SNA Long Questions

1. **Explain Network traffic management/monitoring in detail also provide the steps through which network traffic can be secured.**

Traffic monitoring, also known as network monitoring, is **the method of studying the incoming and outgoing traffic on a computer network via specialized hardware and/or software**.

Network traffic analysis (NTA) is a method of monitoring network availability and activity to identify anomalies, including security and operational issues. Common use cases for NTA include:

- Collecting a real-time and historical record of what's happening on your network
- Detecting malware such as ransomware activity
- Detecting the use of vulnerable protocols and ciphers
- Troubleshooting a slow network
- Improving internal visibility and eliminating blind spots

Implementing a solution that can continuously monitor network traffic gives you the insight you need to optimize network performance, minimize your attack surface, enhance security, and improve the management of your resources. However, knowing how to monitor network traffic is not enough. It's important to also consider the data sources for your network monitoring tool; two of the most common are flow data (acquired from devices like routers) and packet data (from SPAN, mirror ports, and network TAPs).

2. **What is system administration and explain its primary components for data center point of view.**

System administration refers to the management of one or more hardware and software systems.

The task is performed by a system administrator who monitors system health, monitors and allocates system resources like disk space, performs backups, provides user access, manages user accounts, monitors system security and performs many other functions.

Primary Components

- Servers.
- Racks.
- Network connectivity infrastructure.
- Security measures and appliances.
- Monitoring structures.
- Storage infrastructure.
- Cooling and air flow systems (as well as fire protection)
- Policies to maintain efficiency, security and performance.

3. **Discuss advantages of Share Point 2010 along with its configuration steps.**

Microsoft SharePoint is a web-based application used for document sharing, business intelligence, advanced search, content collaboration, and much more.

The benefits of Microsoft SharePoint are compelling enough that more than 75% of Fortune 500 companies, including Viacom and Windex, use this software. SharePoint has a similar user interface to Office 365 and is known for its ease of use and great user experience.

Microsoft SharePoint Features and Benefits

1. Multi-purpose functionality built in

The greatest of all the SharePoint benefits is its flexibility. The collaborative platform serves as an intranet, which is simply a company's internal website for information sharing, task scheduling, contacts, and much more.

Administrators can assign different permission levels depending on the user's status. Beyond that, the software has functions for document sharing, file management, social networking, business information, and virtually everything else involved in the day-to-day operations of your business.

2. Centralized administration

Ease of management is one of the most significant SharePoint 2010 benefits. Administrators can quickly access operation features, including security settings, call, back up sites and site data, perform restorations, and update privileges all on a single dashboard.

3. Customizable

You can keep the default online SharePoint features and benefits, or you can tailor them to your business needs.

Your team will have the ability to build custom elements in each of the Microsoft SharePoint features. You can similarly customize the entire application's interface to reflect your branding and improve employees' perceptive experience with the app through the drag and drop functions.

4. Document management and collaboration

Microsoft SharePoint 2013 makes it possible to organize your company's information in an accessible manner. The central benefits of SharePoint include a streamlined flow of information and cloud storage that can be accessed by mobile devices.

Informed employees make better decisions, meet deadlines, understand the shared business strategy, and contribute better to it. File sharing on SharePoint is done by a simple click or touch of a button. Yes, mobility is one of the numerous benefits of SharePoint 2013.

5. Site consolidation

You can integrate all your sites (shared work environments) into one platform and slash down the costs of a siloed site administration. The consolidation of the internet and intranet sites makes it easily accessible and managed by internal teams.

6. Integration with your existing apps

Microsoft SharePoint offers a seamless integration with the rest of your business applications. The product will work seamlessly with your Microsoft Office Suite (Excel, Word, and PowerPoint), MS Exchange Server, MS Unified Communications, ERP, CRM, and many other back-office systems and previous versions.

For SharePoint Online, compatibility is not limited to Microsoft Edge and Internet Explorer; SharePoint also works well with all modern web browsers.

7. Enhanced security

SharePoint 2013 benefits include advanced security features that reduce the risk of outages and unauthorized access. These features include new workflow upgrades and authentication enhancements. As much as information access and shareability are optimized, your data integrity remains reliable. Other security configurations and access/editing privileges can be set at the document or item level.

The collaboration application similarly promises improved security for organizations that handle sensitive data. You can configure different settings for controlling shareability, storage, and auditing to help expedite compliance with your industry's regulatory requirements on data security.

8. Ease of use and design assistance

You won't need to hire a team of web developers to improve your website or create database management systems because the Microsoft SharePoint 2010 features and benefits include the ability to build solutions that better meet your business needs.

SharePoint Online and SharePoint Server have the application programming interfaces (APIS) for such jobs. Using SharePoint development features for app building is an excellent way to cut costs.

9. Content management

You can prepare and schedule content for publishing on various websites on the internet and social platforms. The social networking in SharePoint 2013 enables easy sharing of ideas, updates, and content.

Users can publish Office documents on the platform and share it within or outside the organization. They can similarly create and edit tasks from any device and convert documents to and from various formats, including PDF, Word, and Excel.

10. Speed up and streamline business process

A collaboration platform like Microsoft SharePoint makes it possible to collect and organize data in one place.

Information from suppliers, communication with customers, or interactions with partners and others are harvested in SharePoint's form-driven solutions. Your employees can create business intelligence portals and display this data on dashboards, web parts, or scorecards. It will help them make better decisions, track and trace consumer preferences or predict fluctuations in demand and supply.

Configuration steps:

VM > Setting > Options > Shared Folder > Enable and Select your Pre-request software download folder. Run > SharePoint Server 2010 Application file, system will extract files and show the above screen, under Install > click Install Software prerequisites.

4. Write configurations steps for establishing FTP Server and Samba Server.

Configuring FTP Server:

$ sudo apt update
$ sudo apt install -y vsftpd
$ sudo nano /etc/vsftpd

listen=NO
anonymous_enable=NO
local_enable=YES
write_enable=YES
local_umask=022
dirmessage_enable=YES
use_localtime=YES
xferlog_enable=YES
connect_from_port_20=YES
chroot_local_user=YES

secure_chroot_dir=/var/run/vsftpd/empty
pam_service_name=vsftpd
rsa_cert_file=/etc/ssl/certs/ssl-cert-snakeoil.pem
rsa_private_key_file=/etc/ssl/private/ssl-cert-snakeoil.key
ssl_enable=Yes
pasv_enable=Yes
pasv_min_port=10000
pasv_max_port=10100
allow_writeable_chroot=YES
ssl_tlsv1=YES
ssl_sslv2=NO
ssl_sslv3=NO

Configuring Samba Server:
$ sudo cp /etc/samba/smb.conf
$ sudo cp /etc/samba/smb.conf /etc/samba/smb_bkp.conf
$ sudo nano /etc/samba/smb.conf

comment = Ubuntu File Server Share
path = /srv/samba/share
browsable = yes
guest ok = yes
read only = no
create mask = 0755 Comment: is a short description of the share.
Path: the path of the directory to be shared.

5. Explain User Management and file permissions for Windows and Linux.
6. Write a note on Bash Shell scripting and Network Traffic Configurations.
7. Explain the partitioning structure of Windows and Directory structure of Linux.

8. What is Active Directory, how it works briefly explain Kerberos?

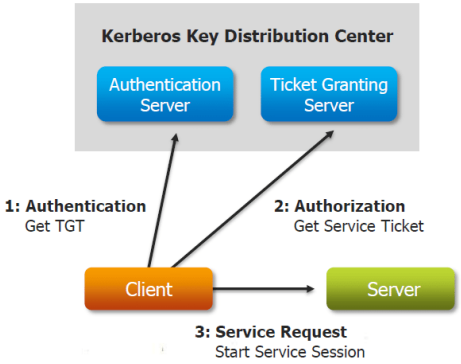
Active Directory (AD) is **a database and set of services that connect users with the network resources they need to get their work done**. The database (or directory) contains critical information about your environment, including what users and computers there are and who's allowed to do what.

Active Directory (AD) is **a directory service for Windows domain networks**. The best example of AD is when a user signs in to a computer that is part of a Windows domain. AD checks the credentials against a database, if the username and password are valid, the user can log into the computer.

Kerberos was designed **to provide secure authentication to services over an insecure network**. Kerberos uses tickets to authenticate a user and completely avoids sending passwords across the network.

Kerberos has three parts: **a client, server, and trusted third party (KDC)** to mediate between them. Clients obtain tickets from the Kerberos Key Distribution Center (KDC), and they present these tickets to servers when connections are established.

Components of Kerberos:



Kerberos comprises of 3 components; Key Distribution Center (KDC), Client User and Server with the desired service to access. The KDC performs 2service functions:

- Authentication Service (AS)
- Ticket-Granting Service (TGS)

As shown in the above figure, three exchanges occurs when the client accesses a server:

- AS Exchange
- TGS Exchange
- Client/Server (CS) Exchange

How Does Kerberos Work?

Instead of client sending password to application server, a Request Ticket is placed from authentication server and the Ticket along with the encrypted request is sent to application server. Now, how to request tickets without repeatedly sending credentials? This is done through Ticket granting ticket (TGT).

9. How we configure Apache Server?

Step 1: Installation Apache on Linux

1. Open the terminal
2. Open root user by using **su** command and password
3. Install Apache by using the command **#yum install httpd**
4. You will be asked for confirmation: Is this ok [y/N] – **type Y**

Step 2: Configure Apache Server

1. Open the terminal
2. Open root user by using **su** command and password
3. Open configuration file by using the command **#view /etc/httpd/conf/httpd.conf**
4. Now **httpd.conf** file is opened to be configured. You may do changes accordingly.

   ServerRoot "/etc/httpd" | you may change the location of httpd.conf file here.
   Listen 80 | you may change port number for your Apache server.

ServerAdmin naveed.ahmad@uos.edu.pk | you may change the email address.
DocumentRoot "/var/www/html" | you may update web page location.
DirectoryIndex index.html | home page for a website. Eg. index.php

Step 3: Start Apache Server

1. Open the terminal
2. Open root user by using **su** command and password
3. Start Apache by using the command **#systemctl start httpd**
4. Check Apache running successfully of not, using command **#systemctl status httpd**
5. It will show **Active (running)** if started successfully.

10. What services require to resolve IP request for Domain Names?

Domain Name System or DNS

When you want to visit a website, your computer needs to know the exact IP address; it does not care about the domain name.

DNS keeps the record of all domain names and the associated IP addresses. When you type in a URL in your browser, DNS resolves the domain name into an IP address.

In other words, DNS is a service that maps domain names to corresponding IP addresses**.**

DNS Cached

DNS caching or flushing is an effective way to reduce potential DNS queries towards DNS nameservers. These speeds up the domain name resolving procedure.

Caching happens at multiple locations. This includes your computer, sometimes routers, while all DNS servers have their own databases with cached information.

Step 1 – Send a Request to Resolve a Domain Name

When you type **www.google.com** into a browser, in order to load the webpage, your computer asks for the IP address. Computers do not know in advance where they can find the necessary information, so they try searching through the DNS cache and any available external source.

Step 2 – Search for an IP Locally

Before going externally, your computer loads the local DNS cache database to see if you already requested the IP for that domain name. Every computer has a temporary cache with the most recent DNS requests and attempts to connect to online sources.

When the DNS cache has the IP data for the website that you are trying to connect to, the page loads immediately. DNS cache speed up this lookup process since the computer contains the information it needs and does not have to forward the request to your ISP.

Step 3 – Contact ISP and its Recursive DNS Server to Resolve a Domain Name

A computer's local DNS cache database does not always contain the necessary data to resolve a domain name. In that case, the request goes further to your Internet Service Provider (ISP) and its DNS server.

Once it gets a request, the resolver looks in its records to provide the correct IP address. When the necessary information is present in the ISP server's cached records, the computer gets back the IP and connects to the website. If ISP's recursive DNS server cannot resolve the domain name, it contacts other DNS servers to provide the information back to you. This is why we call them recursive servers. Every Internet Service Provider has at least a secondary DNS server setup to ensure maximum high availability of the service.

Step 4 – Ask Outside DNS Servers to Provide an IP Address

ISP DNS resolvers are configured to ask other DNS servers for correct IP address mapping until they can provide data back to the requester. These are iterative DNS queries.
When a DNS client sends such a request, the first responding server does not provide the needed IP address. Instead, it directs the request to another server that is lower in the DNS hierarchy, and that one to another until the IP address is fully resolved. There are a few stops in this process.

1. **Root domain nameservers**. Root servers themselves do not map IP addresses to domain names. Instead, they hold the information about all top-level domain (TLD) nameservers and point to their location. TLD is the rightmost section of a domain name, for example, **.com** in **www.google.com** or **.org** in **www.technology.org**. Root servers are critical since they are the first stop for all DNS lookup requests.
2. **TLD nameservers**. These servers contain the data for second-level domains, such as '**google**' in **www.google.com**. Previously, the root server pointed to the location of the TLD server. Then, the TLD server needs to direct the request toward the server that contains the necessary data for the website we are trying to reach.
3. **Authoritative nameserver.** Authoritative servers are the final destination for DNS lookup requests. They provide the website's IP address back to the recursive DNS servers. If the site has subdomains, the local DNS server will keep sending requests to the authoritative server until it finally resolves the IP address.

Step 5 – Receive the IP Address

Once the ISP's recursive DNS server obtains the IP address by sending multiple iterative DNS queries, it finally returns it to your computer. The record for this request now stays cached on the hard drive. The browser can then fetch this IP from the cache and connect it to the website's server. When we break it down like this, the process of DNS lookup seems to take a long time to complete. In fact, it takes milliseconds, with maybe a few milliseconds more if the DNS record is not in the local cache. In both cases, users cannot tell the difference. This is a basic description of how DNS works, and it should give you an idea what goes on under the hood when you browse or send an email.

11. How DHCP Server dynamically assign IP address to host?

- Addresses are leased to a host. A host will usually keep the same address by periodically contacting the DHCP server to renew the lease.
- Addresses are assigned for a fixed period of time. At the end of that period, a new request for an address must be made, and another address is then assigned to the host.
- Addresses are allocated after a negotiation between the server and the host to determine the length of the agreement.

When a DHCP server dynamically allocates addresses, the client leases its IP address for a certain period of time (configured at the server) and must renew the lease to continue using it. The lease renewal process begins when a bound client (a DHCP client with a leased address) reaches what is known as the renewal time value, or T1 value, of its lease. By default, the renewal time value is 50 percent of the lease period. When a client reaches this point, it enters the renewing state and begins generating DHCPREQUEST messages. The client transmits the DHCPREQUEST messages as unicasts to the server that holds the lease. If the server is available to receive the message, it responds with either a DHCPACK message, which renews the lease and restarts the lease time clock or a DHCPNACK message, which terminates the lease and forces the client to begin the address assignment process again from the beginning.

How DHCP assigns IP addresses

DHCP assigns an IP address when a system is started, for example:

1. A user turns on a computer with a DHCP client.
2. The client computer sends a broadcast request (called a DISCOVER or DHCPDISCOVER), looking for a DHCP server to answer.
3. The router directs the DISCOVER packet to the correct DHCP server.
4. The server receives the DISCOVER packet. Based on availability and usage policies set on the server, the server determines an appropriate address (if any) to give to the client. The server then temporarily reserves that address for the client and sends back to the client an OFFER (or DHCPOFFER) packet, with that address information. The server also configures the client's DNS servers, WINS servers, NTP servers, and sometimes other services as well.
5. The client sends a REQUEST (or DHCPREQUEST) packet, letting the server know that it intends to use the address.
6. The server sends an ACK (or DHCPACK) packet, confirming that the client has a been given a lease on the address for a server-specified period of time.

12. Briefly explain about any two Server/Services list below.

a. Exchange server

Exchange server, being a product of Microsoft, is a mail server and calendar server, that helps small and medium scale companies to achieve better reliability and improved performance.
It runs only on Windows Server Operating systems. It can also be called as a server-side application which provides data to the client-side collaborative application platform. This messaging platform or exchange mail server provides flexibility for sending emails, calendaring, voicemail transcriptions, scheduling, and tools to customize collaboration and messaging service applications.
There are various other email protocols apart from an exchange server, like POP3, IMAP, MAPI, and Exchange ActiveSync.

b. Application Server

An application server exposes *business logic* to the clients, which generates dynamic content. It is a software framework that transforms data to provide the specialized functionality offered by a business, service, or application. Application servers enhance the interactive parts of a website that can appear differently depending on the context of the request.

c. Samba server

Samba is an extremely useful networking tool for anyone who has both Windows and Unix systems on his network. Running on a Unix system, it allows Windows to share files and printers on the Unix host, and it also allows Unix users to access resources shared by Windows systems.

d. IP-PABX

The acronym PABX stands for a Private Automated Branch Exchange. A PABX is a type of telephone network used by call centres and medium-to-large companies. This exchange system provides multiple lines for outside callers to reach staff, as well as numerous external lines for those in the organisation to utilise.

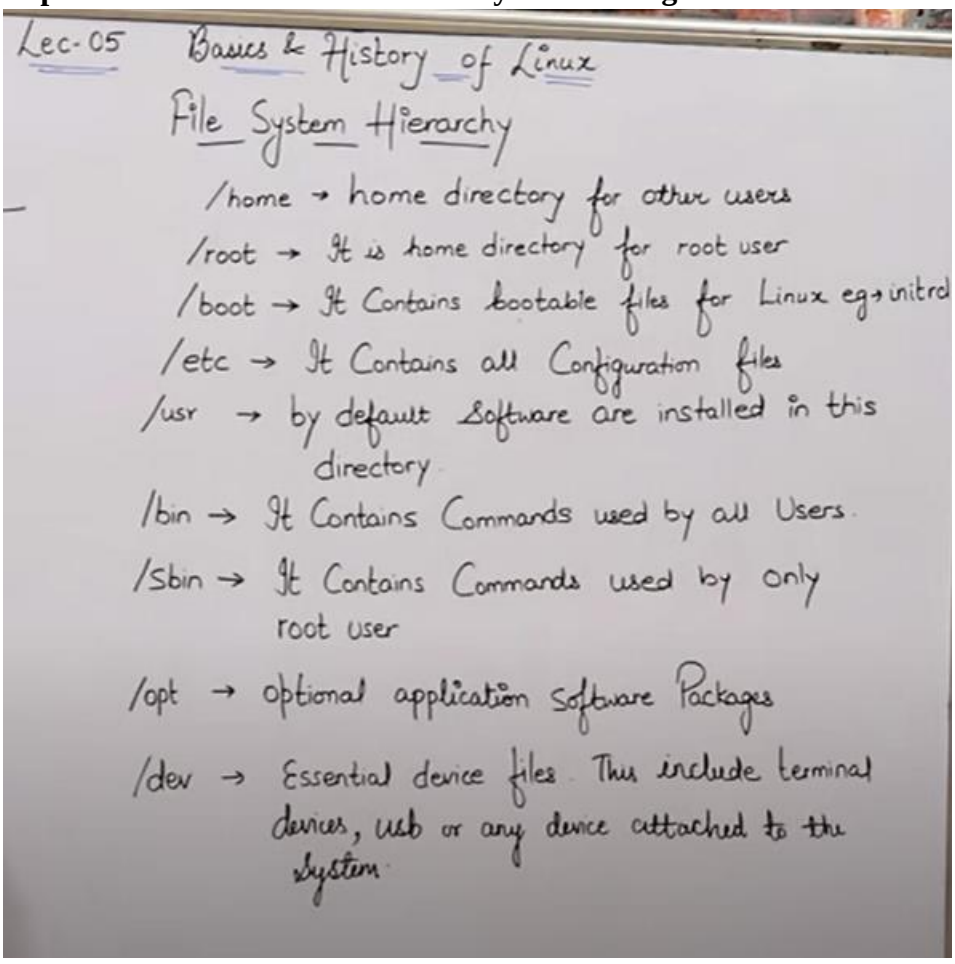
e. SAN

A Storage Area Network (SAN) is a specialized, high-speed network that provides block-level network access to storage. SANs are typically composed of hosts, switches, storage elements, and storage devices that are interconnected using a variety of technologies, topologies, and protocols.

f. Cloud Computing

The practice of using a network of remote servers hosted on the internet to store, manage, and process data, rather than a local server or a personal computer.

13. Explain in detail the advanced file System Management in Red Hat Linux.



14. How can we access the server remotely? What will be the issues in remote access?

Steps:

a. Click the Start button.
b. Click Run...
c. Type “mstsc” and press the Enter key.
d. Next to Computer: type in the IP address of your server
e. Click Connect.
f. If all goes well, you will see the Windows login prompt.

15. Explain scenarios for picking appropriate maintenance contracts for server?

4.1.4 Consider Maintenance Contracts and Spare Parts

When purchasing a server, consider how repairs will be handled. All machines eventually break.[4] Vendors tend to have a variety of maintenance contract options. For example, one form of maintenance contract provides on-site service with a 4-hour response time, a 12-hour response time, or next-day options. Other options include having the customer purchase a kit of spare parts and receive replacements when a spare part gets used.

Following are some reasonable scenarios for picking appropriate maintenance contracts:

- *Non-critical server.* Some hosts are not critical, such as a CPU server that is one of many. In that situation, a maintenance contract with next-day or 2-day response time is reasonable. Or, no contract may be needed if the default repair options are sufficient.
- *Large groups of similar servers.* Sometimes, a site has many of the same type of machine, possibly offering different kinds of services. In this case, it may be reasonable to purchase a spares kit so that repairs can be done by local staff. The cost of the spares kit is divided over the many hosts. These hosts may now require a lower-cost maintenance contract that simply replaces parts from the spares kit.
- *Controlled introduction.* Technology improves over time, and sites described in the previous paragraph eventually need to upgrade to newer models, which may be out of scope for the spares kit. In this case, you might standardize for a set amount of time on a particular model or set of models that share a spares kit. At the end of the period, you might approve a new model and purchase the appropriate spares kit. At any given time, you would have, for example, only two spares kits. To introduce a third model, you would first decommission all the hosts that rely on the spares kit that is being retired. This controls costs.
- *Critical host.* Sometimes, it is too expensive to have a fully stocked spares kit. It may be reasonable to stock spares for parts that commonly fail and otherwise pay for a maintenance contract with same-day response. Hard drives and power supplies commonly fail and are often interchangeable among a number of products.
- *Large variety of models from same vendor.* A very large site may adopt a maintenance contract that includes having an on-site technician. This option is usually justified only at a site that has an extremely large number of servers, or sites where that vendor's servers play a keen role related to revenue. However, medium-size sites can sometimes negotiate to have the regional spares kit stored on their site, with the benefit that the technician is more likely to hang out near your building. Sometimes, it is possible to negotiate direct access to the spares kit on an emergency basis. (Usually, this is done without the knowledge of the technician's management.) An SA can ensure that the technician will spend all his or her spare time at your site by providing a minor amount of office space and use of a telephone as a base of operations. In exchange, a discount on maintenance contract fees can sometimes be negotiated. At one site that had this arrangement, a technician with nothing else to do would unbox and rack-mount new equipment for the SAs.
- *Highly critical host.* Some vendors offer a maintenance contract that provides an on-site technician and a duplicate machine ready to be swapped into place. This is often as expensive as paying for a redundant server but may make sense for some companies that are not highly technical.

16. What is firewall? What different types of firewalls exits? Give commands for Filtering.

Firewall:

In computing, a firewall is a network security system that monitors and controls incoming and outgoing network traffic based on predetermined security rules. A firewall typically establishes a barrier between a trusted network and an untrusted network, such as the Internet.

Types of firewalls:

a. **packet filtering firewall.**
   They compare each packet received to a set of established criteria, such as the allowed IP addresses, packet type, port number.
b. **circuit-level gateway.**
   Circuit-level gateways monitor TCP handshakes and other network protocol session initiation messages across the network.
c. **application-level gateway (aka proxy firewall)**
   Application-level gateways filter packets not only according to the service for which they are intended -- as specified by the destination port -- but also by other characteristics, such as the HTTP request string.
d. **stateful inspection firewall.**
   Keep track of whether or not that packet is part of an established TCP or other network session.
e. **next-generation firewall (NGFW)**
   A typical NGFW combines packet inspection with stateful inspection and also includes some variety of deep packet inspection (DPI), as well as other network security systems, such as an IDS/IPS, malware filtering and antivirus.

Commands for filtering:

iptables -t filter --append INPUT -j DROP

iptables -t filter --append INPUT -j ACCEPT

iptables -t filter --append INPUT -j REJECT

17. Write different steps of configuring DNS.

Step 1: Installation DNS on Linux

1. Open the terminal
2. Open root user by using **su** command and password
3. Install Apache by using the command **# yum install bind**
4. You will be asked for confirmation: Is this ok [y/N] – **type Y**

Step 2: Configure Apache Server

1. Open the terminal
2. Open root user by using **su** command and password
3. Open configuration file by using the command **# vim /etc/named.conf**
4. Now **named.conf** file is opened to be configured. You may do changes accordingly.