NETWORKING AND COMMUNICATION

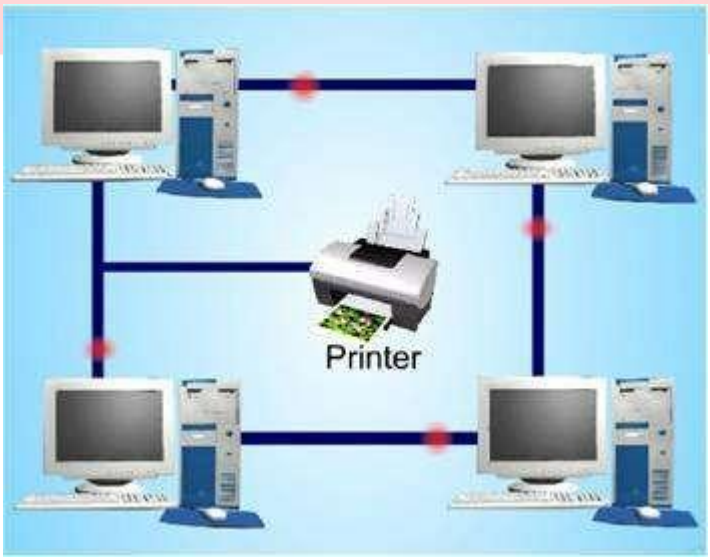
WHY WE NEED COMPUTER NETWORKS? NEED FOR COMPUTER NETWORKING

Computer networks help users on the network to share the resources and in communication. Can you imagine a world now without emails, online newspapers, blogs, chat and the other services offered by the internet?

The following are the important uses and benefits of a computer network.

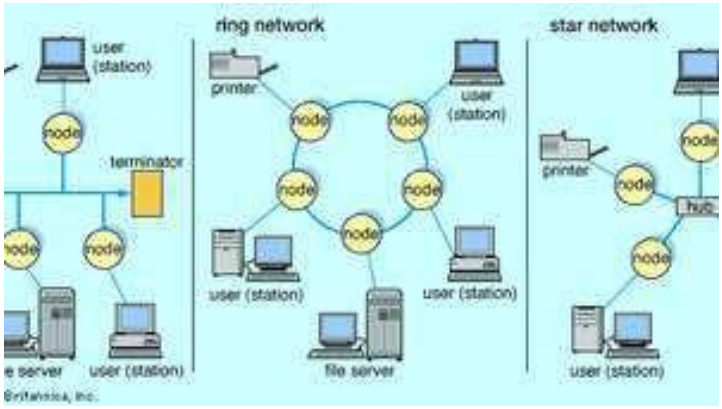
File sharing: Networking of computers helps the network users to share data files.

Hardware sharing: Users can share devices such as printers, scanners, CD-ROM drives, hard drives etc. Without computer networks, device sharing is not possible.



Application sharing: Applications can be shared over the network, and this allows to implement client/server applications

User communication: Networks allow users to communicate using e-mail, newsgroups, and video conferencing etc.



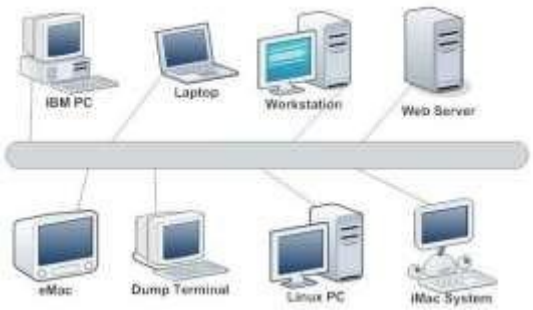
Network gaming: A lot of network games are available, which allow multi-users to play from different locations.

Voice over IP (VoIP): Voice over Internet Protocol (IP) is a revolutionary change in telecommunication which allows to send telephone calls (voice data) using standard Internet Protocol (IP) rather than by traditional PSTN.

WHAT IS BUS TOPOLOGY, ADVANTAGES AND DISADVANTAGES OF BUS TOPOLOGY

Bus Topology

A bus topology consists of a main run of cable with a terminator at each end. All nodes like workstations, printers, laptops, servers etc., are connected to the linear cable. The terminator is used to absorb the signal when the signal reaches the end, preventing signal bounce. When using bus topology, when a computer sends out a signal, the signal travels the cable length in both directions from the sending computer. When the signal reaches the end of the cable length, it bounces back and returns in the direction it came from. This is known as signal bounce. Signal bounce may create problems in the computer network, because if another signal is sent on the cable at the same time, the two signals will collide. Collisions in a computer network can drastically reduce the performance of the computer network.



Advantages of Bus Topology

- Easy to connect a computer or peripheral to a linear bus.
- Requires less cable length than a star topology.

Disadvantages of Bus Topology

- Entire network shuts down if there is a break in the main cable.
- Terminators are required at both ends of the backbone cable.
- Difficult to identify the problem if the entire network shuts down.
- Not meant to be used as a stand-alone solution.

CHECKSUMS

This is a block code method where a checksum is created based on the data values in the data blocks to be transmitted using some algorithm and appended to the data. When the receiver gets this data, a new checksum is calculated and compared with the existing checksum. A non-match indicates an error.

Error Detection by Checksums

For error detection by checksums, data is divided into fixed sized frames or segments.

- **Sender's End** − The sender adds the segments using 1's complement arithmetic to get the sum. It then complements the sum to get the checksum and sends it along with the data frames.
- **Receiver's End** – The receiver adds the incoming segments along with the checksum using 1's complement arithmetic to get the sum and then complements it.

If the result is zero, the received frames are accepted; otherwise they are discarded.

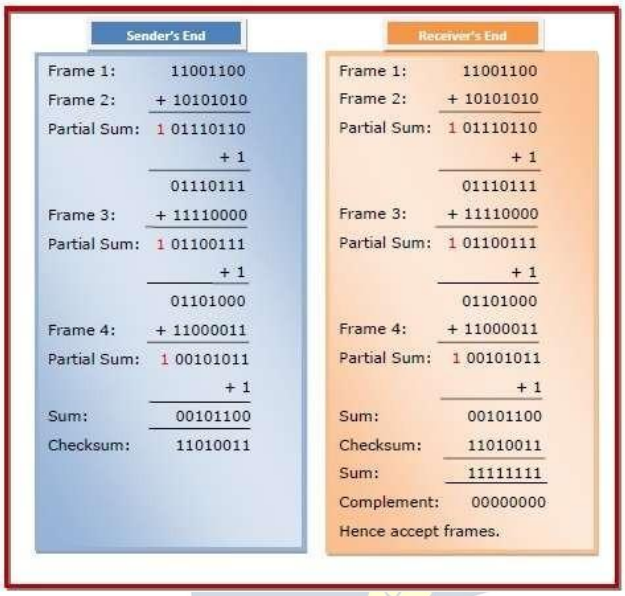
Example

Suppose that the sender wants to send 4 frames each of 8 bits, where the frames are 11001100, 10101010, 11110000 and 11000011.

The sender adds the bits using 1s complement arithmetic. While adding two numbers using 1s complement arithmetic, if there is a carry over, it is added to the sum.

After adding all the 4 frames, the sender complements the sum to get the checksum, 11010011, and sends it along with the data frames.

The receiver performs 1s complement arithmetic sum of all the frames including the checksum. The result is complemented and found to be 0. Hence, the receiver assumes that no error has occurred.



Sender's End		Receiver's End	
Frame 1:	11001100	Frame 1:	11001100
Frame 2:	+ 10101010	Frame 2:	+ 10101010
Partial Sum:	1 01110110	Partial Sum:	1 01110110
	+ 1		+ 1
	01110111		01110111
Frame 3:	+ 11110000	Frame 3:	+ 11110000
Partial Sum:	1 01100111	Partial Sum:	1 01100111
	+ 1		+ 1
	01101000		01101000
Frame 4:	+ 11000011	Frame 4:	+ 11000011
Partial Sum:	1 00101011	Partial Sum:	1 00101011
	+ 1		+ 1
Sum:	00101100	Sum:	00101100
Checksum:	11010011	Checksum:	11010011
		Sum:	11111111
		Complement:	00000000
		Hence accept frames.	

Channel

Physical medium like cables over which information is exchanged is called **channel**. Transmission channel may be **analog** or **digital**. As the name suggests, analog channels transmit data using **analog signals** while digital channels transmit data using **digital signals**.

In popular network terminology, path over which data is sent or received is called **data channel**. This data channel may be a tangible medium like copper wire cables or broadcast medium like **radio waves**.

Data Transfer Rate

The speed of data transferred or received over transmission channel, measured per unit time, is called data transfer rate. The smallest unit of measurement is bits per second (bps). 1 bps means 1 bit (0 or 1) of data is transferred in 1 second.

Here are some commonly used data transfer rates −

- 1 Bps = 1 Byte per second = 8 bits per second
- 1 kbps = 1 kilobit per second = 1024 bits per second
- 1 Mbps = 1 Megabit per second = 1024 Kbps
- 1 Gbps = 1 Gigabit per second = 1024 Mbps

Bandwidth

Data transfer rates that can be supported by a network is called its bandwidth. It is measured in bits per second (bps). Modern day networks provide bandwidth in Kbps, Mbps and Gbps. Some of the factors affecting a network's bandwidth include −

- Network devices used
- Protocols used
- Number of users connected
- Network overheads like collision, errors, etc.

Throughput

Throughput is the actual speed with which data gets transferred over the network. Besides transmitting the actual data, network bandwidth is used for transmitting error messages, acknowledgement frames, etc.

Throughput is a better measurement of network speed, efficiency and capacity utilization rather than bandwidth.

Protocol

Protocol is a set of rules and regulations used by devices to communicate over the network. Just like humans, computers also need rules to ensure successful communication. If two people start speaking at the same time or in different languages when no interpreter is present, no meaningful exchange of information can occur.

Similarly, devices connected on the network need to follow rules defining situations like when and how to transmit data, when to receive data, how to give error-free message, etc.

Some common protocols used over the Internet are –

- Transmission Control Protocol
- Internet Protocol
- Point to Point Protocol
- File Transfer Protocol
- Hypertext Transfer Protocol
- Internet Message Access Protocol

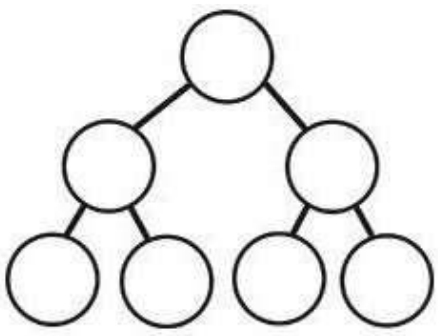
TREE TOPOLOGY IN NETWORKING

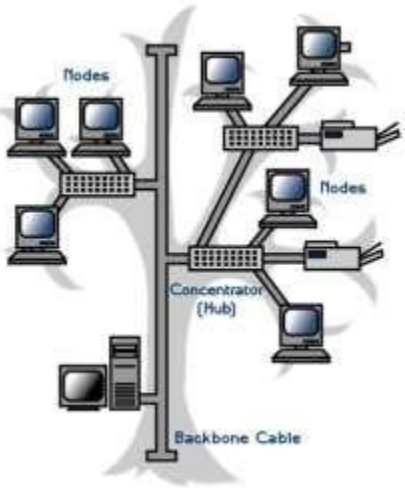
TREE TOPOLOGY

A **tree topology** is a special type of structure where many connected elements are arranged like the branches of a tree. For example, tree topologies are frequently used to organize the computers in a corporate network, or the information in a database.

In a tree topology, there can be only one connection between any two connected nodes. Because any two nodes can have only one mutual connection, tree topologies create a natural parent and child hierarchy.

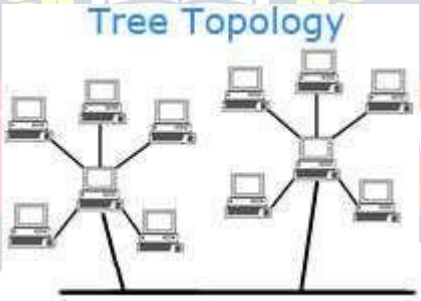
- Tree topology in computer networking.
- Tree topology in computer programming.
- Tree topology in binary trees
- B-trees





Tree topology in computer networking

In computer networks, a tree topology is also known as a **star bus topology**. It incorporates elements of both a bus topology and a star topology. Below is an example network diagram of a tree topology, where the central nodes of two star networks are connected to one another.

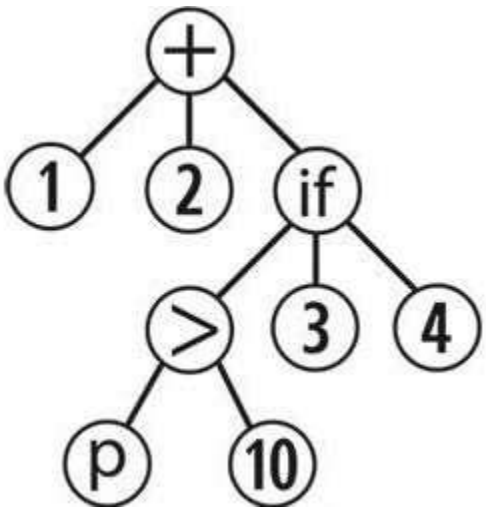


In the picture, if the main cable (trunk) between the two star topology networks failed, those networks would be unable to communicate with each other. However, computers on the same star topology would still be able to communicate.

Tree topology in computer programming

In computer programming, tree topologies can structure many kinds of data, including a computer program itself.
For example, this is a computer program written in Lisp:

```
(+ 1 2 (if (> p 10) 3 4))
```

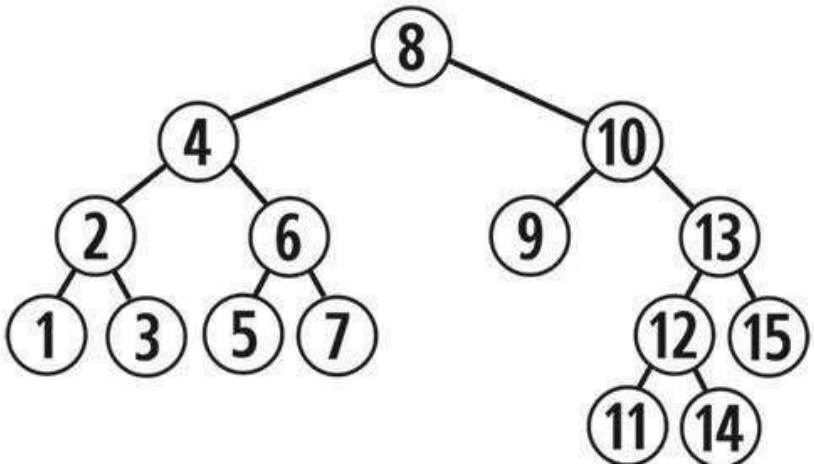


This program says "If p is greater than 10, add the numbers 1, 2, and 3. Otherwise, add the numbers 1, 2, and 4." Like all Lisp programs, it has an inherent tree topology structure. If we draw it as a graph, it looks like the tree shown at right. Representing a program this way can be useful because it clearly shows how all the operations and data are connected.

Programs in this kind of structure also have special uses. For instance, genetic programming techniques can evolve new computer programs by exchanging branches between existing programs structured as trees.

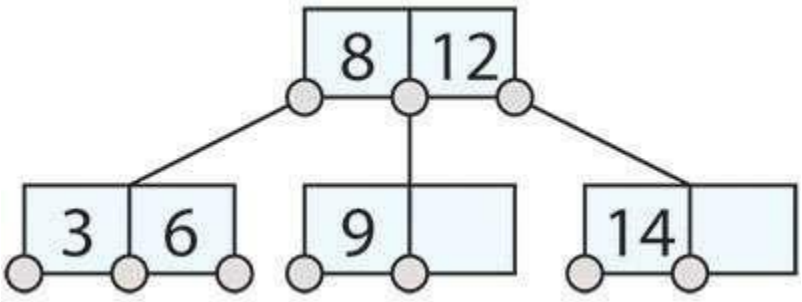
Tree topology in binary trees

A **binary tree** is a tree topology where every node has a maximum of two children. The child nodes are labeled as "left child" or "right child." This type of data structure is often used for sorting and searching large amounts of data. In the binary tree shown below, each parent's left child has a value less than the right child.



B-trees

A **B-tree** is a variation of a binary tree that was invented by Rudolf Bayer and Ed McCreight at Boeing Labs in 1971. Its nodes have children that fall within a predefined minimum and maximum, usually between 2 and 7. A B-tree graph might look like the image below.



B-trees are "self-balancing," meaning the height of the branches is managed so that they do not get arbitrarily large. Each node contains partitioning "key values" that indicate the values of the children. Their design is optimized for handling very large data files, and for writing data to memory or disk. They are used extensively in database systems like MySQL, PostgreSQL, and Redis, and filesystems such as NTFS, HFS+, and ext4.

WIRELESS TRANSMISSION MEDIA IN NETWORKING

Many users opt for wireless transmission media because it is more convenient than installing cables. In addition, businesses use wireless transmission media in locations where it is impossible to install cables. Types of wireless transmission media used in communications include infrared, broadcast radio, cellular radio, microwaves, and communications satellites.

Infrared

As discussed earlier in the chapter, infrared (IR) is a wireless transmission medium that sends signals using infrared light waves. Mobile computers and devices, such as a mouse, printer, and smart phone, often have an IrDA port that enables the transfer of data from one device to another using infrared light waves.

Broadcast Radio

Broadcast radio is a wireless transmission medium that distributes radio signals through the air over long distances such as between cities, regions, and

countries and short distances such as within an office or home. Bluetooth, UWB, Wi-Fi, and WiMAX communications technologies discussed earlier in this chapter use broadcast radio signals.

Cellular Radio

Cellular radio is a form of broadcast radio that is used widely for mobile communications, specifically wireless modems and cell phones. A cell phone is a telephone device that uses high-frequency radio waves to transmit voice and digital data messages.

Some mobile users connect their notebook computer or other mobile computer to a cell phone to access the Web, send and receive e-mail, enter a chat room, or connect to an office or school network while away from a standard telephone line. Read Looking Ahead 8-2 for a look at the next generation of cellular communications.

Personal Communications Services (**PCS**) is the term used by the United States Federal Communications Commission (FCC) to identify all wireless digital communications. Devices that use PCS include cell phones, PDAs, pagers, and fax machines.

Microwaves

Microwaves are radio waves that provide a high-speed signal transmission. Microwave transmission, often called fixed wireless, involves sending signals from one microwave station to another (shown in Figure 8-1 on page 296). Microwaves can transmit data at rates up to 4,500 times faster than a dial-up modem.

A microwave station is an earth-based reflective dish that contains the antenna, transceivers, and other equipment necessary for microwave communications. Microwaves use line-of-sight transmission. To avoid possible obstructions, such as buildings or mountains, microwave stations often sit on the tops of buildings, towers, or mountains.

Microwave transmission is used in environments where installing physical transmission media is difficult or impossible and where line-of-sight transmission is available. For example, microwave transmission is used in wide-open areas such as deserts or lakes; between buildings in a close geo- graphic area; or to communicate with a satellite. Current users of microwave transmission include universities, hospitals, city governments, cable television providers, and telephone companies. Home and small business users who do not have other high-speed Internet connections available in their area also opt for lower-cost fixed wireless plans.

Communications Satellite

A **communications satellite** is a space station that receives microwave signals from an earth-based station, amplifies (strengthens) the signals, and broadcasts the signals back over a wide area to any number of earth-based stations.

These earth-based stations often are microwave stations. Other devices, such as smart phones and GPS receivers, also can function as earth-based stations.

Transmission from an earth-based station to a satellite is an uplink.

Transmission from a satellite to an earth-based station is a downlink.

Applications such as air navigation, television and radio broadcasts, weather forecasting, video conferencing, paging, global positioning systems, and Internet connections use communications satellites. With the proper satellite dish and a sat- ellite modem card, consumers access the Internet using satellite technology. With satellite Internet connections, however, uplink transmissions usually are slower than downlink transmissions. This difference in speeds usually is acceptable to most Internet satellite users because they download much more data than they upload. Although a satellite Internet connection is more expensive than cable Internet or DSL connections, sometimes it is the only high-speed Internet option in remote areas.

WHAT IS SPAM

What comes to mind when you think of spam? Miracle pills from Internet pharmacies, requests for money from “princes” of other countries, or perhaps the food, Spam? This article is all about spam with a lowercase “s.” While many people enjoy the food Spam, no one wants to be tricked into losing money or downloading malware because of the other kind of spam.

Spam is annoying, but it’s also a threat. While many of us might think we’re savvy enough to recognize any form of it, spammers regularly update their methods and messages to trick potential victims. The reality is that we’re all constantly under attack from cybercriminals and the proof is in your inbox.

So read on to learn what spam is, how to recognize it, and how to protect yourself against it.

SPAM DEFINITION

Spam is any kind of unwanted, unsolicited digital communication that gets sent out in bulk. Often spam is sent via email, but it can also be distributed via text messages, phone calls, or social media.

What does spam stand for?

Spam is not an acronym for a computer threat, although some have been proposed (stupid pointless annoying malware, for instance). The inspiration for using the term “spam” to describe mass unwanted messages is a Monty Python skit in which the actors declare that everyone must eat the food Spam, whether they want it or not. Similarly, everyone with an email address must unfortunately be bothered by spam messages, whether we like it or not.

If you’re interested in the origins of spam in greater detail, see the history of spam section below.

TYPES OF SPAM

Spammers use many forms of communication to bulk-send their unwanted messages. Some of these are marketing messages peddling unsolicited goods. Other types of spam messages can spread malware, trick you into divulging personal information, or scare you into thinking you need to pay to get out of trouble.

Email spam filters catch many of these types of messages, and phone carriers often warn you of a “spam risk” from unknown callers. Whether via email, text, phone, or social media, some spam messages do get through, and you want to be able to recognize them and avoid these threats. Below are several types of spam to look out for.

PHISHING EMAILS

Phishing emails are a type of spam cybercriminals send to many people, hoping to “hook” a few people. Phishing emails trick victims into giving up sensitive information like website logins or credit card information.

Adam Kujawa, Director of Malwarebytes Labs, says of phishing emails: “Phishing is the simplest kind of cyberattack and, at the same time, the most

dangerous and effective. That is because it attacks the most vulnerable and powerful computer on the planet: the human mind."

EMAIL SPOOFING

Spoofed emails mimic, or spoof, an email from a legitimate sender, and ask you to take some sort of action. Well-executed spoofs will contain familiar branding and content, often from a large well-known company such as PayPal or Apple. Common email spoofing spam messages include:

- A request for payment of an outstanding invoice
- A request to reset your password or verify your account
- Verification of purchases you didn't make
- Request for updated billing information

TECH SUPPORT SCAMS

In a tech support scam, the spam message indicates that you have a technical problem and you should contact tech support by calling the phone number or clicking a link in the message. Like email spoofing, these types of spam often say they are from a large technology company like Microsoft or a cybersecurity company like Malwarebytes.

If you think you have a technical issue or malware on your computer, tablet, or smartphone, you should always go to the official website of the company you want to call for tech support to find the legitimate contact information. Remote tech support often involves remote access to your computer to help you, and you don't want to accidentally give that access to a tech support scammer.

CURRENT EVENT SCAMS

Hot topics in the news can be used in spam messages to get your attention. In 2020 when the world was facing the Covid-19 pandemic and there was an increase in work-from-home jobs, some scammers sent spam messages promising **remote jobs that paid in Bitcoin**. During the same year, another popular spam topic was related to **offering financial relief for small businesses**, but the scammers ultimately asked for bank account details. News headlines can be catchy, but beware of them in regards to potential spam messages.

ADVANCE-FEE SCAMS

This type of spam is likely familiar to anyone who has been using email since the 90s or 2000s. Sometimes called “Nigerian prince” emails as that was the purported message sender for many years, this type of spam promises a financial reward if you first provide a cash advance. The sender typically indicates that this cash advance is some sort of processing fee or earnest money to unlock the larger sum, but once you pay, they disappear. To make it more personal, a similar type of scam involves the sender pretending to be a family member that is in trouble and needs money, but if you pay, unfortunately the outcome is the same.

Malspam

Short for “malware spam” or “malicious spam,” malspam is a spam message that delivers malware to your device. Unsuspecting readers who click on a link or open an email attachment end up with some type of malware including ransomware, Trojans, bots, info-stealers, cryptominers, spyware, and keyloggers. A common delivery method is to include malicious scripts in an attachment of a familiar type like a Word document, PDF file, or PowerPoint presentation. Once the attachment is opened, the scripts run and retrieve the malware payload.

SPAM CALLS AND SPAM TEXTS

Have you ever received a robocall? That’s call spam. A text message from an unknown sender urging you to click an unknown link? That’s referred to as text message spam or “smishing,” a combination of SMS and phishing.
If you’re receiving spam calls and texts on your Android or iPhone, most major carriers give you an option to report spam. Blocking numbers is another way to combat mobile spam. In the US, you can add your phone number to the National Do Not Call Registry to try to cut down on the amount of unwanted sales calls you receive, but you should still be alert to scammers who ignore the list.

HOW CAN I STOP SPAM?

While it may not be possible to avoid spam altogether, there are steps you can take to help protect yourself against falling for a scam or getting phished from a spam message:

LEARN TO SPOT PHISHING

All of us can fall victim to phishing attacks. We may be in a rush and click a malicious link without realizing. If a new type of phishing attack comes out, we may not readily recognize it. To protect yourself, learn to check for some key signs that a spam message isn't just annoying—it's a phishing attempt:

1. Sender's email address: If an email from a company is legitimate, the sender's email address should match the domain for the company they claim to represent. Sometimes these are obvious, like example@abkljzr09348.biz, but other times the changes are less noticeable, like example@paypa1.com instead of paypal.com.
2. Missing personal information: If you are a customer, the company should have your information and will likely address you by your first name. A missing personal greeting alone isn't enough to spot a phishing email, but it's one thing to look for, especially in messages that say they are from a company with whom you do business. Receiving an email that says your account has been locked or you owe money is cause to worry, and sometimes we rush to click a link in order to fix the problem. If it's phishing, that's exactly what the sender wants, so be careful and check if the email is generic or addressed specifically to you.
3. Links: Beware of all links, including buttons in an email. If you get a message from a company with whom you have an account, it's wise to log in to your account to see if there is a message there rather than just clicking the link in the message without verifying first. You can contact the company to ask if a suspicious message is legitimate or not. If you have any doubts about a message, don't click any links.
4. Grammatical errors: We all make them, but a company sending out legitimate messages probably won't have a lot of punctuation errors, poor grammar, and spelling mistakes. These can be another red flag to indicate that the email could be suspect.
5. Too-good-to-be-true offers: Many phishing messages pretend to be from large, well-known companies, hoping to ensnare readers who happen to do business with the company. Other phishing attempts offer something for free like cash or a desirable prize. The saying is often true that if something sounds too good to be true it probably is, and this can be a warning that a spam message is trying to get something from you, rather than give you something.

6. Attachments: Unless you are expecting an email with attachments, always be wary before opening or downloading them. Using anti-malware software can help by scanning files that you download for malware.

You can read even more about phishing emails and how to spot them on the Malwarebytes Labs blog.

WHAT IS HTTP PROTOCOL

The Hypertext Transfer Protocol (HTTP) is the foundation of the World WideWeb, and is used to load web pages using hypertext links. HTTP is an application layer protocol designed to transfer information between networked devices and runs on top of other layers of the network protocol stack. A typical flow over HTTP involves a client machine making a request to a server, which then sends a response message.

What's in an HTTP request?
An HTTP request is the way internet communications platforms such as web browsers ask for the information they need to load a website.
Each HTTP request made across the Internet carries with it a series of encoded data that carries different types of information. A typical HTTP request contains:

1. HTTP version type
2. a URL
3. an HTTP method
4. HTTP request headers
5. Optional HTTP body.

Let's explore in greater depth how these requests work, and how the contents of a request can be used to share information.

What's an HTTP method?
An HTTP method, sometimes referred to as an HTTP verb, indicates the action that the HTTP request expects from the queried server. For example, two of the most common HTTP methods are 'GET' and 'POST'; a 'GET' request expects information back in return (usually in the form of a website), while a 'POST' request typically indicates that the client is submitting information to the web server (such as form information, e.g. a submitted username and password).

What are HTTP request headers?

HTTP headers contain text information stored in key-value pairs, and they are included in every HTTP request (and response, more on that later). These headers communicate core information, such as what browser the client is using what data is being requested.

Example of HTTP request headers from Google Chrome's network tab:

What's in an HTTP request body?

The body of a request is the part that contains the 'body' of information the request is transferring. The body of an HTTP request contains any information being submitted to the web server, such as a username and password, or any other data entered into a form.

What's in an HTTP response?

An HTTP response is what web clients (often browsers) receive from an Internet server in answer to an HTTP request. These responses communicate valuable information based on what was asked for in the HTTP request.

A typical HTTP response contains:

1. an HTTP status code
2. HTTP response headers
3. optional HTTP body

Let's break these down:

What's an HTTP status code?

HTTP status codes are 3-digit codes most often used to indicate whether an HTTP request has been successfully completed. Status codes are broken into the following 5 blocks:

1. 1xx Informational
2. 2xx Success
3. 3xx Redirection
4. 4xx Client Error
5. 5xx Server Error

The “xx” refers to different numbers between 00 and 99.
Status codes starting with the number ‘2’ indicate a success. For example, after a client requests a web page, the most commonly seen responses have a status code of ‘200 OK’, indicating that the request was properly completed.
If the response starts with a ‘4’ or a ‘5’ that means there was an error and the webpage will not be displayed. A status code that begins with a ‘4’ indicates a client-side error (It’s very common to encounter a ‘404 NOT FOUND’ status code when making a typo in a URL). A status code beginning in ‘5’ means something went wrong on the server side. Status codes can also begin with a ‘1’ or a ‘3’, which indicate an informational response and a redirect, respectively.

What are HTTP response headers?
Much like an HTTP request, an HTTP response comes with headers that convey important information such as the language and format of the data being sent in the response body.
Example of HTTP response headers from Google Chrome's network tab:

What’s in an HTTP response body?
Successful HTTP responses to ‘GET’ requests generally have a body which contains the requested information. In most web requests, this is HTML data which a web browser will translate into a web page.

Can DDoS attacks be launched over HTTP?
Keep in mind that HTTP is a “stateless” protocol, which means that each command runs independent of any other command. In the original spec, HTTP requests each created and closed a TCP connection. In newer versions of the HTTP protocol (HTTP 1.1 and above), persistent connection allows for multiple HTTP requests to pass over a persistent TCP connection, improving resource consumption. In the context of DoS or DDoS attacks, HTTP requests in large quantities can be used to mount an attack on a target device, and are considered part of application layer attacks or layer 7 attacks.

WHAT IS MOBILE TELECOMMUNICATION TECHNOLOGIES

Since the introduction of first commercial mobile phone in 1983 by Motorola, mobile technology has come a long way. Be it technology, protocols, services offered or speed, the changes in mobile telephony have been recorded as generation of mobile communication. Here we will discuss the basic features of these generations that differentiate it from the previous generations.

1G Technology

1G refers to the first generation of wireless mobile communication where analog signals were used to transmit data. It was introduced in the US in early 1980s and designed exclusively for voice communication. Some characteristics of 1G communication are −

- Speeds up to 2.4 kbps
- Poor voice quality
- Large phones with limited battery life
- No data security

2G Technology

2G refers to the second generation of mobile telephony which used digital signals for the first time. It was launched in Finland in 1991 and used GSM technology. Some prominent characteristics of 2G communication are −

- Data speeds up to 64 kbps
- Text and multimedia messaging possible
- Better quality than 1G

When GPRS technology was introduced, it enabled web browsing, e-mail services and fast upload/download speeds. 2G with GPRS is also referred as 2.5G, a step short of next mobile generation.

3G Technology

Third generation (3G) of mobile telephony began with the start of the new millennium and offered major advancement over previous generations. Some of the characteristics of this generation are −

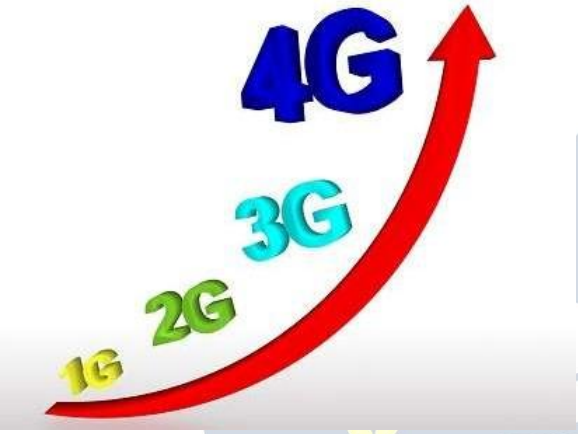
- Data speeds of 144 kbps to 2 Mbps
- High speed web browsing
- Running web based applications like video conferencing, multimedia e-mails, etc.
- Fast and easy transfer of audio and video files

- 3D gaming

Every coin has two sides. Here are some downsides of 3G technology −

- Expensive mobile phones
- High infrastructure costs like licensing fees and mobile towers
- Trained personnel required for infrastructure set up

The intermediate generation, 3.5G grouped together dissimilar mobile telephony and data technologies and paved way for the next generation of mobile communication.



4G Technology

Keeping up the trend of a new mobile generation every decade, fourth generation (4G) of mobile communication was introduced in 2011. Its major characteristics are −

- Speeds of 100 Mbps to 1 Gbps
- Mobile web access
- High definition mobile TV
- Cloud computing
- IP telephony

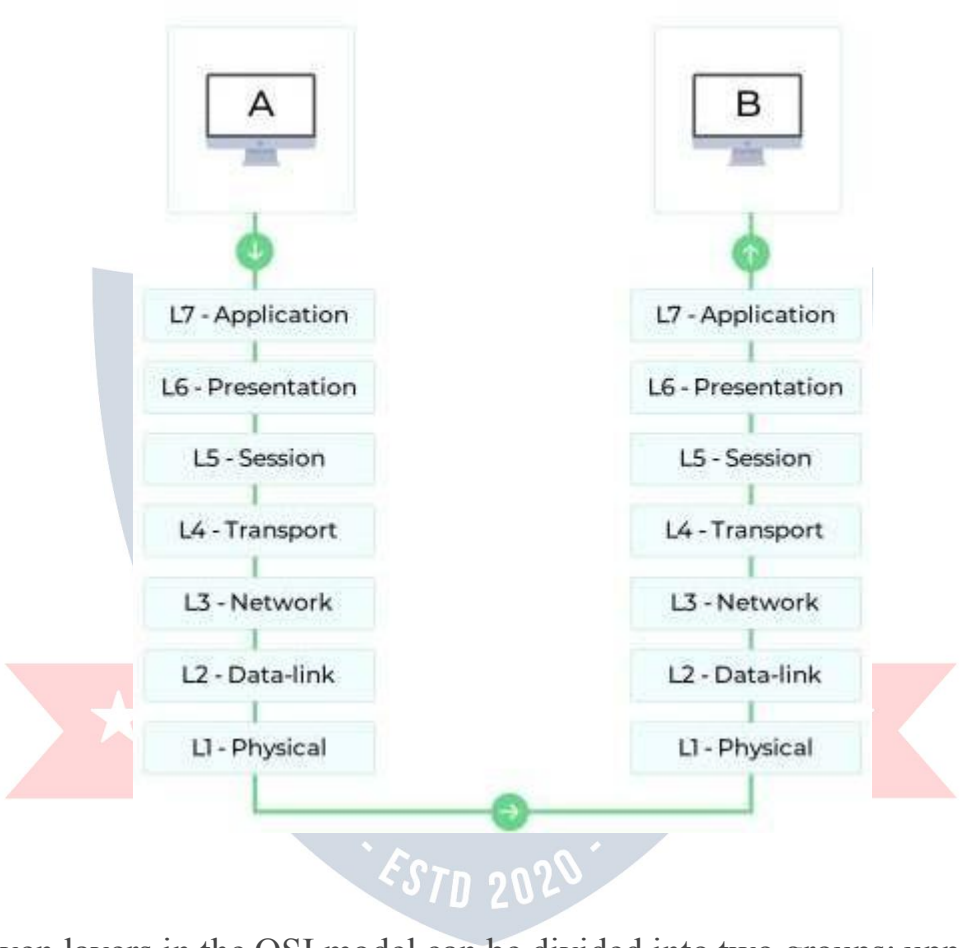
WHAT IS NETWORK PROTOCOL

Network protocols are a set of rules, conventions, and data structures that dictate how devices exchange data across networks. In other words, network protocols can be equated to languages that two devices must understand for seamless communication of information, regardless of their infrastructure and design disparities.

The OSI model: How network protocols work

To understand the nuances of network protocols, it's imperative to know about the Open Systems Interconnection (OSI) model first. Considered the primary

architectural model for internet working communications, the majority of network protocols used today are structurally based on the OSI model.
The OSI model splits the communication process between two network devices into 7 layers. A task or group of tasks is assigned to each of these 7 layers. All the layers are self-contained, and the tasks assigned to them can be executed independently.
To put this into context, here is a representation of the communication process between two network devices following the OSI model:



The seven layers in the OSI model can be divided into two groups: upper layers, including layers 7, 6, and 5, and lower layers, including layers 4, 3, 2, and 1. The upper layers deal with application issues, and the lower layers deal with data transport issues.
Network protocols divide the communication process into discrete tasks across every layer of the OSI model. One or more network protocols operate at each layer in the communication exchange.
Following are the detailed descriptions of the functioning of network protocols in each layer of the OSI model:

Layer 7: Application layer network protocols	Provides standard services such as virtual terminal, file, and job transfer and operations.

Layer 6: Presentation layer network protocols	Masks the differences in data formats between dissimilar systems. Encodes and decodes data, encrypts and decrypts data, and compresses and decompresses data.
Layer 5: Session layer network protocols	Manages user sessions and dialogues. Establishes and terminates sessions between users.
Layer 4: Transport layer network protocols	Manages end-to-end message delivery in networks. Renders reliable and sequential packet delivery through error recovery and flow control mechanisms.
Layer 3: Network layer protocols	Routes packets according to unique network device addresses. Renders flow and congestion control to prevent network resource depletion.
Layer 2: Data link layer network protocols	Frames packets. Detects and corrects packet transmit errors.
Layer 1: Physical layer network protocols	Interfaces between network medium and devices. Defines optical, electrical, and mechanical characteristics.

Though some say the OSI model is now redundant and less significant than the Transmission Control Protocol (TCP)/IP network model, there are still references to the OSI model even today as the model's structure helps to frame discussions of protocols and contrast various technologies.

Classification of network protocols

Now that you know how the OSI model works, you can dive straight into the classification of protocols. The following are some of the most prominent protocols used in network communication.

Application layer network protocols

1. DHCP: Dynamic Host Configuration Protocol

DHCP is a communication protocol that enables network administrators to automate the assignment of IP addresses in a network. In an IP network, every device connecting to the internet requires a unique IP. DHCP lets network admins distribute IP addresses from a central point and automatically send a new IP address when a device is plugged in from a different place in the network. DHCP works on a client-server model.

Advantages of using DHCP

- Centralized management of IP addresses.
- Seamless addition of new clients into a network.
- Reuse of IP addresses, reducing the total number of IP addresses required.

Disadvantages of using DHCP

- Tracking internet activity becomes tedious, as the same device can have multiple IP addresses over a period of time.
- Computers with DHCP cannot be used as servers, as their IPs change over time.

2. DNS: Domain Name System protocol

The DNS protocol helps in translating or mapping host names to IP addresses. DNS works on a client-server model, and uses a distributed database over a hierarchy of name servers.

Hosts are identified based on their IP addresses, but memorizing an IP address is difficult due to its complexity. IPs are also dynamic, making it all the more necessary to map domain names to IP addresses. DNS helps resolve this issue by converting the domain names of websites into numerical IP addresses.

Advantages

- DNS facilitates internet access.
- Eliminates the need to memorize IP addresses.

Disadvantages

- DNS queries don't carry information pertaining to the client who initiated it. This is because the DNS server only sees the IP from where the query came from, making the server susceptible to manipulation from hackers.
- DNS root servers, if compromised, could enable hackers to redirect to other pages for phishing data.

3. FTP: File Transfer Protocol

File Transfer Protocol enables file sharing between hosts, both local and remote, and runs on top of TCP. For file transfer, FTP creates two TCP connections: control and data connection. The control connection is used to transfer control information like passwords, commands to retrieve and store files, etc., and the data connection is used to transfer the actual file. Both of these connections run in parallel during the entire file transfer process.

Advantages

- Enables sharing large files and multiple directories at the same time.

- Let’s you resume file sharing if it was interrupted.
- Let’s you recover lost data, and schedule a file transfer.

Disadvantages

- FTP lacks security. Data, usernames, and passwords are transferred in plain text, making them vulnerable to malicious actors.
- FTP lacks encryption capabilities, making it non-compliant with industry standards.

4. HTTP: Hyper Text Transfer Protocol

HTTP is an application layer protocol used for distributed, collaborative, and hypermedia information systems. It works on a client-server model, where the web browser acts as the client. Data such as text, images, and other multimedia files are shared over the World Wide Web using HTTP. As a request and response type protocol, the client sends a request to the server, which is then processed by the server before sending a response back to the client.
HTTP is a stateless protocol, meaning the client and server are only aware of each other while the connection between them is intact. After that, both the client and server forget about each other's existence. Due to this phenomenon, the client and server can't both retain information between requests.

Advantages

- Memory usage and CPU usage are low because of lesser concurrent connections.
- Errors can be reported without closing connections.
- Owing to lesser TCP connections, network congestion is reduced.

Disadvantages

- HTTP lacks encryption capabilities, making it less secure.
- HTTP requires more power to establish communication and transfer data.

5. IMAP and IMAP4: Internet Message Access Protocol (version 4)

IMAP is an email protocol that lets end users access and manipulate messages stored on a mail server from their email client as if they were present locally on their remote device. IMAP follows a client-server model, and lets multiple client’s access messages on a common mail server concurrently. IMAP includes operations for creating, deleting, and renaming mailboxes; checking for new messages; permanently removing messages; setting and removing flags; and much more. The current version of IMAP is version 4 revision 1.

Advantages

- As the emails are stored on the mail server, local storage utilization is minimal.

- In case of accidental deletion of emails or data, it is always possible to retrieve them as they are stored on the mail server.

Disadvantages

- Emails won't work without an active internet connection.
- High utilization of emails by end users requires more mailbox storage, thereby augmenting costs.

6. POP and POP3: Post Office Protocol (version 3)

The Post Office Protocol is also an email protocol. Using this protocol, the end user can download emails from the mail server to their own email client. Once the emails are downloaded locally, they can be read without an internet connection. Also, once the emails are moved locally, they get deleted from the mail server, freeing up space. POP3 is not designed to perform extensive manipulations with the messages on the mail server, unlike IMAP4. POP3 is the latest version of the Post Office Protocol.

Advantages

- Read emails on local devices without internet connection.
- The mail server need not have high storage capacity, as the emails get deleted when they're moved locally.

Disadvantages

- If the local device on which the emails were downloaded crashes or gets stolen, the emails are lost.

7. SMTP: Simple Mail Transfer Protocol

SMTP is a protocol designed to transfer electronic mail reliably and efficiently. SMTP is a push protocol and is used to send the email, whereas POP and IMAP are used to retrieve emails on the end user's side. SMTP transfers emails between systems, and notifies on incoming emails. Using SMTP, a client can transfer an email to another client on the same network or another network through a relay or gateway access available to both networks.

Advantages

- Ease of installation.
- Connects to any system without any restriction.
- It doesn't need any development from your side.

Disadvantages

- Back and forth conversations between servers can delay sending a message, and also increases the chance of the message not being delivered.
- Certain firewalls can block the ports used with SMTP.

8. Telnet: Terminal emulation protocol

Telnet is an application layer protocol that enables a user to communicate with a remote device. A Telnet client is installed on the user's machine, which accesses the command line interface of another remote machine that runs a Telnet server program.

Telnet is mostly used by network administrators to access and manage remote devices. To access a remote device, a network admin needs to enter the IP or host name of the remote device, after which they will be presented with a virtual terminal that can interact with the host.

Advantages

- Compatible with multiple operating systems.
- Saves a lot of time due to its swift connectivity with remote devices.

Disadvantages

- Telnet lacks encryption capabilities and sends across critical information in clear text, making it easier for malicious actors.
- Expensive due to slow typing speeds.

9. SNMP: Simple Network Management Protocol

SNMP is an application layer protocol used to manage nodes, like servers, workstations, routers, switches, etc., on an IP network. SNMP enables network admins to monitor network performance, identify network glitches, and troubleshoot them. SNMP protocol is comprised of three components: a managed device, an SNMP agent, and an SNMP manager.

The SNMP agent resides on the managed device. The agent is a software module that has local knowledge of management information, and translates that information into a form compatible with the SNMP manager. The SNMP manager presents the data obtained from the SNMP agent, helping network admins manage nodes effectively.

Currently, there are three versions of SNMP: SNMP v1, SNMP v2, and SNMP v3. Both versions 1 and 2 have many features in common, but SNMP v2 offers enhancements such as additional protocol operations. SNMP version 3 (SNMP v3) adds security and remote configuration capabilities to the previous versions.

Presentation layer network protocols

LPP: Lightweight Presentation Protocol

The Lightweight Presentation Protocol helps provide streamlined support for OSI application services in networks running on TCP/IP protocols for some constrained environments. LPP is designed for a particular class of OSI applications, namely those entities whose application context contains only an Association Control Service Element (ACSE) and a Remote Operations Service Element (ROSE). LPP is not applicable to entities whose application context is more extensive, i.e., contains a Reliable Transfer Service Element.

Session layer network protocols

RPC: Remote Procedure Call protocol

RPC is a protocol for requesting a service from a program in a remote computer through a network, and can be used without having to understand the underlying network technologies. RPC uses TCP or UDP for carrying the messages between communicating programs. RPC also works on client-server model. The requesting program is the client, and the service providing program is the server.

Advantages

- RPC omits many protocol layers to improve performance.
- With RPC, code rewriting or redeveloping efforts are minimized.

Disadvantages

- Not yet proven to work effectively over wide-area networks.
- Apart from TCP/IP, RPC does not support other transport protocols.

Transport layer network protocols

1. TCP: Transmission Control Protocol

TCP is a transport layer protocol that provides a reliable stream delivery and virtual connection service to applications through the use of sequenced acknowledgement. TCP is a connection-oriented protocol, as it requires a connection to be established between applications before data transfer. Through flow control and acknowledgement of data, TCP provides extensive error checking. TCP ensures sequencing of data, meaning the data packets arrive in order at the receiving end. Retransmission of lost data packets is also feasible with TCP.

Advantages

- TCP ensures three things: data reaches the destination, reaches it on time, and reaches it without duplication.
- TCP automatically breaks data into packets before transmission.

Disadvantages

- TCP cannot be used for broadcast and multicast connections.

2. UDP: User Datagram Protocol

UDP is a connection-less transport layer protocol that provides a simple but unreliable message service. Unlike TCP, UDP adds no reliability, flow control, or error recovery functions. UDP is useful in situations where the reliability mechanisms of TCP are not necessary. Retransmission of lost data packets isn't possible with UDP.

Advantages

- Broadcast and multicast connections are possible with UDP.
- UDP is faster than TCP.

Disadvantages

- In UDP, it's possible that a packet may not be delivered, be delivered twice, or not be delivered at all.
- Manual disintegration of data packets is needed.

Network layer protocols

1. IP: Internet Protocol (IPv4)

IPv4 is a network layer protocol that contains addressing and control information, which helps packets be routed in a network. IP works in tandem with TCP to deliver data packets across the network. Under IP, each host is assigned a 32-bit address comprised of two major parts: the network number and host number. The network number identifies a network and is assigned by the internet, while the host number identifies a host on the network and is assigned by a network admin. The IP is only responsible for delivering the packets, and TCP helps puts them back in the right order.

Advantages

- IPv4 encrypts data to ensure privacy and security.
- With IP, routing data becomes more scalable and economical.

Disadvantages

- IPv4 is labor intensive, complex, and prone to errors.

2. IPv6: Internet Protocol version 6

IPv6 is the latest version of the Internet Protocol, a network layer protocol that possesses addressing and control information for enabling packets to be routed in the network. IPv6 was created to deal with IPv4 exhaustion. It increases the IP address size from 32 bits to 128 bits to support more levels of addressing.

Advantages

- More efficient routing and packet processing compared to IPv4.
- Better security compared to IPv4.

Disadvantages

- IPv6 is not compatible with machines that run on IPv4.
- Challenge in upgrading the devices to IPv6.

3. ICMP: Internet Control Message Protocol

ICMP is a network layer supporting protocol used by network devices to send error messages and operational information. ICMP messages delivered in IP packets are used for out-of-band messages related to network operation or misoperation. ICMP is used to announce network errors, congestion, and timeouts, as well assist in troubleshooting.

Advantages

- ICMP is used to diagnose network issues.

Disadvantages

- Sending a lot of ICMP messages increases network traffic.
- End users are affected if malicious users send many ICMP destination unreachable packets.

Data link layer network protocols

1. ARP: Address Resolution Protocol

The Address Resolution Protocol helps map IP addresses to physical machine addresses (or a MAC address for Ethernet) recognized in the local network. A table called an ARP cache is used to maintain a correlation between each IP address and its corresponding MAC address. ARP offers the rules to make these correlations, and helps convert addresses in both directions.

Advantages

- MAC addresses need not be known or memorized, as the ARP cache contains all the MAC addresses and maps them automatically with IPs.

Disadvantages

- ARP is susceptible to security attacks called ARP spoofing attacks.
- When using ARP, sometimes a hacker might be able to stop the traffic altogether. This is also known as ARP denial-of-services.

2. SLIP: Serial Line IP

SLIP is used for point-to-point serial connections using TCP/IP. SLIP is used on dedicated serial links, and sometimes for dial-up purposes. SLIP is useful for allowing mixes of hosts and routers to communicate with one another; for example, host-host, host-router, and router-router are all common SLIP network configurations. SLIP is merely a packet framing protocol: It defines a sequence of characters that frame IP packets on a serial line. It does not provide addressing, packet type identification, error detection or correction, or compression mechanisms.

Advantages

- Since it has a small overhead, it is suitable for usage in microcontrollers.
- It reuses existing dial-up connections and telephone lines.
- It's easy to deploy since it's based on the Internet Protocol.

DIsadvantages

- SLIP doesn't support automatic setup of network connections in multiple OSI layers at the same time.
- SLIP does not support synchronous connections, such as a connection created through the internet from a modem to an internet service provider (ISP).

VIDYAPITH ACADEMY
WWW.VIDYAPITH.IN
ESTD 2020

VIDYAPITH ACADEMY
WWW.VIDYAPITH.IN
ESTD 2020