replaced with the value /boot.

[Read More](https://www.debian-administration.org/article/316/An_introduction_to_bash_completion_part_1)

* What command will show the available disk space on the Unix/Linux system?

df - report file system disk space usage

Simple run command and you will see available disk space in your system

$ df -h

* What commands do you know that can be used to check DNS records?

$ host [example.com](http://example.com/)

$ nslookup [example.com](http://example.com/)

$ dig [example.com](http://example.com/)

$ python -c "import socket;print(socket.gethostbyname('example.com'))"

* What Unix/Linux commands will alter a files ownership, files permissions?

chown - command to change file owner and group information.

chmod - command to change file access permissions such as read, write, and access.

* What does chmod +x FILENAMEdo?

This command will set executation bit to FILENAME for everybody owner\group\other.

* What does the permission 0750 on a file mean?

$ chmod 750 FILENAME

-rwxr-x--- 1 root root 24 Jan 22 18:02 FILENAME\*

This permissions means that owner can read\write\execute this file, also members of group can read and execute, other users can do nothing with it.

* What does the permission 0750 on a directory mean?

$ chmod 750 DIRECTORY

drwxr-x--- 5 root root 4.0K Nov 10 12:36 DIRECTORY

This permissions means that owner can read\write\execute(see file list of directory) this directory, also members of group can read and list, other users can do nothing with it.

* How to add a new system user without login permissions?
* How to add/remove a group from a user?
* What is a bash alias?
* How do you set the mail address of the root/a user?
* What does CTRL-c do?
* What is in /etc/services?
* How to redirect STDOUT and STDERR in bash? (> /dev/null 2>&1)
* What is the difference between UNIX and Linux.
* What is the difference between Telnet and SSH?
* Explain the three load averages and what do they indicate.

To see load averages numbers you can run commands:

$ top (see load average section)

$ cat /proc/loadavg

1.00 1.01 0.98 2/198 21533

$ uptime

18:37:28 up 4 days, 7:17, 4 users, load average: 1.00, 1.01, 0.98

The three numbers after load average - 1.00, 1.01, 0.98 - represent the 1-, 5-, and 15-minute load averages on the machine. A system load average is equal to the average number of processes in a runnable or uninterruptible state. Runnable processes are either currently using the CPU or waiting to do so, and uninterruptible processes are waiting for I/O.

[Read More](https://en.wikipedia.org/wiki/Load_(computing))

**[[⬆]]Medium Linux Questions:**

* What do the following commands do and how would you use them?
* tee

tee - read from standard input and write to standard output and files

For example you can use this command like this:

$ echo "deb <http://pkg.jenkins-ci.org/debian> binary/" | sudo tee -a /etc/apt/sources.list.d/jenkins.list

* awk

The awk is most useful when handling text files that are formatted in a predictable way. For instance, it is excellent at parsing and manipulating tabular data. It operates on a line-by-line basis and iterates through the entire file.

The awk syntax looks like this:

awk '/search\_pattern/ { action\_to\_take\_on\_matches; another\_action; }' file\_to\_parse

For example you can use this command like this:

$ awk '{print}' /etc/fstab

* tr

We can use tr for translating, or deleting, or squeezing repeated characters.

It will read from STDIN and write to STDOUT.

For example you can use this command like this:

$ tr a-z A-Z

$ tr '()' '{}'

* cut

The command cut is used for text processing.

We can use this command to extract portion of text from a file by selecting columns.

cut OPTION... [FILE]...

For example you can use this command like this:

The example displays only the first field of each lines from /etc/passwd file using the field delimiter : (colon). In this case, the 1st field is the username.

$ cut -d ':' -f 1 < /etc/passwd

* tac

tac (which is "cat" backwards) concatenate and print files in reverse

For example you can use this command like this:

$ cat ok

1

2

3

$ tac ok

3

2

1

* curl

Curl is a tool to transfer data from or to a server, using one of the supported protocols (DICT, FILE, FTP, FTPS, GOPHER, HTTP, HTTPS, IMAP, IMAPS, LDAP, LDAPS, POP3, POP3S, RTMP, RTSP, SCP, SFTP, SMTP, SMTPS, TELNET and TFTP). The command is designed to work without user interaction.

For example you can use this command like this:

$ curl [https://example.com](https://example.com/)

* wget

Wget is a free utility for non-interactive download of files from the Web.

It supports HTTP, HTTPS, and FTP protocols, as well as retrieval through HTTP proxies.

Wget is non-interactive, meaning that it can work in the background, while the user is not logged on.

This allows you to start a retrieval and disconnect from the system, letting Wget finish the work.

By contrast, most of the Web browsers require constant user's presence, which can be a great hindrance when transferring a lot of data.

For example you can use this command like this:

$ wget -S [https://example.com](https://example.com/)

* watch

watch runs command repeatedly, displaying its output and errors (the first screenfull). This allows you to watch the program output change over time. By default, the program is run every 2 seconds. By default, watch will run until interrupted.

For example you can use this command like this:

To watch the contents of a directory change, you could use

$ watch -d ls -l

* head

Print the first 10 lines of each FILE to standard output.

With more than one FILE, precede each with a header giving the file name.

With no FILE is read standard input.

For example you can use this command like this:

To print first 10 lines

$ head /etc/passws

* tail

Print the last 10 lines of each FILE to standard output.

With more than one FILE, precede each with a header giving the file name.

With no FILE is read standard input.

For example you can use this command like this:

To print last 10 lines

$ tail /etc/passws

* What does a & after a command do?

This is known as job control under unix. The & informs the shell to put the command in the background.

This means it continues to run the command but returns you to your shell to allows you to continue doing parallel commands and do not have to wait until the script is finished. If you forget to add & after command, you can stop the current running process with Ctrl-Z and continue it in the background with bg (or in the foreground with fg).

[Read More](https://unix.stackexchange.com/questions/86247/what-does-ampersand-mean-at-the-end-of-a-shell-script-line)

* What does & disown after a command do?

& puts the job in the background, that is, makes it block on attempting to read input, and makes the shell not wait for its completion.

disown removes the process from the shell's job control, but it still leaves it connected to the terminal. One of the results is that the shell won't send it a SIGHUP. Obviously, it can only be applied to background jobs, because you cannot enter it when a foreground job is running.

[Read More](https://unix.stackexchange.com/questions/3886/difference-between-nohup-disown-and)

* What is a packet filter and how does it work?

Packet filters act by inspecting the "packets" which are transferred between computers on the Internet. If a packet does not match the packet filter's set of filtering rules, the packet filter will drop.

[Read More](https://en.wikipedia.org/wiki/Firewall_(computing))

* What is Virtual Memory?

In computing, virtual memory is a memory management technique that is implemented using both hardware and software. It maps memory addresses used by a program, called virtual addresses, into physical addresses in computer memory. Main storage as seen by a process or task appears as a contiguous address space or collection of contiguous segments. The operating system manages virtual address spaces and the assignment of real memory to virtual memory.

[Read More](https://en.wikipedia.org/wiki/Virtual_memory)

* What is swap and what is it used for?

Swap is a special type of memory.

Swap space in Linux is used when the amount of physical memory (RAM) is full. If the system needs more memory resources and the RAM is full, inactive pages in memory are moved to the swap space. While swap space can help machines with a small amount of RAM, it should not be considered a replacement for more RAM. Swap space is located on hard drives, which have a slower access time than physical memory.

Swapping is a useful technique that enables a computer to execute programs and manipulate data files larger than main memory. The operating system copies as much data as possible into main memory, and leaves the rest on the disk. When the operating system needs data from the disk, it exchanges a portion of data (called a page or segment) in main memory with a portion of data on the disk.

[Read More](https://www.centos.org/docs/5/html/5.2/Deployment_Guide/s1-swap-what-is.html)

* What is an A record, an NS record, a PTR record, a CNAME record, an MX record?
* Are there any other RRs and what are they used for?
* What is a Split-Horizon DNS?
* What is the sticky bit?

A sticky bit is a permission bit that is set on a directory that allows only the owner of the file within that directory or the root user to delete or rename the file. No other user has the needed privileges to delete the file created by some other user.

To remove sticky bit:

sudo chmod -t /tmp

To set sticky bit:

$ sudo chmod +t /tmp

[Read More](https://askubuntu.com/questions/432699/what-is-the-t-letter-in-the-output-of-ls-ld-tmp)

* What does the immutable bit to a file?
* What is the difference between hardlinks and symlinks? What happens when you remove the source to a symlink/ hardlink?
* What is an inode and what fields are stored in an inode?

inode is a "database" of all file information that tells about file structure.

The inode of each file uses a pointer to point to the specific file, directory or object.

The pointer is a unique number which usually is referred to as the inode number.

* Howto force/trigger a file system check on next reboot?
* What is SNMP and what is it used for?
* What is a runlevel and how to get the current runlevel?

Runlevel is a mode of operation in OS, and a runlevel represents the different system state of a Linux system. When the Linux system boots, the kernel is initialized , and then enters one (and only one) runlevel. When a service starts, it will try to start all the services that are associated with that runlevel.

In general, when a computer enters runlevel 0, the system shuts down all running processes, unmounts all file systems, and powers off.

When it enters runlevel 6, it reboots.

The intermediate runlevels (1-5) differ in terms of which drives are mounted, and which network services are started. Default runlevels are typically 3, 4, or 5.

Runlevel 1 is reserved for single-user mode-a state where only a single user can log in to the system. Generally, few processes are started in single-user mode, so it is a very useful runlevel for diagnostics when a system won't fully boot. Even in the default GRUB menu we will notice a recovery mode option that boots us into runlevel 1.

In other words, runlevels define what tasks can be accomplished in the current state (or runlevel) of a Linux system. Every Linux system supports three basic runlevels, plus one or more runlevels for normal operation.

Lower run levels are useful for maintenance or emergency repairs, since they usually don't offer any network services at all.

To check current runlevel:

$ runlevel

N 2

* What is SSH port forwarding?
* What is the difference between local and remote port forwarding?
* What are the steps to add a user to a system without using useradd/adduser?
* What is MAJOR and MINOR numbers of special files?
* Describe a scenario when you get a “filesystem is full” error, but ‘df’ shows there is free space.
* Describe a scenario when deleting a file, but ‘df’ not showing the space being freed.
* Describe how ‘ps’ works.
* What happens to a child process that dies and has no parent process to wait for it and what’s bad about this?
* Explain briefly each one of the process states.
* How to know which process listens on a specific port?
* What is a zombie process and what could be the cause of it?
* You run a bash script and you want to see its output on your terminal and save it to a file at the same time. How could you do it?
* Explain what echo “1” > /proc/sys/net/ipv4/ip\_forward does.
* Describe briefly the steps you need to take in order to create and install a valid certificate for the site [https://foo.example.com](https://foo.example.com/).
* Can you have several HTTPS virtual hosts sharing the same IP?
* What is a wildcard certificate?
* Which Linux file types do you know?
* What is the difference between a process and a thread? And parent and child processes after a fork system call?
* What is the difference between exec and fork?
* What is “nohup” used for?
* What is the difference between these two commands?
* myvar=hello
* export myvar=hello
* How many NTP servers would you configure in your local ntp.conf?
* What does the column ‘reach’ mean in ntpq -p output?
* You need to upgrade kernel at 100-1000 servers, how you would do this?
* How can you get Host, Channel, ID, LUN of SCSI disk?
* How can you limit process memory usage?

**[[⬆]]Hard Linux Questions:**

* What is a tunnel and how you can bypass a http proxy?

A tunnel is a mechanism used to ship a foreign protocol across a network that normally wouldn't support it. Tunneling protocols allow you to use, for example, IP to send another protocol in the "data" portion of the IP datagram. Most tunneling protocols operate at layer 4, which means they are implemented as a protocol that replaces something like TCP or UDP.

You can forward a port from your computer to a remote computer, which has the result of tunneling your data over SSH in the process, making it secure. This may not seem useful, after all, why would I want a port on my computer being forwarded to another computer? The answer lies within some clarification. The port forwarding function of SSH works by first listening on a local socket for a connection. When a connection is made, SSH will forward the entire connection onto the remote host and portable.

For example: 'ssh -L80:workserver.com:80 user@workdesktop.com'

This command creates an SSH connection to your [workdesktop.com](http://workdesktop.com/) computer, but at the same time opens port 80 on your local machine. If you point your web browser at [http://localhost](http://localhost/), the connection will actually be forwarded through your SSH connection to your desktop, and sent onto the [workserver.com](http://workserver.com/) server, port 80.

* What is the difference between IDS and IPS?

IDS - Intrusion Detection System - A device or application that analyzes whole packets, both header and payload, looking for known events. When a known event is detected a log message is generated detailing the event.

IPS - Intrusion Prevention System - A device or application that analyzes whole packets, both header and payload, looking for known events. When a known event is detected the packet is rejected.

* What shortcuts do you use on a regular basis?

A lot, for example check my dotfiles git <https://github.com/jivoi/dotfiles/blob/master/.aliases>

* What is the Linux Standard Base?

LSB is a project to standardize the software system structure, including the filesystem hierarchy used in the Linux operating system. The LSB is based on the POSIX specification, the Single UNIX Specification (SUS), and several other open standards, but extends them in certain areas.

[Read More](https://en.wikipedia.org/wiki/Linux_Standard_Base)

* What is an atomic operation?

For example we can say that atomic operation is a an operation during which a process can simultaneously read a location and write it in the same bus operation. This prevents any other process or I/O device from writing or reading memory until the operation is complete. Atomic implies indivisibility and irreducibility, so an atomic operation must be performed entirely or not performed at all.

* Your freshly configured http server is not running after a restart, what can you do?

If you rebooted server and http server is not running after it, so first you need to check it configuration file and the server error log where you can find the proble why server is not running, and after you can run it manually with init\upstart\systemd script, if you want that server run automatically you need enable autostart for it.

You can run one of this command:

$ chkconfig nginx on (for centos\rhel)

$ update-rc.d nginx enable (for debian\ubuntu)

$ systemctl enable nginx (for linux with systemd)

* What kind of keys are in ~/.ssh/authorized\_keys and what it is this file used for?

This is a public ssh key.

With public key authentication, the authenticating entity has a public key and a private key. Each key is a large number with special mathematical properties. The private key is kept on the computer you log in from, while the public key is stored on the .ssh/authorized\_keys file on all the computers you want to log in to.

[Read More](https://help.ubuntu.com/community/SSH/OpenSSH/Keys)

* I’ve added my public ssh key into authorized\_keys but I’m still getting a password prompt, what can be wrong?

Maybe your ~/.ssh/authorized\_keys permissions are too open by OpenSSH standards.

You need to check this and fix with:

chmod 700 ~/.ssh

chmod 600 ~/.ssh/authorized\_keys

Maybe remote server is configured to disable public keys, you can check it in /etc/sshd\_config configuration file where PubkeyAuthentication option must be set to YES

Maybe it is something with you local ssh configuration ~/.ssh/config

* Did you ever create RPM’s, DEB’s or solaris pkg’s?

For RPM you need to create a spec file

[Read More](https://fedoraproject.org/wiki/How_to_create_an_RPM_package) [Read More](https://wiki.debian.org/IntroDebianPackaging)

* What does :(){ :|:& };: do on your system?

This is a fork bomb using the Bash shell

In computing, a fork bomb (also called rabbit virus or wabbit[1]) is a denial-of-service attack wherein a process continually replicates itself to deplete available system resources, causing resource starvation and slowing or crashing the system.

We can rewrite this code in this way:

bomb() {

bomb | bomb &

};

bomb

The fork bomb in this case is a recursive function that runs in the background, thanks to the ampersand operator. This ensures that the child process does not die and keeps forking new copies of the function, consuming system resources.

[Read More](https://en.wikipedia.org/wiki/Fork_bomb)

* How do you catch a Linux signal on a script?

There is a trap command that allows you to catch a linux signal and execute a command when a signal is received by your shell script. It works like this:

$ trap arg signals

So in real script you can write somethins like this:

trap "rm $TEMP\_FILE; exit" SIGHUP SIGINT SIGTERM

Here we have added a trap command that will execute "rm $TEMP\_FILE" if any of the listed signals is received.

[Read More](http://linuxcommand.org/wss0160.php)

* Can you catch a SIGKILL?

SIGKILL or signal 9 is one signal that you cannot trap and catch. The linux kernel immediately terminates any process sent this signal and no signal handling is performed. Since it will always terminate a program that is stuck, hung, or otherwise screwed up, it is tempting to think that it's the easy way out when you have to get something to stop and go away.

* What’s happening when the Linux kernel is starting the OOM killer and how does it choose which process to kill first?
* Describe the linux boot process with as much detail as possible, starting from when the system is powered on and ending when you get a prompt.

The first step of the boot process is the BIOS (Basic Input Output System).

The BIOS initializes hardware, including detecting hard drives, USB disks, CD-ROMs, network cards, and any other hardware.

The BIOS will then go step-by-step through each boot device based on the boot device order it is configured to follow until it finds one it can successfully boot from. In the case of a Linux server, that usually means reading the MBR (master boot record: the first 512 bytes on a hard drive) and loading and executing the boot code inside the MBR to start the boot process.

After the BIOS initializes the hardware and finds the first device to boot, the boot loader takes over. The following list shows the boot loader depending on the device from a boot starts:

GRUB : boot from a hard drive

syslinux : boot from a USB

isolinux : boot from a CD-ROM

pxelinux : boot from a network

Once we select a particular kernel in GRUB, GRUB will load the Linux kernel into RAM and execute it.

Usually GRUB will also load an initrd (initial RAM disk) along with the kernel. initrd (initial RAM disk) has some crucial configuration files, kernel modules, and programs that the kernel needs in order to find and mount the real root file system.

The final step is to execute the /sbin/init program, which takes over the rest of the boot process.

The /sbin/init program is the parent process of every program running on the system. This process always has a PID of 1 and is responsible for starting the rest of the processes that make up a running Linux system.

Here is the list of how we initialize a NIX OS:

System V init such as runlevels and /etc/rc?.d directories - the init process reads a configuration file called /etc/inittab to discover its default runlevel. It then enters that runlevel and starts processes that have been configured to run at that runlevel. Linux distros: Debian 6 and earlier\Ubuntu 9.04 and earlier\CentOS 5 and earlier

Upstart - Upstart was designed not only to address some of the shortcomings of the System V init process, but also to provide a more robust system for managing services.

One main feature of Upstart is that it is event-driven. Upstart constantly monitors the system for certain events to occur, and when they do, Upstart can be configured to take action based on those events.

Upstart scripts reside in /etc/init. Linux distros: Ubuntu 9.10 to Ubuntu 14.10, including Ubuntu 14.04

CentOS 6

systemd is the init system for the most recent linux distros: Debian 7 and Debian 8\Ubuntu 15.04\CentOS 7

[Read More](https://en.wikipedia.org/wiki/Linux_startup_process)

* What’s a chroot jail?
* When trying to umount a directory it says it’s busy, how to find out which PID holds the directory?
* What’s LD\_PRELOAD and when it’s used?
* You ran a binary and nothing happened. How would you debug this?
* What are cgroups? Can you specify a scenario where you could use them?

**[[⬆]]Expert Linux Questions:**

* A running process gets EAGAIN: Resource temporarily unavailable on reading a socket. How can you close this bad socket/file descriptor without killing the process?

$ man errno | grep EAGAIN

EAGAIN is just means "there's nothing to read now; try again later".

**[[⬆]]Networking Questions:**

* What is localhost and why would ping localhost fail?

A localhost is the standard hostname given to the address assigned to the loopback network interface. Translated into an IP address, a localhost is always designated as 127.0.0.1.

Ping can fail if loopback interface is down, also it is possible to configure local iptables(firewall) in such a way as to drop all packets received on localhost.

Also it is possible that icmp\_echo is disable with sysctl net.ipv4.icmp\_echo\_ignore\_all=1

* What is the similarity between “ping” & “traceroute” ? How is traceroute able to find the hops.

Both of this programs can be used to troubleshoot connection problems.

Traceroute shows you the path that packets take from your local system to a remote host. You see the response time to each step along the way, because each datagram (Unix "traceroute" uses UDP datagrams by default, but you can also choose between ICMP, TCP rather than ICMP on Windows) has a TTL (time-to-live) that's one hop longer than the previous one.

By default you need a superuser privileges to run ping and traceroute with ICMP option

$ ping [example.com](http://example.com/)

ping: icmp open socket: Operation not permitted

$ traceroute -I [example.com](http://example.com/)

You have no enough privileges to use this traceroute method.

[Read More](https://serverfault.com/questions/68307/what-is-the-difference-between-ping-and-tracert)

* What is the command used to show all open ports and/or socket connections on a machine?

$ lsof -i

$ netstat -natupx

$ ss -lptuxa

* Is 300.168.0.123 a valid IPv4 address?

No, IPv4 addresses are canonically represented in dot-decimal notation, which consists of four decimal numbers, each ranging from 0 to 255, separated by dots, e.g., 172.16.254.1. Each part represents a group of 8 bits (octet) of the address. So 2 \*\* 8 = 256(255) is a max number for each octet.

[Read More](https://en.wikipedia.org/wiki/IP_address)

* Which IP ranges/subnets are “private” or “non-routable” (RFC 1918)?

The Internet Assigned Numbers Authority (IANA) has reserved the following three blocks of the IP address space for private internets:

10.0.0.0 - 10.255.255.255 (10/8 prefix)

172.16.0.0 - 172.31.255.255 (172.16/12 prefix)

192.168.0.0 - 192.168.255.255 (192.168/16 prefix)

[Read More](https://tools.ietf.org/html/rfc1918)

* What is a VLAN?

A virtual LAN (VLAN) is any broadcast domain that is partitioned and isolated in a computer network at the data link layer (OSI layer 2).

To subdivide a network into virtual LANs, one configures a network switch or router. Simpler network devices can only partition per physical port (if at all), in which case each VLAN is connected with a dedicated network cable (and VLAN connectivity is limited by the number of hardware ports available). More sophisticated devices can mark packets through tagging, so that a single interconnect (trunk) may be used to transport data for multiple VLANs. Since VLANs share bandwidth, a VLAN trunk might use link aggregation and/or quality of service prioritization to route data efficiently.

[Read More](https://en.wikipedia.org/wiki/Virtual_LAN)

* What is ARP and what is it used for?

The Address Resolution Protocol (ARP) is a protocol used for resolution of network layer addresses into link layer addresses, a critical function in multiple-access networks. ARP is used for mapping a network address (e.g. an IPv4 address) to a physical address like an Ethernet address (also named a MAC address).

When we try to ping an IP address on our local network, say 192.168.1.2, our system has to turn the IP address 192.168.1.2 into a MAC address. This involves using ARP to resolve the address, hence its name.

[Read More](https://en.wikipedia.org/wiki/Address_Resolution_Protocol)

* What is the difference between TCP and UDP?

TCP is connection-oriented protocol.

UDP is connectionless protocol

TCP provides delivery guarantee

UDP is unreliable, it doesn't provide any delivery guarantee.

TCP guarantees order of message

UDP doesn't provide any ordering or sequencing guarantee

TCP is slow

UDP is fast

TCP has bigger header than UDP

[Read More](http://javarevisited.blogspot.ru/2014/07/9-difference-between-tcp-and-udp-protocol.html)

* What is the purpose of a default gateway?

A default gateway in computer networking is the node that is assumed to know how to forward packets on to other networks. Typically in a TCP/IP network, nodes such as servers, workstations and network devices each have a defined default route setting, (pointing to the default gateway), defining where to send packets for IP addresses for which they can determine no specific route. The gateway is by definition a router.

[Read More](https://en.wikipedia.org/wiki/Default_gateway)

* What is command used to show the routing table on a Linux box?

You can use one of this:

$ route -n

$ netstat -rn

$ ip route list

* A TCP connection on a network can be uniquely defined by 4 things. What are those things?

remote-ip-address, remote-port, source-ip-address, source-port

* When a client running a web browser connects to a web server, what is the source port and what is the destination port of the connection?

destination port - is 80 for HTTP or 443 for HTTPS

source port - will be random number from option net.ipv4.ip\_local\_port\_range, by default it will be something like between 32768 and 61000 (around 28K source ports available (for a single destination IP:port))

[Read More](https://www.iana.org/assignments/service-names-port-numbers/service-names-port-numbers.xhtml)

* How do you add an IPv6 address to a specific interface?

Using ip:

Usage: /sbin/ip -6 addr add <ipv6address>/<prefixlength> dev <interface>

Example: /sbin/ip -6 addr add 2001:0db8:0:f101::1/64 dev eth0

Using ifconfig:

Usage: /sbin/ifconfig <interface> inet6 add <ipv6address>/<prefixlength>

Example: /sbin/ifconfig eth0 inet6 add 2001:0db8:0:f101::1/64

It is temporarily, you will lost this configuration after reboot. To add permanent ipv6 you need to add option to config file, on Fedora, Redhat Enterprise Linux, and clones like Centos add lines to these files:

/etc/sysconfig/network

NETWORKING\_IPV6=yes

IPV6FORWARDING=no

IPV6\_AUTOCONF=no

IPV6\_AUTOTUNNEL=no

IPV6\_DEFAULTGW=fe80::1

IPV6\_DEFAULTDEV=eth0

/etc/sysconfig/network-scripts/ifcfg-eth0

IPV6INIT=yes

IPV6ADDR=2607:f388:xxxx:yyyy::zzzz/64 # replace with your static address

For Debian and derivatives like Ubuntu add lines to these files:

/etc/sysctl.conf

net.ipv6.conf.eth0.accept\_ra=0

/etc/network/interfaces

iface lo0 inet6 loopback

iface eth0 inet6 static

address 2607:f388:xxxx:yyyy::zzzz # replace with your static address

netmask 64

gateway fe80::1

* You have added an IPv4 and IPv6 address to interface eth0. A ping to the v4 address is working but a ping to the v6 address gives yout the response sendmsg: operation not permitted. What could be wrong?

This means that your server is not allowed to send ICMP packets.

Check firewall rules:

$ ip6tables -P INPUT ACCEPT

$ ip6tables -P OUTPUT ACCEPT

$ ip6tables -P FORWARD ACCEPT

* What is SNAT and when should be used?

Source Network Address Translation (SNAT) - changes the source address in IP header of a packet. It may also change the source port in the TCP/UDP headers. The typical usage is to change the a private (rfc1918) address/port into a public address/port for packets leaving your network.

[Read More](http://www.commercialventvac.com/finao/DNATs-and-SNATs.html)

* Explain how could you ssh login into a Linux system that DROPs all new incomming packets using a SSH tunnel.

Need to think =)

* How do you stop a DDoS?

It is very complicated questions.

Before to do something you need answer a lot of questions.

Simple way is:

- Limiting the ammount of concurrent connections from ddos IP address to your Server with firewall rules.

- Optimize you server configuration options

[Read More](https://www.reddit.com/r/linux/comments/1klq5r/preventing_a_dos_attack/)

* How can you see content of ip packet?

You can use tcpdump\tshark to display captured packets in HEX and ASCII

$ tcpdump -XX -i eth0

$ tshark -i eth0 -x

You can write a python\c script for this

import socket

s = socket.socket(socket.AF\_INET, socket.SOCK\_RAW, socket.IPPROTO\_TCP)

while True:

print s.recvfrom(65565)

[Read More](http://www.binarytides.com/packet-sniffer-code-c-linux/)

**[[⬆]]MySQL questions:**

* How do you create a user?

$ mysql -u root -ppassword -hsomehost -e 'CREATE USER login@"ip";'

* How do you provide privileges to a user?

# read only

GRANT select ON somedb.\* TO 'login'@'ip' IDENTIFIED BY 'agoodpassword';

# all privileges

GRANT all privileges ON somedb.\* TO 'login'@'ip' IDENTIFIED BY 'agoodpassword';

* What is the difference between a “left” and a “right” join?

Table from which you are taking data is 'LEFT'.

Table you are joining is 'RIGHT'.

LEFT JOIN: Take all items from left table AND (only) matching items from right table.

RIGHT JOIN: Take all items from right table AND (only) matching items from left table.

Most people only use LEFT JOIN since it seems more intuitive

* Explain briefly the differences between InnoDB and MyISAM.

MYISAM:

- MYISAM supports Table-level Locking

- MyISAM designed for need of speed

- MyISAM does not support foreign keys hence we call MySQL with MYISAM is DBMS

- MyISAM stores its tables, data and indexes in diskspace using separate three different files. (- tablename.FRM, tablename.MYD, tablename.MYI)-

- MYISAM not supports transaction. You cannot commit and rollback with MYISAM. Once you issue a c- ommand - it’s done.

- MYISAM supports fulltext search

You can use MyISAM, if the table is more static with lots of select and less update and delete.

INNODB:

- InnoDB supports Row-level Locking

- InnoDB designed for maximum performance when processing high volume of data

- InnoDB support foreign keys hence we call MySQL with InnoDB is RDBMS

- InnoDB stores its tables and indexes in a tablespace

- InnoDB has better crash recovery.

- InnoDB supports transaction. You can commit and rollback with InnoDB

* Describe briefly the steps you need to follow in order to create a simple master/slave cluster.

AT Master:

- enable binlog

- set server-id=1

- create user with replication grant

- create dump with master-data

AT Slave:

- enable binlog \ relay-log

- set server-id=2

- restore dump

- set master\_host \ master\_log\_file \ maste\_log\_pos

* Why should you run “mysql\_secure\_installation” after installing MySQL?

mysql\_secure\_installation is a script that improve MySQL installation security in the following ways:

- set a password for root accounts

- remove root accounts that are accessible from outside the local host

- remove anonymous-user accounts

- can remove the test database (which by default can be accessed by all users, even anonymous users), and privileges that permit anyone to access databases with names that start with test\_

* How do you check which jobs are running?

$ mysql -e "show full processlist"

**[[⬆]]DevOps Questions:**

* Can you describe your workflow when you create a script?

1. Create\check task in tfs\jira

2. Analysis task description.

3. Analysis current script collection.

4. Analysis internet for same job\problem.

5. Write and test script prototype in test environment.

6. Commit script to git\svn

7. Build package\use CMS to deploy script in production.

8. Close task in tfs\jira

* What is GIT?

Git is a distributed version control system developed by Linus Torvalds

* What is a dynamically/statically linked file?

Statically file means that the linker program (ld) after source code compilation adds all librarys and other dependencies directly to executable file

Dynamically file means that the above step doesn't happen. The operating system's loader needs to find the dependencies code, load it into memory, each time the program is run.

* What does “configure && make && make install” do?

This commands is need if you what to build software from source code.

Configure - is a script which is responsible for getting ready to build the software on your specific system. It makes sure all of the dependencies for the rest of the build and install process are available, and finds out whatever it needs to know to use those dependencies.

Make - is a command which runs a series of tasks defined in a Makefile to build the finished program from its source code.

Make install - is a command which will copy the built program, and its libraries and documentation, to the correct locations.

* What is puppet/chef/ansible used for?

Puppet/Chef/Ansible - are a free software platform for configuring and managing computers.

* How do you create a new postgres user?

$ psql -c "CREATE USER testuser WITH PASSWORD 'XXXXX';"

* What is a virtual IP address? What is a cluster?

A virtual IP address (VIP or VIPA) is an IP address that doesn't correspond to an actual physical network interface (port). Uses for VIPs include Network Address Translation (especially, One-to-many NAT), fault-tolerance, and mobility.

Virtual IP addresses are commonly used to enable high availability. A standard failover design uses an active/passive server pair connected by replication and watched by a cluster manager. The active server listens on a virtual IP address; applications use it for connections instead of the normal host IP address. Should the active server fail, the cluster manager promotes the passive server and shifts the floating IP address to the newly promoted host. Application connections break and then reconnect to the VIP again, which points them to the new server.

Cluster is a set of loosely or tightly connected computers that work together so that, in many respects, they can be viewed as a single system.

* How do you print all strings of printable characters present in a file?

Use cmd /usr/bin/strings

$ strings /path/somefile

* How do you find shared library dependencies?

ldd - print shared library dependencies

$ ldd /path/somefile

linux-vdso.so.1 (0x00007ffcdabac000)

libselinux.so.1 => /lib/x86\_64-linux-gnu/libselinux.so.1 (0x00007f1a42081000)

* What is Automake and Autoconf?

Automake and Autoconf both are parts of The GNU build system, also known as the Autotools, is a suite of programming tools designed to assist in making source code packages portable to many Unix-like systems.

Automake - is a programming tool to automate parts of the compilation process. It eases usual compilation problems. For example, it points to needed dependencies. It automatically generates one or more Makefile.in from files called Makefile.am. Each Makefile.am contains, among other things, useful variable definitions for the compiled software, such as compiler and linker flags, dependencies and their versions, etc.

Autoconf - generate a configuration script from a TEMPLATE-FILE if given, or configure.ac if present, or else configure.in. Output is sent to the standard output if TEM‐PLATE-FILE is given, else into configure.

* ./configure shows an error that libfoobar is missing on your system, how could you fix this, what could be wrong?

Configure could not find libfoobar in LD\_LIBRARY\_PATH or libfoobar is not installed on your system.

You can fix it by installing libfoobar package with package manager or build it from source.

If libfoobar is already installed just check /etc/ld.so.conf and add right path to libfoobar

* What are the Advantages/disadvantages of script vs compiled program?

Script program have the advantages of:

- flexibility to change the script

- easier to implement (writing good compilers is very hard!!)

- no need to run a compilation stage: can execute code directly "on the fly"

- being more portable.

Script program have the disadvantages of:

- much slow than compiled program

- source code is open

Compiled program have the advantages of:

- faster performance by directly using the native code of the target machine

- opportunity to apply quite powerful optimisations during the compile stage

- hides the source code from the end user

Compiled program have the disadvantages of:

- slow to develop (edit, compile, link and run. The compile/link steps could take serious time).

- to execute you need to compile a different executable for each type of processor and/or platform that you want your program to run on

* What’s the relationship between continuous delivery and DevOps?

Continuous delivery(CD) is an agile way of working whereby quality products—normally software assets—can be developed, built, tested, and shipped in quick succession.

DevOps is another way of working whereby developers and system operators work in harmony with little or no organizational barriers between them towards a common goal.

* What are the important aspects of a system of continous integration and deployment?

Automation\testing are the important aspects of a great development workflow.

Every task that can be done by a machine should be.

Automation gives you the time to focus.

Through testing, you can be sure that the most important steps your customers will take through your system are working, regardless of the changes you make.

This gives you the confidence to experiment, implement new features, and ship updates quickly.

**[[⬆]]Fun Questions:**

* A careless sysadmin executes the following command: chmod 444 /bin/chmod - what do you do to fix this?

Default permission is 755.

Y can use C\C++\Python\Perl and other language to fix this.

#!/usr/bin/python

import os

os.chmod("/bin/chmod", 0755)

* I’ve lost my root password, what can I do?

Simple boot in sigle mode and change it.

Change in grub -> init=/bin/bash -> boot -> run $mount -o remount,rw / -> change root password with $ passwd root

* I’ve rebooted a remote server but after 10 minutes I’m still not able to ssh into it, what can be wrong?

If it does not ping, maybe proble with network\firewall

If it pings but you can not to connect to it with ssh maybe problem with ssh config\firewall rules

Bad permission for ssh keys

Wrong password

* If you were stuck on a desert island with only 5 command-line utilities, which would you choose?

you do not need computer on a desert island because there is no enegry =)

* You come across a random computer and it appears to be a command console for the universe. What is the first thing you type?

It cool to live forever =)

change user 'mylogin' expiration from 'XXXXX-XX-XX' to 'never'

usermod -e "" mylogin

* Tell me about a creative way that you’ve used SSH?

add to .ssh/config this lines and install tor and you can use ssh with tor.

Host \*.onion

ProxyCommand socat - SOCKS4A:localhost:%h:%p,socksport=9050

* You have deleted by error a running script, what could you do to restore it?

While script is running it is not deleted

Find pid of running script and restore it from procfs

ls -l /proc/4607/fd/4

lr-x------ 1 juliet juliet 64 Apr 7 03:19

/proc/4607/fd/4 -> /home/juliet/testing.txt (deleted)

$ cp /proc/4607/fd/4 testing.txt.bk

**[[⬆]]Demo Time:**

* Unpack test.tar.gz without man pages or google.

$ tar xzvf test.tar.gz

* Remove all “\*.pyc” files from testdir recursively?

$ find ./testdir -type f -name "\*.pyc" -ls -delete

$ find ./testdir -type f -name "\*.pyc"|xargs rm -f

* Search for “my konfu is the best” in all \*.py files.

$ find ./testdir -type f -name "\*.py"|xargs grep "my konfu is the best"

* Replace the occurrence of “my konfu is the best” with “I’m a linux jedi master” in all \*.txt files.

$ find ./testdir -type f -name "\*.txt"|xargs sed -i "s/my konfu is the best/I\'m a linux jedi master/"

* Test if port 443 on a machine with IP address X.X.X.X is reachable.

$ nc -z -v X.X.X.X 443

Connection to X.X.X.X 443 port [tcp/https] succeeded!

* Get <http://myinternal.webserver.local/test.html> via telnet.

$ telnet myinternal.webserver.local 80

GET /test.html HTTP/1.1

HOST: myinternal.webserver.local

<ENTER>

<ENTER>

* How to send an email without a mail client, just on the command line?

$ telnet localhost smtp

HELO [example.com](http://example.com/)

mail from: sender@example.com

rcpt to: user@example.com

data

354 Enter mail, end with "." on a line by itself

Hey

This is test email only

Thanks

.

quit

or

$ mail -s "Test Subject" user@example.com

* Write a get\_prim method in python/perl/bash/pseudo.

I don`t undestand what is get\_prim method, if you know, write a comment plz.

* Find all files which have been accessed within the last 30 days.

$ find /\* -type f -atime -30

"-30" means that it was accessed "less than 30 days ago"

"+30" means that it was accessed "more than 30 days ago"

* Explain the following command (date ; ps -ef | awk '{print $1}' | sort | uniq | wc -l ) >> Activity.log

$ date ; ps -ef | awk '{print $1}' | sort | uniq | wc -l

Execute date command which print current datetime, then we execute process list command and print only UID column, than with pipe we sort it and print only uniq values, after wc -l is counting it number after all we append this to file Activity.log

If file we will see something like this:

Fri Jan 22 15:24:07 UTC 2016

6

* Write a script to list all the differences between two directories.

#!/bin/sh

usage="Usage: $0 DIR1 DIR2"

if [ $# -gt 2 ]; then

echo $usage;

exit 1

fi

if [ -z "$1" ]; then

echo $usage;

fi

if [ -d "$1" -a -d "$2" ]; then

echo "Comparing $1 with $2........"

diff -r $1 $2

fi

* In a log file with contents as <TIME> : [MESSAGE] : [ERROR\_NO] - Human readable text display summary/count of specific error numbers that occured every hour or a specific hour.

$ cat log | awk -F ":" '{print $3}'|sort -n |uniq -c

$ cat log | grep "specific hour" | awk -F ":" '{print $3}'|sort -n |uniq -c