Web Development and Database Administration

Level-III

Based on November 2023, Curriculum Version II



Module Title: Evaluating and selecting hosting service

Module code: EIS WDDBA3 M10 1123

Nominal duration: 40 Hours

Prepared by: Ministry of Labor and Skill

November, 2023

Addis Ababa, Ethiopia

Table of Contents

Acknowledgment **4**

Acronym **5**

Introduction to the Module **6**

Unit One: ISP Selection **7**

1.1. Comparable characteristics of hosting services 8

1.2. Flexible Email and Mailing list services 11

1.3. Business needs support service standards 13

1.4. Data capacity for partial outages 14

1.5. Security technologies assessment 16

1.6. Evaluation of scripting language availability 18

1.7. Assessment of optional server applications for advanced web functions 20

1.8. Client selection criteria with ISP hosting service 21

Self-Check 1 ..... **24**

Unit Two: Permanent Online Presence **25**

2.1. Server performance and availability 26

2.2. Negotiate escalation procedures and performance standards 28

2.3. Security and backup procedures for business needs 30

Self-Check-2 ..... **33**

Unit Three: Technical Requirements for Web hosting **34**

3.1. OS compatibility with business software and applications 35

3.2. Web-host server for dynamic websites 38

3.3. Security systems and payment technologies 40

Self-Check-3 ..... **44**

Unit Four: Benchmark and Test Performance **45**

4.1. ISP performance during on and off-peak times 46

4.2. Email and Mailing services backup procedures 49

4.3. Services align with business needs 49

4.4. Quaility of Service Delivered 51

Self-Check-3 ..... **53**

Reference **54**

Developer's Profile **55**

Acknowledgment

Ministry of Labor and Skills wish to extend thanks and appreciation to the many representatives of TVET instructors and respective industry experts who donated their time and expertise to the development of this Teaching, Training and Learning Materials (TTLM).

Acronym

ACL ---------- Access control lists

CDN ---------- Content delivery network

DNS ---------- Domain Name system

ISP ---------- Internet service provider

Mbps ---------- Megabits per second

NIDS ---------- Network-based intrusion detection systems

OS ---------- Operating System

QOS ---------- Quality of Service

SEO ---------- Search engine optimization

SLA ---------- Service Level Agreements

SSL ---------- Secure Sockets Layer

TLS ---------- Transport Layer Security

VPN ---------- Virtual private network

Introduction to the Module

Web hosting provider will be best for you depends on your needs, the size of your business, and your technical expertise and resources.

This module describes the skills and knowledge required to determine a client's current and future internet service providers (ISPs) needs.

The module applies to individuals working in Information and Communications Technology (ICT) who take responsibility for comparing and evaluating internet service provider (ISP) services.

Module covers the units:

- ISP Selection
- Permanent Online Presence
- Meet Technical Requirements
- Benchmark and Testing Performance

Learning Objective of the Module

- Develop the ability to review and compare characteristics of hosting services
- Establish systems and protocols to monitor server performance
- Take proactive measures to ensure that the operating system, web-host servers, and associated technologies
- Implement performance testing methodologies
- Evaluate service delivery against organizational standards

Module Instruction

For effective use these modules trainees are expected to follow the following module instruction:

1. Read the information written in each unit
2. Accomplish the Self-checks at the end of each unit
3. Read the identified reference book for Examples and exercise

Unit One: ISP Selection

This unit is developed to provide you the necessary information regarding the following content coverage and topics:

- Comparable characteristics hosting services
- Flexible Email and Mailing list services
- Business needs support service standards
- Data capacity for partial outages
- Security technologies assessment
- Evaluation of scripting language availability
- Assessment of optional server applications for advanced web functions
- Client selection criteria with ISP hosting service

This unit will also assist you to attain the learning outcomes stated in the cover page.

Specifically, upon completion of this learning guide, you will be able to:

- Conduct a comprehensive review of comparable hosting services.
- Ensure flexibility in email and mailing list services to meet business needs.
- Evaluate support service standards in alignment with business requirements.
- Guarantee data capacity for partial outages.
- Assess the availability of security technologies.
- Work with scripting languages compatible with the chosen hosting service.
- Identify and implement optional server applications to enhance web functionality.
- Confirm and validate that the chosen ISP hosting service meets client selection criteria.

1.1. Comparable characteristics of hosting services

1.1.1. ISP (Internet Service Provider)

An ISP (internet service provider) is a company that provides individuals and organizations access to the internet and other related services. An ISP has the equipment and the telecommunication line access required to have a point of presence on the internet for the geographic area served.

ISPs make it possible for customers to access the internet while also providing additional services such as email, domain registration and web hosting. ISPs may also provide different internet connection types, such as cable and fiber. Connections can also come in the form of high-speed broadband or non-broadband. The Federal Communications Commission (FCC) states that to be considered high-speed, a connection must have download speeds of at least 25 megabits per second (Mbps) and upload speeds a minimum of 3 Mbps.

An ISP is also sometimes referred to as an ***internet access provider***. ISP is also sometimes used as an abbreviation for ***independent service provider*** to distinguish a service provider that is a separate company from a telephone company.

1.1.2. Web Hosting

Web hosting is a service that allows organizations and individuals to post a website or web page onto the Internet.

Web hosting is a necessity for any website it is the physical location of your website on the Internet, an online storage center that houses the information, images, video, and other content that comprises your website.

A web hosting service is a type of Internet hosting service that allows individuals and organizations to make their website accessible via the World Wide Web. Web hosts are companies that provide space on a server owned or leased for use by clients, as well as providing Internet connectivity, typically in a data center.

Web hosting is the place where all the files of your website live. It is like the home of your website where it actually lives.

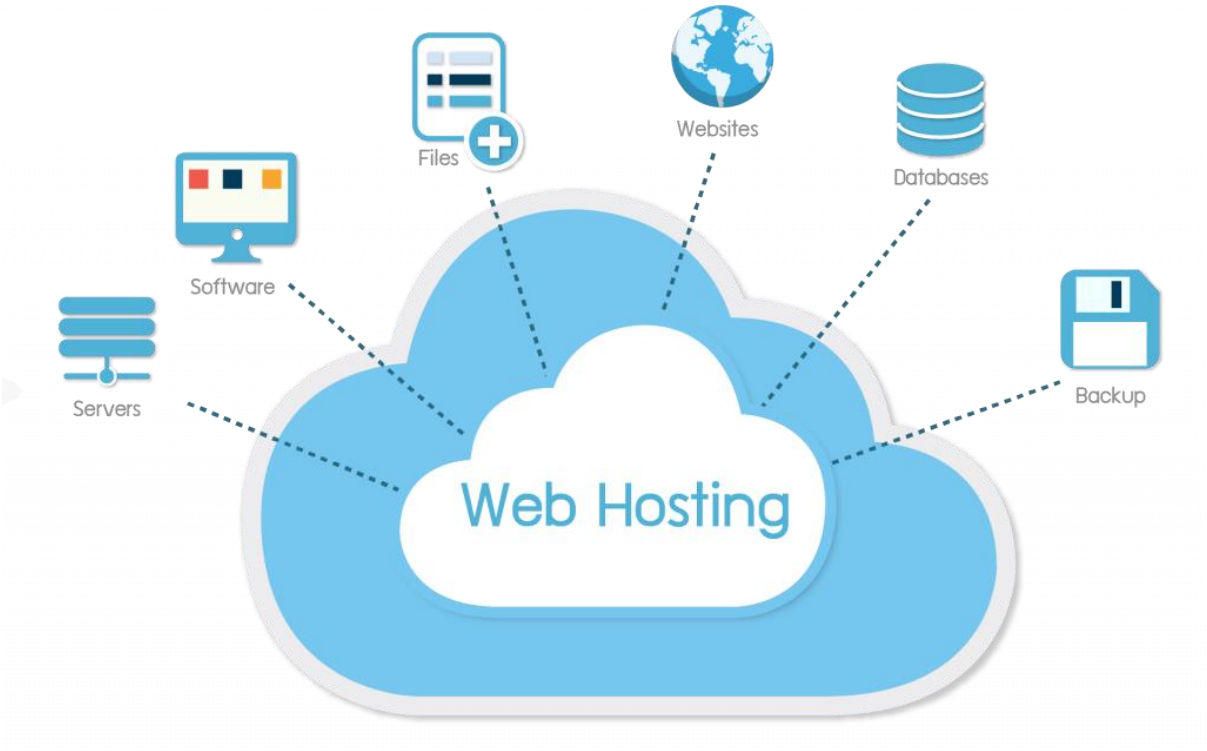


Figure 1.1: web hosting features

In a nutshell, web hosting is the process of renting or buying space to house a website on the World Wide Web. Website content such as HTML, CSS, and images has to be housed on a server to be viewable online.

When a hosting provider allocates space on a web server for a website to store its files, they are hosting a website. Web hosting makes the files that comprise a website (code, images, etc.) available for viewing online. Every website you've ever visited is hosted on a server.

What exactly is a server? A server is a computer that connects other web users to your site from anywhere in the world. As the name implies, web hosting service providers have the servers, connectivity, and associated services to host websites. By offering a variety of hosting plans, they cover the spectrum of hosting needs, from small blogs and large organizations.

1.1.3. Characteristics of a good web hosting company

Many website owners in many cases experience hard times when looking for good web hosting service. In many instances, they will end up with a web hosting company that is cheap but offers very poor services, or they can go for that which offers excellent services but will do this at an exorbitantly high price. With the entry of very many web hosting companies in the market, it is

sometimes confusing on which one to settle on since all of them promise to change all the above.

But before you decide what particular company to deal with, you must first know the attributes and characteristics that a good wed hosting company should have.

A good web hosting company should have

I. Good reputation

A good web hosting company must have a good and excellent reputation in the web hosting business circles. In this, I mean that the companies' customers must say something positive about the company. If this is the case you can determine that their customers are giving them positive feedback and they are complimenting them due to their excellent service delivery.

II. Long existence

A good web hosting service provider should have been in existence for some reasonably long time. One is advised to go for such a company so that they can avoid the many flies by night websites that are formed overnight and usually put up by cons whose only interest is to corn unsuspecting clients by purporting to offer web hosting services. One advantage that comes with the companies that have been in the service for long is that they will be able to give you the reliable service that you so much require.

III. Ability to offer technical support

The other major characteristic that a good web hosting company should offer is that they should have the ability to provide all the technical support where and when you need it. One thing you should note is that in some particular instance, you will be in a situation where you will need to do some troubleshooting on your own, this will only be possible when you have a web hosting provider that can provide technical support to you or customer support by email or trough phone calls on a 24 hours basis.

IV. Customized services

When you are looking for a web hosting service provider be sure to select that which will offer customized services to you. They should have the ability to expand on the things that are already available and disposable to you at that particular moment. They should be able to offer you more

space, and more options for your service, or even they should be able to change the platform that you are using to sort out information.

V. Quality machinery and hardware

You should endeavor to deal with a company that has a good and diverse under the hood. What this means is that the machinery and hardware that they use in running their services are going to be able to offer all the different specialized services that you require.

VI. Security

A good web hosting service provider should have stuff like masking and shadow systems; they should enable easy backup in case of any emergency.

1.2. Flexible Email and Mailing list services

1.2.1. Email Hosting

Email hosting is the service of renting out and managing email servers. The server is a space where you can send, receive and store emails. With email hosting, you can set up professional email addresses on your domain name.

An email hosting account is dedicated to emails. Email hosting providers operate email servers. Email hosting should not be confused with regular email providers such as Google and Yahoo; email hosting is a premium service that operates emails on your own domain.

1.2.2. Email Hosting Services

There are several types of email services that a hosting company may offer. The value of each service depends on your needs. Taking the time to evaluate your email needs today (and how they might change as your business or team grows), will set you up for the future.

A. Free Web-hosting Email services

Web-hosting email services allow you to send and receive mail and manage email accounts through webmail and email clients. There's a variety of free email hosting options that you are probably already familiar with: Google's Gmail, Microsoft's Hotmail/Outlook, Yahoo, and AOL are household names.

Pros:

- Free with no commitment or contract.
- Free email services typically include enough file storage to meet the needs of small businesses and individuals.

Cons:

- Might have irritating banners or on/off page advertisements.
- Weaker security measures.
- Limited help and customer support options.
- Recipients doubt your authenticity.
- Less cloud storage space.
- Email addresses can be harder to remember than you@yoursite.com
- Free providers usually scan your email content for advertisement purposes and sell this data to third parties.

B. Professional Email Hosting

It’s not advised to use free email hosting if your business depends on email as a revenue driver you get what you pay for. For personal usage or start-ups, having reliable and secure software is also beneficial. Free and standard email hosting packages don’t always deliver the kind of quality that professional or private users need. Professional (paid) email hosting services are most likely to fit the needs of a growing business better.

C. Cloud Email Hosting and Shared Hosting

Cloud Email Hosting

Unless you're working in an enormous enterprise, with a budget to match, you almost certainly don't have the disaster recovery infrastructure and processes that the likes of Microsoft, Google, and other major cloud email providers have. So, if you truly are concerned about disaster recovery for your email, Private Email cloud providers are the way to go.

As with other cloud-based services, the advantages of using cloud-based email are operational efficiency and reduced costs. There’s no need to hire IT staff dedicated to managing internal email servers, and there’s no physical server equipment to maintain. Cloud hosting is the most scalable solution. You can take and lose resources as your user count changes, which keeps costs efficient.

Cloud servers are always kept up-to-date with the latest security patches and recent technological advancements. Benefits include increased bandwidth requirements and firewall settings for additional security, among many others. A final benefit to consider is that email lives on the Internet, so if your system goes down, everything is safely backed up.

Shared Hosting vs Cloud Server Hosting

The quality of email hosting varies depending on what you choose, but we can make some generalizations. With email hosted on shared hosting, the email accounts associated with a website are usually stored on the same server as the website. Typically, the email services offered with shared email hosting restrict certain features, from the number of email accounts included (such as how many outgoing emails can be sent), and whether your disk has space. Shared hosting plans include basic spam and virus protection.

On the other hand, when the email is hosted with professional cloud hosting services, accounts are most likely to be on dedicated email hosting servers. Further, users are often offered more premium features, from collaboration tools to more advanced anti-spam and virus protection services, larger email and file storage, full mobile support, and greater security provisions, to name a few.

1.3. Business needs support service standards

Website hosting is not always easy. Problems will come up, and if your web hosting service does not offer quality customer support, then you may find the experience stressful and frustrating.

That is why you need to be sure of any prospective hosting provider’s support system before signing up. Here we have mentioned a few ways to make that happen, along with the value of good customer support in web hosting:

How Important is Customer Support for Web Hosting?

Customer support of a web hosting company does not seem quite so significant initially. But when you run into errors, complications and queries on a daily basis, it turns out to be a pretty big deal. A good web host always makes sure that every member of their support team is fully trained and adequately prepared to guide customers through the intricate processes. Below are the major tasks where you will need help from the customer support team.

I. Installing new tools

Most web host companies nowadays offer many tools and software systems to streamline your website functionalities. Among the most popular software integrations, there Content Management Systems like WordPress, Joomla, and Magento. Such platforms are indispensable for blogging, eCommerce and many such specialized areas of the web.

Sometimes installing them is not just a button click. So, if you lose your way or get stuck, you can just contact the customer support team of that host to find your way back.

II. Site Errors and Malfunctions

Every website can fall victim to unforeseen errors and malfunctions. Not all site owners have technical experts on their team. Besides, the server infrastructure varies from host to host. Even if you have some prior experience in hosting or server management, the new host you have moved on to might not have any common feature.

This is where the customer support representatives can come in and get your website out of the mess. The hosting company usually trains them to resolve such situations in a matter of minutes. So, if you let them take over the situation, they can show a way out faster.

III. Web Hosting Upgrades

Sometimes, our website exceeds our expectation and grows a lot faster than we estimated. In such cases, it ends up demanding more resources than the allocated amount to handle the extra traffic and workload.

You can then seek help from the customer support members to upgrade these resources. They will let you know which packages can provide the required amount of resources and how much each cost. They will also guide you through the plan upgrades so that your website does not suffer from any data loss.

1.4. Data capacity for partial outages

Shared platforms, hosting services, DNS servers and even physical infrastructure all contribute to the interconnected, collective fragility of the Internet.

As the internet ecosystem of applications, services and physical infrastructure becomes more and more interconnected, outages can affect increasingly large portions of end-users' daily lives.

A variety of factors can interrupt service, from temporary disruptions to longer-term incidents or degradations. Common points of failure could be major ISPs, DNS providers, CDN providers, hosting or infrastructure vendors, or even APIs for information exchange.

When these service disruptions happen, the service uses to be unavailable or degraded from the end-user point of view, but what is hidden behind the causes of an outage?

Operators work hard worldwide to maintain the service quality and Internet usage experience, and in general terms, Internet service is stable. However, there are many problems that can affect network performance, and some of them are very complex to identify and understand. In the following, some of the most recurring ones:

- **Internet application (content providers):** Internet application-level concentration is easy to be seen and problematic for outages occurrence. Today, companies such as Google hold the Internet's most popular services. Including web searching, email hosting (Gmail) and video platform (YouTube). Application updates and application server/misconfiguration issues are frequent root causes among service infrastructure providers.
- **Service infrastructure (cloud service providers):** CDNs, DNS and cloud service providers are now a fundamental infrastructure part. For example, over 80% of top websites globally are using CDNs, such as Akamai or Fastly. Software updates during regular maintenance, misconfigurations and failure of HW/SW parts are frequent root causes among service infrastructure providers.
- **International connectivity (ISPs):** Global communications depend heavily on subsea cables and interconnection/peering providers that connect regions as well as telecommunication networks and content providers.
- **Others:** Service might be down because of severe weather such as earthquakes or hurricanes, as well as electrical power outages.
- **Telecommunications operators:**
    - **Access provision:** Internet connectivity depends on access and last-mile providers to get the content to the end-user and any failure in the access network part is critical. A teardown of access links or any access-related failure disconnects the customer from its provider affecting end-user connectivity.

- **Network Congestion**: It is the reduced quality of service that mostly occurs when too many users are trying to access a network at the same time in a certain geographical area. Typical effects include queueing delay, packet loss or the blocking of new connections. The circuit quality may gridlock or deteriorate causing the network collapse and impede users from making an efficient use of the network. Lack of prevision or support of user demand could be considered either a business-related matter or a technical one depending on the circumstances.
- **Transport Link failures:** This failure happens when the physical or logical links between network systems or equipment assets suffers an interruption. Probably link failures occur due to low converging time, previously allocated delay and bandwidth, and iterative loops which degrade network performance.
- **Equipment or node failure:** Lockups and overloads can also cause equipment failure. Furthermore, not grounding or protecting the equipment from surges can leave it vulnerable to circuit damage. Furthermore, these technical issues can be mitigated with the appropriate hardware setup and maintenance. This category may also include crashes or non-planned reboots, line card failures or resets, CPU overload or even human misconfiguration.
- **Routing problems:** In case of link and node failures, the routing might be able to automatically find a new stable configuration, guaranteeing good connections between any pair of nodes in the network. However, sometimes routing protocols do not repair connectivity issues the way they should, or worse, they can create outages of their own that wouldn't have occurred in a properly configured network.

1.5. Security technologies assessment

Internet Service Provider Security Policies

One of the most important elements of a secure network is the written policy that governs it. Any measures an ISP implements to increase security for itself and its subscribers will be ineffective if there is no written policy to back the security measures up. A well written security policy that includes sections on subscriber security, policies for server installation and

hardening, password policies, and network monitoring serves as a means to enforce security at the ISP, while helping to show that the ISP was not negligent in any liability issues.

ISP Secure Network Design

Security must be the foundation of an ISP's network design. Without proper security, compromises could result in service disruptions to thousands of users. The steps that ISPs take to ensure security on their networks could also have a direct effect on the security of their subscribers.

The first step an ISP should take is to place all network access hardware on a subnet that is separate from the subnet that the ISPs main servers are located on. By placing modem poles, DSL equipment, and other network access hardware on a separate subnet, an individual who might be attempting to sniff data would be forced to go through routing and switching equipment which would make it more likely that the ISP could detect that sniffing is taking place, and less likely that the individual would be successful. A network-based intrusion detection system (IDS) is a tool that will give the ISP a good indication of any intrusive activity to which users might be exposed. However, if the users are on the same subnet as the intrusion detection system, the ISP becomes legally responsible for the user’s security, since they are aware of the existence of malicious activity. Instead, if the users are on a separate subnet, and the ISP keeps routine logs of only the subnet it was running the IDS on, then the chance that the ISP can be held legally responsible for system compromises diminishes.

Other Security Measures

To bolster network security, an Internet Service Provider (ISP) can implement various measures beyond the fundamental network design. Access control lists (ACLs) on routers help prevent incoming packets with unauthorized source IP addresses, safeguard outgoing packets without a valid internal network source IP, and deny access to unused lower port numbers, addressing concerns like IP spoofing. ACLs also serve as a frontline defense against port scans and malicious activities from the Internet or home users.

For enhanced security, ISPs can deploy firewalls between servers, the Internet, and users, creating an additional layer of protection. Firewalls not only safeguard the ISP but also indirectly shield users by securing sensitive information stored on ISP servers. Implementing a robust password policy is crucial, mandating passwords to be at least six characters long,

containing alphanumeric and special characters. Additionally, maintaining consistent logs of user activity helps detect trends and potential security threats, aiding in timely intervention and protection against legal implications. Employing SSL on mail and web servers further fortifies user security by encrypting account information transmitted over the network. Network-based intrusion detection systems (NIDS) can also be utilized to monitor and proactively counteract intrusion attempts, contributing to a comprehensive security posture for the ISP.

Home Computer Security

While Internet Service Providers (ISPs) play a crucial role in network security, the most impactful measures occur at the user's home. ISPs should proactively inform customers about potential security risks associated with internet use, possibly through disclaimers or policy statements. This not only serves as legal protection for the ISP but also ensures users are aware of and accept the inherent risks. Supplying customers with printed literature detailing security risks and preventive measures, along with offering online resources and links to security-oriented websites, further empowers users.

Many ISPs provide setup CDs containing configuration utilities for internet access, often bundled with additional software. These CDs could include personal firewall software as an added benefit. Zone Alarm by Zone Labs is an example of a popular, user-friendly personal firewall that can be freely distributed by ISPs. However, encouraging users to install and configure personal firewalls can be challenging. To address this, ISPs could offer classes or demonstrations on internet security, covering topics such as virus protection, software updates, and the installation and configuration of personal firewalls. By actively educating users, ISPs can significantly enhance the security posture of home internet users.

1.6. Evaluation of scripting language availability

Web server scripting languages and frameworks are essential tools for system administrators who want to create dynamic and interactive web applications. However, there are many options to choose from, and each one has its own advantages and disadvantages. How do you decide which one is best for your web server? In this article, we will explore some factors that can help you make an informed choice.

I. Project requirements

The first thing you need to consider is what kind of web application you want to build and what features and functionalities it needs. Some scripting languages and frameworks are more suitable for certain types of projects than others. For example, PHP is widely used for content management systems, e-commerce platforms, and blogging sites, while Python is popular for data analysis, machine learning, and web scraping. You should also think about the scalability, security, and performance of your web application, and how well the scripting language and framework can support them.

II. Server environment

The second factor you need to consider is your web server environment and how compatible it is with the scripting language and framework you want to use. Some scripting languages and frameworks require specific server software, operating systems, or libraries to run properly. For example, Ruby on Rails is a framework that runs on the Ruby programming language, and it needs a web server that supports the Rack interface, such as Apache or Nginx. You should also check the availability and quality of the documentation, support, and community for the scripting language and framework you choose, as they can affect your development and maintenance process.

III. Your personal preference

The third factor you need to consider is your personal preference and comfort level with the scripting language and framework you want to use. Some scripting languages and frameworks have different syntax, style, and paradigms that can affect your coding productivity and quality. For example, Perl is a scripting language that allows multiple ways to accomplish the same task, while JavaScript is a scripting language that has some quirky features and behaviors. You should also consider your existing skills and experience with the scripting language and framework, and how much time and effort you are willing to invest in learning them.

IV. Budget and Resources

The fourth factor you need to consider is your budget and resources for your web application project. Some scripting languages and frameworks are more expensive or resource-intensive than others, depending on their licensing, hosting, development, and maintenance costs. For example, Java is a scripting language that requires a Java Virtual Machine to run, which can

consume more memory and CPU than other scripting languages. You should also consider the availability and cost of the developers, tools, and services that you need for your web application project, and how they fit your budget and resources.

V. Testing and Debugging options

The fifth factor you need to consider is your testing and debugging options for your web application project. Some scripting languages and frameworks have more or less support for testing and debugging tools and techniques, which can affect your code quality and reliability. For example, Python is a scripting language that has a built-in debugger and a rich set of testing frameworks and libraries, while Bash is a scripting language that has limited debugging capabilities and relies on external tools for testing. You should also consider the ease and speed of testing and debugging your web application, and how they affect your development cycle.

VI. Future plans

The sixth factor you need to consider is your future plans for your web application project. Some scripting languages and frameworks are more or less adaptable and flexible for changing requirements, new features, or different platforms. For example, Node.js is a framework that runs on the JavaScript programming language, and it allows you to use the same language for both the front-end and the back-end of your web application, which can simplify your development and deployment process. You should also consider the popularity and demand for the scripting language and framework you choose, and how they affect your career opportunities and marketability.

1.7. Assessment of optional server applications for advanced web functions

In the realm of advanced web business functions, selecting the right server applications is paramount for ensuring performance, security, and scalability. Here's a brief overview of key applications:

A. Web Server

- *Options:* Apache, Nginx, Microsoft IIS
- *Considerations:* Choose based on performance, security features, and compatibility with frameworks. Scalability and ease of configuration are vital.

B. Database Server

- *Options:* MySQL, PostgreSQL, MongoDB

- *Considerations:* Select based on data type, scalability, ACID compliance, and compatibility with your chosen programming language and framework.

C. Application Server

- *Options:* Tomcat, JBoss, Microsoft ASP.NET
- *Considerations:* Evaluate the ability to handle dynamic content, scalability, and compatibility with your programming language and frameworks.

D. Load Balancer

- *Options:* Nginx, HAProxy, F5 BIG-IP
- *Considerations:* Choose one supporting your web and application servers, with features like SSL termination and scalability.

E. Caching System

- *Options:* Varnish, Redis, Memcached
- *Considerations:* Choose based on content type, compatibility, and effective cache invalidation strategies.

F. Security Applications

- *Options:* Web Application Firewall (WAF), IDS, SIEM
- *Considerations:* Prioritize integrated security measures, regular updates, and monitoring against emerging threats.

1.8. Client selection criteria with ISP hosting service

Selecting the right Internet Service Provider (ISP) hosting service for your business is crucial for ensuring a reliable online presence. Here are key client selection criteria to consider when evaluating ISP hosting services:

I. Bandwidth and Speed:

- Ensure the ISP offers sufficient bandwidth to accommodate your current and future needs.
- Consider the speed and latency of the connection, especially if your business relies on real-time applications or large data transfers.

II. **Reliability and Uptime:**

- Check the ISP's historical uptime performance and reliability. Look for guarantees or Service Level Agreements (SLAs) that ensure a high level of service availability.

III. **Scalability:**

- Assess the ISP's ability to scale its services to meet the growing demands of your business. Consider future expansion plans and the ease with which you can upgrade your hosting plan.

IV. **Security Measures:**

- Evaluate the ISP's security measures, including firewalls, DDoS protection, and other security protocols. Ensure that the hosting environment is secure against potential threats.

V. **Support and Customer Service:**

- Consider the responsiveness and quality of customer support. A reliable ISP should offer prompt and effective support to address any issues that may arise.

VI. **Technical Features and Compatibility:**

- Check the technical features offered by the ISP, such as support for specific web servers, databases, programming languages, and content management systems. Ensure compatibility with your existing technology stack.

VII. **Data Backup and Recovery:**

- Assess the ISP's data backup and recovery procedures. Regular backups and a robust recovery plan are essential for safeguarding your business data.

VIII. **Network Redundancy:**

- Look for ISPs with redundant network connections to minimize the risk of downtime in case of a network failure. Redundancy ensures continuity of service.

IX. Location and Geographic Coverage:

- Consider the geographic coverage of the ISP's data centers. Opt for a provider with data centers strategically located to ensure low latency and faster access to your website or applications.

X. Cost and Value for Money:

- Compare the pricing plans and contractual terms of different ISPs. Consider the overall value for money, taking into account the features, support, and reliability offered by each provider.

XI. Service Level Agreements (SLAs):

- Review SLAs carefully. Look for guarantees related to uptime, performance, and issue resolution. SLAs provide a clear understanding of the level of service you can expect.

XII. Reviews and Reputation:

- Research reviews and testimonials from other clients who have used the ISP's hosting services. A positive reputation and feedback from existing clients can be indicative of the provider's reliability.

By carefully evaluating these criteria, you can make an informed decision when selecting an ISP hosting service that aligns with the specific needs and goals of your business.

Self-Check 1

Part-I: Choose the correct answer

1. A company that provides individuals and organizations access to the internet and other related services.
    A. Web Hosting
    B. ISP
    C. Cloud Service
    D. Email Hosting
2. A service that allows organizations and individuals to post a website or web page onto the Internet.
    A. Web Hosting
    B. ISP
    C. Cloud Service
    D. Email Hosting
3. Which one of the following is not a characteristics of a good web hosting company?
    A. Long existence
    B. Good reputation
    C. Cloud Service
    D. Customized services

Part-II: Answer the following questions accordingly

1. What do we mean by Cloud Service?
2. What is the importance of customer support for Web Hosting?
3. Explain the purpose of IDS in ISP security?

Unit Two: Permanent Online Presence

This unit to provide you the necessary information regarding the following content coverage and topics:

- Server performance and availability
- Negotiate escalation procedures and performance standards
- Security and backup procedures for business needs

This guide will also assist you to attain the learning outcomes stated in the cover page. Specifically, upon completion of this learning guide, you will be able to:

- Utilize monitoring tools to track server performance.
- Define performance standards that align with organizational goals.
- Create and implement security measures suitable for business needs.

2.1. Server performance and availability

2.1.1. Server monitoring

It is a vital part of managing your server infrastructure. In addition to keeping track of hardware failures, it helps you identify potential problems before they become serious.

Servers are essential components of modern IT infrastructures and provide services such as email, web hosting, database management, and other applications. If you run a large organization or company, chances are you have servers, at least some of them.

Monitoring servers is important because it lets you detect problems early, preventing downtime and data loss. There are several ways to monitor server performance, from simple tools to complex solutions.

2.1.2. Types of Server Monitoring

Let's take a closer look at the various types of server monitoring software. Different types are available as a function of what they do, and you can better understand what to look out for.

I. Availability/Uptime Monitoring

Availability/uptime is the single most important metric of server monitoring, and other metrics may matter if the server is inaccessible or otherwise unavailable. Server availability/uptime monitoring keeps track of the server to ensure it's working properly and responding to requests sent to the server.

The possible reasons for unavailability are varied. Perhaps a systems administrator tripped on a networking cable or power cord inside the data center that he did not notice, or somebody deliberately turned off the server for hardware repair or maintenance but forgot to warn users.

II. Performance Monitoring

Keeping track of uptimes is crucial, and it's important that your users can reach your servers whenever needed. However, uptime and availability are the bare minimum of server monitoring.

Performance monitoring will let you keep track of all the issues discussed. Performance evaluation ensures applications start quickly and respond to user requests as expected.

III. Resource Monitoring

A server is not one single component; instead, it consists of multiple parts. Monitoring of the server should focus on the performance of these components. Hard Disk, RAM, and Processor are the three main components of a server.

Effective resource monitoring is an important part of any IT infrastructure. You can monitor your servers' temperatures and voltages to see how they're doing. But effective resource monitoring goes beyond just those two items, and it also includes disk space usage, memory utilization, CPU load, network bandwidth, and much more. With this information, you'll know whether your servers are running smoothly and efficiently or if something needs to be fixed.

IV. Error Monitoring

Errors are inevitable. Whether they're caused by users entering invalid data, applications not saving data to databases, or conflicts between multiple systems, errors will happen. However, you should be worried about a sudden increase in the number of errors occurring.

Error monitoring systems will notify administrators when the frequency or type of errors deviates from the usual pattern.

V. Log Monitoring

Server logs can provide valuable information about what is happening on your servers, and application logs can help identify problems with applications running on your servers. Monitoring these types of logs can help you determine if something terrible happened on one of your servers.

For best results, log files should be stored centrally. That speeds up the logging process since the software doesn't have to access the log file remotely.

VI. Database Monitoring

Database monitoring is keeping track of important performance metrics that give insight into how well your databases perform. These metrics include response times, availability, throughput, and memory usage. Tracking these metrics over time allows you to identify trends and patterns that help you decide what changes to make to your systems.

A good database monitoring strategy includes collecting data from various sources, including logs, event handlers, and third-party tools. This allows you to analyze everything happening in your environment while giving you access to historical information that helps you understand how your systems work together.

The key is to find out where the bottlenecks occur in your architecture and design solutions to address those issues. For example, if your database is running slowly because there aren't enough resources to handle requests, consider adding additional servers or moving some workloads onto another server. If your database is responding slowly because of too much load, you might look for ways to reduce the amount of traffic being handled by your applications.

VII. Security Monitoring

The types of monitoring that we've discussed thus far relate to issues that occur unintentionally. However, certain system issues are caused by the deliberate actions of users, malware, or third parties, which may put your data, systems, or business at risk.

The default solution to server security issues is installing an anti-malware program. However, anti-malware alone won't protect your server against malicious threats. A good security monitoring program will not only detect malware but will also watch for unusual system and user activities.

2.2. Negotiate escalation procedures and performance standards

Negotiating escalation procedures and performance standards with an Internet Service Provider (ISP) is a critical aspect of ensuring a reliable and responsive online infrastructure. The following paragraphs outline key considerations and strategies for negotiating these aspects with an ISP:

A. Establishing Clear Performance Standards

In the negotiation process with your ISP, it is imperative to define and establish clear performance standards that align with the specific needs and expectations of your business. This involves identifying metrics such as bandwidth, latency, and uptime, and agreeing on target levels for each. Be explicit in detailing the expected performance benchmarks and ensure that they are measurable and achievable.

B. Defining Escalation Procedures

Escalation procedures are crucial for addressing issues promptly and efficiently. Work with the ISP to define a clear and hierarchical escalation process for different types of incidents, ranging from minor disruptions to critical outages. Clarify the roles and responsibilities of both parties during escalations, and establish communication channels that facilitate swift resolution. This includes specifying points of contact, response times, and steps for elevating concerns to higher levels of support.

C. Customizing Service Level Agreements (SLAs)

Service Level Agreements (SLAs) formalize the agreed-upon performance standards and escalation procedures. Negotiate SLAs that accurately reflect the priorities and requirements of your business. Include details such as uptime guarantees, response times for support inquiries, and the compensation or penalties associated with deviations from agreed-upon performance levels. A well-defined SLA serves as a contractual framework that helps maintain accountability and transparency between your business and the ISP.

D. Continuous Monitoring and Reporting

Incorporate provisions for continuous monitoring and reporting within the negotiation process. Define how performance metrics will be monitored, measured, and reported by the ISP. Real-time monitoring tools can provide both parties with insights into the network's health and performance. Regular reports help track adherence to SLAs and provide data for collaborative performance reviews, enabling both sides to identify areas for improvement and optimization.

E. Flexibility and Review Mechanisms

Negotiate for flexibility within the agreement to accommodate changes in your business requirements or unexpected challenges. Include review mechanisms that allow for periodic assessments of the agreed-upon performance standards and escalation procedures. This ensures that the partnership remains adaptable to evolving technological landscapes and the dynamic needs of your business.

F. Incentives for Performance Improvement

Consider incorporating incentives for exceptional performance and service quality. Mutual success should be celebrated, and incentives can encourage the ISP to go above and beyond in

delivering reliable services. Conversely, establish fair consequences for persistent underperformance, ensuring that there are mechanisms in place to address issues proactively.

Successful negotiations with an ISP involve establishing clear performance standards, defining escalation procedures, customizing SLAs, incorporating continuous monitoring and reporting, ensuring flexibility, and creating mechanisms for both incentives and consequences. A well-negotiated agreement lays the foundation for a robust and collaborative partnership that benefits both parties in maintaining a high-performing online presence.

2.3. Security and backup procedures for business needs

The ever-expanding role of data in every facet of our lives has made it increasingly important to plan for the possibility that something might go wrong. And given the various threats to data, chances are it probably will. That's why you should be prepared all the time. This article provides an easy five-step back up security measures plan.

i. Encrypt Data and Control the Encryption Keys

Without proper encryption, your sensitive files might find their way into the wrong hands, leading to disasters like identity theft. That's why you should create backup copies of all files and encrypt the ones containing vital information.

Data encryption protects your digital data confidentiality while it is transmitted online or through computer networks, or stored on a particular system. No wonder modern encryption algorithms are a crucial aspect of IT systems security and communications.

These algorithms offer confidentiality and drive primary security initiatives, such as integrity, non-repudiation, and authentication.

Integrity serves as proof that the contents of a message remain unchanged since it was sent while authentication permits you to verify the origin of the message. Moreover, non-repudiation makes it so the sender of the message cannot deny sending it.

Moreover, you should manage the encryption keys to add another layer of privacy and security to your data. Chances are different, incompatible encryption tools may be used to secure your data, leading to numerous encryption keys. You must securely store, protect, and retrieve each of them.

After activating all the spoke components, every decryption and encryption activity of the formerly clear text data is locally performed to reduce the risk of a single or network component failure having a widespread impact on the overall state of your data security.

ii. Control the Keys to the Storage

As far as storage of the data backups is concerned, the debate involving cloud storage and on-premises storage still wages on. So, you should consider the pros and cons of each, and make a poignant decision.

One major difference between cloud storage and on-premises storage is the financial aspect. Take a look at the highlights of on-premises storage:

- Storage resources are dedicated to the company.
- High-cost investment.
- Storage resources are procured, owned and handled by the enterprise.
- Enterprise secures the storage data and resources.

The features of cloud storage include: Third-party ownership and management of storage resources.

- Storage resources can be purchased pre-paid or on a pay-as-you-go basis.
- Software gets updated as part of the active subscription.
- Storage resources are often shared in a multi-tenant environment.
- No need for IT to install patches and updates.

iii. Don’t Let Users In

Introduce users to the importance of backup security measures, rules, and responsibilities. Let them know how secure data backups are necessary for data protection, including personal.

You can go one step further and execute special social engineering attacks to scrutinize user awareness and identify possible security breaches.

Deny any permissions that may be requested to enter the backup site for gathering files. Why? Because backup is not the same as file sharing. Remember, the more people have access to your backup data, the more it is likely that you might be compromised. So, try to limit user access to the bare minimum.

If required, users can search for or browse the metadata information associated with files since it is gathered and stored in the backup index.

Allow your users to browse and search all the data backup up from common resources like file servers and shared laptops, but turn down access requests. You may even restrict end-user access to common resources by turning on the access control on the client data.

iv. Create a New User for Backups Instead of Using "Admin"

To implement backup security measures and software on your system, you must operate it under a specific user in the Operating System. In some cases, the software will lack the right to make backup copies of files and folders.

You might be tempted to make the problem go away by giving domain or local admin but this is one of the biggest security mistakes you can make.

The right solution to this backup hurdle involves creating a separate user. When backing up your data to a network share or NAS, provide the necessary permissions to the given user.

v. Think Ahead

Smartphones break. Laptops crash. The dreaded "blue screen of death" makes an unwelcome appearance – these are just a few of the reasons why it's necessary to keep backup copies of your data. Of course, you might not lose all your data in the event of a disaster, but it's never a bad idea to take precautionary measures.

Self-Check-2

Part-I: Say True or False

1. Database monitoring include response times, availability, throughput, and memory usage.
2. Escalation Procedure serves as a contractual framework that helps maintain accountability and transparency between your business and the ISP.
3. Successful negotiations with an ISP involve establishing clear performance standards, and defining escalation procedures.

Part-II: Give short answer

1. List the types of system monitoring. (At least three)
2. Identify the major difference between cloud storage and on-premises storage.
3. What is the need of data encryption?

Unit Three: Technical Requirements for Web hosting

This learning guide is developed to provide you the necessary information regarding the following content coverage and topics:

- OS compatibility with business software and applications
- Web-host servers for dynamic websites
- Security systems and payment technologies

Implementing security systems and payment technologies

This guide will also assist you to attain the learning outcomes stated in the cover page. Specifically, upon completion of this learning guide, you will be able to:

- Understand the operating system requirements of business software and applications.
- Evaluate the capabilities of web-host servers to support dynamic websites.
- Explore and implement robust security systems to safeguard data and sensitive information.

3.1. OS compatibility with business software and applications

An operating system is a system software program that distributes and manages the server's resources. It acts as a communication bridge between user's and computer's hardware hence, prioritizes user's request and programs. An operating system ensures that the user's content on the server does not interfere with other users. Operating System is one of the most important support systems for a server that ensures smooth processes. It is the foundational software on your server.

While availing of the web hosting services, one of the major concerns is to choose the right operating system.



Figure 3.1: OS types

3.1.1. Types of Operating Systems

There are different operating systems (OS), and they have their benefits to offer. Choosing one for your web hosting is a critical decision that can significantly impact your website’s performance. An OS is software that runs your website and creates a bridge between you and your web hosting service.

The two most popular ones used for running websites are Linux and Windows-based OS.

LINUX

Linux is an open-source operating system created out of the need for a free, robust, and secure OS. Open-Source Operating System means you can access the code freely with no cost or any restrictions to edit or change anything you want on your website from here on in. It also allows developers worldwide to contribute new ideas to make it better all the time. Security-wise they are perfect.

They are very secure, and the OS is constantly updated with security patches, making it one of the most secure operating systems available. Speed-wise they are also great, especially when running on a VPS or dedicated server.

WINDOWS

Windows is the most popular OS used globally and has been around since 1985. It is created and owned by Microsoft and used by millions of people all over the globe.

Its popularity comes from it being very user-friendly and easy to use. It makes it perfect for home users as well as businesses. Microsoft also offers a wide range of software compatible with Windows, which can make your life much easier.

Linux vs. Windows: the verdict?

Each OS has its benefits and drawbacks, so it ultimately comes down to what is most important to you when making your decision. If security, speed, and affordability are high on your list, then Linux would be an excellent option for you. However, if ease of use and compatibility with other Microsoft software is more critical, then Windows would be a better choice.

Whichever operating system you choose, make sure to research the best hosting service to suit your needs and find one that offers unlimited bandwidth, disk space as well as 24/7 technical support.

3.1.2. Choose the right OS for Web Hosting

When you select a website hosting operating system, there are a few things that you need to consider.

Budget

The first thing that you need to take into account is your budget. As mentioned above, there are different types of operating systems available for hosting platforms. You should choose one which suits you according to your requirements and financial capacity.

Linux is an open-source platform which means that you will not have to pay any amount. However, some companies host platforms that charge a nominal fee per month or year.

Windows operating system is the other one available in the market, but it will cost you money according to your needs and requirements. It can be paid annually or monthly, depending upon what suits you best.

Requirements

The second factor that you need to consider is your website requirements. Different websites have different requirements when it comes to hosting. Some might require more bandwidth and storage space than others, or they might need a specific type of software installed on the server.

You should choose an operating system that can cater to your website's needs so that you don't have to worry about anything else once it gets hosted.

Linux is known for its security and stability features, while the Windows operating system is best suited for gaming and multimedia purposes. It would be best to decide which one works better for your website.

Technical Knowledge

The third factor is your technical knowledge. It might not be an issue for some people, but if you're not comfortable dealing with code and software, you might want to choose an easy platform to use.

Windows operating system falls in this category as it is a user-friendly platform that does not require any coding knowledge or experience. On the other hand, Linux can be difficult to use for beginners, so make sure you are familiar with its workings before making your decision.

Hosting companies usually have tutorials and manuals available online, which will help you use their services. You can contact their customer support if you have further questions.

Support

The fourth factor you need to consider is the level of support. It is essential because you don't want to be stuck with a platform where you can't get help.

Hosting companies usually have different types of support available, depending on the operating system that you choose. Windows-based hosting platforms usually offer telephone and chat support, while Linux-based hosting platforms offer email and ticketing systems. When making your decision, ensure to check the availability of these forms and their respective benefits before signing up.

Compatibility

The fifth and final factor that you need to consider is compatibility. It means ensuring that the operating system you choose is compatible with the software and applications that your website uses.

Most hosting companies offer a list of compatible software on their websites, so make sure to check this before deciding. Linux is known for its compatibility with various software and applications, while the Windows operating system is not as versatile.

You need to consider five factors when choosing a website hosting operating system. By considering these points, you will be able to make an informed decision that is right for your website.

3.2. Web-host server for dynamic websites

3.2.1. Dynamic Websites

A dynamic website shows different content to different users. The content may depend on their locations, time zones, language preferences, or past behavior on the website.

Dynamic sites use a server-side programming language to connect with a database to enable interactive features and alter the content. Their common use cases include forums, social media platforms, and eCommerce sites.

A dynamic website shows different content to different users. The content may depend on their locations, time zones, language preferences, or past behavior on the website.

Dynamic sites use a server-side programming language to connect with a database to enable interactive features and alter the content. Their common use cases include forums, social media platforms, and eCommerce sites.

3.2.2. Dynamic Website Types

Depending on the scripting language, there are two types of dynamic websites.

Client-Side Scripting

A client-side scripting dynamic website changes its content in response to user actions on the page, such as clicking a button.

Generally speaking, client-side scripted website content is loaded in the visitor's web browser instead of the server. This script determines what user interactions trigger the event and which page content changes.

When building this type of dynamic website, commonly-used client-side scripting languages include JavaScript and VBScript. As it doesn't use any server-side scripting languages, a dynamic site can be hosted statically.

Server-Side Scripting

Server-side scripted web pages' content is rendered on the host and changes before being displayed. This script instructs the application server on how to assemble the requested page.

Users' requests and inputs on the website can trigger the script. For instance, when users log in to their eCommerce accounts, the script will instruct the server to show their cart items.

Server-side scripts are used to build an interactive website. They let users enter data into forms or upload images, which will be stored in a database.

3.2.3. Build Dynamic Websites

Dynamic web pages require complex software and additional scripting language, making them more difficult to develop than static websites. They are also more costly and require more computing power.

A static website has fewer security risks since it doesn't connect to databases or external applications. Cyber criminals often exploit these connections to attack dynamic sites.

That said, a dynamic web page has some advantages:

- **Easier maintenance.** Developers can automatically update multiple dynamic web pages simultaneously. To update static pages, they must modify each file's source code.
- **Content personalization.** Dynamic websites provide personalized content recommendations according to user needs. It helps improve conversion rates and user experience.
- **More features.** Unlike static sites, dynamic pages are interactive and have more features. For instance, users can register an account or create a post on your site.
- **Better search engine optimization (SEO)**. Dynamic websites let you easily add SEO tools to optimize your content. Despite being quicker, a static website may rank lower in search engines.

Since static and dynamic websites have their own advantages and downsides, choose one according to your needs. We recommend creating a static website if you don't need many pages and comprehensive features. On the other hand, a dynamic website is a must if you want to run a successful eCommerce store.

3.3. Security systems and payment technologies

3.3.1. Securing Payments in E-commerce

In the ever-growing world of e-commerce, securing payment transactions has become a top priority for businesses and consumers. With over 4.9 billion internet users worldwide, e-commerce sales continue to increase. As a result, the issue of secure payments becomes critical, and businesses must give it the attention and resources it deserves.

Online security threats are constantly evolving, and e-commerce businesses must stay up to date with the best practices and latest technologies to protect their customers' sensitive financial information. This article will explore the online payment ecosystem, explain why secure payments are essential for e-commerce, and provide insights into payment security standards and regulations.

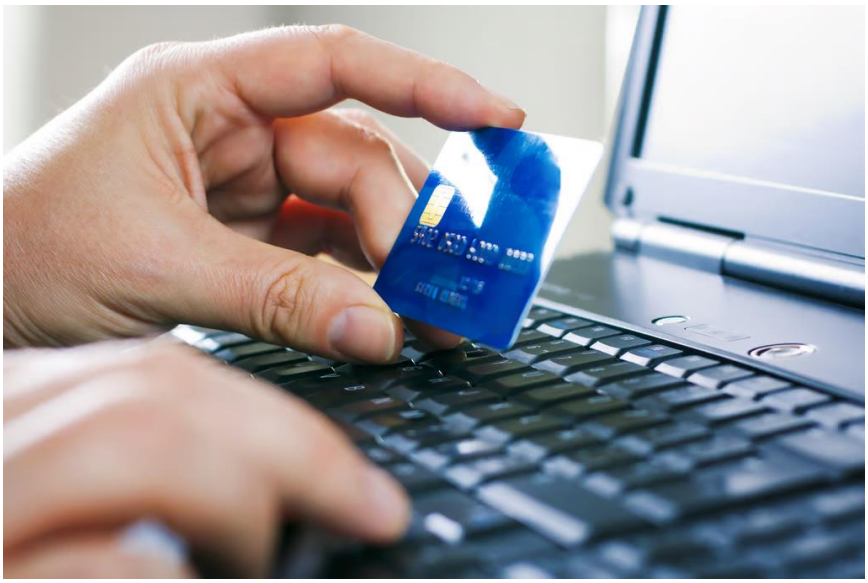


Figure 3.2: E-commerce Payment

3.3.2. Understanding the Online Payment Ecosystem

The online payment ecosystem comprises several components that enable seamless and secure payment transactions. The primary components of this ecosystem are:

- **Customers:** They initiate transactions by choosing the goods or services they want to purchase and providing their payment details.
- **Merchant Websites/Apps:** The e-commerce platform, developed by a merchant, which displays the products and services for purchase and collects customers' payment information.
- **Payment Gateways:** They act as intermediaries between the merchant website and the payment processor. Payment gateways encrypt customer payment details and transmit them securely to the payment processor.
- **Payment Processors:** They receive, validate, and process payment information from the payment gateway, acquiring the funds from the issuing bank and depositing them into the merchant's account.
- **Issuing Banks:** Financial institutions that issue credit or debit cards to consumers on behalf of the card networks (e.g., Visa or Mastercard).

- **Card Networks:** Associations or organizations responsible for establishing and maintaining the rules and parameters that govern how electronic payment transactions are processed (e.g., Visa, Mastercard, American Express, etc.).

To ensure secure transactions, all these components must work together cohesively and implement security measures that protect sensitive customer data.

3.3.3. Secure Payments are Essential for E-Commerce

Securing payments should be among the top priorities for any e-commerce business. Here are some compelling reasons why secure payments are essential for e-commerce:

- **Build Trust and Confidence:** By ensuring that payment transactions are conducted securely, you can instill trust and confidence in your customers, leading to long-term relationships. Customers who trust your ability to protect their financial information will likely make repeat purchases and recommend your business to others.
- **Prevent Fraud:** Online payment fraud can significantly impact an e-commerce business, resulting in lost revenue and damage to its reputation. By implementing strong security measures, businesses can minimize the risk of fraud and protect their customers, transactions, and bottom line.
- **Compliance with Regulations and Standards:** E-commerce businesses must comply with various payment security regulations, such as the Payment Card Industry Data Security Standard (PCI DSS). Ensuring secure payments helps businesses stay compliant and avoid potential non-compliance penalties.
- **Protect Customer Data:** A data breach can lead to the exposure of sensitive customer information, resulting in identity theft, financial loss, and damage to the business's reputation. Strong security measures can help prevent data breaches and protect customer data from theft or misuse.
- **Reduce Chargebacks:** Chargebacks occur when a customer disputes a purchase, often due to unauthorized transactions or fraud. Secure payment processing can help minimize the risk of chargebacks and the associated costs, such as fees, lost revenue, and damage to your merchant account reputation.

3.3.4. Practices for Securing Payments in E-Commerce

Implementing the best practices for securing payments in e-commerce helps businesses comply with security regulations and reduces the likelihood of security breaches and fraud attempts. Here are some best practices that e-commerce merchants should consider:

A. Secure Data Storage

To prevent unauthorized access to sensitive data, businesses should ensure that cardholder information and other sensitive information are stored securely, using encryption, tokenization, or other data protection mechanisms.

B. Encryption

All sensitive data transmitted over public networks, such as payment details, should be encrypted using SSL (Secure Sockets Layer) or TLS (Transport Layer Security). This ensures that attackers cannot easily decipher intercepted data.

C. Strong Authentication and Access Control

Implementing multi-factor authentication (MFA) for all user accounts, limiting access to sensitive systems, and regularly reviewing access permissions significantly reduces the risk of unauthorized access.

D. Secure Code Development

E-commerce websites and applications should be developed using secure coding practices to minimize vulnerabilities that attackers can exploit. Regular code reviews and vulnerability scanning should be conducted to ensure security.

E. System Monitoring

Continuously monitoring network and system activity helps identify suspicious activity or potential breaches, enabling prompt response to mitigate threats. Log reviews, intrusion detection systems, and other monitoring tools can be employed.

F. Regular Security Audits

Conducting regular security audits helps identify gaps in security measures and compliance, providing an opportunity to address them before attackers can exploit them.

Self-Check-3

Part-I: Choose the correct answer

1. Which of the following is an open-source operating system known for security and constant updates?

   A. Windows C. Linux

   B. macOS D. Android

2. What is one advantage of choosing Linux for web hosting?

   A. Limited customization options

   B. Expensive licensing fees

   C. Open-source with no cost restrictions

   D. Compatibility issues with software

3. When considering the right OS for web hosting, what does technical knowledge refer to?

   A. User interface familiarity C. Internet connection speed

   B. Programming and coding skills D. Number of installed applications

4. Which factor is NOT mentioned as a consideration when choosing a website hosting operating system?

   A. Technical knowledge C. Compatibility

   B. Server color D. Budget

5. Why is securing payments essential for e-commerce?

   A. Increase charge C. Encourage online fraud

   B. Build trust and confidence D. Decrease customer satisfaction

Part-II: Matching Questions

A	**B**
1. Payment Gateways	A. Financial institutions issuing cards
2. SSL/TLS Encryption	B. Website or app developed by a merchant
3. Issuing Banks	C. Intermediaries between merchant and processor
4. Dynamic Websites	D. Technology for securing data transmission
5. Merchant Websites/Apps	E. Websites content-based user interactions

Unit Four: Benchmark and Test Performance

This learning guide is developed to provide you the necessary information regarding the following content coverage and topics:

- ISP performance during on and off-peak times
- Email and Mailing services backup procedures
- Services align with business needs
- Quality of service delivered

Implementing security systems and payment technologies

This guide will also assist you to attain the learning outcomes stated in the cover page. Specifically, upon completion of this learning guide, you will be able to:

- Conduct performance testing of the Internet Service Provider (ISP) during both on-peak and off-peak times.
- Develop and implement backup procedures for email and mailing services.
- Evaluate the alignment of support services provided by the ISP with the specific needs of the business.

4.1. ISP performance during on and off-peak times

4.1.1. Navigating Peak and Off-Peak Hours

In today's tech-driven world, it is crucial to understand how data usage works, especially during peak and off-peak hours. With the skyrocketing demand for data consumption, it becomes essential for internet users to optimize their online activities to avoid bottlenecks and unnecessary costs. Join us as we delve into the intricacies of data usage, providing you with valuable insights and practical tips on how to navigate peak and off-peak hours with ease.

4.1.2. Importance of Understanding Peak and Off-Peak Hours

Before we delve into how to efficiently manage data usage, it is important to understand the concept of peak and off-peak hours. Internet service providers often categorize certain times of the day as peak hours, where network traffic is at its highest due to a surge in user activity. These peak hours usually coincide with periods of heavy internet usage, such as evenings when people return from work or school.

During peak hours, network congestion may occur, resulting in slower internet speeds and buffering. This can be frustrating for users who depend on a reliable and fast internet connection for various activities, including streaming, gaming, or remote work. Conversely, off-peak hours refer to the times when internet usage is relatively lower, leading to a smoother and faster online experience.

4.1.3. Understanding Data Usage and Bandwidth

To effectively navigate peak and off-peak hours, it is essential to understand data usage and bandwidth. Data usage refers to the amount of data consumed by an internet user. This can encompass various online activities such as browsing websites, streaming videos, downloading files, or using applications. It is measured in gigabytes (GB) and is an integral component of most internet plans.

Bandwidth, on the other hand, refers to the maximum amount of data that can be transmitted over an internet connection within a given period. It influences the speed at which data is transferred. Higher bandwidth allows for faster data transfer and consequently a smoother online experience.

4.1.4. Optimizing Data Usage during Peak Hours

Now that we understand the basics, let's explore some practical tips to optimize data usage during peak hours:

- **Limit streaming quality:** Adjusting the quality settings on streaming platforms such as Netflix or YouTube can help reduce data consumption. Opting for lower resolutions can significantly lessen the amount of data used while still ensuring an enjoyable viewing experience.
- **Download content in advance:** If you anticipate peak hours and plan to watch or listen to media, consider downloading it during off-peak hours. This way, you can enjoy your favorite content without buffering or interruptions when network traffic is high.
- **Maintain device updates:** Keeping your devices and applications up to date can contribute to more efficient data usage. Software updates often come with optimizations that can help streamline data consumption, allowing you to make the most out of your internet plan.

4.1.5. Mastering Your Data Plan: Maximize Value during Peak and Off-Peak Times

With more and more people relying on smartphones, tablets, and other connected devices, it's essential to optimize your data usage and ensure that you get the most out of your plan.

Whether you are a heavy data user or simply want to avoid unnecessary charges, understanding how to master your data plan will help you save money and have a smoother online experience. In this article, we will explore different strategies to maximize the value of your data plan during peak and off-peak times.

I. Track Your Data Usage

The first step to mastering your data plan is to keep a close eye on your data consumption. Most smartphones provide built-in tools to monitor your data usage, allowing you to track how much data you've used and which apps are consuming the most. By regularly monitoring your usage, you can identify any data-hungry applications and take necessary action.

- Use data tracking apps to gain more detailed insights into your data usage.
- Set up data usage alerts to receive notifications when you reach certain thresholds.

- Review your data usage regularly and adjust your habits as needed.

II. Utilize Wi-Fi Networks

Connecting to Wi-Fi networks whenever possible is one of the easiest ways to conserve your precious mobile data. By using Wi-Fi, you can enjoy faster speeds and avoid using your cellular data altogether. Take advantage of Wi-Fi networks available at home, work, cafes, or public places to limit your reliance on the cellular network.

- Ensure you are connected to a trusted and secure Wi-Fi network.
- Turn on Wi-Fi Assist feature on your phone to automatically switch to Wi-Fi when available.
- Consider using a virtual private network (VPN) when connected to public Wi-Fi networks to enhance security.

III. Optimize App Settings

Many apps have settings that allow you to control how they consume data. By tweaking these settings, you can minimize their impact on your data plan.

- Disable auto-play for videos and disable automatic app updates.
- Set up social media apps to refresh content manually instead of automatically.
- Configure email apps to fetch new messages at specific intervals instead of continuously syncing.

IV. Stream and Download Smartly

Streaming music and videos can quickly eat into your data allowance. However, by making smart choices, you can still enjoy your favorite content without draining your plan.

- Download music and videos over Wi-Fi for offline consumption.
- Consider using streaming services that offer data-saving modes or lower bitrates.
- Adjust streaming quality settings to a lower resolution if needed.

V. Take Advantage of Off-Peak Times

Off-peak times, typically during the late night or early morning hours, often offer faster and more stable network speeds. By scheduling your data-intensive activities during these periods, you can make the most of your data plan without experiencing any slow-downs or congestion.

- Check with your service provider to determine off-peak hours.
- Download large files or perform system updates during off-peak times.
- Utilize cloud storage services to sync and back up your data during off-peak hours.

4.2. Email and Mailing services backup procedures

A backup of a server is often created in order to be able to restore data if the original server crashes or becomes inaccessible. This is especially important in organizations for legal or business reasons.

The process of backups is done by making an exact copy of the server's data storage device in order to prevent data loss. This operation can be done manually by copying all files onto an external storage device. This can be also done automatically by setting up a scheduled process.

The backup process is much more complex in action. It requires a lot of time, expertise, and caution to be successful. There are different factors a system administrator should take into account in order not to lose any data, especially when it's done manually.

Here are some tips when choosing your e-mail and collaboration platform to create a digital workplace for your business:

- Pay attention that an integrated backup system is always preferred over third-party solutions,
- Make sure that you back up all of the important data on a regular basis relying on a real-time backup plan,
- Off-site backups are a good way to protect your data from natural disasters,
- The amount of time and effort required to implement the backup plan,
- Lastly, if the backup system is optimized to work in your environment for better performance.

4.3. Services align with business needs

The following are several types of support services that companies can use to maintain their IT infrastructure and other procedures to increase their effectiveness:

I. Data storage

Many businesses store data and require a place to do so in an easy and effective manner. There are several data storage services available that assist a company in securely storing data. They may store this data in cloud services, in-house technology or off-site locations.

II. HR and people management

There are several functions within the human resources and people management field, such as staffing, job assessment, workforce utilization and analysis of workforce performance. Support services can help streamline this process by offering the necessary support to complete these tasks. This frees up time for HR professionals to focus on the tasks that are most important.

III. Computer support

Computer support may be the most common form of support services. Many companies utilize various technologies to perform tasks, and these technologies require dependability and issue-free use for successful implementation. Many IT support service professionals are aware of the latest technology related to various fields and can help make recommendations on the most appropriate tools for a company. Provided services may include troubleshooting computer systems and programs, installing hard drives, upgrading systems and installing malware detection software.

IV. Administration support

Other support services companies often use include those that help assist in the administrative process within their organizations. There are several small duties required for these tasks, which can take up an administrative professional's time. Examples of available services in this department include updating customer databases, inputting data and responding to correspondence from clients and employees.

V. Customer service

Customer service is a popular support service that many organizations rely on to keep their customers happy. If there aren't enough in-house customer service employees to handle customer needs, customers may feel as though the company cannot meet their needs. Third-party customer service support programs make sure clients receive optimal support in a timely manner.

VI. Web development

Website development and maintenance are important components of support services and help manage various aspects of web-related tasks, including customer service and inventory management. These support services can decrease the time that site owners spend on troubleshooting and fixing issues on their website. There are several resources that can keep

systems and websites functioning and reduce the need for employees to regularly manage the company's sites.

VII. Sales and revenue generation

One way to increase sales and revenue generation is to use support services focused on increasing brand awareness and loyalty. These services typically involve assisting customers in determining the help they require. Services may also include assisting customers in finding products and services that meet their needs and preferences.

4.4. Quaility of Service Delivered

A set of technologies that work on a network to guarantee its ability to dependably run high-priority applications and traffic under limited network capacity. QoS technologies accomplish this by providing differentiated handling and capacity allocation to specific flows in network traffic. This enables the network administrator to assign the order in which packets are handled and the amount of bandwidth afforded to that application or traffic flow.

Types of Traffic on the Network

To understand QoS, you must understand the traffic types it measures. Measurements of concern to QoS are:

1. Bandwidth (maximum rate of transfer) — the speed of a link
2. Throughput (actual rate of transfer)
3. Latency (delay) — the amount of time it takes for a packet to traverse the network, from source to destination
4. Jitter (variance in latency) — when packets don’t arrive in the same order they were sent

QoS is key to:

- Voice and video applications
- Email
- Interactive applications
- Batch applications
- Online purchasing

For example, high-bandwidth, real-time data traffic such as voice over IP (VoIP), video conferencing and video-on-demand have high sensitivity to latency and jitter. These

applications, with minimum bandwidth requirements and maximum latency limits, are called "inelastic."

How to Implement QoS

A successful QoS implementation includes three main stages:

1. Strategically define business objectives to be achieved using QoS.
2. Determine service-level requirements of traffic classes.
3. Design and test QoS policies.

Ongoing service level monitoring, adjustments and tuning of QoS policies should always follow a successful QoS policy deployment. Business conditions are always changing, so organizations must adapt the QoS deployment cycle accordingly. This can include:

- Starting the QoS deployment cycle over
- Redefining objectives
- Testing and tuning designs
- Deployment of new designs
- Monitoring

Depending on the provider, the above services and controls can be managed and consolidated down to a single box. Such is the case for QoS via Palo Alto Networks firewalls. Thus, to communicate QoS measures and classification outside the box and downstream network infrastructure, Differentiated Services Code Point (DSCP) can be implemented. DSCP marks each packet based on its classification and communicates this to each box the packet travels through, ensuring a consistent implementation of QoS policy.

Self-Check-3

Part-I: Choose the correct answer

1. What is the main challenge during peak hours for internet users?
   A) Slow device updates
   B) Network congestion and slower speeds
   C) Limited streaming options
   D) Off-peak discounts
2. Why is tracking data usage important in mastering your data plan?
   A) To increase data charges
   B) To identify data-hungry applications
   C) To disable Wi-Fi networks
   D) To avoid off-peak times
3. When is it advisable to schedule data-intensive activities for optimal performance?
   A) Peak hours
   B) Random times during the day
   C) Off-peak times
   D) Weekends

Part-II: Give short answer

1. Explain the need of QoS?
2. How do we identify the peak hours ISP performance?
3. List the ways to optimize data usage during the peak hours.

Reference

Books

ISP Survival Guide: first edition Geoff Huston

Designing ISP Architectures: First edition By John V. Nguyen

The Competitive Internet Service Provider: First edition By Oliver Heckmann

URL

https://www.techtarget.com/whatis/definition/ISP-Internet-service-provider#:~:text=What%20is%20an%20ISP%3F,for%20the%20geographic%20area%20served.

https://www.technologygateway.org/characteristics-of-a-good-web-hosting-company/

https://www.shahucollegelatur.org.in/Department/Studymaterial/bvoc/Web%20Hosting.pdf

https://www.namecheap.com/guru-guides/what-is-email-hosting/

https://medux.com/blog/why-do-internet-service-outages-happen

https://www.giac.org/paper/gsec/1950/user-security-internet-service-provider/103393

https://www.linkedin.com/advice/0/how-do-you-choose-best-scripting-language

https://www.extnoc.com/blog/server-monitoring-best-practices/

https://www.msp360.com/resources/blog/backup-security-measures/

https://www.milesweb.in/blog/hosting/choose-operating-system-website-hosting/

https://jiwebhosting.com/blog/78/choose-the-right-operating-system-for-your-website-hosting

https://www.bigrock.in/blog/uncategorized/how-to-choose-a-website-hosting-operating-system

https://appmaster.io/blog/securing-payments-in-e-commerce

Developer's Profile

No	Name	Qualification	Field of Study	Organization/ Institution	Mobile number	E-mail
1	Frew Atkilt	M-Tech	Network & Information Security	Bishoftu Polytechnic College	0911787374	frew.frikii@gmail.com
2	Gari Lencha	MSc	ICT Managment	Gimbi Polytechnic	0917819599	Garilencha12@gmail.com
3	Kalkidan Daniel	BSc	Computer Science	Entoto Polytechnic	0978336988	kalkidaniel08@gmail.com
4	Solomon Melese	M-Tech	Computer Engineering	M/G/M/Polytechnic College	0918578631	solomonmelese6@gmail.com
5	Tewodros Girma	MSc	Information system	Sheno Polytechnic College	0912068479	girmatewodiros @gmail.com
6	Yohannes Gebeyehu	BSc	Computer Science	Entoto Polytechnic College	0923221273	yohannesgebeyehu73@gmail.com