Injibara University

College of Engineering and Technology

Department of Information Technology

Network and System Administration (CoSc 4036)

Chapter Four: Network management

Contents

- TCP/IP Networking
- Router
- Web Server
- DNS Server
- Mail Transfer Agents
- Proxy
- Network Services
- TCP/IP troubleshooting
- Remote Administration

TCP/IP networking

- TCP/IP stands for Transmission Control Protocol/Internet Protocol and is a suite of communication protocols used to **interconnect network devices** on the internet.
- TCP/IP is also used as a communications protocol in a **private computer network** (an intranet or extranet).
- TCP/IP specifies **how data is exchanged** over the internet by providing end-to-end communications.

Cont …

- It identifies how it should be broken into packets, addressed, transmitted, routed and received at the destination.
- TCP/IP requires little central management and is designed to **make networks reliable** with the ability to recover automatically from the failure of any device on the network.
- It also manages how a message is **assembled into smaller packets** before they are then transmitted over the internet and reassembled in the right order at the destination address.

Common TCP/IP Protocols include the following:

- **Hypertext Transfer Protocol (HTTP)** handles the communication between a web server and a web browser.
- **HTTP secure** handles secure communication between a web server and a web browser.
- **File Transfer Protocol** handles transmission of files between computers.
- TCP/IP uses the **client-server** model of communication in which a client is provided a service like sending a webpage by another computer (a server) in the network.
- Collectively, the TCP/IP suite of protocols is classified as **stateless**, which means **each client request is considered new** because it is unrelated to previous requests.
- Being stateless **frees up network paths** so they can be used continuously.

Router

- Each computer, in the network, uses a unique software address that is known as the **IP address.**
- For easier management and several technical reasons, IP addresses are grouped into the **IP networks** and the IP networks are further categorized into the **five IP classes**.
- By default, an IP address of an IP network can't communicate with the IP address of another IP network.
- This means, if you have two devices and both use IP addresses from **different IP networks**, they can't communicate with each other.
- Due to any reason, if computers in your network are configured with the IP addresses of the **different IP networks**, then to connect them, you need a device that supports the **IP forwarding**.

Cont …

- IP forwarding is a feature that allows communication between the devices of **different the IP networks.**
- **Router** is a special device that not only provides the **IP forwarding** as the main function but also supports several other IP based features such as **packet filtering**.
- Router as an expensive device and configuring it is also a complex task.
- Every network, especially the **small and home office network** can afford it.

Cont …

- A router is a device that connects two or more packet-switched networks or subnetworks.
- It serves two primary functions:
  - ✓ Managing traffic between these networks by forwarding **data packets** to their intended **IP address** and
  - ✓ Allowing **multiple devices** to use the same internet connection.
- There are several **types of routers**, but most routers pass data between LAN and WAN.

Cont …

- LAN is a group of connected devices restricted to a **specific geographic area**.
- It usually requires a **single router**.
- WAN is a large network spread out over a **vast geographic area**.
- WAN is distributed over a large area, it requires **multiple routers and switches**.
- **A network switch** forwards data packets between groups of devices in the **same network**, whereas a **router** forwards data between **different networks.**

How does Router works

- A router is a **data traffic (data packet) controller** and **packets** headed to different networks.
- Data packets have a unique destination and follows unique route.
- **Each packet** needs to be guided to its destination as efficiently as possible.
- A router helps to direct data packets to their destination IP address.
- In order to direct packets effectively, a router uses an **internal routing table**
- A routing table is a **list of paths** to various network destinations.
- The router reads a **packet's header** to determine where it is going, then consults the routing table to figure out the **most efficient path** to that destination.
- It then forwards the packet to the next network in the path.

Web Server

- A web server is a computer system capable of delivering **web content to end users** over the internet via a web browser.
- A web server is a computer that **stores, processes, and delivers** website files to browsers.
- Web servers consist of hardware and software that use **HTTP** to respond to web users requests made via the WWW.
- Web servers load and deliver the requested page to the **user's browser.**
- Web servers also use **SMTP** and **FTP** to process files for email or storage.

Cont …

- Web server on the hardware side **connects to the internet**, which enables it to **exchange data or files** between other devices that are connected.
- This data can come in different forms, such as HTML files, images, JavaScript files.
- Web server hardware also stores **web server software**.
- Web server **software** controls how web users access.
- It consists of several components, housing at least an **HTTP** hosted files **server**.
- An **HTTP server** is software that can understand HTTP requests and URLs.
- Web servers are primarily used to process and manage **HTTP/HTTPS requests and responses** from the client system.

Cont …

- A web server can also perform the following functions.
- **Store and protect website data:** a web server can store and protect **critical website data** from unauthorized users.
- **Control bandwidth to regulate network traffic:** a web server can help eliminate the downtime caused by **high web traffic**.
- Web hosts can set bandwidth to manage the **rate of data transmission** over the internet and minimize the excess network traffic.
- **Server-side web scripting:** the server-side web scripting feature enables users to create **dynamic web pages** using scripting languages such as Ruby, Python, and PHP.
- **Virtual hosting:** web servers can also be used as **virtual servers** to run multiple applications, websites, data, and other services.

How web servers work

- The end user processes a request via a **web browser** installed on a web server.
- The communication between a web server or **browser and the end user** takes place using Hypertext Transfer Protocol (HTTP).
- The primary role of a web server is to **store, process, and deliver** requested information or webpages to end users.
- Web server uses:

  ✓Physical storage

  ✓Web browser

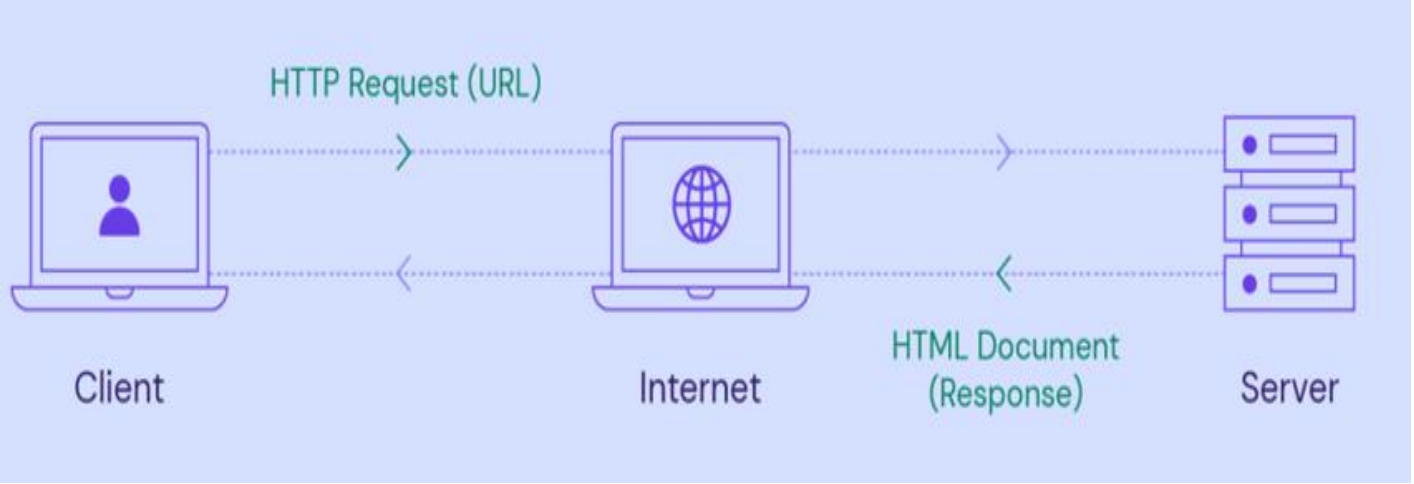
Cont …

Physical Storage

- ✓ All website data is stored on a physical web server to ensure its safety.
- ✓ When an end user enters the URL of your website or searches it using a **keyword** on a browser, a request is generated and **sent to the web server** to process the data.

Web browser

- ✓ The role of web browsers is to **find the web server** on which your website data is located.
- ✓ Once the browser finds your server, it reads the request and processes the information.



Web Server Features

In addition to supporting **HTTP** protocols to process incoming requests and responses, most web servers offer the following standard features.

- **File logging**: log files document **any events or activities** web servers perform, such as requests, security, and errors.
  - ✓ Each time a web server receives a new request, a line of text is added to the log.
- **Authentication**: many servers offer this feature before permitting partial or complete access to a website's resources.
  - ✓ Authentication features often involve **authorization requests** when a username and password are required.

Cont …

- **Bandwidth limiting:** a web server's bandwidth is the amount of data it can transfer or process at any given time.
  - ✓ Bandwidth limiting controls the **speed of responses** to ensure that a network can deliver files smoothly.
- **Storage space**: it refers to the amount of **disk space** available to store files, which determines whether a web server can host a website.

DNS Server

- The Domain Name System (DNS) is the **phonebook** of the internet.
- When users type domain names such as **www.inu.edu.et** into web browsers, DNS is responsible for finding the correct IP address.
- Browsers then use those addresses to communicate with **servers** to access website information.
- A server is dedicated to providing **services to clients**.
- DNS clients are built into desktop and mobile operating systems that enable web browsers to interact with DNS servers.

Mail Transfer Agents - MTA

- A mail server can have many names: **mail relay, mail router, and internet mailer**.
- But the most common alias is an MTA - Mail Transfer Agent or Message Transfer Agent or a Mail Transport Agent.
- MTAs play an essential role in the internet message handling system.
- They transfer **electronic mail messages** between users.
- A mail/message transfer agent (MTA) is a software that **transfers emails** between the computers of a sender and a recipient.

How MTAs work

- MTA is just an element of the **email delivery process**.
- It receives an email from the **mail/message submission agent** (MSA) which in turn receives it from the **mail user agent** (MUA).
- The MUA is commonly known as an **email client.**
- Once the MTA gets the email, relaying comes into play.
- That's why mail transfer agents are often **called mail relays.**
- The email can be **forwarded to other MTAs** if the recipient is not hosted locally.
- Then it hits the **mail delivery agent** (MDA).
- This is the email's last stopover before it is delivered to the recipient's mailbox.
- The email sending is carried out using SMTP (or extended SMTP), and for the final stage (**MDA to MUA**).

Cont …

MTAs do the following:

- Accept emails sent from mail user agents.
- Select a **mail server** to transfer emails.
- Send **auto-response messages** if an email has failed to reach the destination.

Mail queueing in MTAs

- MTAs use a **store-and-forward model** of mail handling.
- This means that outgoing mail is put into a **queue** and waits for the recipient's server response.
- An MTA will recurrently try to send emails.
- If the mail fails to be delivered during the established term, it will be returned to the mail client.

Proxy server

- A proxy server is a computer system that functions as a relay between **client and server.**
- It helps **prevent an attacker** from invading a private network.
- The word proxy means "to act on behalf of another," and a **proxy server** acts on behalf of the user.
- All requests to the internet go to the **proxy server first**, which evaluates the request and forwards it to the Internet.
- **Responses** are also come back to the proxy server and then to the user.
- Proxies are often used in conjunction with **network address translation (NAT),** which hides the users' IP addresses on the internal network.
- Proxy servers may also **cache Web pages** so that the next request for that page can be retrieved much faster.

Cont …

Application Level and Circuit Level

- Application-level proxies or application-level gateways are dedicated to **specific content** such as HTTP (Web) and FTP (file transfer).
- Circuit-level proxy supports **every application**.
- Proxy servers are **forward proxies** that hide the details of the clients from the servers.
- Proxies can also reside at the website to hide details from the clients.

Cont …

- A proxy server acts as an **intermediary** between a user and the websites.
- They can be set up as a **firewall or a web filter**, acting as a layer of cybersecurity that prevents cyber attackers from entering a private network and protects computer against malware and other cyber threats.
- A proxy server is a **gateway** that passes data between users and the internet.
- When an individual uses a browser, they normally communicate **directly with the internet**, but with a proxy server, the **proxy communicates** with the internet on the behalf of user.

Cont …

- When someone uses a proxy server, the internet traffic goes through the proxy before reaching the destination computer.
- Since all communication is happening through the proxy, it offers **security and privacy**.
- Proxy servers perform the following important functions.
  - ✓ To **filter incoming traffic**, making the company's network more secure.
  - ✓ To keep the company's network more **private**.
  - ✓ To **speed up access to resources** through the use of a cache.

How Does a Proxy Server Work?

- All devices connected to the internet have an internet protocol (IP) address.
- This address is how a device is **recognized on the internet**, and it plays a role in how proxy servers work.
- The following steps are common way of working among all proxy servers.
  - ✓ When a device makes a request to the internet through a proxy, the proxy server **reads and interprets the request**.
  - ✓ That request is then forwarded to the right **internet server.**
  - ✓ The internet server reads the IP of the proxy and sends the **requested data** to the IP of that proxy.
  - ✓ The proxy server receives the data, extracts it, and checks it for **possible malware**.
  - ✓ Once marked safe, the data is forwarded to the requesting device.

Cont …

Benefits of Proxy Servers

The following are some of the primary benefits for proxy servers.

- **Improved Security:** this is the main reason why companies use proxy servers, as **data breaches are expensive** and can result in huge losses.
  - ✓ A proxy server filters out **malicious data** from the internet before it reaches the company's servers, it can act as an **additional layer of security.**
  - ✓ A proxy server **alone might not save the company's network** from all hacking attempts, but it can add to the security of the system and lower the risk of cyberattacks.
  - ✓ It can also help a company against **phishing**, identity or brand theft, DDOS attack, and other malware attacks.

Cont …

- **Faster Speed:** caching is another important function performed by proxy servers.
  - ✓ More frequently visited sites can be cached by the proxy.
- **Control internet usage:** proxies can be used to **block undesirable content**.
  - ✓ For example, some companies might want to block certain **social media sites** so their employees aren't distracted from their work.
  - ✓ A proxy server also lets **network administrators monitor** the requests sent to the internet to ensure no illegal or improper activities are being carried out.
- **Bypassing Restrictions:** some websites only allow access to **IPs from a certain location**.
  - ✓ This can be a problem when a business needs to access a geo-restricted website.
  - ✓ When a company uses a proxy server, the **IP is masked** and employees can access the content they need.

Cont …

How are Proxy Servers Used?

- The proxy itself sits outside the firewall and **protects the servers**.
- Companies and organizations can also install **proxy network software** on each individual computer if necessary.
- The proxy can also be a **standalone computer or a router** installed between two separate devices on the company's network.
- When a proxy sits between two devices, it accepts requests, sends them to the required destination, gathers responses, and forwards them to the requesting device.

Cont …

Are Proxy Servers Similar to VPNs?

- Proxy servers are similar to VPNs in some ways.
- Both of them hide users IP addresses and help **bypass geo-restrictions**.
- A proxy server **doesn’t encrypt** the network traffic.
- VPN encrypts network traffic and adds another layer of safety.
- VPN **doesn’t use a cache** to speed up internet access, whereas a proxy can improve the speed of access with its caching capabilities.
- VPN is trusted more by companies due to its ability to **encrypt data**.
- For personal use, a proxy might be enough.
- In business scenarios where breaches are expensive, **VPNs** could be a better choice.

Network Services

- Some types of network services are:
  - ✓ Internet and cloud connectivity.
  - ✓ Branch office and campus connectivity.
  - ✓ Private data center services.
  - ✓ Secure cloud-connectivity services.
  - ✓ Virtual network services.

What is network as a service (NaaS)?

- NaaS is a **cloud model** that enable organizations easily operate their networks and achieve the outcomes they expect.
- NaaS can replace **hardware-centric virtual private networks** (VPNs), load balancers, firewall appliances, and Multiprotocol Label Switching (MPLS) connections.
- As a result, organizations can scale up or down more easily as **demand changes**, rapidly deploy services, and **eliminate some hardware costs**.
- NaaS simplifies how connectivity technologies are managed and consumed.
- It enables greater speed, agility, and scale.

TCP/IP troubleshooting

- TCP/IP is a complex system involving many **layers, protocols, and technologies**.
- It can sometimes be challenging to **troubleshoot problems** that occur within a TCP/IP network.
- When **troubleshooting a TCP/IP network**, it is important to gather as much information.
- This may involve using tools such as **ping and traceroute** to test connectivity, analyzing network traffic, checking the configuration of devices and protocols to ensure they are functioning correctly.

Cont …

- One of the first signs of trouble on the network is a **loss of communications** by hosts.
- If a host refuses to come up at all the first time it is added to the network, the problem might lie in one of the **configuration files, or in the network interface**.
- If a single host suddenly develops a problem, the network interface might be the cause.
- If the hosts on a network can communicate with each other but not with other networks, the problem could lie **with the router**, or it could lie in **another network.**
- You can use the **ifconfig program** to obtain information on network interfaces and **netstat** to display routing tables and protocol statistics.
- **Third-party network diagnostic programs** provide a number of troubleshooting utilities.

Cont …

Gathering information about the network and the problem

- Before attempting to troubleshoot a problem within a TCP/IP network, **gathering information** about the network and the problem is important.
- This will help to **narrow down the possible causes** of the problem and to develop a plan for resolving it.
- Some of the key pieces of information to gather are:
  - ✓ **A description of the problem**: what is happening, and when did it start? Are there any error messages or other indicators that might provide clues about the cause of the problem?

Cont …

- ✓ **A list of the devices and software involved**: what devices are connected to the network, and what software is running on them? Are there any recent changes to the network or to the devices that might be related to the problem?
- ✓ **Network configuration details**: what is the network topology, and how are the devices connected? What IP addresses, subnet masks, and other network settings are in use?
- ✓ **Network logs and other relevant data:** are there any logs or other data that might provide clues about the problem? this may include system logs, network traffic logs, and other data that could be useful for troubleshooting.

Cont …

- **Ping Command**: used to quantify problems like **loss of packets by a host.**
- Use the ping command to find out whether there is **IP connectivity** to a particular host.
- With **ping**, the ICMP protocol sends a datagram to the host you specify, **asking for a response.**
- ICMP is the protocol responsible for error handling on a TCP/IP network.

Cont …

ifconfig Command

- The ifconfig command displays information about the **configuration of an interface** that you specify.

netstat Command

- The netstat command generates displays that show **network status and protocol statistics**.
- We can display the status of TCP and UDP endpoints in **table format, routing table information, and interface information.**
- These displays are the most useful for **system administration.**

Cont …

The ip command

- The **ip command** is used for assigning IP addresses to interfaces, for setting up routes to the internet and to other networks, for displaying TCP/IP configurations etc.

The Traceroute Command

- To check the route that packets follow to a network host, use the **traceroute** command:

Remote Administration

- Remote administration is an approach being followed to control either a **computer system or a network or an application** or all three from a remote location.
- Remote administration refers to any method of controlling a computer **from a remote location.**
- A remote location may refer to a computer in the next room or one on the other side of the world.
- It may also refer to both **legal and illegal** remote administration.
- Remote administration is essentially adopted when it is difficult or impractical to a person to be **physically present** and do administration on a system.