DNS	Service that maps host to ip addresses, A DNS server is a computer server that contains a database of public IP addresses and their associated hostnames, and in most cases serves to resolve, or translate, those names to IP addresses as requested.	1.DNS Query 2.DNS Response -- DNS -- UDP:53
NAT PAT and Overload	static NAT, dynamic NAT Network Address Translation (NAT) is a process in which one or more local IP address is translated into one or more Global IP address and vice versa in order to provide Internet access to the local hosts. Flavor of NAT , Port Address Translation -- single ip SHARE by all devices	1.Before NAT 2.After NAT
NTP	The Network Time Protocol (NTP) is a networking protocol for clock synchronization between computer systems over packet-switched, variable-latency data networks	UDP:123
SNMP	Simple Network Management Protocol (SNMP) is an Internet Standard protocol for collecting and organizing information about managed devices on IP networks and for modifying that information to change device behavior.	1.polling 2.Event Notification
DHCP	In computer science, the Dynamic Host Configuration Protocol is a network management protocol used on Internet Protocol networks, whereby a DHCP server dynamically assigns an IP address and other network configuration parameters to each device on the network, so they can communicate with other IP networks.	1.DHCP Discover 2.DHCP offer 3.DHCP Request 4.DHCP ACK - (Acknowledgement) 5.DHCP Release server port - 67 , client port -68 DORA-R

Performance issues   Solution
1.Low bandwidth
2.High Latency- delay
3.High jitter - in case of video,audio transmission delay
4.High packet loss   Apply QOS(Quality of Service)based
                                                                                                            on applications needs
Complete loss of functionality ----
1.NAT reachability 2.Filewall filtering 3.VPN connections 4.Broken Proxy

VIRL	**Virtual Internet routing lab-** VIRL is Cisco's powerful **network simulation platform.** VIRL is shipped with Cisco OS virtual machines included in the software package. This is your flexible, all-in-one virtual networking lab. ... Easily create connections to actual networking equipment by extending your lab to physical and virtual networking devices.	UDP 123, telnet -23, SSH - 22, HTTP(TCP-80), HTTPS-(tcp-443),
PyATS	Python Automation test system Model and validate a network testbed ties into genie - shell commands	**The** dir() **function** is **used to find out** all **the names defined in a module**.
Puppet	Agent-based - master and manage nodes - communicates using transport layer security TLS .pp file agentless support for cisco routers - SSH	**Pull** configuration is used by **tools** like **Chef**, Pupp

Chef   Chef workstation ,server , projects - communicates using transport layer security TLS ---- RUBY lang

Control machines ,manages the devices ---------**supports yaml lang coding , ansible written in python
SSH,Netconf,http,snmp,vinrm--Automation and orchestration tool**
playbooks-collection of plays , plays-collection of tasks , tasks ---- **Ansible is "agentless",- means no need to install anything at all in your n/w devices
or on your platform for using ansible**
ansible web -m ping , ansible -m ping <hostname>,ansible-playbook stats.yml
time ansible-playbook <filename.yml> --- augment

Inventory -- inventory file includes details of all devices,servers, network items req to manage in ansible
or ansible inventory file which consist list of host and host group or group over the group and credential of the machine-like variables, login username
and password. That will help to perform task on all machine parallelly at a time. There are mainly two type of inventory files.
Static inventory- when there is no need to create container frequently
Dynamic inventory

Modules -- Modules (also referred to as "task plugins" or "library plugins") are discrete units of code that can be used from the command line or in a
playbook task. Ansible executes each module, usually on the remote target node, and collects return values.

At a basic level, **playbooks** can be used to manage configurations of and deployments to remote machines. At a more advanced level, they can
sequence multi-tier rollouts involving rolling updates, and can delegate actions to other hosts, interacting with monitoring servers and load balancers
along the way.

If Ansible modules are the tools in your workshop, playbooks are your instruction manuals, and your inventory of hosts are your raw material.

Variables are used in {{var}}

**Facts --- ansible ubantu -f setup -- Having all information related to the hosts we are using
Register command to store result of facts , debug command , "become : true" or -b (in command) flag is for become the root user ,with_items - this
command is used for looping in ansible**

Ansible   Module - prebuild scripts

YANG   Data modeling language,Hierarchical structure,uses pyang
module{container{list{-key:value},{-key:value}

API Keys were created as somewhat of a fix to the early authentication issues of HTTP Basic Authentication and other such systems. ... The problem,
however, is that API keys are often used for what they're not – an API key is not a method of authorization, it's a method of authentication

Advantages of public clouds:
No maintenance—your service provider provides the maintenance. Near-unlimited scalability—on-demand resources are available to meet your
business needs. High reliability—a vast network of servers ensures against failure.

When the destination MAC address is not found in the MAC address table, the switch forwards the frame out of all ports (flooding) , Data link layer
Switch   device -- Frames

Transport layer Device -- packets ---

Router   . How does a router react when it receives an IP packet with a destination address for which it does not have any matching routes?It drops the packet

CDP   Cisco Discovery Protocol - two cisco devices communicate using this protocol

ARP   ARP (Address Resolution Protocol) translates an IP address into a MAC address.

TCP   Transmission control protocol -- 3 way handshake -   syn
                                                                                                                          ack with syn
                                                                                                                          ack

                          1.packet filtering - filter on the basis of protocols,only secure protocol allowed-TCP:443,SSL/TLS,HTTPS
           Firewall   2.Stateful filtering - state information saved by firewall to identify/filter the traffic
                          3.next generation firewall- applications related , only allow applications which are having permissions

IDS   Intrusion detection system -
IPS   Intrusion prevention system-anomalies,protocols,signatures,reputation