

Diploma in

IT, Networking and Cloud

Module 2

Computer Networking

Theory Manual

Table of Contents

Table of Contents	2
Learning Outcomes	26
Understand basic computer network technology	27
Introduction to networks	28
What is a Computer Network?	28
Characteristics of a Computer Network	29
Basics Components Of Computer Network	32
Features of a Computer Network	35
Advantages Computer Networks	36
Disadvantages Computer Networks	37
Type of area networks - LAN, VLAN, CAN, MAN, WAN	38
Type of Area Networks	38
LAN(Local Area Network)	38
MAN(Metropolitan Area Network)	40
WAN(Wide Area Network)	42
WLAN(Wireless Local Area Network)	43
VLAN(Virtual Local Area Network)	45
VPN(Virtual Private Network)	46
CAN(Campus Area Network)	48
SAN(Storage Area Network)	49
SHAN(Smart Home Area Network)	50

PAN(Personal Area Network)	51
Internet and Intranet etc.	54
Internet	54
Intranet	55
Difference between Internet and Intranet	56
Extranet	57
Uses and benefits of Network	59
Server-client based network	62
Disadvantages of Client-Server Architecture	64
peer to peer networks	66
Advantages of Peer to Peer Networks	67
Disadvantages of Peer to Peer Networks	68
Difference between Client-server and Peer to Peer Networks	68
Network Interface Card	70
What is a Network Interface Card?	70
Components of NIC	70
Types of NIC Cards	71
Wired:	72
Wireless:	72
USB:	73
Advantages of NIC	73
Disadvantages of NIC	73
Transmission Media and Topologies Media Type	75
What is Transmission Media?	75

Types of transmission media	75
Crimping tools and Color standards for Straight crimping and Cross crimping	78
Crimping Tools	78
Ethernet Cable Color	78
T-568A Straight-Through Ethernet Cable	79
RJ-45 Crossover Ethernet Cable	81
Ethernet Cable Instructions	82
Understand and configure server environment and backup services	84
Server	85
What is Server?	85
Characteristics and capabilities of the server	86
How a Server works?	87
Types of servers	88
File servers	88
Print servers	88
Application servers	89
DNS servers	90
Mail servers	90
Web servers	91
Database servers	92
Virtual servers	92
Proxy servers	93
FTP Server	94
Server Structures	95

Computer hardware server	95
Blade servers	95
Combining servers	96
Examples of server operating systems	97
Microsoft Windows servers	97
Linux / Unix servers	97
NetWare	98
Cloud servers	99
Client	100
What does Client mean?	100
Types of Client-	100
Thin Client:	100
Thick/Fat Client:	101
Hybrid Client:	101
Node	102
What is Node?	103
What is Distributed Network?	103
What is Packet Switching Method	103
Segment	104
What is Segment?	105
Types of Segmentation:	105
Collision Domain	105
Broadcast Domain	106
Backbone	106

What is Backbone?	107
Host	107
What is Host?	107
Key Component of Host	108
Hardware:	109
Software:	109
Networks:	109
Analog and Digital Transmission	110
Define Analog and Digital Transmission	110
Analog Transmission	110
Digital Transmission	111
Difference Between Analog and Digital Transmission	113
What are the Advantages of Digital Transmission over Analog Transmission	114
why digital signals better than analog	115
What are the Advantages of Digital Transmission	116
What are the Disadvantages of Digital Transmission	117
What are the Advantages of Analog Transmission	117
What are the Disadvantages of Analog Transmission	118
STP Cable	119
What is STP Cable?	119
Where is STP Cable used?	119
Which Connector is used in STP Cable?	120
UTP Cable	121
Introduction	121

Types	122
Identifying the Cable type	123
Straight Cable	123
Cross Cable	124
Console or Rollover cable	126
Identifying Characteristics of UTP	127
Wiring the UTP Cables	129
Similarities and differences between STP and UTP cables	131
Coaxial cables	131
Types of Coaxial Cables	134
Specifications	137
RG 6 (In-Depth)	138
Fiber Optics (Optical Fiber)	139
Introduction	140
Evolution or History of an Optical Fiber	141
An optical transmission system has three essential components	141
Structure of Optical Fiber	141
Working principle of an optical fiber	142
SMF (Single-mode fiber) optical cable	144
Characteristics of Optical Fiber Cables	145
Baseband and Broadband Transmission	146
Baseband transmission	147
Broadband transmission	148
Differences between baseband and broadband transmissions	150

Cables Connectors	151
USB (Universal Serial Bus)	151
Advantages of USB	153
Limitations	154
RJ-11 (Registered Jack)	155
RJ-45 (Registered Jack)	156
F-Type	156
ST (Straight Tip) and SC (Subscriber Connector or Standard Connector)	157
Fiber LC (Local Connector)	157
MT-RJ (Mechanical Transfer Registered Jack)	158
Network cable Crimping and Testing Tools	159
Network cable crimping tools	159
Network cable testing and troubleshooting tools	161
Troubleshooting tools	161
Network Topology	165
Two different types of network topologies	166
The hierarchical internetworking model	166
Leaf-Spine Network Topology	168
Auto-Discover Network Topologies	169
Bus topology	170
Advantages and Disadvantages	171
Star topology	172
Hybrid Topology	174
Ring Topology	175

What is Ring Topology?	175
Advantages of Ring Topology	176
Disadvantages of Ring Topology	177
Mesh Topology	177
1) Fully Connected Mesh Topology:	178
2) Partial Connected Mesh Topology:	179
Characteristics of Mesh Topology:	180
Advantages of Mesh Topology:	180
Disadvantages of Mesh Topology:	180
Synchronous Transmission	181
Characteristics of Synchronous Transmission	182
Examples of Synchronous Transmission	182
Asynchronous Transmission	183
Characteristics of Asynchronous Transmission	183
Examples of Asynchronous Transmission	183
Synchronous vs. Asynchronous Transmission	184
Configure different protocol services	185
User Authentication Strategy	187
What is the purpose of authentication?	187
What are the different authentication protocols?	188
How do I benefit from a user authentication policy?	189
Types of user authentication	189
Two-factor authentication (2FA)	189
Three-factor authentication (3FA)	189

Four-factor authentication (4FA)	190
Organization Unit	190
The Active Directory object types that can be located in OUs are listed below	192
A few benefits of OUs are summarized below	192
Users can delegate administrative control of Active Directory objects through OUs	193
The administrative tasks that are usually delegated are listed below	193
User Environment	194
What is User Environment?	194
Group Policies	195
Group policy is applied in the following order	196
Planning an OU Structure	196
The following strategy is generally recommended for an OU structure:	197
Group Policies	197
Group policy is process in the order of LSDOU: –	199
AGDLP Process	200
Introduction	200
Advantages	201
Different types of protocols	202
Introduction	202
Transmission Control Protocol	204
TCP offers:	205
TCP Services	205
TCP Benefits	206
Internet Protocol	207

Short Information	210
Hyper Text Transfer Protocol	212
Hyper Text Transfer Protocol Secure	214
Advantages	214
Limitations	215
From an architectural point of view	215
File Transfer Protocol	216
Simple Mail Transfer Protocol	216
Some SMTP Commands:	218
Open System Interconnection Model (OSI)	218
Introduction	218
Physical Layer Functions	219
Data Link Layer Functions	219
Network Layer Functions	220
Transport Layer Functions	221
Session Layer Functions	221
Presentation Layer Functions	222
Application layer Functions	222
Media Access Methods	222
Introductions	222
Carrier Sense Multiple Access with Collision Detection (CSMA/CD)	223
Carrier Sense Multiple Access with Collision Avoidance (CSMA/CA)	223
Token Passing	224
Demand Priority	224

Domain Name Services	225
DNS Records	226
There are 4 DNS servers involved in loading a webpage:	227
Dynamic Host Configuration Protocol	228
DHCP Process	229
Windows Internet Name Service	230
Advantages	231
Example	231
Remote Access Service	232
Web Services	234
Web Services Architecture	235
Types of Web Services	237
SOAP (Simple Object Access Protocol)	237
Web Services Advantages	238
REST stands for Representational State Transfer	239
Advantages	239
Disadvantages	240
Proxy Services	240
Functions:	241
Anonymity: The web server you use can only see the IP address of the proxy and not your system.	242
Control: If you are the owner of a website, you can see who visits your website. You can choose who visits your website. If you have blocked someone from your website they would get a message saying something like “site unavailable”	242
Caching: You can save bandwidth if I cache a web site.	242

Malware: You can intercept unwanted things and stop junks at the proxy.	242
Load Balancing: Efficiently distributing incoming network traffic among servers.	242
Types of Proxy services	242
Forward proxy.	242
Reverse proxy	242
Install and configure Linux server environment	244
In this section, we will read about:	244
Configuration Plan	245
Server Role	245
Vulnerable Services	245
Picking a Platform	245
Network and Access Control	245
Users and Authentication	246
Public and data directory	247
Host file	247
Application	248
SWAT	249
Functions of SWAT	249
Globals	249
Shares	249
Printers	249
Wizard	249
Status	249
View	249

Password	250
Password	251
Install & configure the different types of network devices in a network	253
In this section, we will read about:	253
Network Devices	254
Functions of Network Interface Card (NIC)	254
Repeaters	254
Hub	255
Types of hub	256
Active Hub	256
Passive Hub	256
Switches	257
What is a switch ?	257
Role of switches in networking	259
Types of Switches	260
Advantages of Switches	263
Disadvantages of Switches	263
Routers	263
What is a Router ?	263
Features of Router	267
Types of Routers	268
Advantages of Router	271
Disadvantages of Router	272
Bridges	272

What is a bridge ?	272
Types of Bridges	274
Functions of Bridges	274
Advantages of Bridge	275
Disadvantages of Bridge	275
Internet Service Provider	276
What is an Internet Service Provider ?	277
Types of Internet Service Providers	278
Configure and manage network security	284
In this section, we will read about:	285
Modern Network Security	286
Why Internet security ?	286
Importance of Cyber Security	287
Cybersecurity Practice Areas	294
Threats and the Basics of securing a network	295
Common Network Security Threats	295
Cyber Security Best Practices	298
Network Security Models	299
Secure Administrative Access	304
Techniques for secure administrative access	304
Cyber security policies	307
LAN Security Considerations	309
Understand Types of Network Devices	311
Hub	311

Switch	311
Router	311
Bridge	312
Gateway	312
Know Your Network Defenses	312
Firewall	312
Intrusion Detection System (IDS)	312
Intrusion Prevention System (IPS)	313
Network Access Control (NAC)	313
Web Filter	313
Proxy Server	314
Anti-DDoS	314
Load Balancer	314
Spam Filter	314
Segregate Your Network	314
Types of Network Segments	315
Public Networks	315
Semi-Private Networks	316
Private Networks	316
Demilitarized Zone (DMZ)	316
Software-Defined Networking (SDN)	316
Place Your Security Devices Correctly	317
Use NAT	317
Don't Disable Personal Firewall	318

Use Centralized Loggings	319
Use Web Domain Whitelisting	319
Route through Proxy	319
Use Honeypots and Honeynets	320
Protect From Insider Threat	321
Monitor & Baseline Protocols	321
Use VPNs	322
Use Multiple Vendors	322
Use IDS Properly	322
Anomaly detection	323
Misuse detection	323
Automate Response to Attack	323
Block IP Address	323
Terminate Connections	323
Acquire Additional Information	323
Look For the Point of Initial Access	324
Determine How Malicious Software Was Deployed	324
Physically Secure Network Equipment	324
Network Security Devices	324
Firewall	325
Proxy Server	326
Web Filters	326
Anti DDoS	327
Load Balancer	327

Spam Filters	328
Configure and perform remote accessing & routing	329
In this section, we will read about:	329
Overview of Remote Access	329
Introduction	330
How Remote Access Works	330
Types of Remote Access	332
Broadband	332
Cable Broadband	332
DSL (Digital Subscriber Line)	332
Cellular Internet	332
Satellite Internet	332
Fiber Optics	333
Remote Access Protocols	333
Point-to-Point Protocol (PPP)	333
IPSec	333
Point-to-Point Tunneling (PPTP)	334
Layer Two Tunneling Protocol (L2TP)	334
Remote Authentication Dial-In User Service (RADIUS)	335
Terminal Access Controller Access Control System (TACACS)	335
VPN Concepts	336
Introduction	336
VPN Benefits	337
Desired VPN Features	338

Security	338
Reliability	339
Scalability	339
VPN Types	339
Public VPN	339
Remote-Access VPN	340
Site-to-Site VPN	341
VPN Tunneling	342
Equipment Used For VPN	343
Network access server	343
Firewall	343
AAA Server	343
VPN Concentrator	344
VPN-enabled/VPN-optimized Router	344
VPN-enabled Firewall	344
VPN Client	344
VPN Security	345
L2F (Layer 2 Forwarding)	346
PPTP (Point-to-point Tunneling Protocol)	346
L2TP (Layer 2 Tunneling Protocol)	346
Remote Access Authentication Protocol	346
PAP	348
Features	348
When to use PAP	349

Advantage of CHAP over PAP	349
Advantage of PAP over CHAP	349
CHAP	350
Features	350
CHAP Packets	351
The Extensible Authentication Protocol (EAP)	351
MS-CHAP	353
MS-CHAP v2	354
RADIUS	355
What is RADIUS?	355
How it Works?	356
Background Information	356
RADIUS is a Client/Server Protocol	357
Connection Steps	357
Authentication and Authorization	358
Accounting	359
TCP/IP Routing	359
Introduction	359
Protocols Types	362
Host Route	363
Network Route	363
Default Route	363
Static & Dynamic Routing	363
Gateways	364

Interior and Exterior Gateways	365
Gateway Protocols	366
Routing Information Protocol Next Generation	367
Open Shortest Path First (OSPF)	367
Exterior Gateway Protocol (EGP)	367
Border Gateway Protocol (BGP)	368
Border Gateway Protocol 4+	368
Intermediate System to Intermediate System (IS-IS)	368
Familiarize with internet and E- Commerce sites	370
Introduction to Search Engines	371
Introduction	371
Search Engine Components	372
Search Engine Working	372
Architecture	373
Search Engine Processing	373
Indexing Process	373
Text acquisition	374
Text Transformation	374
Index Creation	374
Query Process	374
User interaction	374
Ranking	374
Evaluation	374
Popular Search engines	375

Search Engine Market Share	376
Google	377
Bing	378
Yahoo	379
Baidu	380
DuckDuckGo	382
Ask.com	383
AOL.com	384
Wolframalpha	385
Internet Archive	386
Concept of Favourites Folder	387
What is an Electronic Mail	389
Definition	389
History of Email	390
Advantages	392
Disadvantages	393
Email Addressing, BCC and CC, Inbox, Outbox, Address book, SPAM	394
Email Addressing	394
BCC and CC	395
BCC	395
CC	395
Inbox	395
Outbox	396
Address book	397

SPAM	398
Introduction to video chatting tools	400
Introduction to Internet Security, Threats and attacks, Malicious Software types, Internet security products and their advantages	402
Introduction to Internet Security	402
Threats and attacks	403
Threats	403
Attacks	403
Web-based attacks	404
System-based attacks	406
Malicious Software types	406
Malicious Software	406
Types of Malware:	407
Internet security products and their advantages	408
Internet security products	408
Advantages	409
IT Act & Law Introduction to Cyber Security	412
IT Act & Law	412
Offences	412
Introduction to Cyber Security	417
Introduction to Cyber Laws & IT Act.	417
Information Technology Act	418
Objectives of the Act	418
Features of the Information Technology Act, 2000	419

Cyber Security	420
Importance of privacy and techniques to manage it	423
List of techniques on Importance of Privacy	423
E commerce	426
Definition of E-Commerce	426
Types of E-Commerce	428
Scope of E-Commerce	431
Benefits of E-Commerce:	433
Difference between E commerce and traditional commerce.	439
Capabilities requirements and Technology issues for E commerce.	443
Types of E commerce web sites	445
Building business on the net.	446
Step 1: Start a business that fills a need.	447
Step 2: Write a copy that sells.	447
Step 3: Design and build your website.	448
Step 4: Use search engines to drive targeted buyers to your site.	448
Step 5: Establish an expert reputation for yourself.	448
Step 6: Use the power of email marketing to turn visitors into buyers.	449
Step 7: Increase your income through back-end sales and upselling.	449
Concepts of online Catalogues, Shopping carts, Checkout pages.	451
Online catalogues	451
Shopping Carts	451
Checkout Pages	453

Payment and Order Processing, Authorization, Chargeback and other payment methods.
456

Payment & Order Processing	456
Authorization	457
Chargeback & Other Payment Methods	458
Security issues and payment gateways	461
Security Issues	461
Payment gateway	463
References	464

Learning Outcomes

After completing this module a student will be able to:

1. Understand basic computer network technology
2. Understand and configure server environment and backup services
3. Configure different protocol services
4. Install and configure Linux server environment
5. Install & configure the different types of network devices in a network
6. Configure and manage network security
7. Configure and perform remote accessing & routing
8. Familiarize with internet and E-Commerce sites

Understand basic computer network technology

In this section, we will read about:

- Introduction to networks
- Type of area networks - LAN, VLAN, CAN, MAN, WAN
- Internet and Intranet etc.
- Uses and benefits of Network
- Server-client based network
- Peer to Peer networks
- Network Interface Card
- Transmission Media and Topologies Media Type
- Crimping tools and Color standards for Straight crimping and Crosscrimping

Introduction to networks

What is a Computer Network?

A computer network is a group of computers that use a set of common communication protocols over digital interconnections for the purpose of sharing resources located on or provided by the network nodes.

Computer networking refers to connected computing devices (such as laptops, desktops, servers, smartphones, and tablets) and an ever-expanding array of IoT devices (such as cameras, door locks, doorbells, refrigerators, audio/visual systems, thermostats, and various sensors) that communicate with one another.

A collection of distributed, intelligent machines that shares data and information through interconnected lines of communication is called networking. When two or more computers are brought together in connection with cable or without cable, which may extend within a limited room or to the entire world, the computers are said to be network connections.



Image 1: Computer Network
Reference: https://www.tutorialspoint.com/computer_fundamentals/computer_networking.htm

Characteristics of a Computer Network

- Share resources from one computer to another.
- Create files and store them in one computer, access those files from the other computer(s) connected over the network.
- Connect a printer, scanner, or a fax machine to one computer within the network and let other computers of the network use the machines available over the network.

Following is the list of hardware's required to set up a computer network.

- Network Cables
- Distributors
- Routers
- Internal Network Cards
- External Network Cards

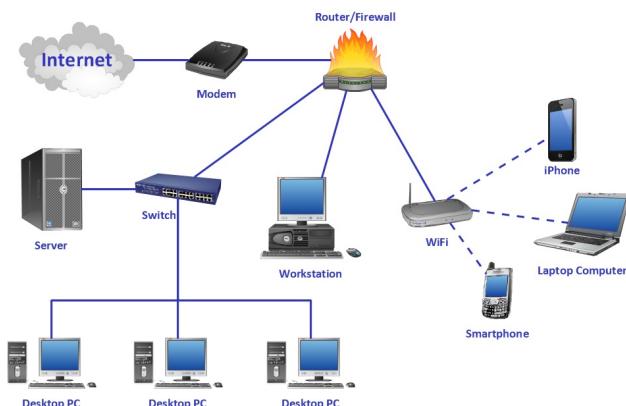


Image 2: Characteristics of a Computer Network
Reference: <https://tyrocity.com/topic/computer-networks/>

Network Cables

Network cables are used to connect computers. The most commonly used cable is Category 5 cable RJ-45.



Image 3: RJ-45

Reference: https://www.tutorialspoint.com/computer_fundamentals/computer_networking.htm

Distributors

A computer can be connected to another one via a serial port but if we need to connect many computers to produce a network, this serial connection will not work.



Image 4: Distributors

Reference: https://www.tutorialspoint.com/computer_fundamentals/computer_networking.htm

The solution is to use a central body to which other computers, printers, scanners, etc. can be connected and then this body will manage or distribute network traffic.

Router

A router is a type of device which acts as the central point among computers and other devices that are a part of the network. It is equipped with holes called ports. Computers and other devices are connected to a router using network cables. Now-a-days routers come in wireless modes using which computers can be connected without any physical cable.



Image 5: Router

Reference: https://www.tutorialspoint.com/computer_fundamentals/computer_networking.htm

Network Card

Network card is a necessary component of a computer without which a computer cannot be connected over a network. It is also known as the network adapter or Network Interface Card (NIC).

Network cards are of two types:

- Internal Network Cards
- External Network Cards

Internal Network Cards

Motherboard has a slot for an internal network card where it is to be inserted. Internal network cards are of two types in which the first type uses Peripheral Component Interconnect (PCI) connection, while the second type uses Industry Standard Architecture (ISA). Network cables are required to provide network access.



Image 6:Internal Network Cards

Reference: https://www.tutorialspoint.com/computer_fundamentals/computer_networking.htm

External Network Cards

External network cards are of two types: Wireless and USB based. Wireless network cards need to be inserted into the motherboard, however no network cable is required to connect to the network.



Image 7:External Network Cards
Reference: https://www.tutorialspoint.com/computer_fundamentals/computer_networking.htm

Basics Components Of Computer Network

A computer network is built up from several components. These components together make it possible to transfer data from one device to another and makes smooth communication between two different devices. In this guide, we will discuss the main components of a computer network.

- Servers
- Clients
- Transmission Media
- Network Interface card
- Modem
- Hub
- Switch
- Cables and connectors
- Router
- LAN cable

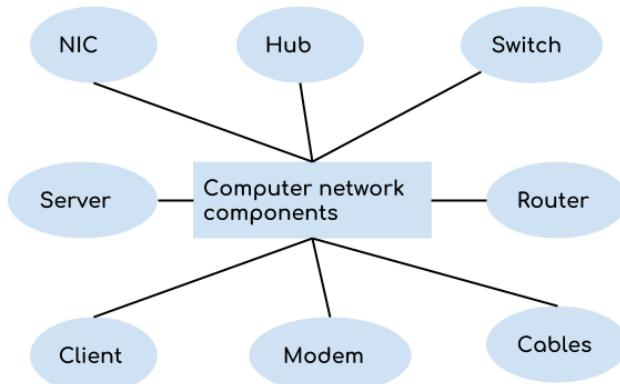


Image 8: Network Components
Reference:<https://beginnersbook.com/2019/03/computer-network-components/>

Server

Servers are computers that run operating systems and hold data that can be shared over a computer network.

Client

A client is a computer that is connected to other computers in the network and can receive data sent by other computers.

Transmission Media

All computers in a computer network are connected with each other through a transmission media such as wires, optical fibre cables, coaxial cables etc.

Network Interface card

Each system or computer in a computer network must have a card called network interface card (NIC). The main purpose of NIC is to format the data, send the data and receive the data at the receiving node.

Modem

Modem Short for modulator-demodulator In a communication modem converts the digital data into analog so that it transmits over the phone line because the phone line transmits analog data. In the same way on the other hand when data is received modem again converts this analog data into a digital single so that computer stores and processes this information.

Modulator means that it converts digital signals into analog signals and sends it over telephone lines. This process is known as modulation.

Demodulator means that receiving modem converts analog signals into digital signals and this process is known as demodulation.

It helps us to transmit data from one computer to another computer using standard telephone lines.

Cables and Connectors

Networking cables are networking hardware used to connect one network device to other network devices or to connect two or more computers to share printers, scanners etc.

Hub

Hub acts as a device that connects all the computers in a network to each other. Any request that comes from a client computer first received by Hub and then hub transmits this request over a network so that the correct server receives and responds to it.

Switch

Switch is similar to hub however instead of broadcasting a incoming data request it uses the physical device address in the incoming request to transfer the request to the correct server computer.

Router

Router joins multiple computer networks to each other. For example let's say a company runs 100 computers over a local area network(LAN) and another company runs another LAN of 150 computers. These both LANs can be connected with each other through an internet connection which is provided by the router.

LAN cable

A wire that is used to connect more than one computers or other devices such as printers and scanners to each other.

Features of a Computer Network

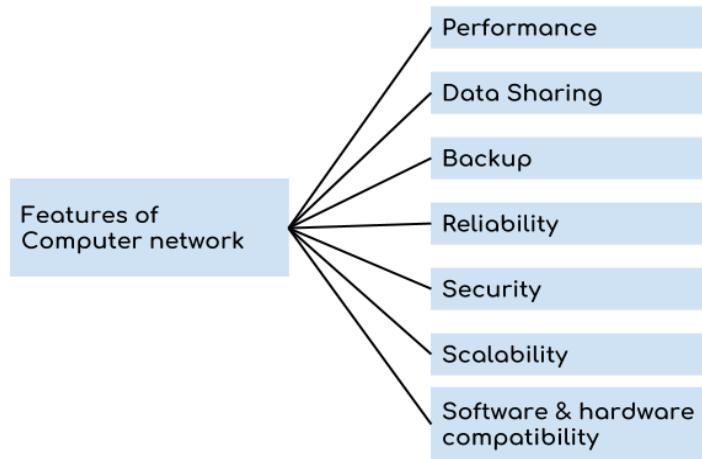


Image 9: Features of a Computer Network

Reference:<https://beginnersbook.com/2019/03/computer-network-features/>

A computer network has following features:

Performance:

Performance of a computer network is measured in terms of response time. The response time of sending and receiving data from one node (computer in a computer network are often referred as node) to another should be minimal.

Data Sharing:

One of the reasons why we use a computer network is to share the data between different systems connected with each other through a transmission media.

Backup:

A computer network must have a central server that keeps the backup of all the data that is to be shared over a network so that in case of a failure it should be able to recover the data faster.

Software and hardware compatibility:

A computer network must not limit all the computers in a computer network to use same software and hardware, instead it should allow the better compatibility between the different software and hardware configuration.

Reliability:

There should not be any failure in the network or if it occurs the recovery from a failure should be fast.

Security:

A computer network should be secure so that the data transmitting over a network should be safe from unauthorised access. Also, the sent data should be received as it is at the receiving node, which means there should not be any loss of data during transmission.

Scalability:

A computer network should be scalable which means it should always allow to add new computers (or nodes) to the already existing computer network.

Advantages Computer Networks

- Workgroups-a group of users can work together on a single project
- Shared databases-many users can access the data,such as bank accounts
- Distributed Systems-a problem can be divided into parts and each part worked on independently
- Communications-Data can be shared,such as emails,video conferencing,VoIP
- Device Sharing-Many users share one pointer
- Software sharing-Software is installed on a server and can be updated centrally
- Security-All work is under a central and breaches can be tracked

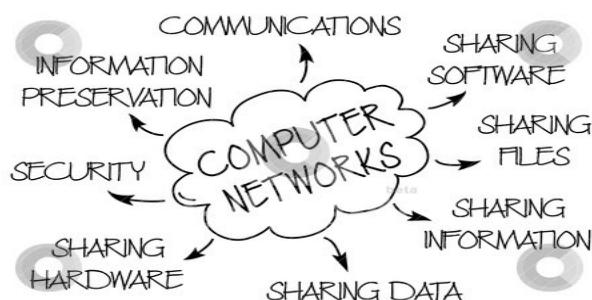


Image 11: Advantages of Computer Network
Reference: <http://wifinotes.com/computer-networks/advantages-of-computer-networking.html>

Disadvantages Computer Networks

- Buying the computer cable and servers can be very expensive.
- Viruses can spread to other computers throughout a computer network.
- People can hack your computer.
- It encourages people to become dependent on computers.
- It comes with the risk of security issues.



Image 12:Disadvantages of Computer Network
Reference: https://www.tutorialspoint.com/computer_fundamentals/computer_networking.htm

Type of area networks - LAN, VLAN, CAN, MAN, WAN

Type of Area Networks

A computer network is a group of computers linked to each other that enables the computer to communicate with another computer and share their resources, data, and applications.

- LAN
- MAN
- WAN
- VLAN
- WLAN
- VPN
- CAN
- SAN
- SHAN
- PAN

LAN(Local Area Network)

- Group of interconnected computers within a small area. (room, building,campus)
- Two or more pc's can from a LAN to share files, folders, printers, applications and other devices
- Coaxial or CAT 5 cables are normally used for connections
- Due to short distances, errors and noise are minimal.
- Local Area Network provides higher security.
- Data transfer rate is 10 to 100 mbps.

Example: A computer lab in a school

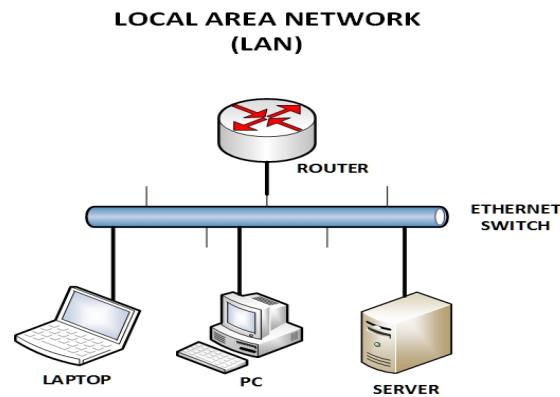


Image 13: LAN

Reference: <https://www.networkstraining.com/different-types-of-networks/>

Advantages of LAN

Resource Sharing:

LAN provides resource sharing such as computer resources like printers, scanners, modems, DVD-ROM drives, and hard disks can be shared within the connected devices. This reduces cost and hardware purchases.

Software Applications Sharing:

In a Local Area Network, it is easy to use the same software in a number of computers connected to a network instead of purchasing the separately licensed software for each client a network.

Easy and Cheap Communication:

Data and messages can easily be shared with the other computer connected to the network.

Centralized Data:

The data of all network users can be stored on a hard disk of the central/server computer. This helps users to use any computer in a network to access the required data.

Data Security:

Since data is stored on the server computer, it will be easy to manage data at only one place and the data will be more secure too.

Internet Sharing:

Local Area Network provides the facility to share a single internet connection among all the LAN users. In school labs and internet Cafes, single internet connection is used to provide internet to all connected computers.

Disadvantages of LAN

High Setup Cost:

The initial setup costs of installing Local Area Networks is high because there is special software required to make a server. Also, communication devices like an ethernet cable, switches, hubs, routers, cables are costly.

Privacy Violations:

The LAN administrator can see and check personal data files of each and every LAN user. Moreover, he can view the computer and internet history of the LAN user.

Data Security Threat:

Unauthorised users can access important data of an office or campus if a server hard disk is not properly secured by the LAN administrator.

LAN Maintenance Job:

Local Area Network requires a LAN Administrator because there are problems such as software installations, program faults or hardware failures or cable disturbances in Local Area Network. A LAN Administrator is required to maintain these issues.

Covers Limited Area:

LANs are restricted in size; they cover a small area like a single office, single building or a group of nearby buildings.

MAN(Metropolitan Area Network)

- Design to extend over a large area.
- Connecting number of LAN's to form larger network, so that resources can be shared.
- Government agencies use MAN to connect to the citizens and private industries
- In MAN, various LANs are connected to each other through a telephone exchange line.
- Networks can be up to 5 to 50 km.
- Data transfer rate is low compared to LAN.

Example: Organization with different branches located in the city.

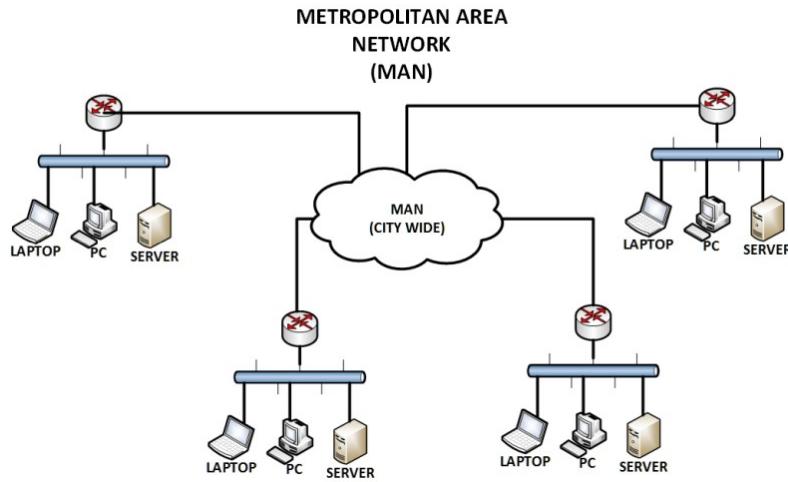


Image 14:MAN

Reference:<https://www.networkstraining.com/different-types-of-networks/>

Advantages of a MAN Network

There are many advantages of the MAN network, some of them given below.

Less Expensive:

It is less expensive to attach MAN with WAN Network. MAN gives you good efficiency of data. All data on MAN is easily manageable in a centralized way.

Sending Local Emails:

You can send local emails fast and free on MAN.

High Speed than WAN:

The speed of data can easily reach 1000 Mbps, as MAN uses fiber optics. Files and database transfer rates are fast.

Sharing of the Internet:

With the installation of MANs, users can share their internet connection. In this way, multiple users can get the same high-speed internet.

Conversion of LAN to MAN is Easy:

MAN is a combination of two or more LAN networks. So it is a faster way to connect two LAN networks together. It is possible by the fast configuration of links.

High Security:

MAN's has a higher-security level than WAN.

Disadvantages of MAN Network

Difficult To Manage:

It is very difficult to manage if the size and number of LANs network increase. This is due to security and extra configuration problems.

Internet Speed Difference:

As it cannot work on phone copper wires. Copper wires affect the speed of MAN. So high cost is needed for fiber optics.

Hackers Attack:

In this network, there is a high risk of attacking hackers as compared to LAN. So data may be a leak. Highly security staff is the need in MAN.

Technical Staff Requires to Set up:

Highly technical people are required to set up MAN. The technical people are network administrators and troubleshooters.

Need More wires:

In MAN more than LAN networks, cables require. As you know, it is a combination of two LANs.

WAN(Wide Area Network)

- A Wide Area Network is a network that extends over a large geographical area such as states or countries.
- Contains multiple LAN's and MAN's.
- A Wide Area Network is quite a bigger network than the LAN.
- Distinguished in terms of geographical range.
- Data transfer rate depends upon the ISP provider and varies over the location.

Example: Internet

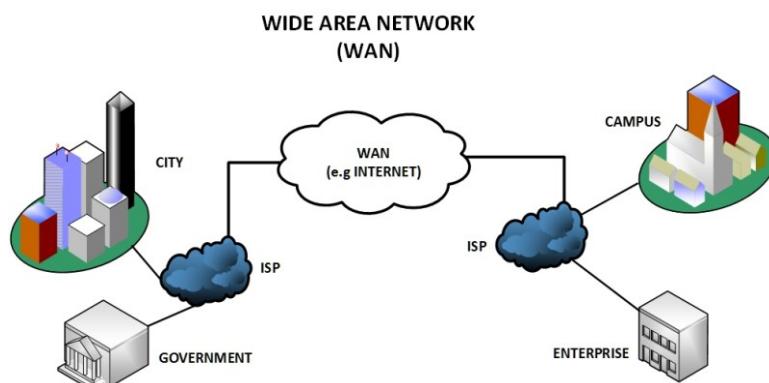


Image 15: WAN

Reference: <https://www.networktraining.com/different-types-of-networks/>

Advantages of WAN :

WAN covers a larger geographical area. Hence business offices situated at longer distances can easily communicate.

Like LAN, it allows sharing of resources and application softwares among distributed workstations or users.

The software files are shared among all the users. Hence all will have access to the latest files. This avoids use of previous versions by them.

Organizations can form their global integrated network through WAN. Moreover it supports global markets and global businesses.

The emergence of IoT (Internet of Things) and advanced wireless technologies such as LAN or LAN-Advanced have made it easy for the growth of WAN based devices. Messages can be sent very quickly across the globe with the help of applications such as WhatsApp, facebook messenger etc.

Disadvantage of WAN :

- Initial investment costs are higher.
- It is difficult to maintain the network. It requires skilled technicians and network administrators.
- There are more errors and issues due to wide coverage and use of different technologies. Often it requires more time to resolve issues due to involvement of multiple wired and wireless technologies.
- It has lower security compared to LAN and MAN due to wider coverage and use of more technologies.
- Security is a big concern and requires use of firewall and security softwares/protocols at multiple points across the entire system. This will avoid chances of hacking by intruders.

WLAN(Wireless Local Area Network)

- A WLAN makes use of a Wireless Access Point (WAP) device, which serves as the point of connectivity for wireless clients on the network.
- A LAN that uses high frequency radio waves for communication.
- Provides short range connectivity with high speed data transmission

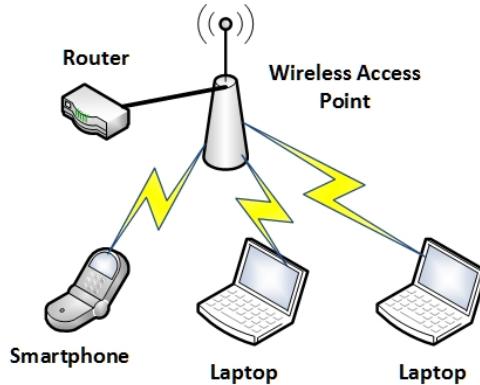


Image 16: WLAN

Reference:<https://www.networkstraining.com/different-types-of-networks/>**Advantages of WLAN:**

- It is a reliable type of communication
- As WLAN reduces physical wires so it is a flexible way of communication
- WLAN also reduces the cost of ownership
- It is easier to add or remove workstation
- It provides high data rate due to small area coverage
- You can also move workstation while maintaining the connectivity
- For propagation, the light of sight is not required
- The direction of connectivity can be anywhere i.e. you can connect devices in any direction unless it is in the range of access point
- Easy installation and you need don't need extra cables for installation
- WLAN can be useful in disaster situations e.g. earthquake and fire. People can still communicate through the wireless network during a disaster
- It is economical because of the small area access
- If there are any building or trees then still wireless connection works

Disadvantages of WLAN:

- WLAN requires license
- It has a limited area to cover
- Government agencies can limit the signals of WLAN if required. This can affect data transfer from connected devices to the internet
- If the number of connected devices increases then data transfer rate decreases
- WLAN uses radio frequency which can interfere with other devices which use radio frequency
- If there is rain or thunder then communication may interfere

- Attackers can get access to the transmitted data because wireless LAN has low data security
- Signals may be affected by the environment as compared to using fiber optics
- The radiation of WLAN can be harmful to the environment
- As WLAN uses access points and access points are expensive than wires and hubs
- Access points can get signals of nearest access points
- It is required to change the network card and access point when standard changes
- LAN cable is still required which acts as the backbone of the WLAN
- Low data transfer rate than wired connection because WLAN uses radio frequency
- Chances of errors are high
- Communication is not secure and can be accessed by unauthorized users

VLAN(Virtual Local Area Network)

- Virtual Local Area Networks (VLANs) divide a single existing physical network into multiple logical networks.
- Thereby, each VLAN forms its own broadcast domain.
- Communication between two different VLANs is only possible through a router that has been connected to both VLANs.
- VLANs behave as if they had been constructed using switches that are independent of each other.

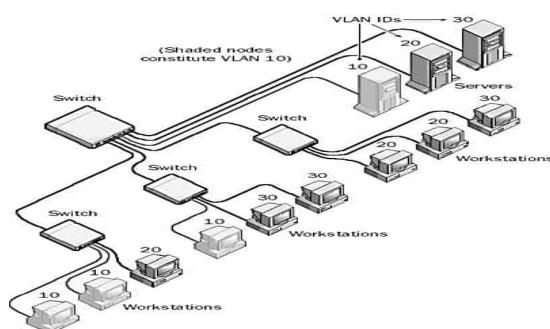


Image 17: VLAN
Reference:<https://networkencyclopedia.com/virtual-lan-vlan/>

Advantages of VLANs:

- VLANs provide enhanced network security. In a VLAN network environment, with multiple broadcast domains, network administrators have control over each port and user.
- Allowing network administrators to apply additional security to network communication.

-
- Making expansion and relocation of a network or a network device easier.
 - Providing flexibility because administrators are able to configure in a centralized environment while the devices might be located in different geographical locations.
 - Decreasing the latency and traffic load on the network and the network devices, offering increased performance.
 - VLANs enable logical grouping of end-stations that are physically dispersed on a network.
 - It allows higher performance and reduced latency.
 - It allows users to work on sensitive information which should not be seen by other users.
 - VLAN Removes the physical boundary.

Disadvantages of VLANs:

- High risk of virus issues because one infected system may spread a virus through the whole logical network.
- Equipment limitations in very large networks because additional routers might be needed to control the workload.
- More effective at controlling latency than a WAN, but less efficient than a LAN.
- For Inter-VLAN communication we need a router.
- Management is complex.
- Possible problems in interoperability.

VPN(Virtual Private Network)

- A Virtual Private Network is a type of network that makes use of existing private or public network infrastructure(e.g the Internet) to provide a secure network connection.
- This is often achieved by creating an encrypted tunnel for secured end-to-end connectivity.
- A Virtual Private Network uses data encryption techniques to provide security for files that are sent or received over the network.
- This is often used by organizations that have highly sensitive data to transfer.

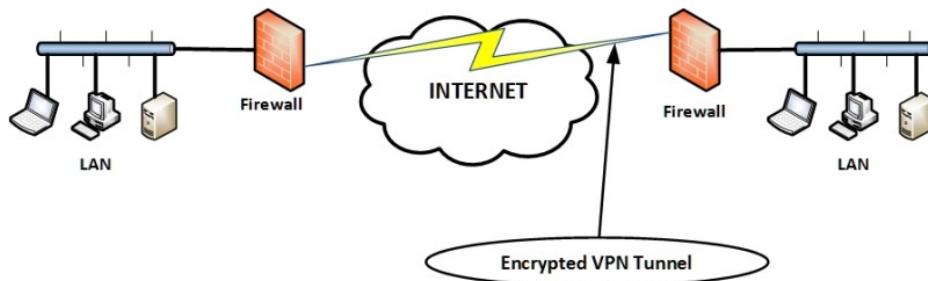


Image 18: VPN

Reference: <https://www.networktraining.com/different-types-of-networks/>

VPN Advantages

- A VPN service hides your real IP address, effectively masking your online identity and allowing you to bypass geo-blocks.
- Since a VPN masks your IP address, it also helps you bypass firewalls.
- A VPN encrypts your online connections, protecting your data from hackers and ISP/government surveillance.
- By encrypting your online traffic, a VPN ensures your ISP can't throttle your bandwidth.
- A VPN offers you a better online gaming experience by keeping you safe from IP bans, DDoS attacks, and by giving you access to geo-blocked/banned video games.
- With a VPN, you are much safer when downloading torrents since your ISP can't see what you're doing, and other people who are downloading/uploading the same torrent can't see your real IP address.
- A VPN can potentially help you avoid online price discrimination (like when airline companies charge more for the same ticket if you're from a different geographical area) since it hides your IP address.

VPN Disadvantages

- VPN services will usually cost money, as free VPNs aren't an option since they don't work right and endanger your data.
- Not all devices and operating systems natively support VPN applications, so you might have to manually set up a connection sometimes.
- Using a VPN will usually lower your online speeds to a certain extent because of various factors (distance from the server, type of encryption that's used, what VPN protocol you use, etc.).
- Some VPN providers log user data, which can put your privacy in danger.

CAN(Campus Area Network)

- A campus area network (CAN) is a network of multiple interconnected local area networks (LAN) in a limited geographical area.
- CAN is smaller than WAN (Wide Area Network)
- CAN is also known as a controller area network.

Example: Network in university

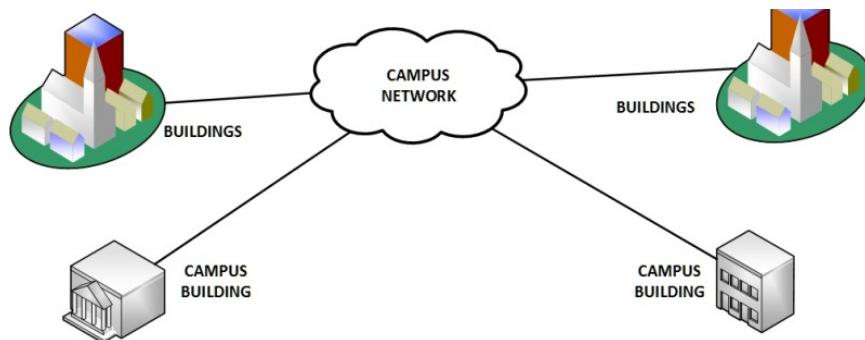


Image 19: CAN

Reference: <https://www.networktraining.com/different-types-of-networks/>

Advantages of CAN:

Economical:

CAN is economical in the sense that it uses fewer cables, switches, hubs and routers.

Sharing of data is easy:

In CAN, the message is sent one time and is transferred to all the linked departments easily.

Use a wireless connection:

CAN use a wireless connection for connecting different departments and buildings across one organization.

Transferring files is fast:

In CAN, files are transferred with high speed over the network (internet).

One ISP across all departments:

In CAN, the internet is used from the same ISP (Internet Service Provider).

Disadvantages of CAN:

- Limitation for connecting nodes:
- The connection between nodes (computers) is limited in size i.e. you cannot connect a large number of nodes together in CAN. And also CAN have a maximum length of 40 meters.

- Maintenance is expensive:
- Troubleshooting and maintenance of CAN are expensive as compared to other networks.

SAN(Storage Area Network)

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

Example: Used for daily backup of organization or a mirror copy

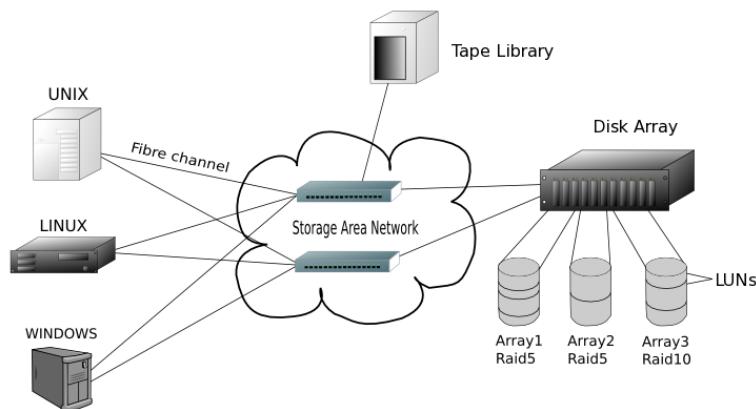


Image 20: SAN

Reference: <https://www.networkstraining.com/different-types-of-networks/>

Advantages of Storage Area Networks

The different advantages of storage area networks are:

- The storage devices are independent of the system and their data is accessed using the storage area network. So the storage devices can be increased and decreased as required.
- The storage is removed from the purview of the system and moved onto a separate network. This leads to a better performance overall as the data is not affected by local traffic or bottlenecks.
- The storage data is very secure on the storage area network and cannot be copied or stolen by anyone else.
- There can be a remote copy of the storage data kept separately using the storage area network. This can be useful if there is a primary data failure or natural disaster.

Disadvantages of Storage Area Networks

The different disadvantages of storage area networks are:

- If there is a lot of traffic in the storage area network, then operations will be extremely slow. So it is better not to use storage area networks for data extensive applications.
- The storage area network operates in a shared environment. So there is a chance that data may be leaked for sensitive operations.

SHAN(Smart Home Area Network)

A home area network (HAN) is a network contained within a user's home that connects a person's digital devices, from multiple computers and their peripheral devices to telephones, VCRs, televisions, video games, home security systems, smart appliances, fax machines and other digital devices that are wired into the network.

The SHAN network is generally used in homes and office space.

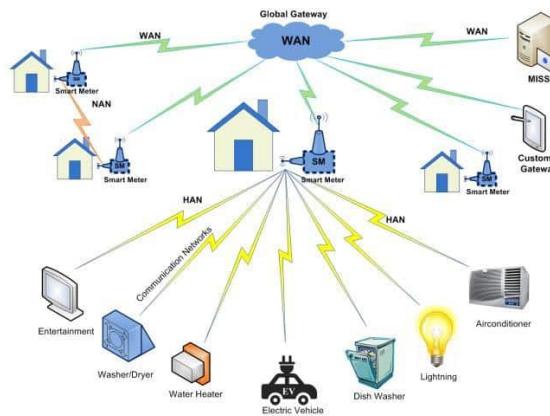


Image 21: SHAN
Reference:<https://networkencyclopedia.com/home-area-network-han/>

Advantages of SHAN

Accessibility:

This is a better way which gives the better accessibility for all the devices in the network for accessing Internet connection.

Management:

The resources on this network can be managed and controlled by this easy manner and data usage also can be managed.

Security:

It enhances the home network security and reliability. Internet network also password protected. It can support MAC Address filtering. So Internet can be accessed by authorised peoples only.

Resources sharing:

Resources on the network can be shared over the network. such as files, folders, printers, faxes etc..

Multi User:

Multiple users can access the network resources such as the Internet, shared devices, files etc simultaneously.

Life Style:

It makes the quality of life and home with digital communication by its style.

Disadvantages of SHAN**Lack of Wifi Password:**

If the wifi password is easily guessed by others then anybody within the range can steal Internet access and resources on the network.

Wifi-Microwaves:

Wireless devices use the microwave as a medium for communication. This microwave signals will specially affect brains. It is not good for health.

Expensive:

The devices which are used for communication should be capable of accessing the Internet which is expensive. etc... smart TV, laptops, smart phones...

Internet slow:

When multiple people access the Internet with the same share point then Internet speed will be shared to all users with equivalent speed. If one person is downloading a large file from the Internet then it will slow down the speed for all other uses.

PAN(Personal Area Network)

- Personal Area Network is a network arranged within an individual person, typically within a range of 10 meters.
- Personal Area Network is used for connecting the computer devices of personal use is known as Personal Area Network.
- Personal computer devices that are used to develop the personal area network are the laptop, mobile phones, media player and play stations.
- Personal Area Network covers an area of 30 feet.



Image 22: PAN

Reference: <https://www.javatpoint.com/types-of-computer-network>

There are two types of Personal Area Network:

Computer Network Types

- Wired Personal Area Network
- Wireless Personal Area Network

Wireless Personal Area Network:

Wireless Personal Area Network is developed by simply using wireless technologies such as WiFi, Bluetooth. It is a low range network.

Wired Personal Area Network:

Wired Personal Area Network is created by using the USB.

Advantages of personal area network:

- As PANs are for personal use, so benefits are more easily understandable than LAN,WAN,MAN.
- In PAN no extra space is required.
- No need for extra cable and wire.
- Easy to connect to many devices at a time.
- Affordable Cost.
- PAN is easy to use.
- It is very reliable.
- This Network is fully Secure.
- We can use it in office meetings.
- It is used in TV remotes, AC remotes etc.
- Data can Synchronize between different devices.
- Portable

Disadvantages of personal area network:

- Its range is less.
- Its interference is with radio signals.
- Transfer of data is slow.
- It creates Health problems.
- Cost is high in terms of communication devices.
- Infrared signals travel only in a straight line

Internet and Intranet etc.

Internet

The Internet is a global network of millions of private, public, academic, business, and government networks worldwide connected with each other over the network to share massive amounts of information, resources and services.

- It is a public network therefore anyone can access the internet.
- The Internet consists of a network of computers that anyone can access.
- Many intranets together make up the internet.
- There is no limit to the number of users who can use the internet at any given time
- The information available on the internet is gathered from different sources. Anyone can easily access any data on the internet.

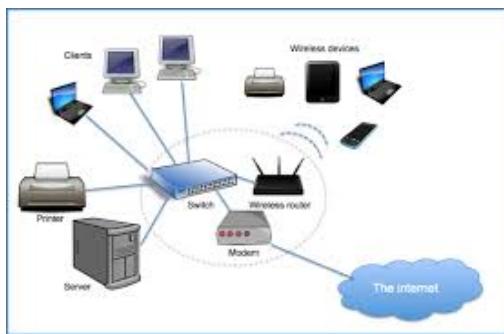


Image 23:Internet
Reference:<https://www.shutterstock.com/search/intranet>

Advantages:

- huge amounts of information can be accessed almost anywhere
- can help with disabilities to be more independent
- improved communication

Disadvantages:

- increased problems due to hacking and viruses
- paedophiles look at the children on the internet
- addiction to gambling.

Intranet

The term "Intranet" basically stands for the network of a specific organization or the private network of an organization. It may be used for organizations or networks that do not want their information to be able to be accessed by outside sources, and is especially important for organizations that require a high amount of secrecy - such as a server that holds military secrets or a database for the CIA. It has a firewall surrounding the system to avoid the unauthorized user from accessing the network. Only authorized users have permission to access the network.

- It is a private network therefore anyone can't access intranet.
- An intranet is a smaller network of computers that allows access to a particular group of users.
- One can access the intranet from the internet. However, there are restrictions on the number of users.
- Only a specific few users can access the intranet.
- There are limitations on the volume of traffic at any given time.
- Intranet contains a specific kind of information only.

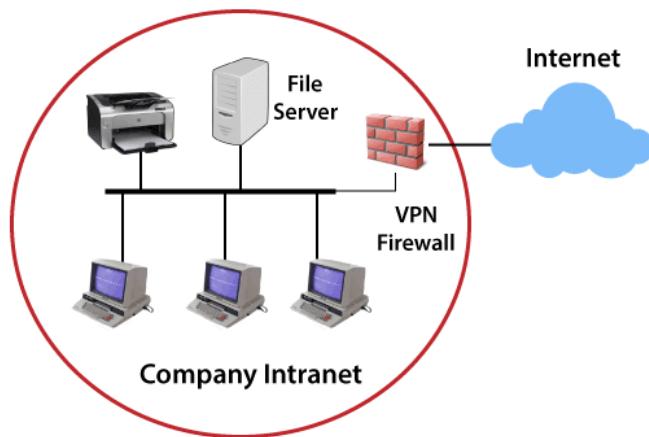


Image 24: Intranet
Reference:<https://www.javatpoint.com/intranet>

Advantages:

- ideal for school because they can be used to prevent students from accessing unsafe websites the email system is more secure
- only information relevant to the organisation can be accessed- saves time

Disadvantages:

-
- less information
 - can't go on websites needed

Difference between Internet and Intranet

Internet

- The Internet is a wide network of computers and is open for all.
- The Internet itself contains a large number of intranets.
- The number of users who use the internet is Unlimited.
- The Visitors traffic is unlimited.
- The Internet contains different sources of information and is available for all.

Intranet

- Intranet is also a network of computers designed for a specific group of users.
- Intranet can be accessed from the Internet but with restrictions.
- The number of users is limited.
- The traffic allowed is also limited.
- Intranet contains only specific group information.

Therefore the Internet is an open, public space, while an intranet is designed to be a private space. An intranet may be accessible from the Internet, but it is protected by a password and accessible only to authorized users.

Internet	Intranet
The term ' Internet ' comes from the phrase International Network .	The term ' Intranet ' comes from the phrase Internal Restricted Access Network .
The internet is used to share data globally .	Intranets are used to share data locally and privately .
The internet is used to provide information that is relevant to a wide range of people.	Intranets are used to provide information which is relevant to a single company or organisation .
The internet can be accessed from anywhere as long as you have an internet connection.	Intranets can only be accessed from within the company or organisation that owns it.

Image 25:Difference between Internet and Intranet
Reference:<https://techdifferences.com/difference-between-internet-and-intranet.html>

Extranet

An extranet is a private network that only authorized users can access. These authorized users may include business partners, suppliers, and even some customers. They can use the extranet to exchange information with each other without having to enter the host company's main network.

An extranet is like a secure file room located somewhere off the company premises. Only those issued a key can enter and browse through the filing cabinets.

- An extranet is a communication network based on the internet protocol such as Transmission Control protocol and internet protocol.
- It is used for information sharing.
- The access to the extranet is restricted to only those users who have login credentials.

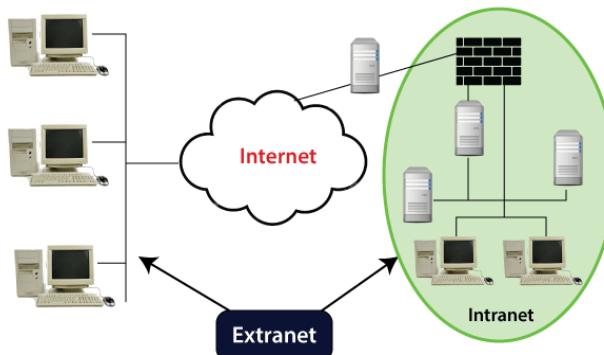


Image 26:Extranet
Reference: <https://invidgroup.com/what-is-an-extranet/>

Advantages of an Extranet

- Communicate and collaborate more effectively with their stakeholders and clients via a secure network.
- Integrate supply chains like consolidated processes.
- Reduce costs by making relevant documentation like manuals available online to all the relevant parties.
- Improve their business relationships through the collaboration within the extranet.
- Simplify their internal processes by using a single interface.
- Secure company communication in a controlled environment.

-
- Work flexibly as the extranet allows people to work remotely and be more mobile. More so, people are given 24/7 access to the core business information irrespective of their location.

Disadvantages of an Extranet

- If hosted internally instead of via an active server page, the implementation of an extranet within an organization tends to be quite expensive.
- Extranets can reduce personal contact (face-to-face meetings) with customers and business partners. This could cause a lack of connections made between people and a company, which hurts the business when it comes to the loyalty of its business partners and customers.
- The security of extranets can be a big concern because it deals with valuable information. Systems, therefore, need to be carefully controlled in order to avoid hacks or misuse of data.

Uses and benefits of Network

Networking benefits

The benefits of networking on computers and other devices include low costs and higher productivity. Thanks to networks, resources can be shared, which reduces data duplication and corruption.

Fewer peripherals are needed.

Every computer on the network does not need its printer, scanner, or backup device. It is possible to configure several printers in a central location and share them among network users. All network users send print jobs to a central print server that manages print requests. The print server can distribute print jobs among the various printers, or it can queue jobs that require a particular printer.

Greater communication capabilities

Networks offer various collaboration tools that can be used to establish communications between network users. Online collaboration tools include email, forums and chat, voice and video, and instant messaging. With these tools, users can communicate with friends, family, and colleagues.

Duplication and file corruption are avoided

A server manages network resources. The servers store the data and share it with the users of a network. Confidential or essential data can be protected and shared with users who have permission to access such data. Document tracking software can be used to prevent users from overwriting or modifying files that other users are accessing at the same time.

Lower cost in license acquisition

Acquiring application licenses can be expensive for individual computers. Many software providers offer site licenses for networks, which can significantly reduce the cost of the software. The site license allows a group of people or an entire organization to use the application for a single fee.

Centralized administration

Centralized administration reduces the number of people needed to manage devices and data on the network, allowing the company to save time and money.

Individual users of the network do not need to manage their data and devices. An administrator can control the data, devices, and permissions of network users. Creating backup copies of the data is more comfortable because of the data stored in a central location.

Resources are conserved

It is possible to distribute data processing among many computers to prevent a computer from being overloaded with processing tasks.

Uses of Networking

Information and Resource Sharing – Computer networks allow organizations having units which are placed apart from each other, to share information in a very effective manner. Programs and software in any computer can be accessed by other computers linked to the network. It also allows sharing of hardware equipment, like printers and scanners among varied users.

Retrieving Remote Information – Through computer networks, users can retrieve remote information on a variety of topics. The information is stored in remote databases to which the user gains access through information systems like the World Wide Web.

Speedy Interpersonal Communication – Computer networks have increased the speed and volume of communication like never before. Electronic Mail (email) is extensively used for sending texts, documents, images, and videos across the globe. Online communications have increased by manifold times through social networking services.

E-Commerce – Computer networks have paved the way for a variety of business and commercial transactions online, popularly called e-commerce. Users and organizations can pool funds, buy or sell items, pay bills, manage bank accounts, pay taxes, transfer funds and handle investments electronically.

Highly Reliable Systems – Computer networks allow systems to be distributed in nature, by the virtue of which data is stored in multiple sources. This makes the system highly reliable. If a failure occurs in one source, then the system will still continue to function and data will still be available from the other sources.

Cost-Effective Systems – Computer networks have reduced the cost of establishment of computer systems in organizations. Previously, it was imperative for organizations to set up expensive mainframes for computation and storage. With the advent of networks, it is sufficient to set up interconnected personal computers (PCs) for the same purpose.

VoIP – VoIP or Voice over Internet protocol has revolutionized telecommunication systems. Through this, telephone calls are made digitally using Internet Protocols instead of the regular analog phone lines.



Image 27:Uses of Computer Network
Reference: <https://www.ccsipro.com/blog/uses-of-computer-network/>

Server-client based network

- A Computer networking model where one or more powerful computers (servers) provide the different computer network services and all other users of the computer network (clients) access those services to perform the user's tasks is known as client/server computer networking model.
- In such networks, there exists a central controller called server. A server is a specialized computer that controls the network resources and provides services to other computers in the network.
- All other computers in the network are called clients. A client computer receives the requested services from a server.
- A server performs all the major operations like security and network management.
- All the clients communicate with each other via centralized server
- If client 1 wants to send data to client 2, it first sends a request to the server to seek permission for it. The server then sends a signal to client 1 allowing it to initiate the communication.
- A server is also responsible for managing all the network resources such as files, directories, applications & shared devices like printers etc.
- If any of the clients wants to access these services, it first seeks permission from the server by sending a request.
- Most Local Area Networks are based on client server relationships.

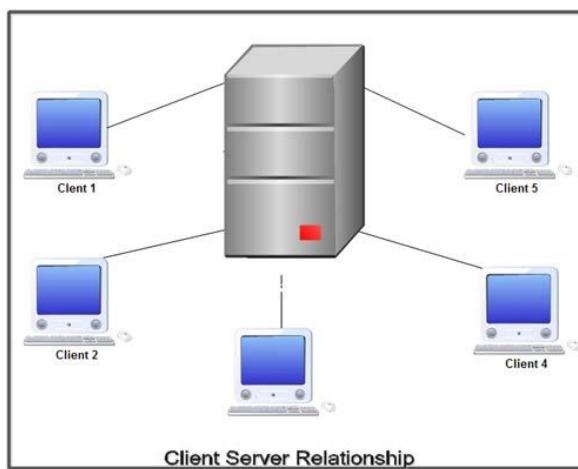


Image 28: Client-server Relationship

Reference: <http://ecomputernotes.com/computernetworkingnotes/computer-network/explain-clientserver-networking-model>

The design of applications for a distributed computing environment required that they effectively be divided into two parts: client (front end) and server (back end). The network model on which they were implemented mirrored this client-server model with a user's PC (the client) typically acting as the requesting machine and a more powerful server machine to which it was connected via either a LAN or a WAN acting as the supplying machine. It requires a special networking operating system. It provides user level security and it is more expensive.

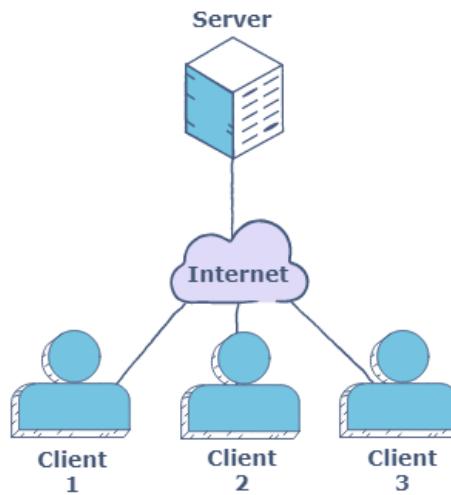


Image 29: Client-server Network Model
Reference: <https://www.educative.io/edpresso/what-are-p2p-and-clientserver-networks>

Advantages of Client-Server Architecture

Organizations often seek opportunities to maintain services and quality competition to sustain its market position with the help of technologies. Deployment of client-server computing in an organization will effectively increase its productivity through the usage of cost-effective user interface, enhanced data storage, vast connectivity and reliable application services

Improved Data Sharing:

Data is retained by usual business processes and manipulated on a server is available for designated users (clients) over an authorized access.

Integration of Services:

Every client is given the opportunity to access corporate information via desktop interface eliminating the necessity to log into a terminal mode or processor.

Shared Resources Amongst Different Platforms:

Application used for client-server model is built regardless of the hardware platform or technical background of the entitled software (operating system software) providing an open computing environment, enforcing users to obtain the services of clients and servers (database, application and communication services)

Data Processing Capability Despite the Location:

Client-server users can directly log into a system despite the location or technology of the processors.

Easy Maintenance:

Client-server architecture is a distributed model representing dispersed responsibilities among independent computers integrated across a network. Therefore, it's easy to replace, repair, upgrade and relocate a server while the client remains unaffected. This unaware change is called Encapsulation.

Security:

Servers have better control access and resources to ensure that only authorized clients can access or manipulate data and server updates are administered effectively.

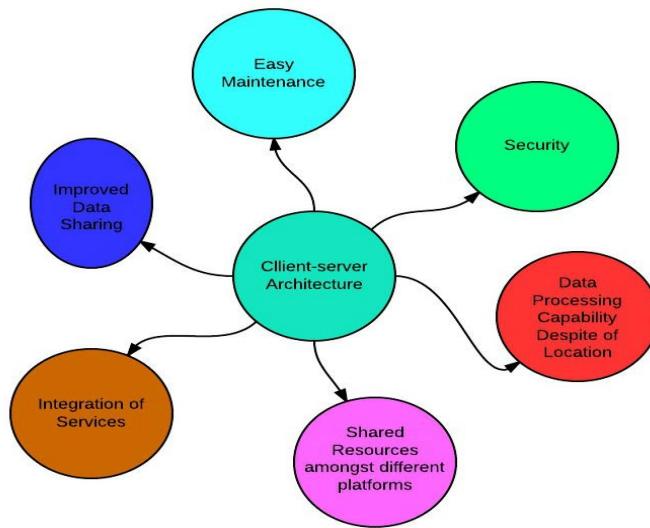


Image 30: Advantages of Client-Server

Reference:<https://sites.google.com/site/clientserverarchitecture/advantages-of-client-server-architecture>

Disadvantages of Client-Server Architecture

Overloaded Servers:

When there are frequent simultaneous client requests, servers severely get overloaded, forming traffic congestion.

Impact of Centralized Architecture:

Since it is centralized, if a critical server fails, client requests are not accomplished. Therefore, client-servers lack the robustness of a good network.

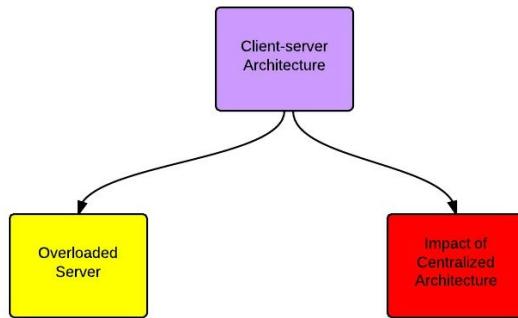


Image 31: Disadvantages of Client-Server

Reference:<https://sites.google.com/site/clientserverarchitecture/advantages-of-client-server-architecture>

peer to peer networks

- In the peer to peer computer network model we simply use the same Workgroup for all the computers and a unique name for each computer in a computer network.
- There is no master or controller or central server in this computer network and computers join hands to share files, printers and Internet access.
- It is practical for workgroups of a dozen or less computers making it common environments, where each PC acts as an independent workstation and maintains its own security that stores data on its own disk but which can share it with all other PCs on the network.
- Software for peer-to-peer network is included with most modern desktop operating systems such as Windows and Mac OS.
- Peer to peer relationship is suitable for small networks having less than 10 computers on a single LAN.
- In a peer to peer network each computer can not act as both a server and a client.

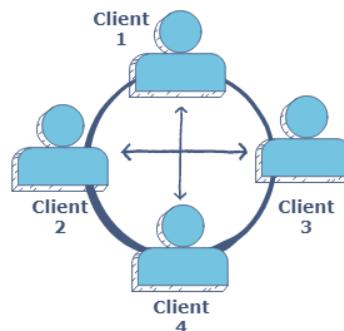


Image 32:Peer-to-Peer

Reference:<https://sites.google.com/site/clientserverarchitecture/advantages-of-client-server-architecture>

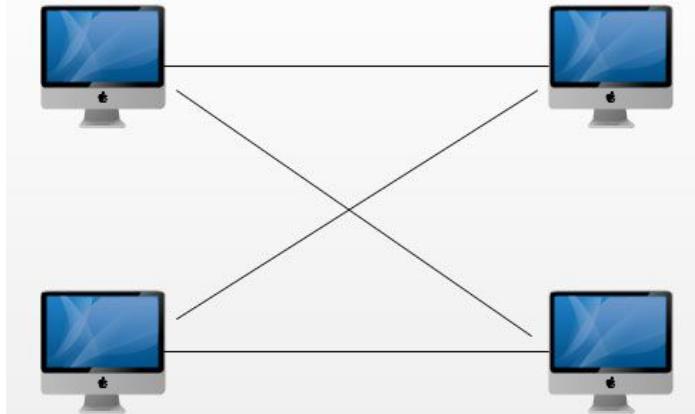


Image 33: Workgroup

Reference:<http://ecomputernotes.com/computernetworkingnotes/computer-network/explain-peer-to-peer-networking-model>

Advantages of Peer to Peer Networks

1. Such networks are easy to set up and maintain as each computer manages itself.
2. It eliminates extra cost required in setting up the server.
3. Since each device is master of its own, they are not dependent on other computers for their operations.

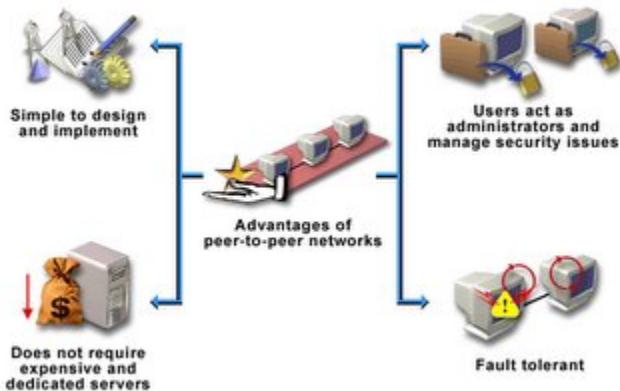


Image 34: Advantages of Peer to peer Network

Reference: <http://mdalikhaja.blogspot.com/2006/04/advantages-of-peer-to-peer-networks.html>

Disadvantages of Peer to Peer Networks

1. In a peer-to-peer network, the absence of a centralized server makes it difficult to backup data as data is located on different workstations.
2. Security is weak as each system manages itself only.
3. There is no central point of data storage for file archiving.



Image 35: Disadvantages of Peer to peer Network
Reference:<https://eternalsunshineoftheismind.wordpress.com/2013/02/18/advantages-and-disadvantages-of-p2p/>

Difference between Client-server and Peer to Peer Networks

Both peer-to-peer and client-server networks connect computers so that they can share resources from one computer to others such as files, videos, and pictures.

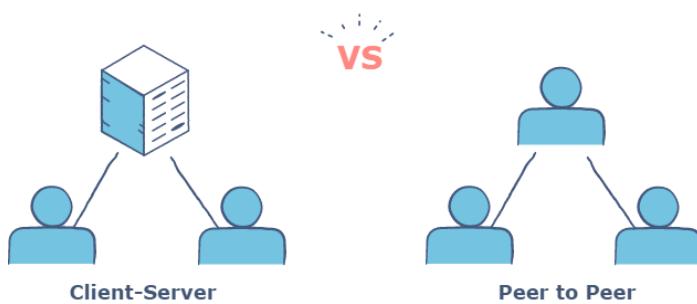


Image 36:Client-server and Peer to Peer Networks
Reference:<https://www.educative.io/edpresso/what-are-p2p-and-clientserver-networks>

SNo.	Client Server Model	Peer to Peer (P2P) Model
1	It requires two types of machines, Server (high end processors, large memory and secondary storage) and client which are simpler machines, which can access remote data.	In P2P network all the devices have same power.
2	Specialized Network operating systems is required to manage usage of the model.	No specialized operating systems is required to manage the network.
3	It offers centralized control to manage the network through servers like, application , database servers etc.	It offers decentralized control as all the devices manage the resources.
4	Best model for large networks	Best model for small networks.
5	It require costly hardware devices so cost is high	Cost depends on the type of machine used by users
6	Offers better security model.	Peer to peer network is less secure.
7	Network administrators are required to manage the system.	Do not require network administrator to manage the network.

Image 37: Difference between Client-server and Peer to Peer Networks

Reference: <http://mynetgyan.com/chapter/8/38>

Network Interface Card

What is a Network Interface Card?

Network Interface Card is a hardware device that is installed on the computer so that it can be connected to the internet. It is also called Ethernet Card or Network Adapter. Every NIC has a 48-bit unique serial number called a MAC address which is stored in ROM carried on the card. Every computer must have at least one NIC if it wants to connect to the internet.

Purpose

- NIC allows both wired and wireless communications.
- NIC allows communications between computers connected via local area network (LAN) as well as communications over large-scale network through Internet Protocol (IP).
- NIC is both a physical layer and a data link layer device, i.e. it provides the necessary hardware circuitry so that the physical layer processes and some data link layer processes can run on it.

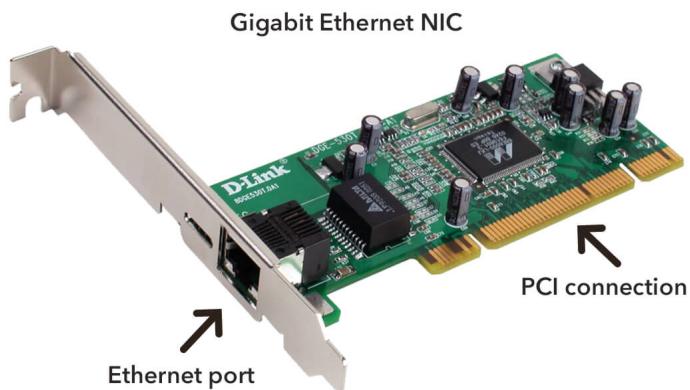


Image 38: NIC
Reference: <https://techterms.com/definition/nic>

Components of NIC

The main components of the Network Interface Card are as follows

- An external Memory is used to store the data temporarily and uses the stored data whenever required while processing the communication.

- Connectors are used to make the physical link between cables and plugin with the board, this type of connection is especially seen in Ethernet type of NIC cables.
- A Processor converts the data message into a signal format for communication to take place easily.
- Different types of standard Buses are plugged into Buses Connector slots, based on the compatibility of the operation process buses are chosen.
- Jumpers or Dual in package switches are used to control the communication operation, which is either by turning on or turning off the switch.
- MAC address which is a unique identity address is given to network interface cards where ethernet packets are communicated with the computer. MAC address is also known as a physical network address.
- A router is an NIC device that is used to connect wirelessly to the internet.

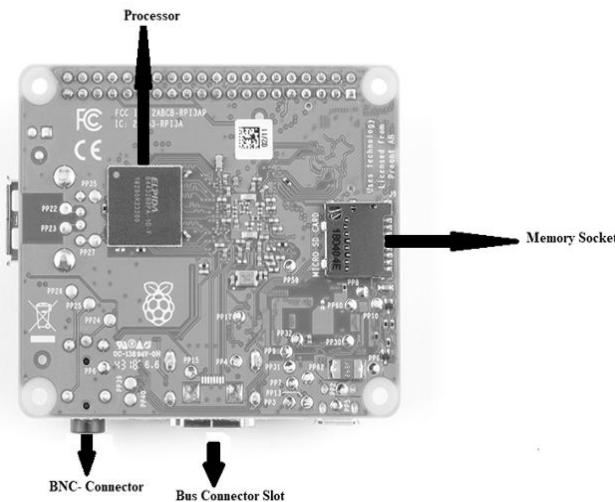


Image391:Components of NIC
Reference: <https://www.elprocus.com/network-interface-card-nic/>

Types of NIC Cards

- Wired
- Wireless
- USB

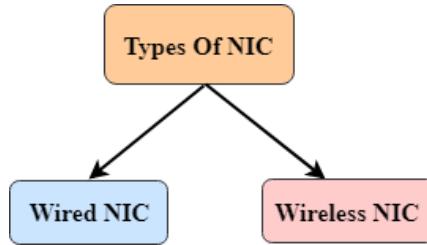


Image 40: Types of NIC
Reference: <https://www.javatpoint.com/computer-network-components>

Wired:

These NIC have input jacks made of cables(Ethernet Cable). The motherboard has a slot for the network cards where they are inserted. The most widely used LAN technology is Ethernet. Ethernet-based NIC is available in hardware shops. The speed of Ethernet-based NIC can be 10/100/1000 Mbps.

Example: TP-LINK TG-3468 Gigabit PCI Express Network Adapter



Image 41: Wired
Reference: <https://afteracademy.com/blog/what-is-a-network-interface-card>

Wireless:

Wireless network cards are inserted into the motherboard but no network cables are required to connect the computer to the internet. These NICs are designed for Wi-Fi connections.

Example: Intel 3160 Dual-Band Wireless Adapter



Image 42: Wireless

Reference: <https://afteracademy.com/blog/what-is-a-network-interface-card>

USB:

These are NICs that provide network connection over the device plugged in the USB port. For Example, if you are a gamer and you are tired of watching helplessly that your gaming character dies due to Wi-Fi-induced lags. So the USB-ethernet adapter can be a solution to your problem.

Example: TP-Link TL-UE300 USB 3.0 to RJ45 Gigabit Ethernet Network Adapter



Image 43: USB

Reference: <https://afteracademy.com/blog/what-is-a-network-interface-card>

Advantages of NIC

- The communication speed using the Internet is high usually in Gigabytes
- Highly reliable connection
- Many peripheral devices can be connected using many ports of NIC cards.
- Bulk data can be shared among many users.

Disadvantages of NIC

- Inconvenient in case of wired cable NIC, as it is not portable like a wireless router

-
- The configuration should be proper for better communication.
 - Data is unsecured.

Transmission Media and Topologies Media Type

What is Transmission Media?

A communication channel that is used to carry the data from the transmitter to the receiver through the electromagnetic signals.

The main function of this is to carry the data in the bits form through the Local Area Network (LAN). In data communication, it works like a physical path between the sender & the receiver.

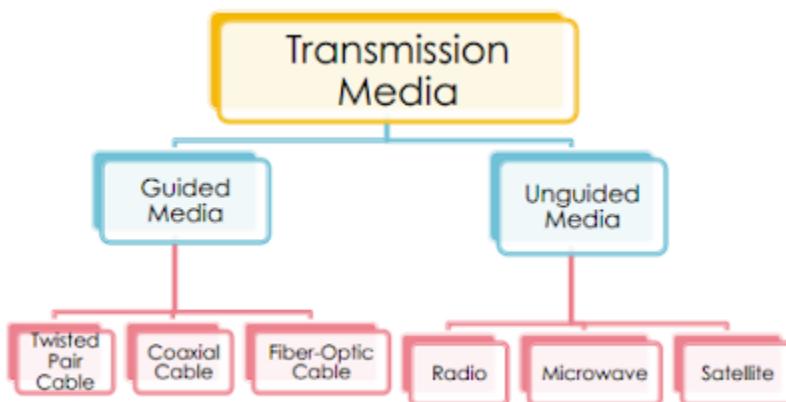


Image 44: Transmission Media
Reference:<https://mangoguys.wordpress.com/2013/12/03/wireless-transmission-media/>

Types of transmission media

1. Physical transmission media/Guided media/Wired
 - Twisted-Pair Cable, Coaxial Cable, Fiber-Optic Cable
2. Wireless transmission media/Unguided media/Wireless
 - Infrared, Broadcast Radio, Cellular Radio, Microwave, communications satellite

Bounded or Guided Media

Coaxial Cables:

These are made up of copper. A plastic layer provides insulation between the copper wire and metal shield. Metal shield helps to block any outside interference.

-
- Transmission rate is 10 Megabits per second (Mbps).
 - It is less expensive than Fiber Optic.
 - Mostly used for long distance transmission.
 - Provide high quality data transmission without distortion or loss of signal.
 - It can be classified in two categories

UTP (Unshielded Twisted Pair Cable)

- It has a maximum range of 100 meters (328 feet).
- It consists of 2 or 4 twisted wire pairs.
- Widely used in LANs.

STP (Shielded Twisted Pair Cable)

- Same as UTP but it is covered with a shield for resistance.
- It is more reliable and faster than UTP.
- It covers a long distance.
- Normally used as a back bone cable.

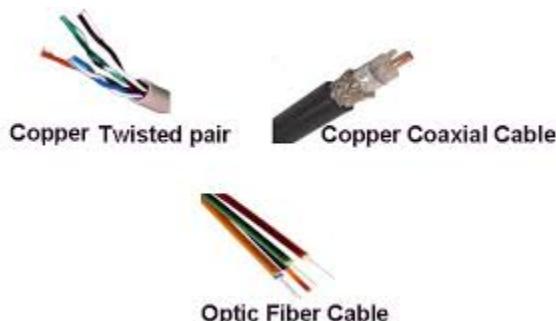


Image 45: Guided media
Reference: <http://computernetworkingsimplified.in/physical-layer/overview-guided-unguided-media/>

Unbounded or UnGuided Media

Infrared:

- Infrared signals can be used for short range communication in a closed area
- using line-of-sight propagation.

Microwaves:

- Microwaves are used for unicast communication such as cellular
- telephones, satellite networks, and wireless LANs.

- Higher frequency ranges cannot penetrate walls.
- Use directional antennas - point to point line of sight communications.
-

Radio Waves:

- Radio waves are used for multicast communications, such as radio and television, and paging systems. They can penetrate through walls.
- Highly regulated. Use omni directional antennas

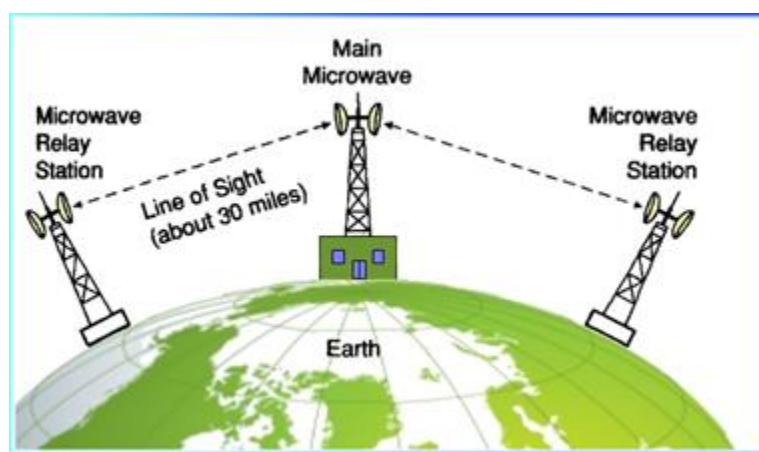
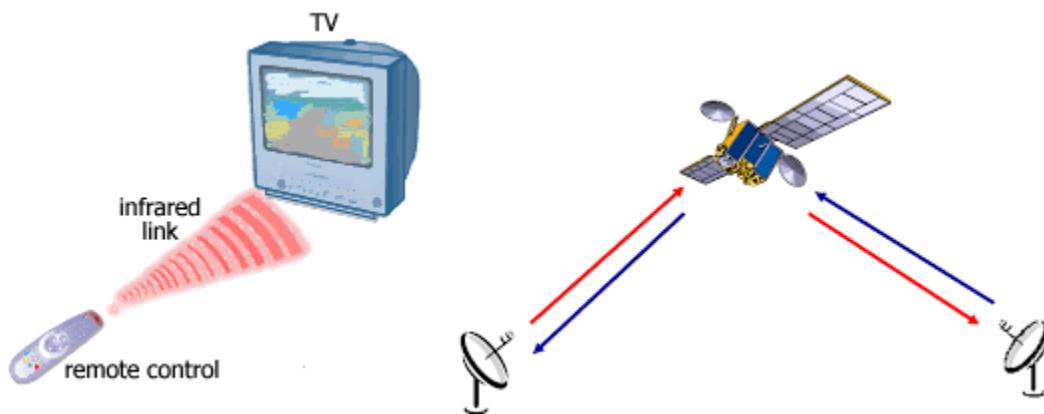


Image 46: Unguided media
Reference: <http://www.datacom2u.com/ENWirelessMedia.php>

Crimping tools and Color standards for Straight crimping and Cross crimping

Crimping Tools

A crimping tool is a device used to conjoin two pieces of metal by deforming one or both of them in a way that causes them to hold each other. The result of the tool's work is called a crimp.



Image 47: Crimping Tool
Reference:<https://www.computerhope.com/jargon/c/crimp.htm>

Ethernet Cable Color

- A straight-thru is used as a patch cord in Ethernet connections.
- A crossover is used to connect two Ethernet devices without a hub or for connecting two hubs.
- A crossover has one end with the Orange set of wires switched with the Green set.

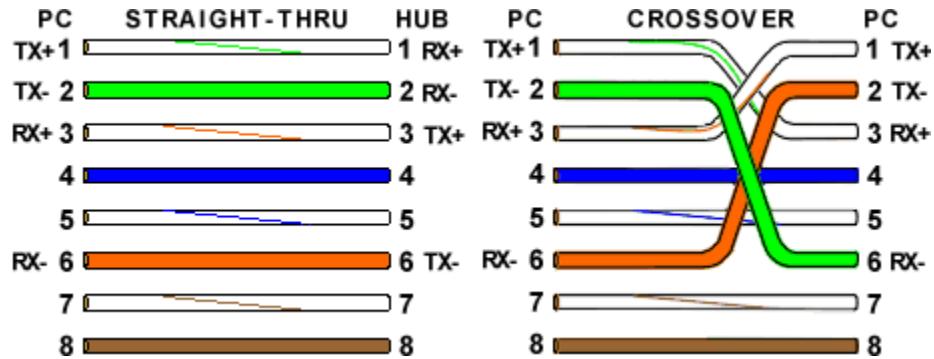


Image 48: Cable Color
Reference: <https://incentre.net/ethernet-cable-color-coding-diagram/>

Ethernet Cable Color Coding Diagram for:

- Category-5 cables
- Category-5E cables
- Category-6 cables
- Category-6E cables

The information listed here is to assist network administrators in the color coding of Ethernet cables. Please be aware that modifying Ethernet cables improperly may cause loss of network connectivity. Use this information at your own risk, and ensure all connectors and cables are modified in accordance with standards. The Internet Centre and its affiliates cannot be held liable for the use of this information in whole or in part.

T-568A Straight-Through Ethernet Cable

STRAIGHT THROUGH Ethernet cables are the standard cable used for almost all purposes, and are often called "patch cables". It is highly recommended you duplicate the color order as shown on the left. Note how the green pair is not side-by-side as are all the other pairs. This configuration allows for longer wire runs.

T-568A Straight-Through Ethernet Cable

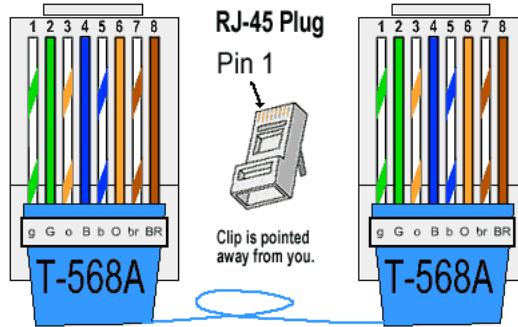


Image 49: T-568A Straight-through Cable

Reference: <https://incentre.net/ethernet-cable-color-coding-diagram/>

The TIA/EIA 568-A standard which was ratified in 1995, was replaced by the TIA/EIA 568-B standard in 2002 and has been updated since. Both standards define the T-568A and T-568B pin-outs for using Unshielded Twisted Pair cable and RJ-45 connectors for Ethernet connectivity. The standards and pin-out specification appear to be related and interchangeable, but are not the same and should not be used interchangeably.

T-568B Straight-Through Ethernet Cable

T-568B Straight-Through Ethernet Cable

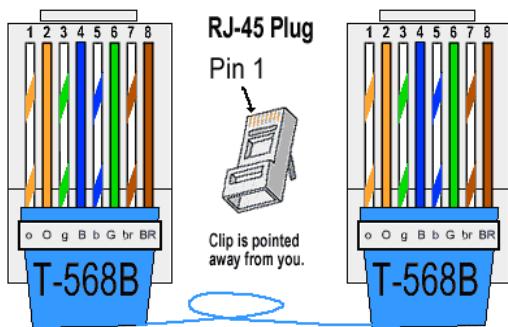


Image 50: T-568B Straight-through Cable

Reference: <https://incentre.net/ethernet-cable-color-coding-diagram/>

Both the T-568A and the T-568B standard Straight-Through cables are used most often as patch cords for your Ethernet connections. If you require a cable to connect two Ethernet devices

directly together without a hub or when you connect two hubs together, you will need to use a Crossover cable instead.

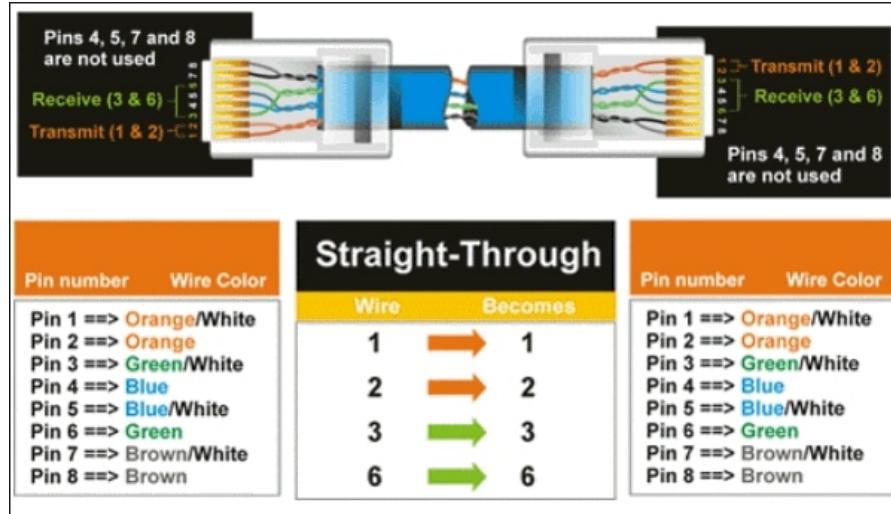


Image 51: Straight Through cable Color

Reference: <https://www.networkkings.org/color-coding-of-straight-and-crossover-cable/>

RJ-45 Crossover Ethernet Cable

CROSSOVER CABLES - The purpose of a Crossover Ethernet cable is to directly connect one computer to another computer (or device) without going through a router, switch or hub.

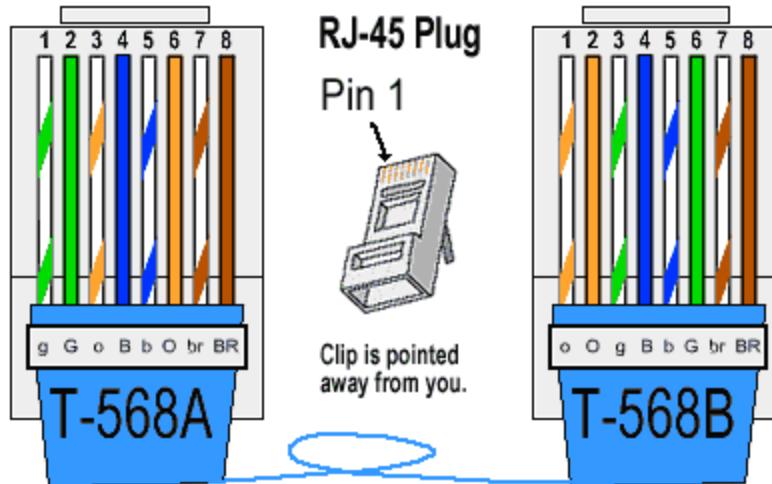


Image 52: RJ-45 crossover cable

Reference: <https://www.networkkings.org/color-coding-of-straight-and-crossover-cable/>

A good way of remembering how to wire a Crossover Ethernet cable is to wire one end using the T-568A standard and the other end using the T-568B standard. Another way of remembering the color coding is to simply switch the Green set of wires in place with the Orange set of wires. Specifically, switch the solid Green (G) with the solid Orange, and switch the green/white with the orange/white.

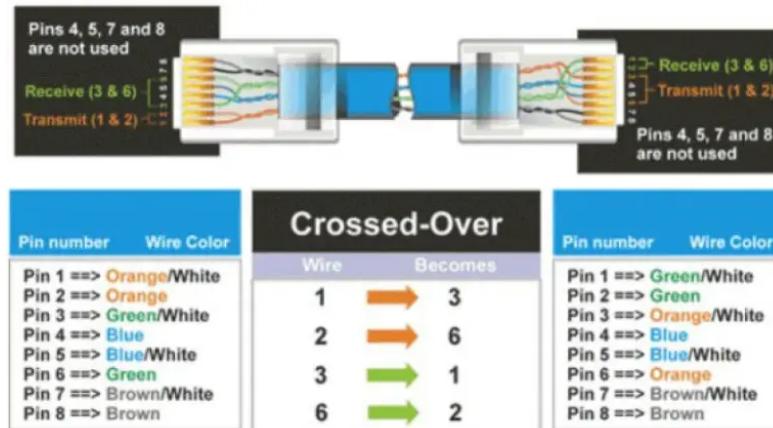


Image 53: RJ-45 crossover cable Color
Reference:<https://www.networkkings.org/color-coding-of-straight-and-crossover-cable/>

Ethernet Cable Instructions

- Pull the cable off the reel to the desired length and cut. If you are pulling cables through holes, it's easier to attach the RJ-45 plugs after the cable is pulled. The total length of wire segments between a PC and a hub or between two PC's cannot exceed 100 Meters (328 feet) for 100BASE-TX and 300 Meters for 10BASE-T.
- Start on one end and strip the cable jacket off (about 1") using a stripper or a knife. Be extra careful not to nick the wires, otherwise you will need to start over.
- Spread, untwist the pairs, and arrange the wires in the order of the desired cable end. Flatten the end between your thumb and forefinger. Trim the ends of the wires so they are even with one another, leaving only 1/2" in wire length. If it is longer than 1/2" it will be out-of-spec and susceptible to crosstalk. Flatten and insure there are no spaces between wires.
- Hold the RJ-45 plug with the clip facing down or away from you. Push the wires firmly into the plug. Inspect each wire is flat even at the front of the plug. Check the order of the wires. Double check again. Check that the jacket is fitted right against the stop of the plug. Carefully hold the wire and firmly crimp the RJ-45 with the crimper.

- Check the color orientation, check that the crimped connection is not about to come apart, and check to see if the wires are flat against the front of the plug. If even one of these are incorrect, you will have to start over. Test the Ethernet cable.



Image 54: Ethernet Cable Instructions

Reference: https://www.tutorialspoint.com/computer_fundamentals/computer_networking.htm

Understand and configure server environment and backup services

In this section, we will read about:

- Server
- client
- node
- segment
- backbone
- host
- Analog and Digital transmission
- STP cable
- UTP cable
- Coaxial cable
- Fiber cable
- Base band and Broadband transmission
- Cables and Connectors
- Network Cable Crimping and troubleshooting
- Physical and logical topologies
- Bus topology
- Star topology,
- Ring topology
- Mesh topology
- Asynchronous Transmission
- Synchronous Transmission

Server

What is Server?

- A **server** is a computer that provides data to other computers. It may serve data to systems on a local area network (LAN) or a wide area network (WAN) over the Internet. Many types of **servers** exist, including web **servers**, mail **servers**, and file **servers**. Each type runs software specific to the purpose of the **server**.
- An individual system can provide resources and use them from another system at the same time. This means that a device could be both a server and a client at the same time.
- Some of the first servers were mainframe computers or minicomputers. Minicomputers were much smaller than mainframe computers, hence the name. However, as technology progressed, they ended up becoming much larger than desktop computers, which made the term microcomputer somewhat farcical.
- Initially, such servers were connected to clients known as terminals that did not do any actual computing. These terminals, referred to as dumb terminals, existed simply to accept input via a keyboard or card reader and to return the results of any computations to a display screen or printer. The actual computing was done on the server.
- Later, servers were often single, powerful computers connected over a network to a set of less-powerful client computers. This network architecture is often referred to as the client-server model, in which both the client computer and the server possess computing power, but certain tasks are delegated to servers. In previous computing models, such as the mainframe-terminal model, the mainframe did act as a server even though it wasn't referred to by that name.



Image 1: Server -What is Server?

Reference: <https://qph.fs.quoracdn.net/main-qimg-c2a31b87978f3f6606f86902941949b4.webp>

Characteristics and capabilities of the server

In order to operate in the unique network environment where many computers and hardware/software systems are dependent on just one or several server computers, a server often has special characteristics and capabilities, including:

- The ability to update hardware and software without a restart or reboot.
- Advanced backup capability for frequent backup of critical data.
- Advanced networking performance.
- Automatic (invisible to the user) data transfer between devices.
- High security for resources, data and memory protection.

Server computers often have special operating systems not usually found on personal computers. Some operating systems are available in both server and desktop versions and use similar interfaces.

However, an increase in the reliability of both server hardware and operating systems has blurred the distinctions between desktop and server operating systems.



Image 2: Characteristics and capabilities of the Server

Reference: https://encrypted-tbn0.gstatic.com/images?q=tbn%3AANd9GcRe4Bi-i0DhXP0YbCDPc9n_SuTXfYecSwhibvl8oJ-ywWfqBOj-&usqp=CAU

How a Server works?

To function as a server, a device must be configured to listen to requests from clients on a network connection. This functionality can exist as part of the operating system as an installed application, role, or a combination of the two.

For example, Microsoft's Windows Server operating system provides the functionality to listen to and respond to client requests. Additionally installed roles or services increase which kinds of client requests the server can respond to. In another example, an Apache web server responds to Internet browser requests via an additional application, Apache, installed on top of an operating system.

When a client requires data or functionality from a server, it sends a request over the network. The server receives this request and responds with the appropriate information. This is the request and response model of client-server networking, also known as the call and response model.

A server will often perform numerous additional tasks as part of a single request and response, including verifying the identity of the requestor, ensuring that the client has permission to access the data or resources requested, and properly formatting or returning the required response in an expected way.

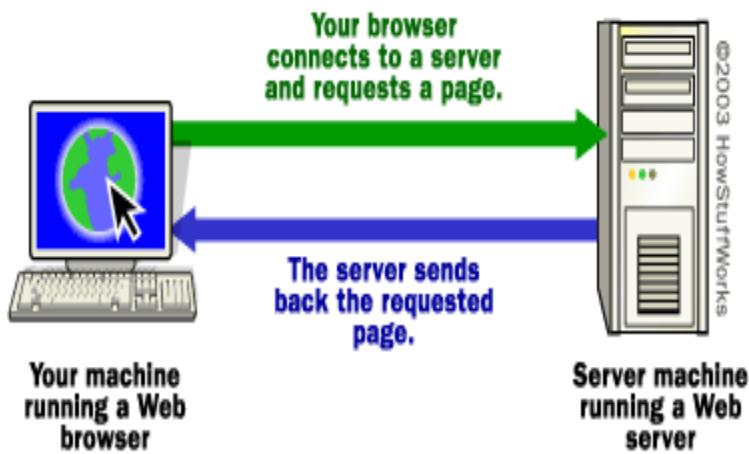


Image 3: How a Server Works?

Reference:<https://cdn.hswstatic.com/gif/webserver-basic-sm.gif>

Types of servers

There are many types of servers that all perform different functions. Many networks contain one or more of the common server types:

File servers

File servers store and distribute files. Multiple clients or users may share files stored on a server. In addition, centrally storing files offers easier backup or fault tolerance solutions than attempting to provide security and integrity for files on every device in an organization. File server hardware can be designed to maximize read and write speeds to improve performance.



Image 4: File Server
Reference:<https://www.computerhope.com/jargon/f/file-server.jpg>

Print servers

Print servers allow for the management and distribution of printing functionality. Rather than attaching a printer to every workstation, a single print server can respond to printing requests from numerous clients. Today, some larger and higher-end printers come with their own built-in print server, which removes the need for an additional computer-based print server. This internal print server also functions by responding to print requests from a client.



Image 5: Print Server

Reference : https://ic.pics.livejournal.com/cybatrones/84069556/324/324_original.gif

Application servers

Application servers run applications in lieu of client computers running applications locally. Application servers often run resource-intensive applications that are shared by a large number of users. Doing so removes the need for each client to have sufficient resources to run the applications. It also removes the need to install and maintain software on many machines as opposed to only one.



Image 6: Application Server

Reference : <https://cdn.educba.com/academy/wp-content/uploads/2019/04/What-is-Application-Server-1.jpg>

DNS servers

Domain Name System (DNS) servers are application servers that provide name resolution to client computers by converting names easily understood by humans into machine-readable IP addresses. The DNS system is a widely distributed database of names and other DNS servers, each of which can be used to request an otherwise unknown computer name. When a client needs the address of a system, it sends a DNS request with the name of the desired resource to a DNS server. The DNS server responds with the necessary IP address from its table of names.

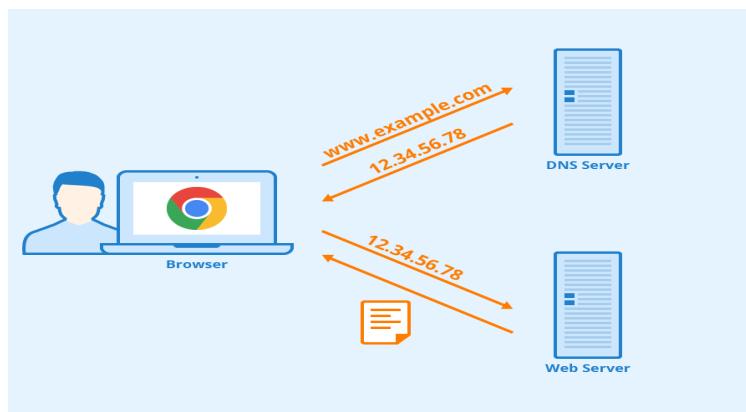


Image 7: DNS Server

Reference : <https://www.seobility.net/en/wiki/images/d/d0/DNS-Server.png>

Mail servers

Mail servers are a very common type of application server. Mail servers receive emails sent to a user and store them until requested by a client on behalf of said user. Having an email server allows for a single machine to be properly configured and attached to the network at all times. It is then ready to send and receive messages rather than requiring every client machine to have its own email subsystem continuously running.

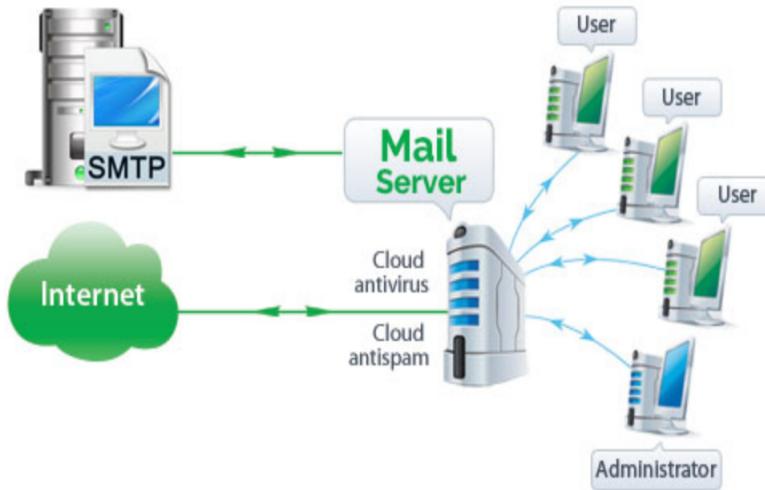


Image 8: Mail Server
Reference : https://miro.medium.com/max/968/1*dQZE1Ipbnhv7VGukbaxxg.png

Web servers

One of the most abundant types of servers in today's market is a web server. A web server is a special kind of application server that hosts programs and data requested by users across the Internet or an intranet. Web servers respond to requests from browsers running on client computers for web pages, or other web-based services. Common web servers include Apache web servers, Microsoft Internet Information Services (IIS) servers and Nginx servers.

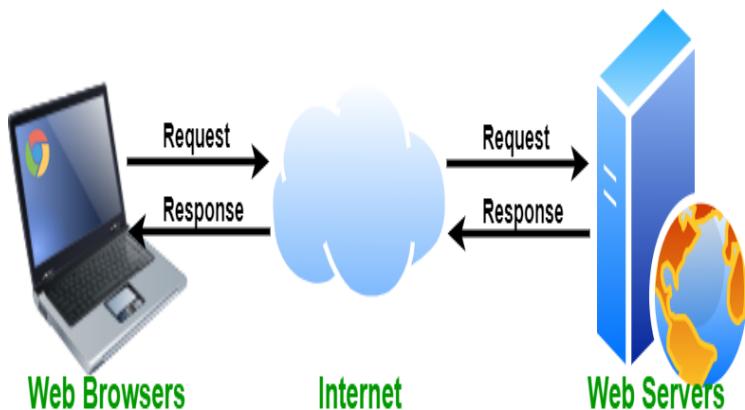


Image 9: Web Server
Reference : <https://media.geeksforgeeks.org/wp-content/uploads/20190927155217/webserver.png>

Database servers

The amount of data used by companies, users, and other services is staggering. Much of that data is stored in databases. Databases need to be accessible to multiple clients at any given time and can require extraordinary amounts of disk space. Both of these needs lend themselves well to locating such databases on servers. Database servers run database applications and respond to numerous requests from clients. Common database server applications include Oracle, Microsoft SQL Server, DB2, and Informix.

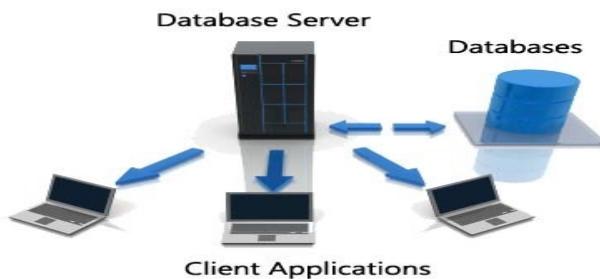


Image 10: Database Server

Reference : <https://3.imimg.com/data3/LQ/GC/MY-8728205/database-server-500x500.jpg>

Virtual servers

Virtual servers are taking the server world by storm. Unlike traditional servers that are installed as an operating system on machine hardware, virtual servers exist only as defined within specialized software called hypervisor. Each hypervisor can run hundreds, or even thousands, of virtual servers all at once. The hypervisor presents virtual hardware to the server as if it were real physical hardware. The virtual server uses the virtual hardware as usual, and the hypervisor

passes the actual computation and storage needs onto the real hardware beneath, which is shared among all the other virtual servers.

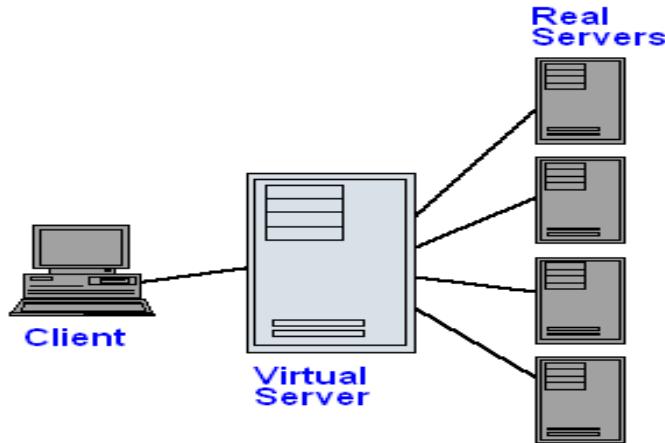


Image 11: Virtual Server

Reference : <https://cf.ycdn.net/latest/images/computer/VIRTSERV.GIF>

Proxy servers

A proxy server acts as an intermediary between a client and a server. Often used to isolate either the clients or servers for security purposes, a proxy server takes the request from the client. Instead of responding to the client, it passes the request on to another server or process. The proxy server receives the response from the second server and then replies to the original client as if it were replying on its own. In this way, neither the client nor the responding server needs to directly connect to each other.

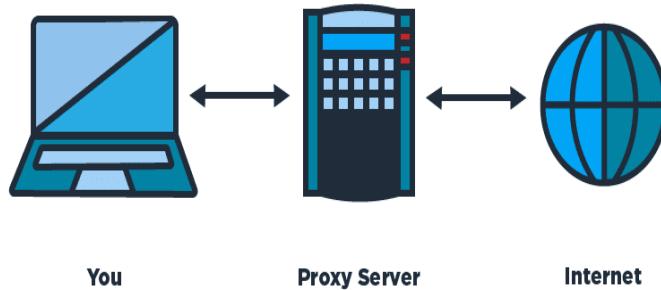


Image 12: Proxy Server
Reference : https://miro.medium.com/max/826/1*QerJ1gJTmxrNJ63oPmUOgA.png

FTP Server

An FTP server is a computer which has a file transfer protocol (FTP) address and is dedicated to receiving an FTP connection.

An FTP server needs a TCP/IP network for functioning and is dependent on usage of dedicated servers with one or more FTP clients. In order to ensure that connections can be established at all times from the clients, an FTP server is usually switched on.

An FTP server is an important component in FTP architecture and helps in exchanging files over the internet.

An FTP server is also known as an FTP site.



Image 13: FTP Server

Reference :

<https://www.serv-u.com/-/media/solarwinds/serv-u/features/windows-setup/ftp-setup-windows-image-1.ashx?rev=022de70a7ab6435cb0ecd3435edab50d>

Server Structures

Computer hardware server

The next major wave of servers included computer-based servers. In many respects, these servers were nothing more than larger, more powerful desktop computers. Such servers were generally more expensive and held far more memory and disk space than most client computers. Each server was still a self-contained unit with its own motherboard, processor, memory, disk drives, and power supply. Servers like this were often warehoused in air-conditioned rooms called server rooms, and were later bolted into racks for better storage and accessibility.



Image 14: Computer Hardware Server

Reference :

https://encrypted-tbn0.gstatic.com/images?q=tbn%3AANd9GcT4pxPUzZFXuj1pK_pbuYS5q960GNi_5yQXVboeo-PGGDv_MK7M&usqp=CAU

Blade servers

The original computer server hardware was large and stored in racks that could hold hundreds of pounds. Over time, however, faster means of connecting hardware resulted in parts of the server being extracted from a single self-contained device. By removing hard drives, eliminating internal cooling, and the ongoing miniaturization of computing parts, servers were eventually reduced to a single thin server known as a blade server. While still stored in racks in server rooms, blade servers are smaller and can be replaced more easily.

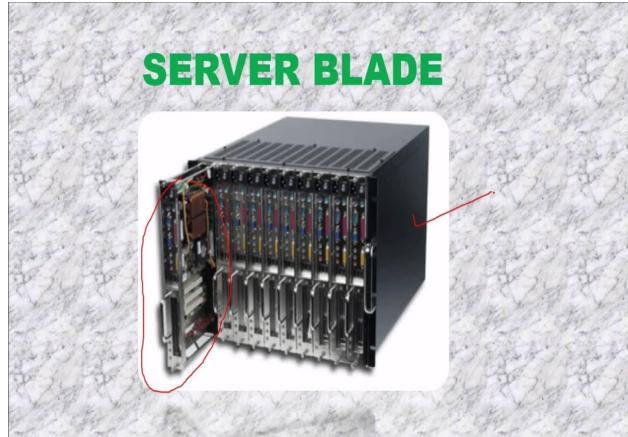


Image 15: Blade Server
Reference : <https://i.ytimg.com/vi/gDHmsoFtw4/maxresdefault.jpg>

Combining servers

Even before virtualization, servers were being extracted from the standard model of a single server operating system installed on a hardware machine. Technology, such as network-attached storage, removed the need for a server to have its own storage. Other technologies, such as mirroring and clustering, enabled pieces of hardware to be combined into larger, more powerful servers. Such a server might consist of several blades, several attached storage devices, and an external power supply, and each piece could be swapped out for another while the server was still running.

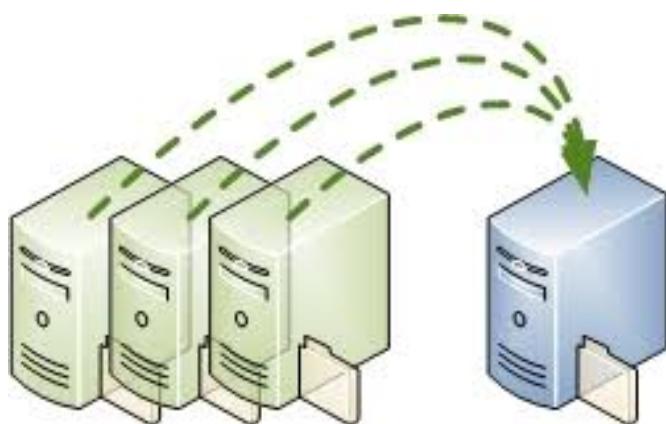


Image 16: Combining Server
Reference :https://omicro.net/wp-content/uploads/2016/12/srv_srv.jpg

Examples of server operating systems

Microsoft Windows servers

An argument can be made that Windows for Workgroups was Microsoft's first server operating system. In that version, certain computers could be set to share resources and respond to requests from clients, which made them servers by definition. Microsoft's first real server operating system was Windows NT. Its 3.5 and 3.51 versions ran on many business networks until Microsoft released its Windows Server line that continues to exist today. The most current Windows Server version is Windows Server 2016. This version supports numerous applications and databases as well as a hypervisor that allows virtual servers.



Image 17: Microsoft Windows Server
Reference : <https://4.imimg.com/data4/BQ/SJ/MY-22811923/microsoft-windows-server-500x500.png>

Linux / Unix servers

The other major player in server operating systems is the Linux/Unix realm. There are multiple versions and flavors of Linux/Unix including Red Hat Enterprise Linux, Debian, and CentOS. As an open-source operating system, Linux is very popular as a web server, often with the Apache web application server installed.



Image 18 :Linux/Unix Server
Reference :<https://visiontrainingsystems.com/wp-content/uploads/2014/06/itu-unix-linux-1024x576.jpg>

NetWare

Although no longer made, NetWare was a major player in the server software space as the client-server era was ramping up. Eventually, NetWare moved its server operating system to a Linux-based kernel and named it a Novell Open Enterprise Server (OES).



Image 19 : NetWare
Reference :<https://www.computerhope.com/jargon/n/netware.jpg>

Cloud servers

Virtual servers hosted on a third-party infrastructure on an open network, such as the Internet, are called cloud servers. There are numerous cloud server providers these days, including Google's Cloud Platform, Microsoft Azure, and IBM Cloud.

However, the main pioneer of corporate cloud computing was Amazon's AWS platform. It originally started using spare capacity of Amazon's own servers and networks, but AWS now allows customers to create a virtual server nearly instantly and then adjust the amount of resources that server may use on the fly.

Today, a server can be nothing more than the data of physical hardware that consists of multiple processors, disk drives, memory, and network connections. But, even now, a server is still just a system that responds to a request from a client.



Image 20 :Cloud Server

Reference : <https://5.imimg.com/data5/XM/CL/MY-43004084/cloud-server-software-500x500.jpg>

Client

What does Client mean?

A client is the receiving end of a service or the requestor of a service in a client/server model type of system. The client is most often located on another system or computer, which can be accessed via a network. This term was first used for devices that could not run their own programs, and were connected to remote computers that could via a network. These were called dumb terminals and they were served by time-sharing mainframe computers.

A client can be a simple application or a whole system that accesses services being provided by a server. A client can connect to a server through different means like domain sockets, named, shared memory or through Internet protocols, which is the most common method being used since the wide adoption of the Internet.

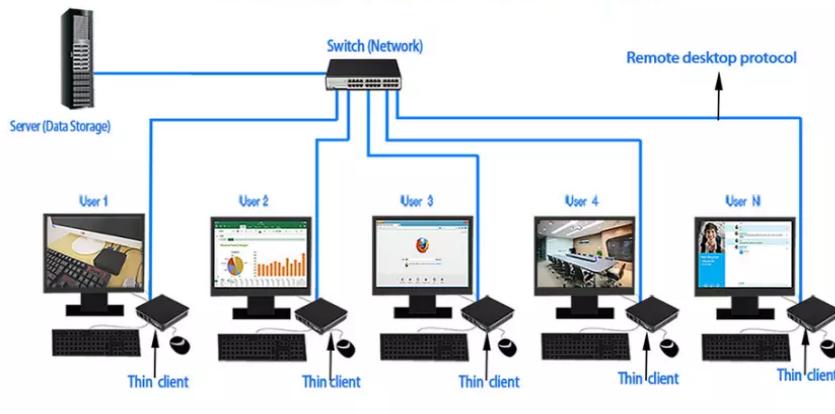
Types of Client-

Clients are classified into three types:

Thin Client:

A client application with minimum functions that uses the resources provided by a host computer and its job is usually just to display results processed by a server. It simply relies on a server to do most or all of its processing.

How is thin client works?



NW: 0.35KG

Size:10X10X2.5(CM)

Image 21:Thin Client

Reference : https://sc01.alicdn.com/kf/HTB13t_ANZfpK1RjSZFOq6y6nFXab/235276409/HTB13t_ANZfpK1RjSZFOq6y6nFXab.jpg_.webp

Thick/Fat Client:

This is the opposite of the thin client. It can do most of its processing and does not necessarily rely on a central server, but may need to connect to one for some information, uploading, or to update data or the program itself. Anti-virus software belong to this category because they do not really need to connect to a server to do their job, although they must connect periodically to download new virus definitions and upload data.

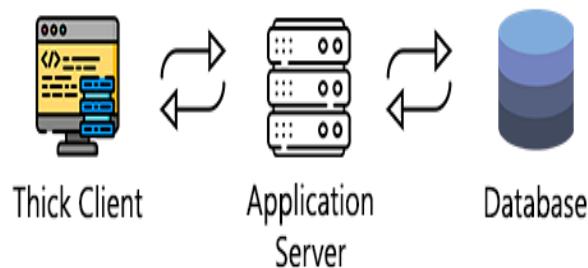


Image 22 :Thick Client

Reference : <https://www.cyberark.com/wp-content/uploads/2020/02/3.png>

Hybrid Client:

Exhibits characteristics from the two above types. It can do most processes on its own but may rely on a server for critical data or for storage.

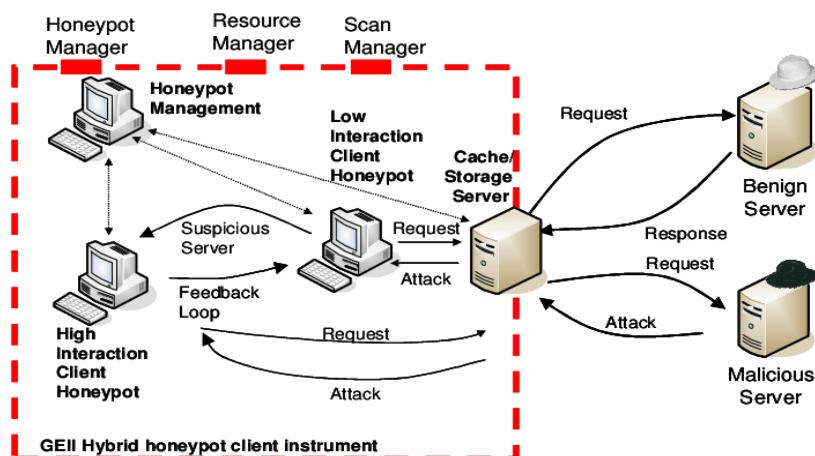


Image 23 :Hybrid Client

Reference :

https://www.researchgate.net/profile/Peter_Komisarczuk/publication/202141505/figure/fig2/AS:667681795624961@1536199153132/Hybrid-client-honeypot-architecture-23.png

Node

What is Node?

A node is a point of connection within the range of the network. It is a major hub through which internet traffic is generally routed. The nodes are also known as internet hubs. The concept of a node is familiarized with the notion of a distributed network and packet switching theory. In this background, nodes are like gateways in which the signals are received, stored and shared through the distributed network.

What is Distributed Network?

- A **distributed network** is a type of computer **network** that is spread over different networks.
- This provides a single data communication **network**, which can be managed jointly or separately by each **network**.
- Besides shared communication within the **network**, a **distributed network** often also distributes processing.

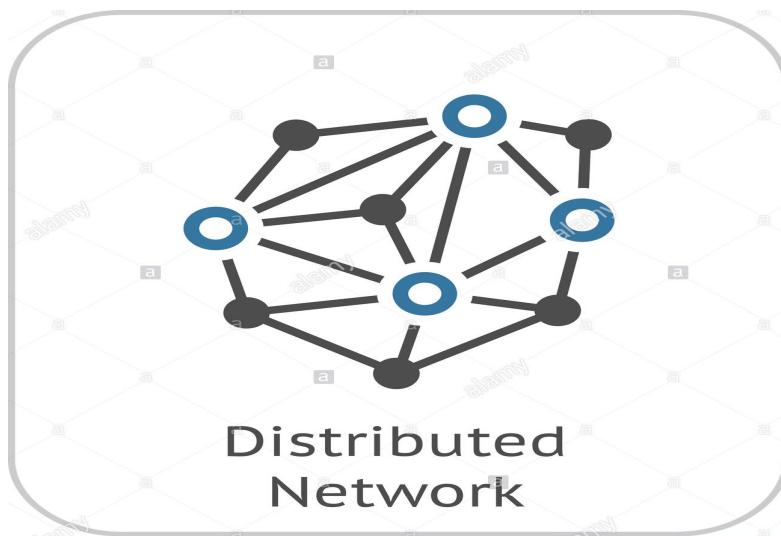


Image 24 :Distributed Network

Reference : https://encrypted-tbn0.gstatic.com/images?q=tbn%3AANd9GcT8cBUqLabB_dMlb3hlrZuF3tFBtS6HxTzGCZx_xC4JeS0lx30T&usqp=CAU

What is Packet Switching Method

- **Packet switching** is a method of transferring the data to a network in form of **packets**.
- In order to transfer the file fast and efficient manner over the network

- And minimize the transmission latency, the data is broken into small pieces of variable length, called **Packet**.

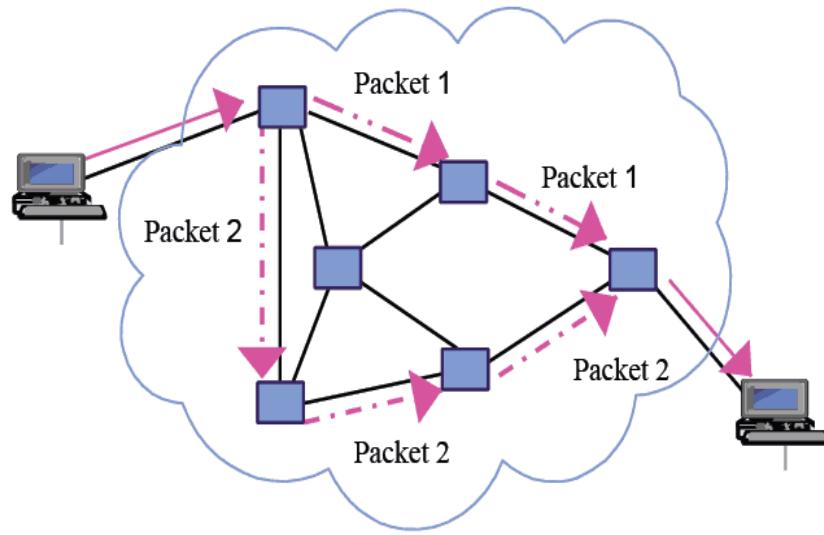


Image 25 : Packet Switching Method
Reference : <https://networkencyclopedia.com/wp-content/uploads/2019/10/packet-switching.png>

Segment

What is Segment?

A network segment is a portion of a computer network that is parted from the rest of the whole network by a device such as a hub, switch, repeater, bridge or router. Each segment can comprise one or many computers and hosts.

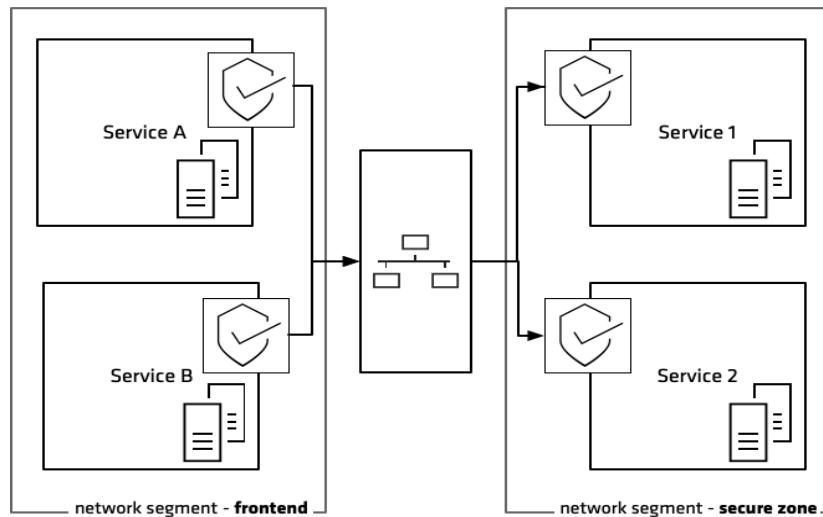


Image 26 : What is Segment
Reference :<https://www.datocms-assets.com/2885/1537309136-networksegments2.png>

Types of Segmentation:

The type of segmentation differs according to the type of device used. For example, a bridge separates collision domains, while a router separates both collision domains and broadcast domains.

Collision Domain

A collision domain is a logical area in a network where data packets can collide with one another. A collision occurs when two or more network devices attempt to send a signal along the same transmission channel at the same time, and it can result in garbled, and thus useless, messages.

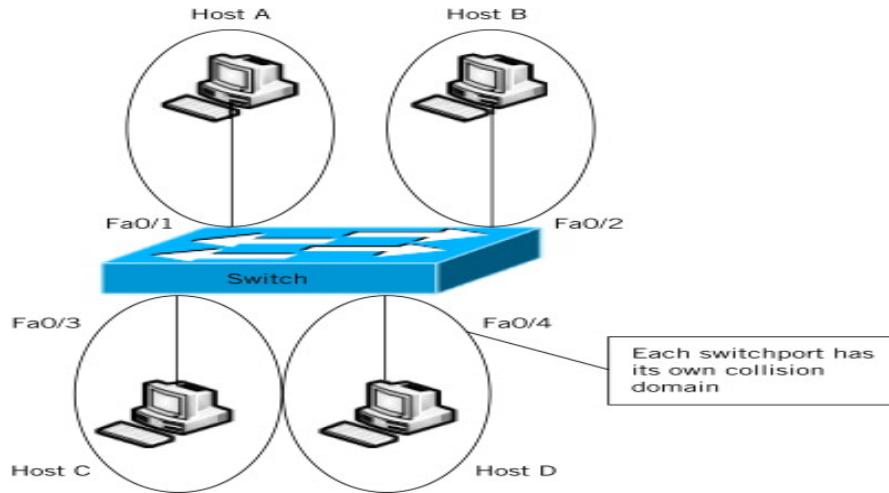


Image 27: Collision Domain

Reference : <https://ars.els-cdn.com/content/image/3-s2.0-B9781597493062000154-f11-12.jpg>

Broadcast Domain

A broadcast domain is the portion of a network that is reachable by a network broadcast, i.e., a simultaneous transmission of a single message to all hosts on the network, or part, thereof.

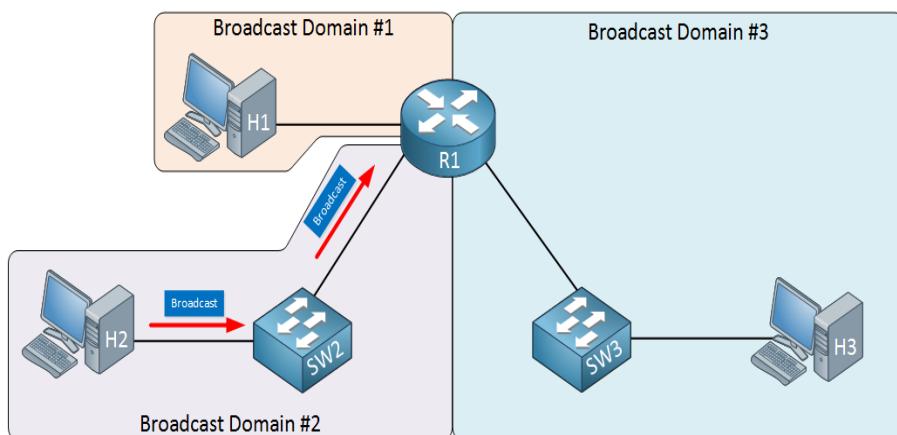


Image 28: Broadcast Domain

Reference : https://cdn.networklessons.com/wp-content/uploads/2016/11/xrouter-breaks-broadcast-domain.png.pagespeed.ic.FzR4ox_5t4.png

Backbone

What is Backbone?

A backbone is a fragment of a network that connects several bits of the network, providing a route for the sharing of data between different networks. A backbone can couple networks in the same building or in different infrastructures or over wide areas.

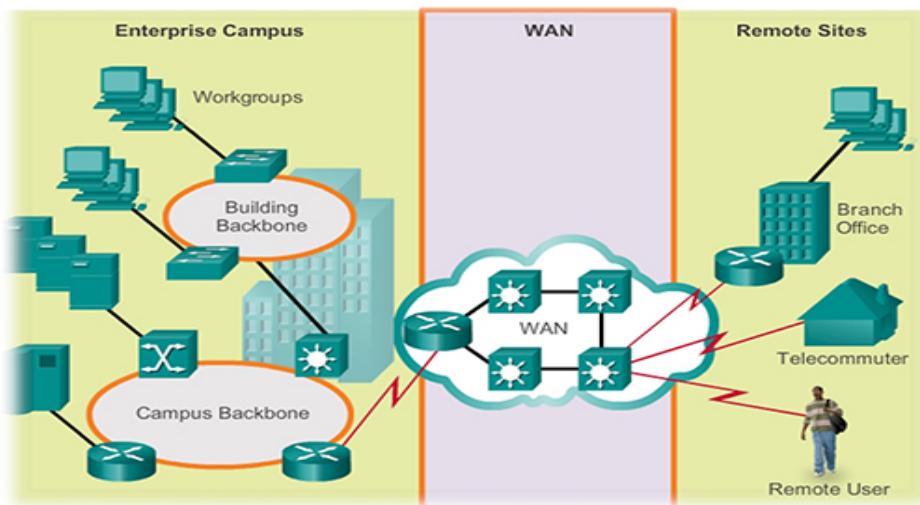


Image 29: What is Backbone?

Reference :https://www.open.edu/openlearncreate/pluginfile.php/259785/mod_oucontent/oucontent/35343/4d74da75/dc44f95b/cn_white_fiq1.jpg

Host

What is Host?

A host is a type of Web server that stores, serves and manages websites and/or Web-based applications and services. It is a remote server that provides the collective hardware, software, storage and networking capabilities for hosting websites.

A host may also be known as a Web host.

A host acts as a replacement for an in-house Web server and is the basic building block behind Web hosting services. A host is built, delivered and managed by a hosting service provider that rents out host(s) some portion of its computing power by sharing those resources among several websites/users.

A host functions as a typical Web server but is generally shared and has a different delivery/access mode.

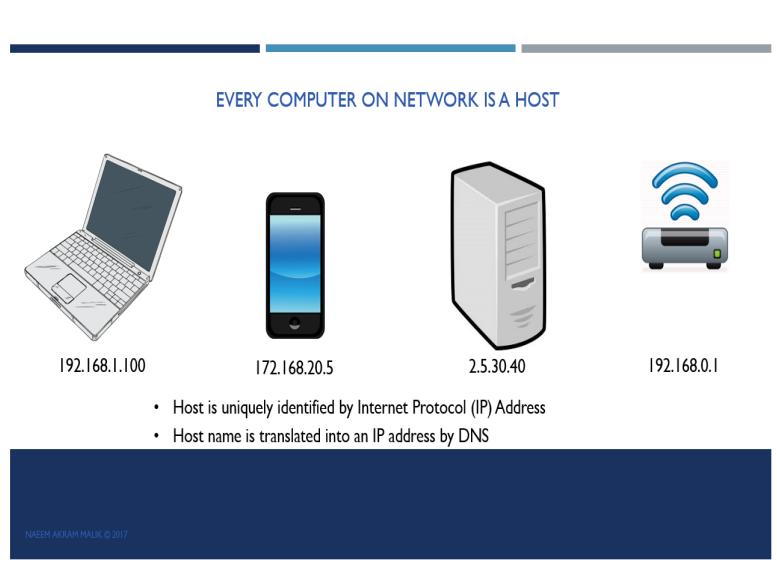


Image 30: What is Host?

Reference

https://2.bp.blogspot.com/-nw1guSvWmGM/XEjORHYceOI/AAAAAAAFA2I/Bw8aMuv2mEw9p5_dLb6zE828NUU-USWUQCLcBGAs/s1600/host-tcpip-udp-socket-programming-computer-networking.png

Key Component of Host

Key components of a host are:

Hardware:

This includes the computing server, storage and other critical components of a Web server

Software:

A basic operating system with specialized Web hosting and management software

Networks:

Interconnectivity, data routing and other types of networking

Analog and Digital Transmission

Define Analog and Digital Transmission

Analog and **digital** signals are used to transmit information, usually through electric signals. In both these technologies, the information, such as any audio or video, is transformed into electric signals.

The **difference between analog and digital** technologies is that in analog technology, information is translated into electric pulses of varying amplitude. In digital technology, translation of information is into binary format (zero or one) where each bit is representative of two distinct amplitudes.

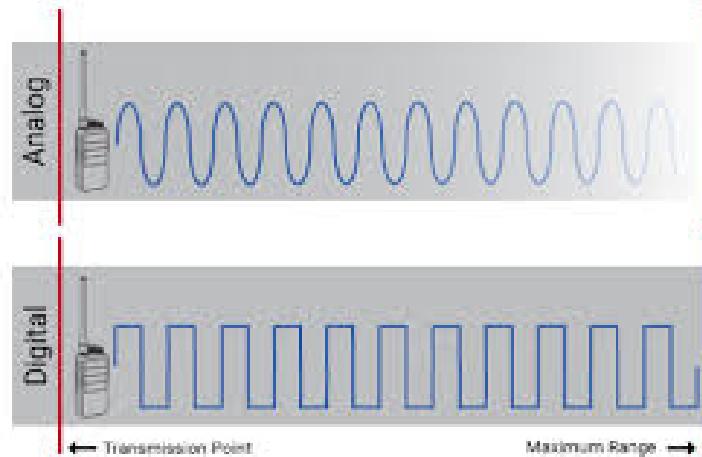


Image 31: Analog and Digital Transmission
Reference : <https://www.ruggedradios.com/blog/wp-content/uploads/2018/04/coverage-comparison.jpg>

Analog Transmission

An **Analog signal** is any continuous signal for which the time varying feature (variable) of the signal is a representation of some other time varying quantity, i.e., analogous to another time varying signal. It differs from a digital signal in terms of small fluctuations in the signal which are meaningful.

An analog waveform (or signal) is characterized by being continuously variable along amplitude and frequency. In the case of telephony, for instance, when you speak into a handset, there are changes in the air pressure around your mouth. Those changes in air pressure fall onto the

handset, where they are amplified and then converted into current, or voltage fluctuations. Those fluctuations in current are an analog of the actual voice pattern—hence the use of the term *analog* to describe these signals

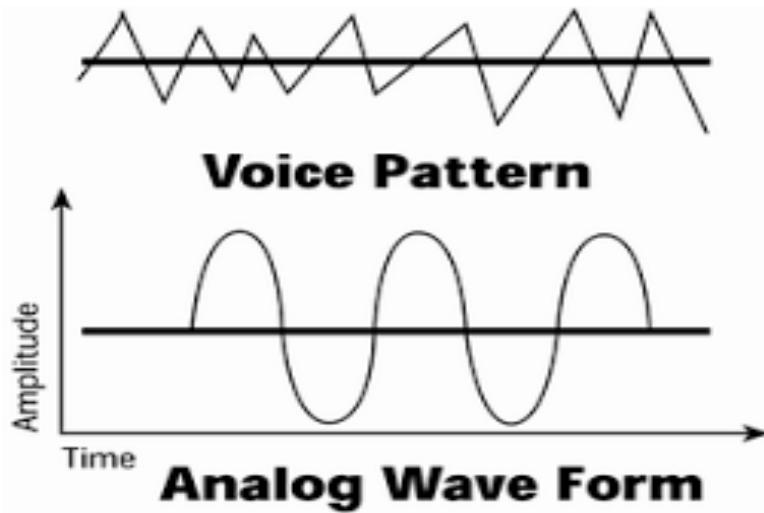


Image 32: Analog Transmission

Reference :https://flylib.com/books/2/567/1/html/2/016_files/image001.gif

When it comes to an analog circuit—what we also refer to as a voice-grade line—we need to also define the frequency band in which it operates. The human voice, for example, can typically generate frequencies from 100Hz to 10,000Hz, for a bandwidth of 9,900Hz. But the ear does not require a vast range of frequencies to elicit meaning from ordinary speech; the vast majority of sounds we make that constitute intelligible speech fall between 250Hz and 3,400Hz. So, the phone company typically allotted a total bandwidth of 4,000Hz for voice transmission.

Remember that the total frequency spectrum of twisted-pair is 1MHz. To provision a voice-grade analog circuit, bandwidth-limiting filters are put on that circuit to filter out all frequencies above 4,000Hz. That's why analog circuits can conduct only fairly low-speed data communications. The maximum data rate over an analog facility is 33.6Kbps when there are analog loops at either end.

elicit meaning from ordinary speech; the vast majority of sounds we make that constitute intelligible speech fall between 250Hz and 3,400Hz. So, the phone company typically allotted a total bandwidth of 4,000Hz for voice transmission. Remember that the total frequency spectrum of twisted-pair is 1MHz. To provision a voice-grade analog circuit, bandwidth-limiting filters are put on that circuit to filter out all frequencies above 4,000Hz. That's

why analog circuits can conduct only fairly low-speed data communications. The maximum data rate over an analog facility is 33.6Kbps when there are analog loops at either end.

Digital Transmission

Transmission of signals that vary discreetly with time between two values of some physical quantity, one value representing the binary number 0 and the other representing 1.

With copper cabling, the variable quantity is typically the voltage or the electrical potential. With fiber-optic cabling or wireless communication, variation in intensity or some other physical quantity is used.

Digital signals use discrete values for the transmission of binary information over a communication medium such as a network cable or a telecommunications link. On a serial transmission line, a digital signal is transmitted 1 bit at a time.

The opposite of digital transmission is analog transmission, in which information is transmitted as a continuously varying quantity. An analog signal might be converted to a digital signal using an analog-to-digital converter (ADC) and vice versa using a digital-to-analog converter (DAC). ADCs use a method called “quantization” to convert a varying AC voltage to a stepped digital one.

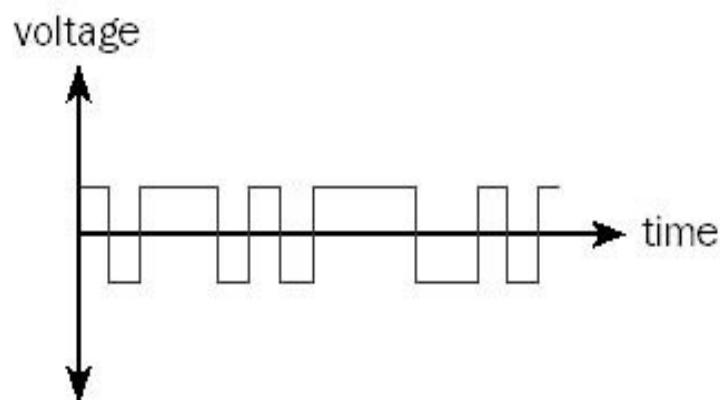


Image 33: Digital Transmission

Reference :<https://networkencyclopedia.com/wp-content/uploads/2019/08/digital-transmission.jpg>

Difference Between Analog and Digital Transmission

When we talk about analogue or digital, we are referring to the type of transmission of a signal. There are a number of key differences between analogue and digital signal transmission.



Image 34: Difference between Analog and Digital Transmission
Reference :https://www.guru99.com/images/2/030720_0729_AnalogvsDig3.png

Analog	Digital
An analog signal is a continuous signal that represents physical measurements.	Digital signals are time separated signals which are generated using digital modulation.
It is denoted by sine waves	It is denoted by square waves
It uses a continuous range of values that help you to represent information.	Digital signal uses discrete 0 and 1 to represent information.
Temperature sensors, FM radio signals, Photocells, Light sensor, Resistive touch screen are examples of Analog signals.	Computers, CDs, DVDs are some examples of Digital signal.

The analog signal bandwidth is low

Analog signals are deteriorated by noise throughout transmission as well as write/read cycle.

Analog hardware never offers flexible implementation.

It is suited for audio and video transmission.

Processing can be done in real-time and consumes lesser bandwidth compared to a digital signal.

Analog instruments usually have a scale which is cramped at lower end and gives considerable observational errors.

Analog signal doesn't offer any fixed range.

The digital signal bandwidth is high.

Relatively a noise-immune system without deterioration during the transmission process and write/read cycle.

Digital hardware offers flexibility in implementation.

It is suited for Computing and digital electronics.

It never gives a guarantee that digital signal processing can be performed in real time.

Digital instruments never cause any kind of observational errors.

Digital signal has a finite number, i.e., 0 and 1.

What are the Advantages of Digital Transmission over Analog Transmission

Digital transmission has several advantages over analog transmission:

- 1. Analog circuits require amplifiers, and each amplifier adds distortion and noise to the signal.

- 2. In contrast, digital amplifiers regenerate an exact signal, eliminating cumulative errors. An incoming (analog) signal is sampled, its value is determined, and the node then generates a new signal from the bit value; the incoming signal is discarded. With analog circuits, intermediate nodes amplify the incoming signal, noise and all.
- 3. Voice, data, video, etc. can all be carried by digital circuits. What about carrying digital signals over analog circuit? The modem example shows the difficulties in carrying digital over analog.

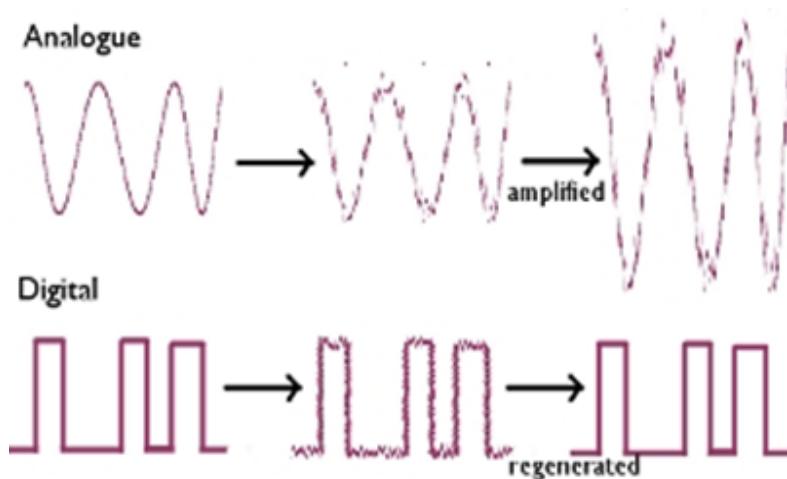


Image 35: Advantages of Digital Transmission over Analog Transmission

Reference :https://2.bp.blogspot.com/-VdvEo1bKvps/Vt1RnTArZ_I/AAAAAAAAC0/f0J643LkIw0/s320/Regenerationofsi%253Dgnals..png

why digital signals better than analog

- **Digital signals** are **more** secure, and they do not get damaged by noise.
- They allow the **signals** transmitted **over** a lengthy distance.
- By using these **signals**, we can translate the messages, audio, video into device language.

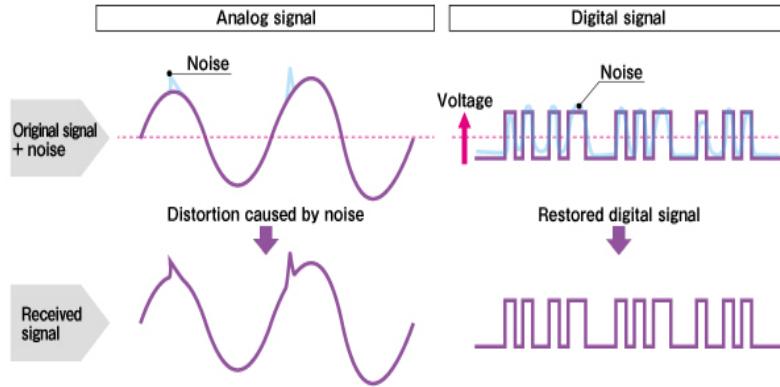


Image 36: Digital Signals better than Analog

Reference : https://2.bp.blogspot.com/-J3YUIQrcYLI/Vt1RcJ8r5HI/AAAAAAAACw/oEx_z0NpB3o/s1600/NoiseImmunity.png

What are the Advantages of Digital Transmission

Here, are pros/advantages of Digital Signals:

- Digital data can be easily compressed.
- Any information in the digital form can be encrypted.
- Equipment that uses digital signals is more common and less expensive.
- Digital signal makes running instruments free from observation errors like parallax and approximation errors.
- A lot of editing tools are available
- You can edit the sound without altering the original copy
- Easy to transmit the data over networks

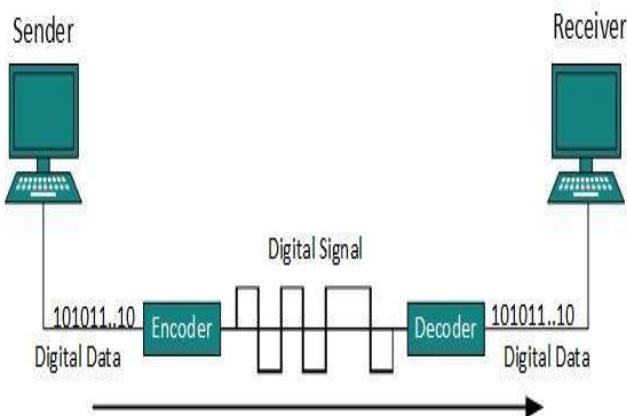


Image 37: Advantages of Digital Transmission

Reference : https://www.tutorialspoint.com/data_communication_computer_network/images/line_coding.jpg

What are the Disadvantages of Digital Transmission

- Sampling may cause loss of information.
- A/D and D/A demands mixed-signal hardware
- Processor speed is limited
- Develop quantization and round-off errors
- It requires greater bandwidth
- Systems and processing is more complex.

What are the Advantages of Analog Transmission

Here, are pros/benefits of Analog Signals

- Easier in processing
- Best suited for audio and video transmission.
- It has a low cost and is portable.
- It has a much higher density so that it can present more refined information.
- Not necessary to buy a new graphics board.
- Uses less bandwidth than digital sounds
- Provide more accurate representation of a sound
- It is the natural form of a sound.

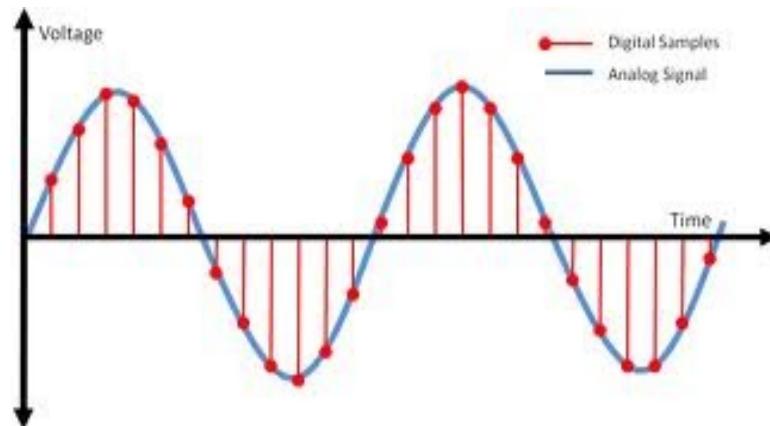


Image 38: Advantages of Analog Transmission

Reference :

<https://4.bp.blogspot.com/-EM5VV2XpYAI/UNL8xlegSAI/AAAAAAAAMJM/5ipPgtxIU4s/s1600/what+is+analog+signal+maximum+amplitude.bmp>

What are the Disadvantages of Analog Transmission

Here are cons/drawback of Analog Signals:

- Analog tends to have a lower quality signal than digital.
- The cables are sensitive to external influences.
- The cost of the Analog wire is high and not easily portable.
- Low availability of models with digital interfaces.
- Recording analog sound on tape is quite expensive if the tape is damaged
- It offers limitations in editing
- Tape is becoming hard to find
- It is quite difficult to synchronize analog sound
- Quality is easily lost
- Data can become corrupted
- Plenty of recording devices and formats which can become confusing to store a digital signal
- Digital sounds can cut an analog sound wave which means that you can't get a perfect reproduction of a sound
- Offers poor multi-user interfaces

STP Cable

What is STP Cable?

Shielded twisted pair (STP) cable was originally designed by IBM for token ring networks that include two individual wires covered with a foil shielding, which prevents electromagnetic interference, thereby transporting data faster.

STP is similar to unshielded twisted pair (UTP); however, it contains an extra foil wrapping or copper braid jacket to help shield the cable signals from interference. STP cables are costlier when compared to UTP, but has the advantage of being capable of supporting higher transmission rates across longer distances.

The additional covering in STP cable stops electromagnetic interference from leaking out of or into the cable.

STP Cable



Image 39: STP Cable

Reference :

<https://image.slidesharecdn.com/networking-170626234624/95/networking-utp-and-stp-cable-straight-and-crossover-by-mark-john-lado-6-638.jpg?cb=1499931283>

Where is STP Cable used?

STP cables are often used in Ethernet networks, particularly fast-data-rate Ethernets. The effectiveness of the additional covering varies according to the substance used for the shielding, such as:

- Frequency

-
- Thickness
 - Type of electromagnetic noise field
 - Distance from the shield to the noise source
 - Shield discontinuity
 - Grounding practices

Some STP cablings make use of a thick copper braided shield which makes the cable thicker, heavier, and in turn much more difficult for installation as compared to the UTP cables.

The other usual STP cables, often called foil twisted-pair cables or screened twisted-pair cables, make use of just a thinner outer foil shield. These cables are thin and more affordable versus the braided STP cable; but they are very difficult to install. Except in cases where the maximum pulling tension and minimum bend radius are strictly observed, these thinner cables may be torn during the installation process.

Furthermore, STP cables have some other drawbacks. STP cables function by drawing external interference to the shield, then getting rid of it into a grounded cable. If the ground cable is not properly grounded, STP's noise-canceling functionality can be seriously compromised.

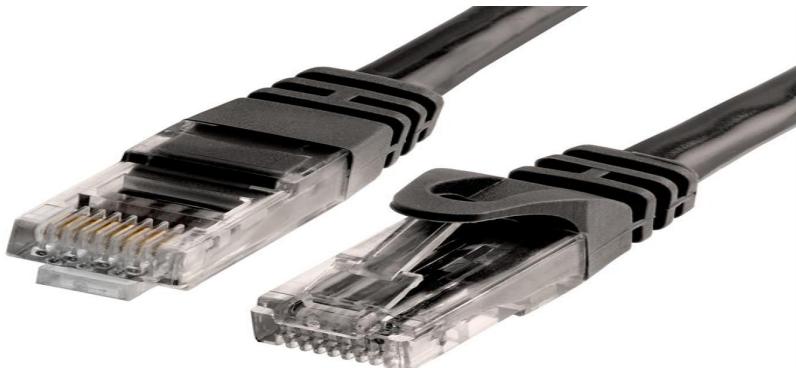


Image 40: STP Cable
Reference : <https://www.cmples.com/Content/Images/uploaded/UTP%20Cable.jpeg>

Which Connector is used in STP Cable?

Now you know about cables we need to know about connectors. This is pretty important and you will most likely need the RJ-45 connector. This is the cousin of the phone jack connector and looks real similar with the exception that the RJ-45 is bigger. Most commonly your connector are

in two flavors and this is BNC (Bayonet Naur Connector) used in thicknets and the RJ-45 used in smaller networks using UTP/STP.



Image 41: Connector used in STP Cable
Reference :<https://i.ytimg.com/vi/HpDgbGqqcas/maxresdefault.jpg>

UTP Cable

Introduction

- In the Un-Shielded Twisted Pair (UTP) cable, digital signal protection comes from the twists in the wire. The more twists per inch, the farther the digital signal can supposedly travel without interference. For example, categories 5 and 6 have many more twists per inch than category 3 UTP has. The Twists are given to the wire to reduce the Cross talk or interference to electrical signals.
- There are 4 twisted pairs with four different color wires.
- Only Two pairs are used with cable numbers 1, 2, 3, and 6 for Tx and Rx signals. You would notice Tx+/Tx- and Rx+/Rx- terms in this blog while reading. + And - terms are the voltages. 10BaseT uses two different voltages i.e. +2.5V and -2.5V.

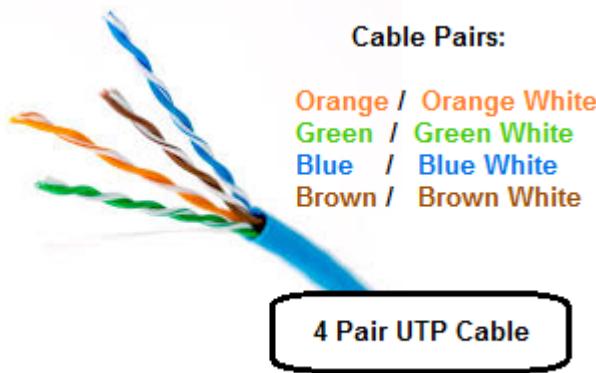


Image Source <https://www.networkurge.com/2017/10/utp-cable-color-coding.html>

Types

- Straight
- Cross
- Rollover or Console

Identifying the Cable type

- Hold both ends/RJ-45connectors of cable with their Jack in downward position. Now start matching the color coding from left pin of connector towards right. Below is example to identify a cross cable.

Straight Cable

- It is used to connect devices having different function. For example
 - Connecting a router to a hub or switch.
 - Connecting a server to a hub or switch.
 - Connecting workstations to a hub or switch.
- Below is the color coding of Straight cable. The color coding is kept same on both ends.

How to Identify type of cable

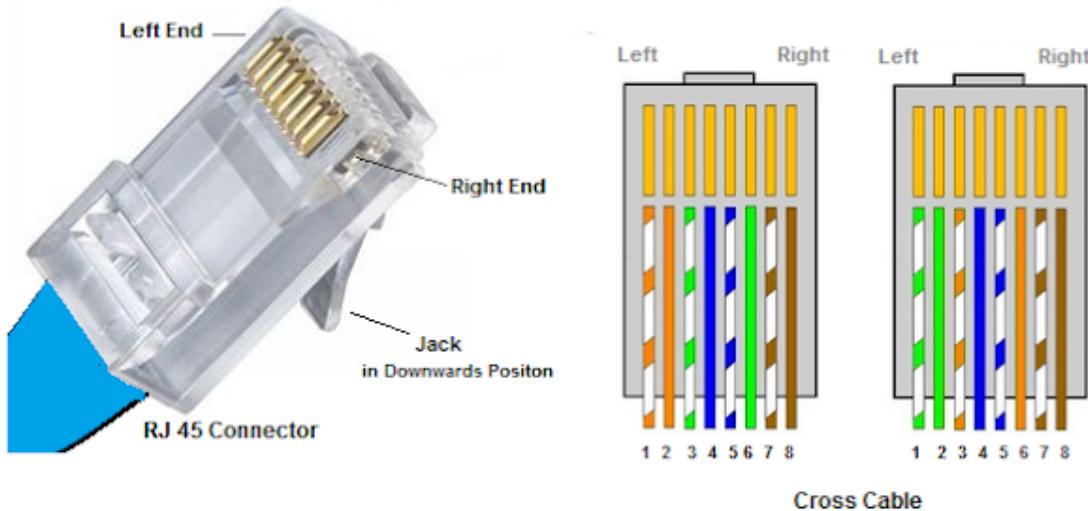
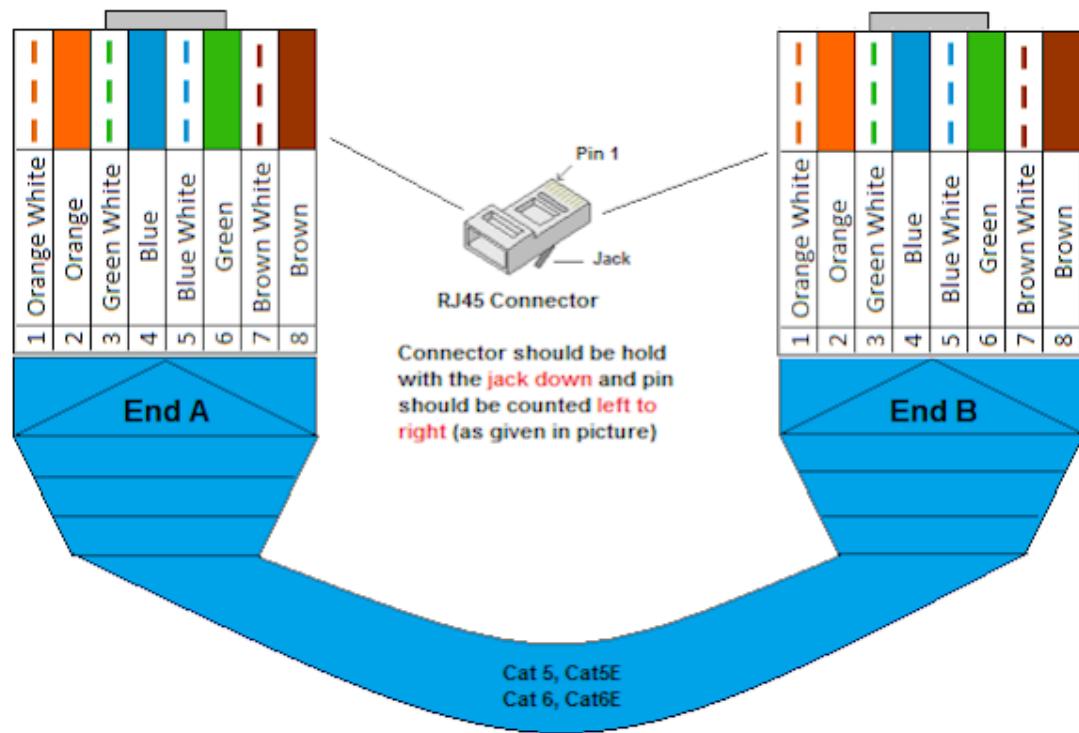


Image Source <https://www.networkurge.com/2017/10/utp-cable-color-coding.html>



**Straight Cable Color Coding
As per Standard EIA/TIA T-568B**

Image Source <https://www.networkurge.com/2017/10/utp-cable-color-coding.html>

Left	1	Tx+	—	—	—	—	Rx+	1	Left
	2	Tx-	—	—	—	—	Rx-	2	
	3	Rx+	—	—	—	—	Tx+	3	
	4		—	—	—	—		4	
	5		—	—	—	—		5	
	6	Rx-	—	—	—	—	Tx-	6	
	7		—	—	—	—		7	
Right	8		—	—	—	—		8	Right

Straight Cable

Image Source <https://www.networkurge.com/2017/10/utp-cable-color-coding.html>

Cross Cable

- It is used to connect devices having same functions or roles. For example:
 - Connecting uplinks between switches.
 - Connecting hubs to switches.
 - Connecting a hub to another hub.
 - Connecting PC to PC
 - Connecting PC to a Router
 - Connecting 2 routers together without a hub or a switch.
- Below is the color coding for a Cross cable. The only difference with respect to straight cable is that 1st and 3rd // 2nd and 6th numbered cables are swapped on the 2nd end of the cable.

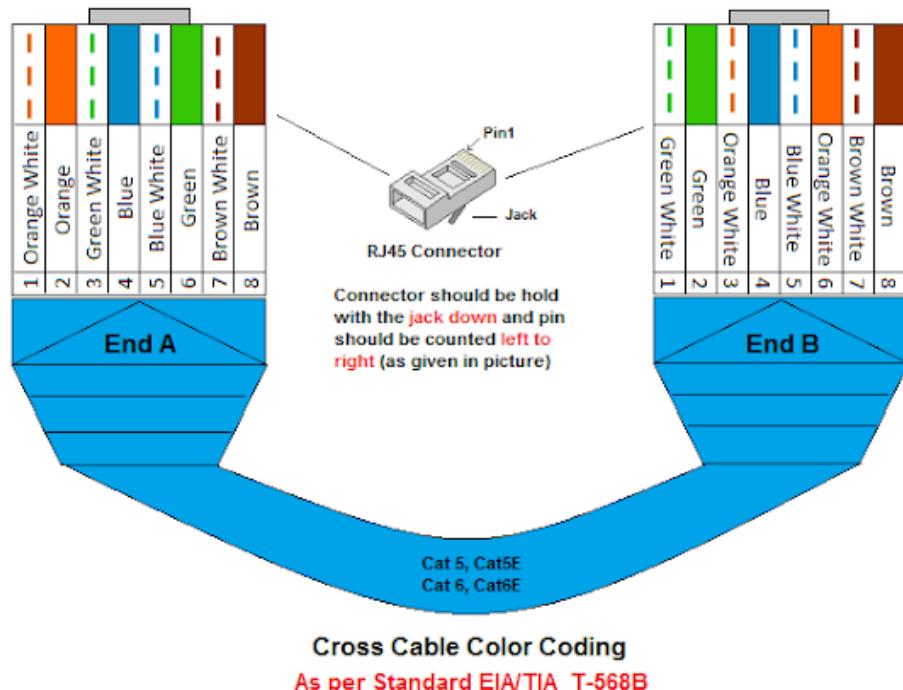


Image Source <https://www.networkurge.com/2017/10/utp-cable-color-coding.html>

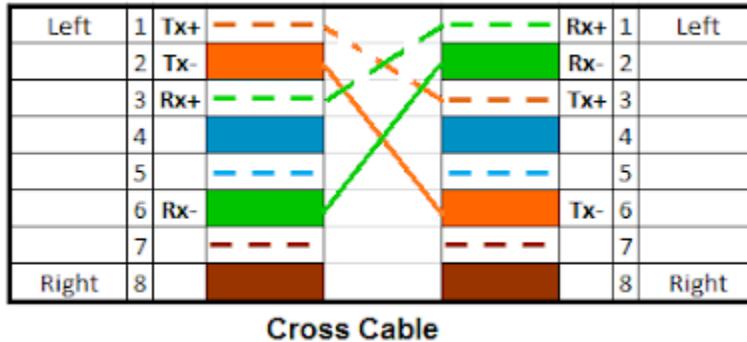


Image Source <https://www.networkurge.com/2017/10/utp-cable-color-coding.html>

Console or Rollover cable

- It is used for device configuration. For example you have bought a new router and what to configure it with initial configuration.
- You need a console cable for same. One end of console cable is connected to console port of the router or a switch and other end would be connected to NIC port of your laptop or PC.
- Below is the color coding of Console cable. The color coding of both ends are totally reversed.

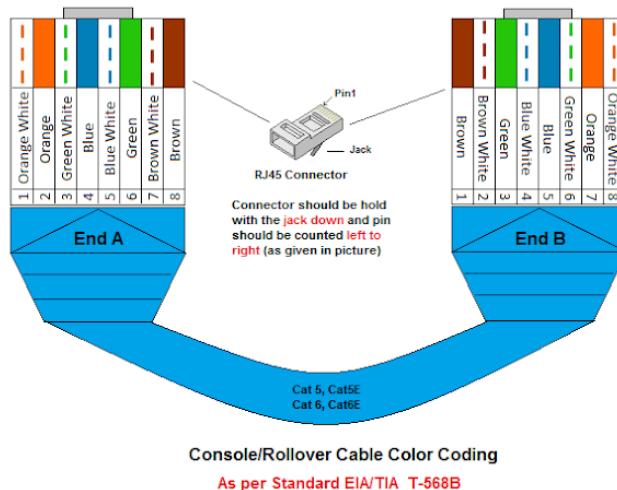


Image Source <https://www.networkurge.com/2017/10/utp-cable-color-coding.html>

Identifying Characteristics of UTP

The characteristics of UTP are very good and make it easy to work with, install, expand and troubleshoot and we are going to look at the different wiring schemes available for UTP.

UTP categories available today along with their specifications:

UTP Categories - Copper Cable				
UTP Category	Data Rate	Max. Length	Cable Type	Application
CAT1	Up to 1Mbps	-	Twisted Pair	Old Telephone Cable
CAT2	Up to 4Mbps	-	Twisted Pair	Token Ring Networks
CAT3	Up to 10Mbps	100m	Twisted Pair	Token Ring & 10BASE-T Ethernet
CAT4	Up to 16Mbps	100m	Twisted Pair	Token Ring Networks
CAT5	Up to 100Mbps	100m	Twisted Pair	Ethernet, FastEthernet, Token Ring
CAT5e	Up to 1 Gbps	100m	Twisted Pair	Ethernet, FastEthernet, Gigabit Ethernet
CAT6	Up to 10Gbps	100m	Twisted Pair	GigabitEthernet, 10G Ethernet (55 meters)
CAT6a	Up to 10Gbps	100m	Twisted Pair	GigabitEthernet, 10G Ethernet (55 meters)
CAT7	Up to 10Gbps	100m	Twisted Pair	GigabitEthernet, 10G Ethernet (100 meters)

Image source: <http://www.firewall.cx/networking-topics/cabling-utp-fibre/112-network-cabling-utp.html>

- Category 1/2/3/4/5/6/7 – a specification for the type of copper wire (most telephone and network wire is copper) and jacks. The number (1, 3, 5, etc) refers to the revision of the specification and in practical terms refers to the number of twists inside the wire (or the quality of connection in a jack).
- CAT1 is typically used for telephone wire. This type of wire is not capable of supporting computer network traffic and is not twisted. CAT1 is also used by telco companies providing ISDN and PSTN services. In such cases the wiring between the customer's site and the telco's network is performed using CAT 1 type cable.

-
- CAT2, CAT3, CAT4, CAT5/5e, CAT6 & CAT 7 are network wire specifications. This type of wire can support computer network and telephone traffic. CAT2 is used mostly for token ring networks, supporting speeds up to 4 Mbps. For higher network speeds (100 Mbps or higher) CAT5e must be used, but for the almost extinct 10 Mbps speed requirements, CAT3 will suffice.
 - CAT3, CAT4 and CAT5 cables are actually 4 pairs of twisted copper wires and CAT5 has more twists per inch than CAT3 therefore can run at higher speeds and greater lengths. The "twist" effect of each pair in the cables ensures any interference presented/picked up on one cable is cancelled out by the cable's partner which twists around the initial cable. CAT3 and CAT4 are both used for Token Ring networks -- where CAT 3 can provide support of a maximum 10Mbps, while CAT4 pushed the limit up to 16Mbps. Both categories have a limit of 100 meters.
 - The more popular CAT5 wire was later on replaced by the CAT5e specification which provides improved crosstalk specification, allowing it to support speeds of up to 1Gbps. CAT5e is the most widely used cabling specification world-wide and unlike the category cables that follow, is very forgiving when the cable termination and deployment guidelines are not met.
 - CAT6 wire was originally designed to support gigabit Ethernet, although there are standards that will allow gigabit transmission over CAT5e wire.. It is similar to CAT5e wire, but contains a physical separator between the four pairs to further reduce electromagnetic interference. CAT6 is able to support speeds of 1Gbps for lengths of up to 100 meters, and 10Gbps is also supported for lengths of up to 55 meters.
 - Today, most new cabling installations use CAT6 as a standard, however it is important to note that all cabling components (jacks, patch panels, patch cords etc) must be CAT6 certified and extra caution must be given to the proper termination of the cable ends.
 - In 2009, CAT6A was introduced as a higher specification cable, offering better immunization to crosstalk and electromagnetic interference.

-
- Organizations performing installations using CAT6 cabling should request a thorough test report using a certified cable analyzer, to ensure the installation has been performed according to CAT6 guidelines & standards.
 - CAT7 is a newer copper cable specification designed to support speeds of 10Gbps at lengths of up to 100 meters. To achieve this, the cable features four individually shielded pairs plus an additional cable shield to protect the signals from crosstalk and electromagnetic interference (EMI).
 - Due to the extremely high data rates, all components used throughout the installation of a CAT7 cabling infrastructure must be CAT7 certified. This includes patch panels, patch cords, jacks and RJ-45 connectors. Failing to use CAT7 certified components will result in the overall performance degradation and failure of any CAT7 certification tests (e.g using a Cable Analyzer) since CAT7 performance standards are most likely not to be met. Today, CAT7 is usually used in Datacenters for backbone connections between servers, network switches and storage devices.

Wiring the UTP Cables

- There are two popular wiring schemes that most people use today: the T-568A and T-568B. These differ only in which color-coded pairs are connected -- pairs 2 and 3 are reversed. Both work equally well, as long as you don't mix them.
- UTP cables are terminated with standard connectors, jacks and punchdowns. The jack/plug is often referred to as a "RJ-45," but that is really a telephone company designation for the "modular eight-pin connector" terminated with the USOC pinout used for telephones. The male connector on the end of a patch cord is called a "plug" and the receptacle on the wall outlet is a "jack."

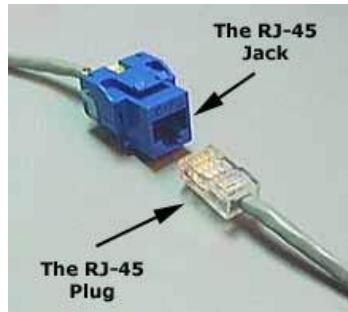


Image source: <http://www.firewall.cx/networking-topics/cabling-utp-fibre/112-network-cabling-utp.html>

As already mentioned, UTP has four twisted pairs of wires. The illustration shows the pairs and the color codes they have. As you can see, the four pairs are labeled:

UTP Colour Codes	
	Pair 1
	Pair 2
	Pair 3
	Pair 4

A diagram showing a cross-section of four twisted pairs of wires. The pairs are color-coded: Pair 1 (blue), Pair 2 (orange), Pair 3 (green), and Pair 4 (red). The wires are twisted in pairs to reduce interference.

Image source: <http://www.firewall.cx/networking-topics/cabling-utp-fibre/112-network-cabling-utp.html>

Figure: Color codes & Pairs of UTP CAT 5, CAT 5e, CAT6, CAT7 Cable

Pairs 2 and 3 are used for normal 10/100 Mbps networks, while pairs 1 and 4 are reserved. In Gigabit Ethernet, all four pairs are used. UTP cables are now available in a variety of colors, making it possible to have different colored cables for different applications.



Figure: Different colored UTP cables

Image source: <http://www.firewall.cx/networking-topics/cabling-utp-fibre/112-network-cabling-utp.html>

Similarities and differences between STP and UTP cables

- Both STP and UTP can transmit data at 10Mbps, 100Mbps, 1Gbps, and 10Gbps.
- Since the STP cable contains more materials, it is more expensive than the UTP cable.
- Both cables use the same RJ-45 (registered jack) modular connectors.
- The STP provides more noise and EMI resistant than the UTP cable.
- The maximum segment length for both cables is 100 meters or 328 feet.
- Both cables can accommodate a maximum of 1024 nodes in each segment.
- The following image shows both types of twisted-pair cable.

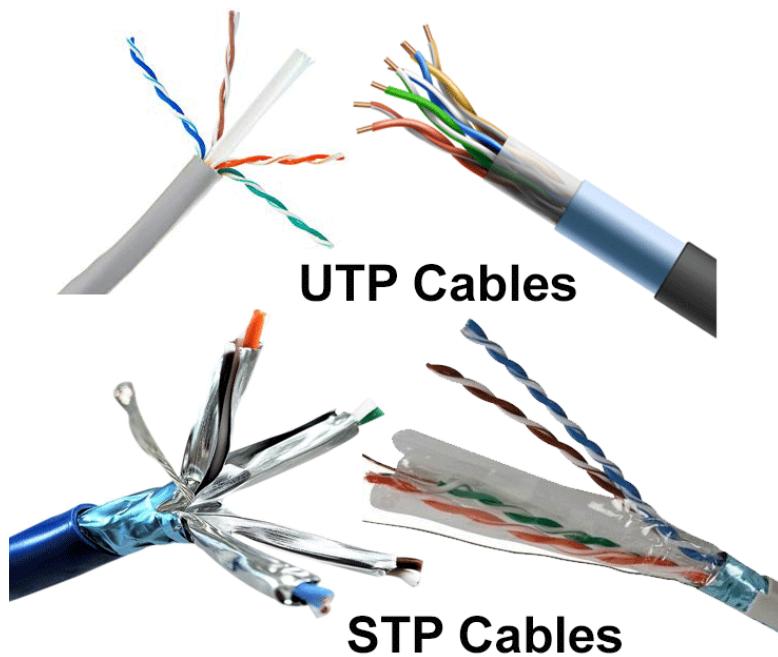


Image Source: computernetworkingnotes.com/networking-tutorials/network-cable-types-and-specifications.html

Coaxial cables

- Coaxial cables are the guided media that carries the signal of higher frequency range compared to twisted pair cable. Coaxial cables are also called *coax*. (Short form). Two types of coaxial cables are widely used: 50 ohm cable and 75 ohm cable. 50 ohm cable is used for digital transmission and 75 ohm cable is used for analogue transmission.
- Due to the shield provided, this cable has excellent noise immunity. It has a large bandwidth and low losses. Co-axial cables are easy to install. They are often installed either in a device to device daisy chain (Ethernet) or a star (ARC net).
- A coaxial cable consists of many small cables in a protective cover. The cover shields the cable from physical dangers as well as from electromagnetic interference. Within the cover, the various cables are shielded from interference with one another. Coaxial cables are used in communication networks that require many simultaneous communication links.
- Each coaxial cable can provide more than 5000 links. It has a data rate of 10 Mbps which can be increased with the increase in diameter of the inner conductor. The specified

maximum number of nodes on a thin net segment is 30 nodes and on a thick net it is 100 nodes.

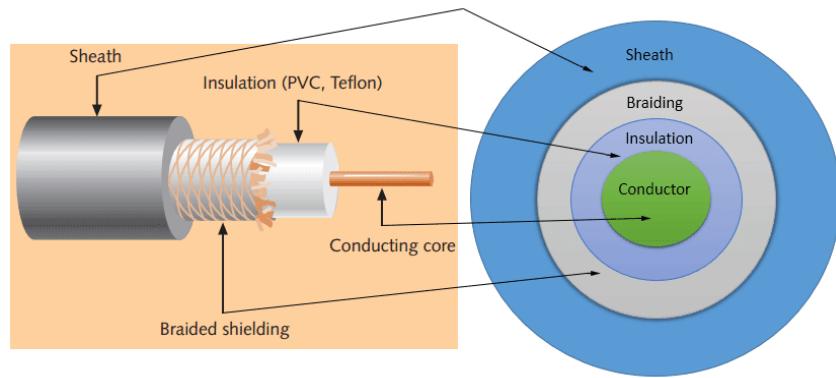


Image Source: computernetworkingnotes.com/networking-tutorials/network-cable-types-and-specifications.html

- Coaxial cable is a two-conductor cable in which one conductor forms an electromagnetic shield around the other. The two conductors are separated by insulation. It is a constant impedance transmission cable.
- This media is used in base band and broadband transmission.
- Coaxial cables do not produce external electric and magnetic fields and are not affected by them. This makes them ideally suited, although more expensive, for transmitting signals.
- This cable is suitable for point to point or point to multipoint applications. In fact this is the most widely used medium for local area networks. These cables are costlier than twisted pair cables but they are cheaper than the optical fiber cables.

General Properties of Coaxial Cable

- **Gauge:** The gauge of coaxial cable is thicker than the twisted pair. While this increases the available bandwidth and increases the distance of transmission, it also increases the cost. Traditional coaxial cable is quite thick, heavy and bulky of which Ethernet LAN 10Base5 is an example. Ethernet LAN 10Base2 is of much lesser dimensions but offers less in terms of performance,

-
- **Configuration:** Coaxial cables consist of a single, two-conductor wire, with a centre conductor and an outer shield (conductor), which is of solid metal. Sometimes, braided or stranded metal is used. Twin axial cables contain two such configurations within a single cable sheath. As the centre conductor carries the carrier signal and the outer conductor generally is used for electrical grounding. Coaxial cable connectivity can be extended through the use of twisted pair with a BALUN (Balanced/Unbalanced) connector serving to accomplish the interface.
 - **Bandwidth:** The effective capacity of coaxial cable depends on several factors, including the gauge of the center conductor, the length of the circuit, and the spacing of amplifiers and other intermediate devices. The available bandwidth over coaxial cable very significant, hence it is used in high capacity applications, such as data and image transmission.
 - **Error:** Performance Coaxial cable performs exceptionally well due to the outer shielding. As a result, it is often used in data applications.
 - **Distance:** Coaxial cable is not so limited as UTP, although amplifiers or other intermediate devices must be used to extend high frequency transmissions over distances of any significance.
 - **Security:** Coaxial cable is inherently quite secure. It is relatively difficult to place physical taps on coaxial cable. Radiation of energy is also minimal hence interception of it is not easy.
 - **Cost:** The acquisition, deployment, and rearrangement costs of coaxial cables are very high, compared with UTP. In high capacity data applications, however, that cost is often outweighed by its positive performance characteristics.
 - **Applications:** Coaxial cables superior performance characteristics make it the favoured medium in many short hauls, bandwidth-intensive data applications. Current and continuing applications include LAN backbone, host-to-host, host-to-peripheral and CATV.

Types of Coaxial Cables

- **Single-core** coaxial cable uses a single central metal (usually copper) conductor.
- **Multi-core** coaxial cable uses multiple thin strands of metal wires.



Single core coaxial cable



Multi-core coaxial cable

Image Source: computernetworkingnotes.com/networking-tutorials/network-cable-types-and-specifications.html

- The coaxial cables were not primarily developed for the computer network. These cables were developed for general purposes. They were in use even before computer networks came into existence. They are still used even their use in computer networks has been completely discontinued.
- At the beginning of computer networking, when there were no dedicated media cables available for computer networks, network administrators began using coaxial cables to build computer networks.
- Because of low-cost and long durability, coaxial cables were used in computer networking for nearly two decades (80s and 90s). Coaxial cables are no longer used to build any type of computer network.
- Coaxial cable uses RG rating to measure the materials used in shielding and conducting cores.
- RG stands for the Radio Guide. Coaxial cable mainly uses radio frequencies in transmission.

-
- Impedance is the resistance that controls the signals. It is expressed in the ohms.
 - AWG stands for American Wire Gauge. It is used to measure the size of the core.
 - The larger the AWG size, the smaller the diameter of the core wire.

Features

- It provides better immunity than twisted pair. This cable is able to transmit data at higher rates.

Limitations

- High installation cost.
- High maintenance cost.

Advantages of Coaxial Cables

- It can be used for both analog and digital transmission.
- It offers higher bandwidth as compared to twisted pair cable and can span longer distances.
- Because of better shielding in coaxial cable, loss of signal or attenuation is less.
- Better shielding also offers good noise immunity.
- It is relatively inexpensive as compared to optical fibres.
- It has lower error rates as compared to twisted pair.
- It is not as easy to tap as twisted pair because copper wire is contained in plastic jacket.

Disadvantages of Coaxial Cables

- It is usually more expensive than twisted pair.

Applications of Co-axial Cables

- Analog telephone networks.
- Digital telephone network.
- Cable TV
- Traditional Ethernet LANs
- Digital transmission
- Thick Ethernet

Specifications

- Coaxial cable uses RG rating to measure the materials used in shielding and conducting cores.
- RG stands for the Radio Guide. Coaxial cable mainly uses radio frequencies in transmission.
- RG6 cable is heavier gauge and has insulation and shielding tuned for high-bandwidth, high-frequency applications such as Internet, Cable TV, and Satellite TV signals. If you aren't sure which cable to get, then RG6 cable is your best bet.
- RG59 cable is thinner and is recommended in low bandwidth and lower frequency applications such as analog video and CCTV installations.

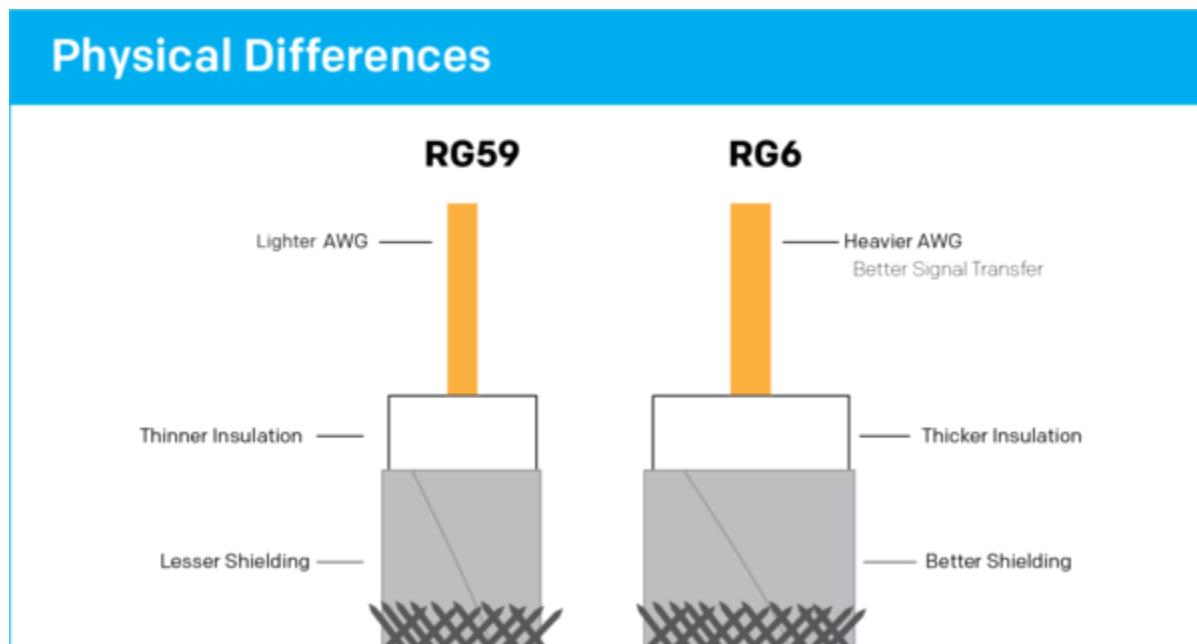


Image Source: <https://sewelldirect.com/blogs/learning-center/what-is-the-difference-between-rg59-and-rg6>

RG 6 vs. RG 59 Applications

RG 6 is recommended for your CATV, satellite, TV antenna, or broadband internet. RG 59 is generally better for most CCTV systems and other analog video signals. What you really need to

consider are the frequency ratings your equipment uses. If your equipment uses higher frequencies (above 50 MHz), then you'll want to go with RG 6. If your frequencies are lower than that, then you'll want to use RG 59.

RG 59 (In-Depth)



Image Source: <https://sewelldirect.com/blogs/learning-center/what-is-the-difference-between-rg59-and-rg6>

RG59 cable has been around for a long time. This cable used to be what most people used for their cable TV connection and is very commonly installed in older homes and commercial buildings. However, many modern signal requirements have made this cable less popular in the last few years. RG 59 has a smaller conductor than RG 6, which means that it can't achieve the same signal quality as RG 6. The way its shielding is designed also means that it doesn't keep Gigahertz level signals inside the conductor very well. This is why RG 59 probably isn't a good choice for your TV or internet connection.

The braided shielding in RG 59 was designed around (relatively) long waveforms of megahertz interference. That makes it good for lower frequency signals (anything under about 50 MHz). It is commonly used for composite or component video signals (often in the mini-coax variety). That also makes it a good choice for a closed circuit television (CCTV) video surveillance system. You can even make your installation easier by getting what's called "Siamese coaxial cable." This cable consists of a RG 59 cable merged together with a 2C power cable. By using this type of cable, you can run the power and video for your security cameras simultaneously, effectively cutting your install time in half.

RG 6 (In-Depth)



Image Source: <https://sewelldirect.com/blogs/learning-center/what-is-the-difference-between-rg59-and-rg6>

Satellite and internet signals run at higher frequencies than traditional analog video, and when TV broadcasts changed from analog to digital, and cable companies started switching to digital, the higher frequencies made it necessary to find a more effective coaxial cable. RG6 cable was designed to fulfill these requirements. It has a larger conductor, which gives you much better signal quality. The dielectric insulation was made thicker as well. RG 6 is also made with a different kind of shielding, which allows it to more effectively handle Ghz level signals. While many RG 59 cables use a foil shield in addition to the braid, RG 6 made it mandatory. The braid was originally in a looser weave (e.g. 60% versus the 90%+ of RG59) but many RG6 cables use a high-percentage braid now too.

Fiber Optics (Optical Fiber)

Introduction

- Optical fiber consists of thin glass fibers or plastic or any dielectric medium which can carry light signals from one end to the other. Optical fiber refers to the medium and the technology which is related, or you can say that it is connected with the transmission of information in the form of light impulses and this transmission is done along with a glass or plastic wire or fiber.
- The wires of fiber optic cable can carry much more information than any other conventional copper wire. The typical optical fiber consists of a very narrow strand of glass called the core. Around the core is a concentric layer of glass called the cladding?

-
- Optical fibers make use of light to send information through the optical medium.

Evolution or History of an Optical Fiber

- The optical fiber was first time demonstrated by Daniel Colladon and Jacques Babinet in Paris in the early 1840s. They made this by refraction of light. After 12 years, John Tyndall included a demonstration on it. In 1960, the laser light was first used as a light source. In 1965, high loss of light discovered. In 1970s, the refining of the manufacturing process is there. Later on in the 1980s, optical fibre technology becomes the backbone of long-distance telephone networks in network administration.

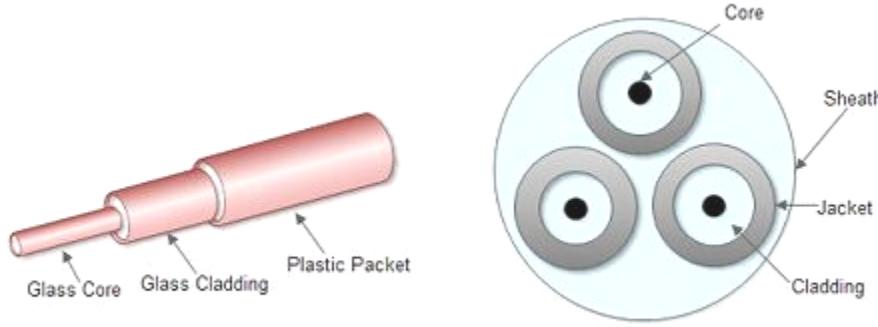
An optical transmission system has three essential components

- Light source: In such a system a pulse of light indicates bit 1 and the absence of light indicates bit 0. Light source can be an LED or a laser beam.
- Transmission medium: Transmission medium is the ultra-thin fiber of glass.
- Detector: A detector generates an electrical pulse when the light falls on it.

Structure of Optical Fiber

It has three parts shown in the diagram given below.

- Core: It is a central tube as shown in the diagram. It is of skinny size and made up of the optically transparent dielectric medium. It carries the light from the transmitter to the receiver. The diameter of the core varies from 5um to 100um.
- Cladding: it is the outer optical material surrounding the core. Its reflective index is lower than the core. It helps to keep the light within the core as it uses the phenomena of total internal reflection.
- Buffer coating: It is the plastic coating which protects the fiber. It is made up of silicon rubber. The diameter of the fiber after the coating is 250-300um.



(a)Optical fibre (b) Bundle of 3 fibers with outer sheath

Image Source: <http://ecomputernotes.com/images/Construction-of-Optical-fiber.jpg>

A typical core diameter is 62.5 microns .Typically cladding has a diameter of 125 microns. 100 microwatts power (roughly) a light emitting diode can couple into an optical fiber. Coating the cladding is a protective coating consisting of plastic, it is called the Jacket.

The loss in signal power as light travels down the fiber is called attenuation. An important characteristic of fiber optics is refraction. Refraction is the characteristic of a material to either pass or reflect light. When light passes through a medium, it “bends” as it passes from one medium to the other. An example of this is when we look into a pond of water If the angle of incidence is small, the light rays are reflected and do not pass into the water.

If the angle of incident is great, light passes through the media but is bent or refracted. Optical fibers work on the principle that the core refracts the light and the cladding reflects the light. The core refracts the light and guides the light along its path. The cladding reflects any light back into the core and stops light from escaping through it - it bounds the medium! Fast data transmission rate is an advantage to using fiber optics data transmission.

Working principle of an optical fiber

- The working principle of optical fiber cable is the total internal reflection.

Total internal reflection

- When a ray of light travels from denser medium to rarer medium in a way such that the angle of incidence is greater than the critical angle, then the ray reflects into the same medium.
- This phenomenon is known as total internal reflection. Using this phenomenon, the rays in the optical fiber undergo repeated total internal reflections until it emerges out of the other end of the fiber. It does not depend upon the shape of the fiber cable, i.e. the cable can be in bent shape.

Types of Modes

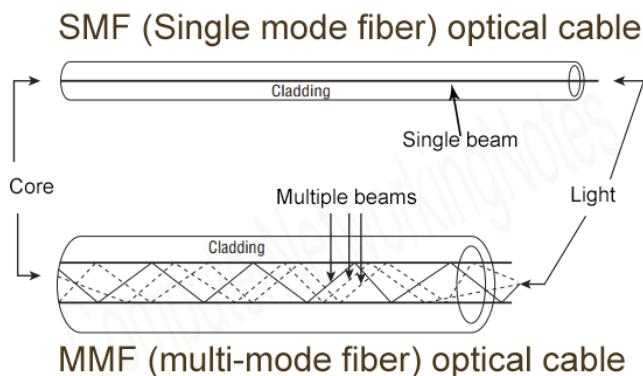


Image Source: <https://www.computernetworkingnotes.com/networking-tutorials/network-cable-types-and-specifications.html>

Fiber optic uses light to send data. It reflects light from one endpoint to another. Based on how many beams of light are transmitted at a given time, there are two types of fiber optical cable; SMF and MMF.

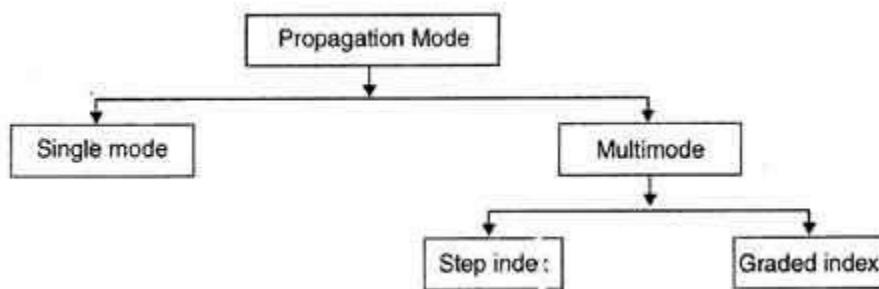


Image Source: <http://ecomputernotes.com/images/Construction-of-Optical-fiber.jpg>

SMF (Single-mode fiber) optical cable

- This cable carries only a single beam of light. This is more reliable and supports much higher bandwidth and longer distances than the MMF cable. This cable uses a laser as the light source and transmits 1300 or 1550 nano-meter wavelengths of light.

MMF (multi-mode fiber) optical cable

- This cable carries multiple beams of light. Because of multiple beams, this cable carries much more data than the SMF cable. This cable is used in shorter distances. This cable uses an LED as the light source and transmits 850 or 1300 nano-meter wavelengths of light.

Advantages of Optical Fiber

- They are not affected by electrical and magnetic interference as the data travel in form of light.
- Optical fiber offers higher bandwidth than twisted pair or coaxial cable.
- Optical fibers are thin, lighter in weight and small in size as compared to other wired Medias. It is easier to group several optical fibers in one bundle.
- Glass is more resistant to corrosive materials as compared to copper. Hence can be laid in different environments.
- In optical fibers, attenuation (loss of signal) is very low. Therefore these fibers can run several kilometres without amplification.
- Fibers do not leak light and are quite difficult to tap. So they provide security against potential wire tappers.
- There is no cross-talk problem in optical fibers.
- They are highly suitable for environments where speed is needed with full accuracy.
- Photons in fiber do not affect one another (as they have no charge) and are not affected by stray photons outside the fiber. But when electrons move in a wire they affect each other and are themselves affected by electrons outside the wire.

-
- The size (diameter) of the optical fibers is very small (it is comparable to the diameter of human hair). Therefore a large number of optical fibers can fit into a cable of small diameter.
 - The material used for the manufacturing of optical fibers is "silica glass". This material is easily available. So the optical fibers cost lower than the cables with metallic conductors.
 - As the light rays have a very high frequency in the GHz range, the bandwidth of the optical fiber is extremely large. This allows transmission of more number of channels. Therefore the information carrying capacity of an optical fiber is much higher than that of a co-axial cable.

Disadvantages of Optical Fiber

- Fiber optic cables are fragile i.e. more easily broken than wires.
- Being fragile, optical fibers need to be put deep into the land. This causes a lot of installation cost. Also the interface used for these fibers are expensive.
- Optical fibers are unidirectional for two-way communication, two fibers are required.
- It is a newer technology and requires skilled people to administer and maintain them.
- There is requirement of highly skilled staff for the maintenance of the cable. So, the maintenance cost of the optical fiber system is high.
- It accepts unipolar codes only.
- There is requirement of precise and costly instruments for the optical fiber.
- Jointing of fiber and splicing is a time consuming process.
- It seems to be costly if it is underutilized, i.e. if we don't make use of optical fiber cable for long time after doing installations.
- Only point-to-point working is possible in optical fiber.

Characteristics of Optical Fiber Cables

- Fiber optic cabling can provide extremely high bandwidths in the range from 100 mbps to 2 gigabits because light has a much higher frequency than electricity.

-
- The number of nodes which a fiber optic can support does not depend on its length but on the hub or hubs that connect cables together.
 - Fiber optic cable has much lower attenuation and can carry signal to longer distances without using amplifiers and repeaters in between.
 - Fiber optic cable is not affected by EMI effects and can be used in areas where high voltages are passing by.
 - The cost of fiber optic cable is more compared to twisted pair and co-axial.
 - The installation of fiber optic cables is difficult and tedious.

Baseband and Broadband Transmission

- Both baseband and broadband describe how data is transmitted between two nodes. Baseband technology transmits a single data signal/stream/channel at a time while

broadband technology transmits multiple data signalsstreams/channels simultaneously at the same time.

- The following image shows an example of both technologies.

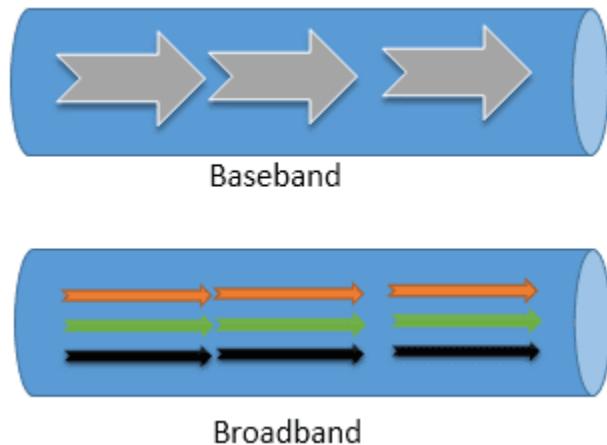


Image Source: <https://www.computernetworkingnotes.com/networking-tutorials/differences-between-baseband-and-broadband-explained.html>

- To understand the basic differences between both technologies, consider the baseband as a railway track and the broadband as a highway. Like, at a time, only one train can go on a railway track, in the baseband transmission only one data signal can be transmitted at a time.
- Unlike a railway track on a highway, multiple vehicles can go simultaneously. For example, on a 3 lanes highway, 3 vehicles can go at the same time. Same as a highway, in the broadband transmission, multiple data signals can be transmitted at the same time.



Image Source: <https://www.computernetworkingnotes.com/networking-tutorials/differences-between-baseband-and-broadband-explained.html>

Baseband transmission

- Baseband technology uses digital signals in data transmission. It sends binary values directly as pulses of different voltage levels. Digital signals can be regenerated using repeaters in order to travel longer distances before weakening and becoming unusable because of attenuation.
- Baseband supports bidirectional communication. It means, this technology can send and receive data simultaneously. To support bidirectional communication, this technology uses two separate electric circuits together; one for sending and another for receiving.
- The following image shows an example of this.

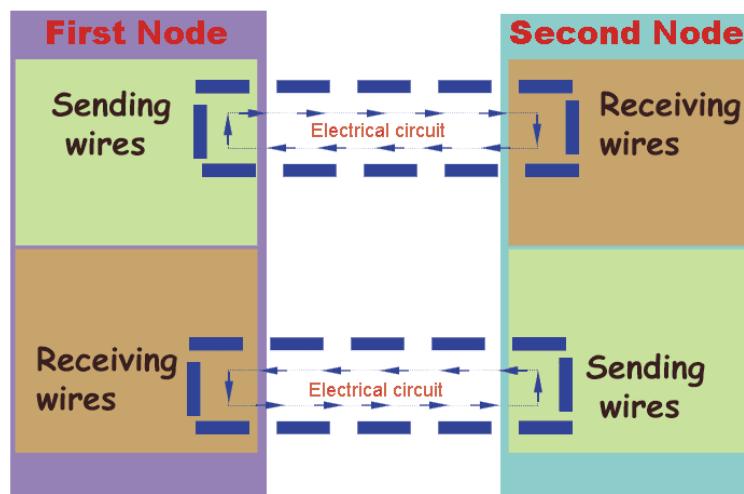


Image Source: <https://www.computernetworkingnotes.com/networking-tutorials/differences-between-baseband-and-broadband-explained.html>

- Although baseband transmits only a single data stream at a time, it is possible to transmit signals of multiple nodes simultaneously. This is done by combining all the signals into a single data stream. To combine the signals of multiple nodes, a technology known as multiplexing is used. Baseband supports the Time Division Multiplexing (TDM).
- Baseband technology is mainly used in Ethernet networks to exchange data between nodes. This technology can be used on all three popular cable media types of Ethernet; coaxial, twisted-pair, fiber-optic.

Broadband transmission

- Broadband technology uses analog signals in data transmission. This technology uses a special analog wave known as the **carrier wave**. A carrier wave does not contain any data but contains all properties of the analog signal. This technology mixes data/digital signal/binary values into the carrier wave and sends the carrier wave across the channel/medium.
- To transmit data of multiple nodes simultaneously, this technology supports the Frequency Division Multiplexing. FDM (Frequency Division Multiplexing) divides the channel (medium or path) into several sub-channels and assigns a sub-channel to each node. Each sub-channel can carry a separate carrier wave.
- The following image shows an example of this process.

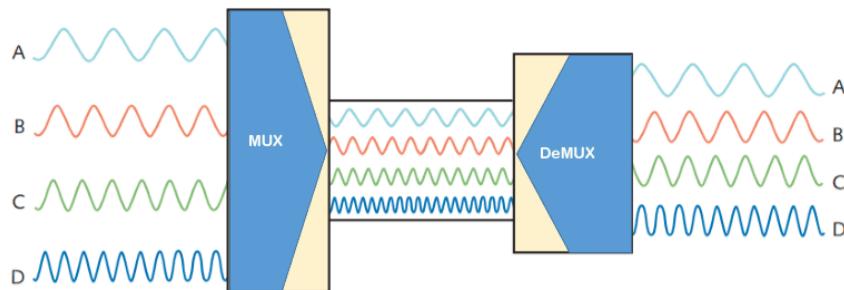


Image Source: <https://www.computernetworkingnotes.com/networking-tutorials/differences-between-baseband-and-broadband-explained.html>

- Analog signals can be regenerated using amplifiers in order to travel longer distances.
- Broadband supports only unidirectional communication. It means, nodes connected at both ends of a medium can send or receive data but can't perform both actions simultaneously. Only one action is allowed at a time.
- For example, two nodes A and B are connected through a cable that uses broadband technology to transmit signals. When node A transmits signals, node B receives the transmitted signals and when node B transmits signals, node A receives the transmitted signals.
- The following image shows this example.

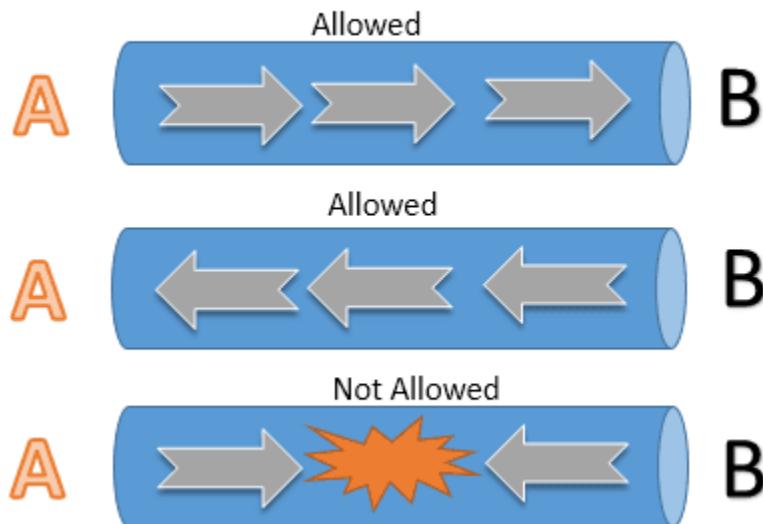


Image Source: <https://www.computernetworkingnotes.com/networking-tutorials/differences-between-baseband-and-broadband-explained.html>

- Broadband is typically used in an environment that transmits audio, video, and data simultaneously. For example, Cable TV Networks, Radio stations, and Telephone companies. Usually radio waves, coaxial, fiber-optic cables are used for broadband transmission.

Differences between baseband and broadband transmissions

Baseband transmission	Broadband transmission
Transmit digital signals	Transmit analog signals
To boost signal strength, use repeaters	To boost signal strength, use amplifiers
Can transmit only a single data stream at a time	Can transmit multiple signal waves at a time
Support bidirectional communication simultaneously	Support unidirectional communication only
Support TDM based multiplexing	Support FDM based multiplexing
Use coaxial, twisted-pair, and fiber-optic cables	Use radio waves, coaxial cables, and fiber optic cables

Mainly used in Ethernet LAN networks

Mainly used in cable and telephone networks

Cables Connectors

Type of network cable connector (such as Rj-45, J Rj-11, USB, MT-RJ, Coaxial BNC, LC Local Connector, MT-RJ, USB BNC and AUI) is used to connect what type of network cable.

USB (Universal Serial Bus)

- Universal Serial Bus (USB) is the de facto interface for computer peripherals to communicate with the personal computers. The interface that saw the light of day around

the mid-1990s was a joint effort of seven companies – Compaq, DEC, IBM, Intel, Microsoft, Nortel, and NEC. These companies were aiming to replace the then parallel ports and the external power chargers with a universal communication standard that could simplify data exchange and could double duty to supply power as well.

- Nowadays, USB is the standard and must-have interface on almost all motherboards, single board computers and the embedded microcontroller boards and almost every digital peripheral from regular computer peripherals like keyboard, mouse and joysticks to smart digital devices like cameras, flash drives, smartphones and tablets, all comes equipped with the USB port(s). Till now, USB 3.1 (launched in July 2013) has been released and the standard is now maintained and developed by USB Implementers Forum.



Image Source: <https://static.makeuseof.com/wp-content/uploads/2016/08/usb-3-micro-cable.jpg>

- Any USB interface connects two devices where one device is connected as Host and the other device connects as peripheral. For example, when a USB flash drive (Pen drive) is inserted into USB port of a personal computer, the flash drive is the peripheral and a personal computer is the host device. By the “Host”, here means that the data communication is managed by the host device with the help of relevant driver software. Many peripherals can be connected to a single host device. Even a single USB port can be extended to multiple USB ports using an extension hub.

-
- The initial versions of USB (pre-release versions and USB 1.0) were developed for slower devices. But by the year 2000, demand for high-speed communication had surged up and USB 2.0 was released to meet out the expectations.
 - The current version USB 3.0 supports four different data transfer modes:

Modes	Performance	Application
Low Speed	1.5Mbit/s	Keyboard, Mouse, Game Peripherals
Full Speed	12Mbit/s	Scanner, Printer, Digital audio
High Speed	480Mbit/s	Broadband, Mass storage, Imaging
Super Speed	5Gbit/s	Real Time Streaming, Portable Storage Devices

The new version releases of USB obviously have greater data transfer speeds for different file formats:

Data Size	Time Taken		
	USB 1.0	USB 2.0	USB 3.0
Image/MP3 (4MB)	5.3 Sec	0.1 Sec	0.01 Sec
Flash Drive (1 GB)	22 Min	33 Sec	3.3 Sec
HD-Movie (16 GB)	9.3 Hr	13.9 Min	70 Sec

Advantages of USB

- Ease of Use: USB was for obvious reasons designed to be a simplified interface. The simplicity of the interface lies with following aspects:
 - Single Interface for multiple devices: The versatile nature of USB removes the complexity of different connector type and hardware requirements for each peripheral
 - Auto-configuration: The operating system of the host device only needs to install the USB device driver for once. Later whenever the peripheral device is plugged

in, the driver is automatically loaded to configure the plugged in device. Usually, the device driver specific to any USB peripheral is automatically installed the first time device is connected with the host.

- Easy to expand: Generally personal computers (Motherboards) have 3 or 4 USB ports. In case if more USB ports are required, USB hubs can be used to add external ports.
- Compact Size: USB sockets are small in dimensions as compared to RS232 or parallel ports.
- No external power needed: The USB interface was developed from the first day to double duty as DC power supply. Any host device through its USB port can supply 5V DC delivering 500mA (USB 1.0 and 2.0) to 900 mA (USB 3.0) to the peripheral.
- Speed: USB provides various speed modes which make it more efficient and swift compared to RS232 and parallel ports. It offers speed ranges from 1.5Mbit/s to 5Gbit/s. With the introduction of USB 3.1 in 2013, the speed has been increased to 10Gbit/s. It is also referred as Super Speed+.
- Reliability: The USB protocol can catch errors during data transfer and notify the transmitter to retransmit the data. The generic USB driver and specific driver software ensure an error-free data communication.
- Low cost: With its versatile nature and high demand, it has become inexpensive to manufacture USB supported devices as the manufacturing can be easily scaled. So the components, connector, and cable are also easily available at low cost.
- Low power consumption: The USB devices generally works on +5V and consumes current in Mill ampere. During Suspend mode, the peripheral consumes 500 microamperes or less for USB 2.0 and 2.5 mill amperes or less for USB 3.0.
- Besides so many advantages there are some limitations which make USB ineffective for some task.

Limitations

- Speed: With the introduction of USB 3.0, it is possible to achieve 5Gbits/sec. But it is still lower than Gigabit Ethernet. The FireWire 800(IEEE-1394b) is also a competitor for USB.
- Peer to Peer Communication: As per the USB standard, the communication takes place between the host and the peripheral. Two hosts cannot communicate directly to each other. Same is the case for a peripheral. On the other hand, interfaces like FireWire supports peripheral to peripheral communication. For overcoming this limitation, the USB introduced the concept of OTG (On The Go). The OTG device normally functions as peripheral, but it can also function as host with some limited capability when required.
- Distance: According to USB standards, the connecting cable can be as long as 5 meters, beyond which, USB hubs need to be used for expanding the connectivity.
- Broadcasting: Universal Serial Bus does not provide the broadcasting feature, only individual messages can be communicated between host and peripheral.

RJ-11 (Registered Jack)

Standard telephone cable connectors, **RJ-11** has 4 wires (and RJ-12 has 6 wires). **RJ-11** is the acronym for Registered Jack-11, a four- or six-wire connector primarily used to connect telephone equipment.



Image Source: <https://microchipdeveloper.com/jlink:mchp-adapter>

RJ-11 Pin	Signal Name
-----------	-------------

1	VCC (5 volts regulated)
2	Power Ground
3	One Wire Data
4	One Wire Ground

RJ-45 (Registered Jack)

The acronym for Registered Jack-45 is RJ-45. The RJ-45 connector is an eight-wire connector that is commonly used to connect computers to a local area network (LAN), particularly Ethernet LANs. Although they are slightly larger than the more commonly used RJ-11 connectors, RJ-45s can be used to connect some types of telephone equipment.

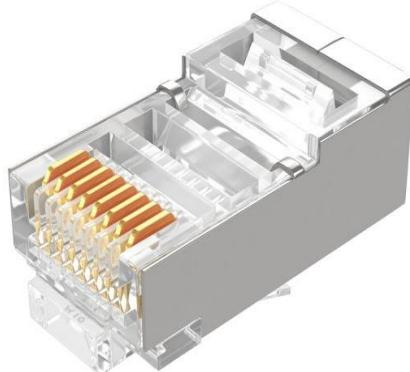


Image Source: <https://microchipdeveloper.com/jlink:mchp-adapter>

F-Type

The F connector is a type of RF connector commonly used for cable and universally for satellite television. They are also used for the cable TV connection in DOCSIS cable modems, usually with RG-6 tri-shield cable.

The F connector is inexpensive, yet has good performance up to 1 GHz. One reason for its low cost is that it uses the center wire of the coaxial cable as the pin of the male connector. The male connector body is typically crimped onto the exposed outer braid.

Female connectors have a 3/8-32 thread. Most male connectors have a matching threaded connecting ring, though push-on versions are also available.



Image Source: <https://www.computernetworkingnotes.com/networking-tutorials/network-cable-connectors-types-and-specifications.html>

ST (Straight Tip) and SC (Subscriber Connector or Standard Connector)

- Fiber network segments always require two fiber cables: one for transmitting data, and one for receiving.
- Each end of a fiber cable is fitted with a plug that can be inserted into a network adapter, hub, or switch. In the North America, most cables use a square SC connector (Subscriber Connector or Standard Connector) that slides and locks into place when inserted into a node or connected to another fiber cable; Europeans use a round ST connector (Straight Tip) instead.



Image Source: <https://www.computernetworkingnotes.com/networking-tutorials/network-cable-connectors-types-and-specifications.html>

Fiber LC (Local Connector)

- These connectors are used for single-mode and multimode fiber-optic cables. FC connectors offer extremely precise positioning of the fiber-optic cable with respect to the transmitter's optical source emitter and the receiver's optical detector. FC connectors feature a position locatable notch and a threaded receptacle.



Image Source : <https://www.computernetworkingnotes.com/networking-tutorials/network-cable-connectors-types-and-specifications.html>

MT-RJ (Mechanical Transfer Registered Jack)

- MT-RJ connectors are used with single-mode and multimode fiber-optic cables. The MT-RJ connectors are constructed with a plastic housing and provide for accurate alignment via their metal guide pins and plastic ferrules.
- Used for Gigabit Ethernet. To connect to modules with MT-RJ interfaces, use multimode fiber-optic cables.



Image Source: <https://www.computernetworkingnotes.com/networking-tutorials/network-cable-connectors-types-and-specifications.html>

Network cable Crimping and Testing Tools

- Cables are the backbone of a wired network. The stability, reliability, and performance of a wired network depend on cables. Installing and maintaining cables in a wired network is a difficult task.
- To make this task easier, a variety of network cable crimping and testing tools are available. In this tutorial, we will not only discuss some of the most common network cable crimping and testing tools but also understand their features and functions.

Network cable crimping tools

- Crimping tools are used for the following purposes.
- To cut the network cable of the required length from the bundle.
- To remove the outer and inner jackets of the network cable.
- To attach the connectors on both ends of the cable.
- Some crimping tools provide all the functionality while others provide one or two functionalities.
- The most common twisted-pair network cable crimping tools are described below.
 - **Wire Cutter:** - To cut the network cable of the required length from the bundle, you can use any standard wire cutter tool or can use a wire cutter tool that is specially designed for the twisted-pair cable. A twisted-pair wire cutter usually includes additional blades for stripping the wire.
 - **Wire Stripper:** - This tool is used to remove the outer and inner jackets of the network cable. Typically, you do not need to purchase this tool separately as all standard twisted-pair wire cutters are equipped with wire-stripers.

- o The following image shows two twisted-pair wire cutter tools equipped with wire-strippers.



Image source: <https://www.computernetworkingnotes.com/networking-tutorials/network-cable-crimping-and-testing-tools.html>

Crimp tool: This tool is used to attach the connectors to the cable. Typically, this tool also includes a wire-cutter and wire-stripper. So if you buy a crimp tool, you don't have to buy a wire-cutter and wire-striper separately. The following image shows a crimping device equipped with a wire-stripper and wire-cutter.



Image source: <https://www.computernetworkingnotes.com/networking-tutorials/network-cable-crimping-and-testing-tools.html>

Network cable testing and troubleshooting tools

A network cable testing and troubleshooting tool is used for the following purposes.

- To measure the length of a segment or network cable.
- To detect loose connectors.
- To identify an un-labelled network cable from all network cables.
- To find a break in the network cable.
- To certify the cable installation.

Troubleshooting tools

- **Cable certifier:** This device thoroughly tests a network cable and certifies that the cable installation meets a special wiring standard such as Cat 5e, Cat 6, Cat 6a, and so forth. This device can check and test total segment length, crosstalk, noise, wire map, resistance, impedance, and the capability to transfer data at the maximum frequency rated for the cable. The following image shows a network cable certifier.

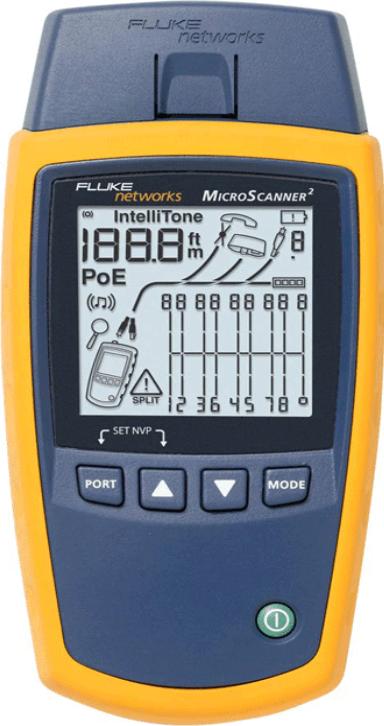


Image source: <https://www.computernetworkingnotes.com/networking-tutorials/network-cable-crimping-and-testing-tools.html>

- Since this device performs a complete test and certifies the cable installation, it will cost you more than all the other test devices listed in this section. If you have a mid-size network or if you can buy this device, then you should always buy and use this device to manage network cables.

Basic cable tester: If you can't afford a network cable certifier, you can buy and use this device to manage your network cables. Besides certifying the cable installation, this device provides all remaining functionalities of a network cable certifier. It can test cable length, cross talk, and breaks in the cable. It can also check whether the connectors on both ends of a network cable are properly attached or not. The following image shows a basic network cable tester tool.



Image source: <https://www.computernetworkingnotes.com/networking-tutorials/network-cable-crimping-and-testing-tools.html>

Tone generator and the probe: This device is used to trace the unlabeled network cables. This device comes in two pieces: the tone generator and the probe. The tone generator generates tones or signals and places them on the network cable. The probe detects these signals on the other end of the cable.

- You can use this tool to identify network cables that run from a central location to remote locations. For example, if you are working on a patch-panel or switch and trying to figure out which network cable connects back to an end-device (such as a PC), then you can use this device.

- Place a tone generator at one end of the connection (end-device), and use the probe on another side (switch or patch-panel) to determine which network cable the tone generator is connected to. The following image shows an example of a tone generator and probe.



Image source: <https://www.computernetworkingnotes.com/networking-tutorials/network-cable-crimping-and-testing-tools.html>

Time domain reflectometer: This device is used to measure the length of a network cable as well as the breaks in the cable. This device transmits a signal on one end and measures the time the signal takes to reach the end of the cable. You can also use this device to find breaks in the cable. For example, this device can tell you approximately how far the break is located in the cable. The following image shows a time domain reflectometer.



Image source: <https://www.computernetworkingnotes.com/networking-tutorials/network-cable-crimping-and-testing-tools.html>

Network Topology

Network topology is the layout of a network. It consists of two parts; physical and logical. The physical part describes the physical layout of a network while the logical part describes how the data flows in that network. Both, physical and logical parts are also known as the physical topology and the logical topology.

Physical part (topology) + Logical part (topology) = Network topology

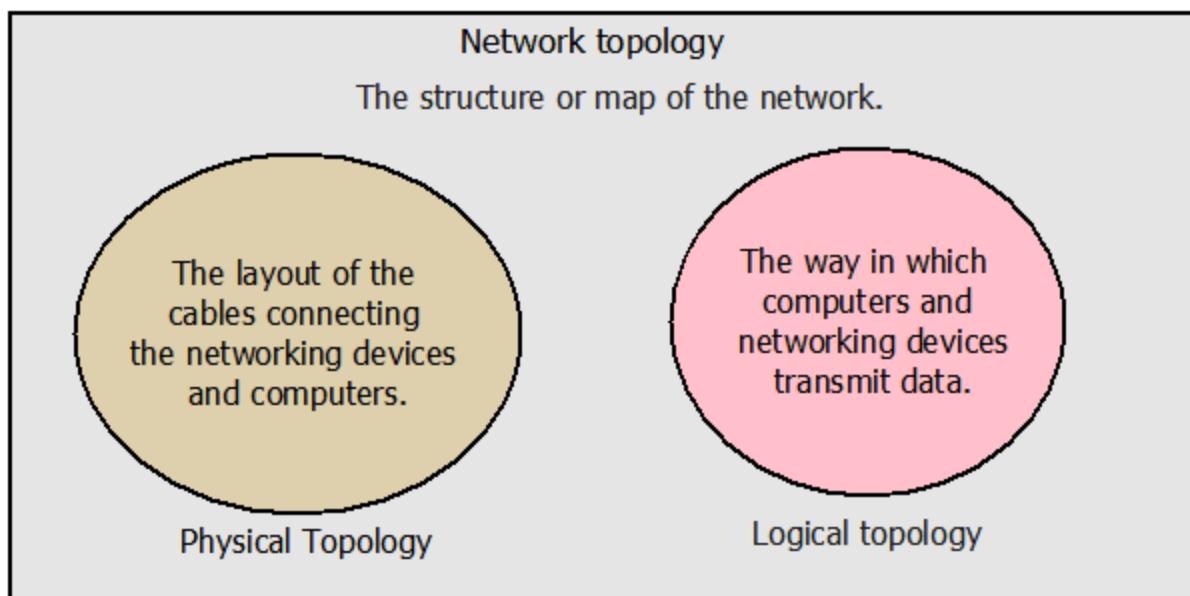


Image Source : <https://www.computernetworkingnotes.com/networking-tutorials/network-topologies-explained-with-examples.html>

Two different types of network topologies

- Physical network topology is the placement of the various components of a network and the different connectors usually represent the physical network cables, and the nodes represent usually the physical network devices (like switches).
- Logical network topology illustrates, at a higher level, how data flows within a network. Usually, in campus LAN topologies, focusing at layer 2 (at the switching layer), some

kind of a structured, multi-tier models are used to simplify the design and the network implementation.

The hierarchical internetworking model

- The hierarchical internetworking model is a three-layer network topology that divides enterprise networks into three layers:
 - Core, composed by the highest-speed switches, with high resiliency and usually routing and other high-level functions.
 - Distribution or aggregation, composed by high-speed switches with redundancy and availability.
 - Access, composed of switches to which the client devices are connected.
- There are also other models, for example a simplified two-layer model (with only core and access layers, mostly used in the SMB segment) or also other new types of models like the leaf-spine model, which focuses more on cloud computing or data center environments.
- Anyway, the terms core, distribution/aggregation and access are so commonly used, that the switches are usually classified for their intended purpose. For example see the Aruba Switch portfolio.
- Common logical topology of a three-layer model:

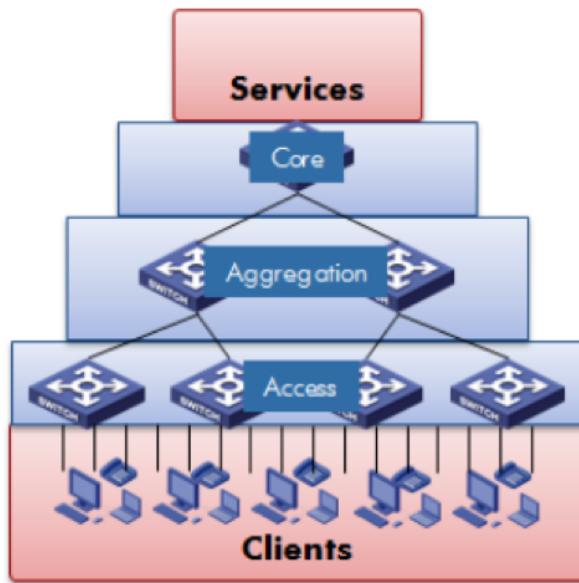


Image Source: <https://www.ciscopress.com/articles/article.asp?p=2202410&seqNum=4>

Three-layer hierarchical layer 2 topology

- Potentially this can be directly translated in a physical topology, will be a totally non-redundant solution, where each node is just a single switch and the switches in each layer have a single link to switches in the adjacent layers.

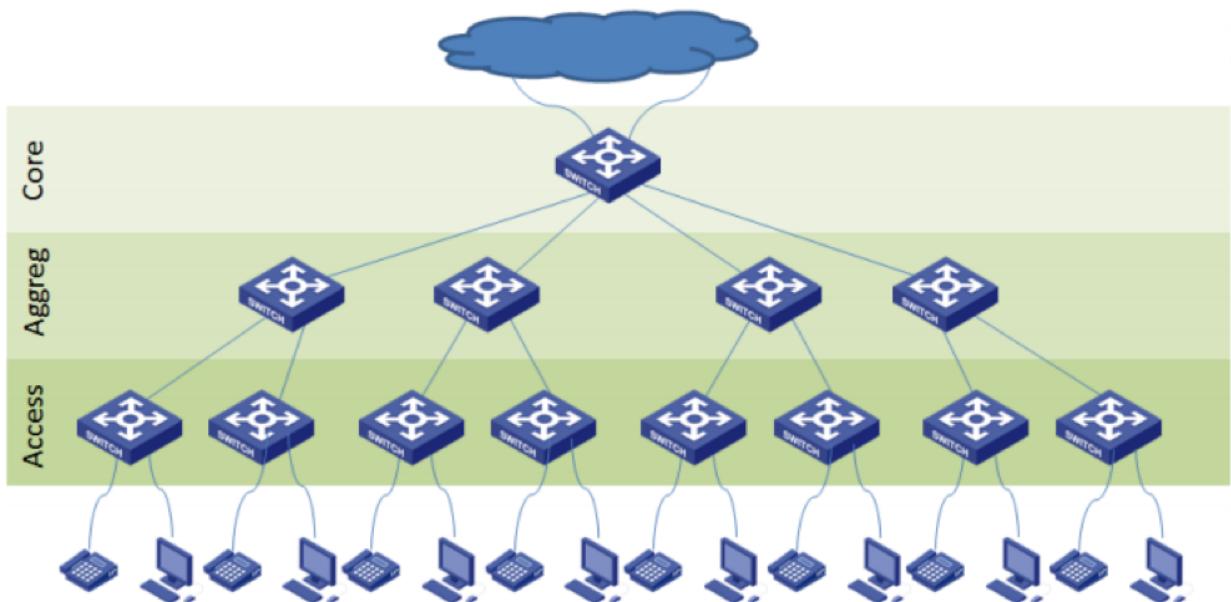


Image Source: <https://www.ciscopress.com/articles/article.asp?p=2202410&seqNum=4>

Leaf-Spine Network Topology

- The leaf-spine topology is a special case of a two-layer model, designed to build fast, predictable, scalable and efficient data centre network infrastructure.
- The main difference between the previous topology is the spine level, where there are more independent switches that are more scalable. The switches on the spine level are not connected to each other.
- Leaf-spine network topology
- Another big difference is that the leaf-spine topology is natively a layer 3 network that uses layer 3 routing and each node is a router. Usually, all routes are configured in an active state through the use of Equal-Cost Multipath (ECMP) to have all links active.
- So, the first big problem with this topology is how stretch layer 2 networks (usually the different VLANs) on a layer 3 network? Network virtualization and protocols like VxLAN can help in this goal.
- Another aspect is how match this topology in a physical topology? Can it be done 1:1? Depending on your type of network and level, maybe. In some cases, each leaf node represents a couple of physical switches (usually the top-of-rack switches) configured to be a single logical switch (with stacking or virtual chassis features).
- The leaf-spine topology is not really used in the SMB market.

Auto-Discover Network Topologies

- There are some tools and protocols that are useful to build your network topology.
- In most cases those tools are used in the Wi-Fi network to simplify the deployment and configuration.
- But there are also some interesting options for the wired LAN. For example, Link Layer Discovery Protocol (LLDP) is a vendor-neutral link layer protocol used by network devices for advertising their identity, capabilities and neighbours on a local area network

based on IEEE 802 technology, specifically 802.1AB. This permits automatically discovery and advertising of the node neighbours.

- Several tools use this protocol to automatically build the network topology. For example, in Aruba Central, the topology map provides a graphical representation of the network layout, details of the devices deployed in a branch site, and the health of the links.

Bus topology

- In this topology, all computers connect through a single continuous coaxial cable. This cable is known as the backbone cable. Both ends of the backbone cable are terminated through the terminators. To connect a computer to the backbone cable, a drop cable is used. To connect the drop cable to the computer and backbone cable, the BNC plug and BNC T connector are used respectively.
- The following image shows the bus topology.

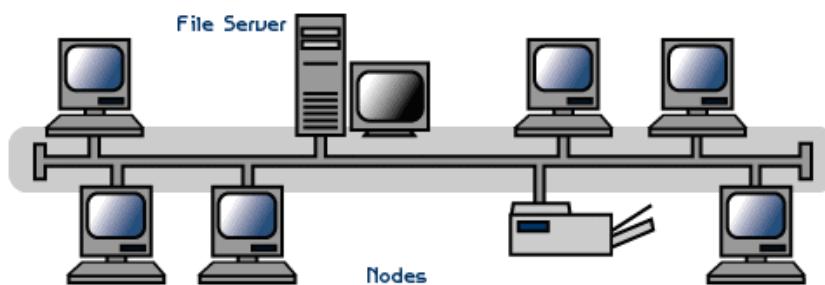


Image Source: <https://fcit.usf.edu/network/chap5/chap5.htm>

- When a computer transmits data in this topology, all computers see that data over the wire, but only that computer accepts the data to which it is addressed. It is just like an announcement that is heard by all but answered only by the person to whom the announcement is made.

Advantages and Disadvantages

Advantages	Disadvantages
It is very simple to install.	It is very difficult to troubleshoot.
It uses less cable than other topologies.	It provides slow data transfer speed.
It is relatively inexpensive.	A single fault can bring the entire network down.

-
- This topology is no longer used. But there was a time when this topology used to be the first choice among the network administrators. The concept that this topology uses to transmit the data is also used in the other topologies.

Star topology

- In this topology, all computers connect to a centralized networking device. Usually, a networking switch or a Hub (in earlier days) is used as the centralized device. Each computer in the network uses its own separate twisted pair cable to connect to the switch. Twisted pair cable uses RJ-45 connectors on both ends.
- The following image shows an example of the star topology.

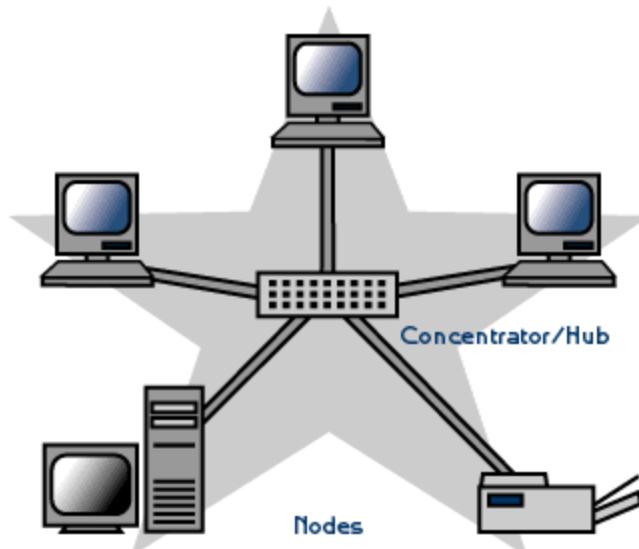


Image Source: <https://fcit.usf.edu/network/chap5/chap5.htm>

- To transmit data, the star topology uses the same concept which the bus topology uses. It means, if you build a network using the star topology, then that network will use the bus topology to transmit the data.

Lists of advantages and disadvantages

Advantages	Disadvantages
It is easy to install.	It uses more cables than other topologies.
Relocating of computers is easier than other topologies.	If the centralized device fails, it brings the entire network down.
Since each computer uses its own separate cable, a fault in cable does affect other computers of the network.	The total installation cost is higher than the other topologies.
Troubleshooting is relatively easy.	Use the twisted pair cable which is prone to break.
It provides higher data transfer speed.	Too many cables make the network messy.

- In modern computer networks, the star topology is the king. Nearly all new network installations, including small home and office networks, use some form of the star topology.

Hybrid Topology

- This topology is a mix of two or more topologies. For example, there are two networks; one is built from the star topology and another is built from the bus topology. If we connect both networks to build a single large network, the topology of the new network will be known as the hybrid topology.
- You are not restricted to the bus and star topologies. You can combine any topology with another topology. In modern network implementations, the hybrid topology is mostly used to mix the wired network with the wireless network.
- The following image shows an example of the hybrid network topology.

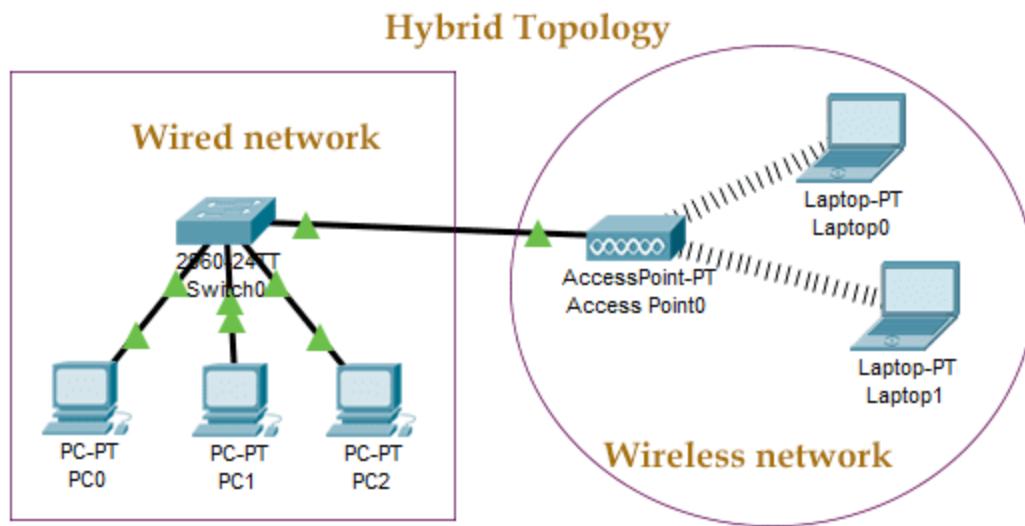


Image source: <https://www.computernetworkingnotes.com/networking-tutorials/network-topologies-explained-with-examples.html>

- Unlike a wired network, a wireless network does not use cables to connect computers. A wireless network uses radio spectrum to transmit data.

Ring Topology

What is Ring Topology?

In **ring topology** each terminal is connected to exactly **two nodes**, giving the network a circular shape. Data travels in only one pre-determined direction.

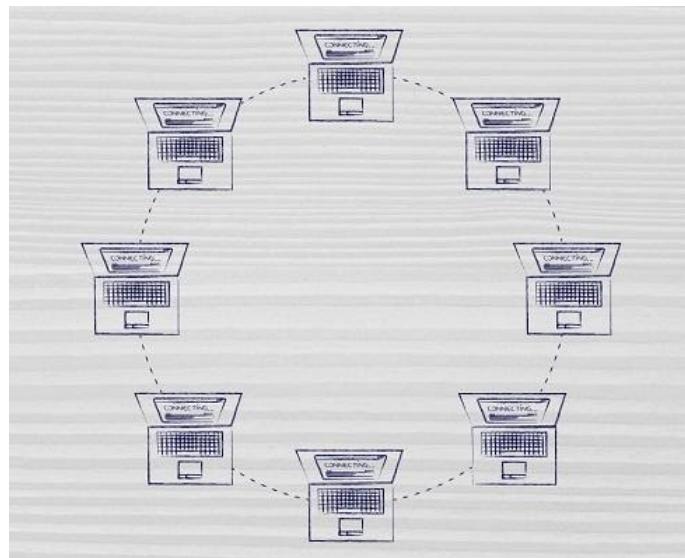


Image 1: Ring Topology

Reference:https://www.tutorialspoint.com/communication_technologies/images/ring_topology.jpg

When a terminal has to send data, it transmits it to the neighboring node which transmits it to the next one. Before further transmission data may be amplified. In this way, data traverses the network and reaches the destination node, which removes it from the network. If the data reaches the sender, it removes the data and resends it later.

Advantages of Ring Topology

These are the advantages of using ring topology –

-
- Small cable segments are needed to connect two nodes
 - Ideal for optical fibers as data travels in only one direction
 - Very high transmission speeds possible

Disadvantages of Ring Topology

These are some the disadvantages of using ring topology –

- Failure of single node brings down the whole network
- Troubleshooting is difficult as many nodes may have to be inspected before faulty one is identified
- Difficult to remove one or more nodes while keeping the rest of the network intact

Mesh Topology

In Mesh Topology, all the computers are inter-connected to each other in a network. Each computer not only sends its own signals but also relays data from other computers. This type of topology is very expensive as Its very difficult to establish the connections of the mesh topology. In a Mesh topology every node has a point-to-point connection to the other node. The connections in the mesh topology can be wired or wireless.

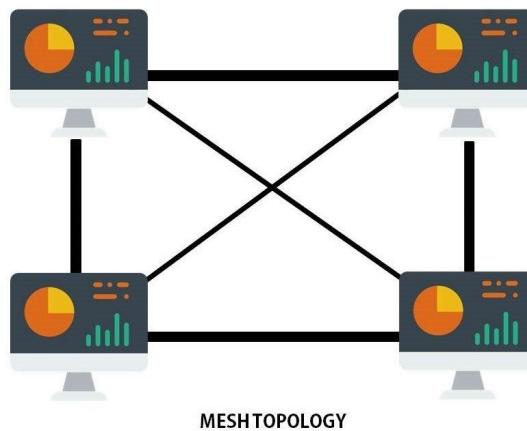


Image 2: Mesh Topology

Reference:<https://computernetworktopology.com/wp-content/uploads/2019/03/mesh-topology-847x700.jpg>

Mesh Topology can be divided into two types:

1. Fully connected mesh topology
2. Partially connected mesh topology

1) Fully Connected Mesh Topology:

A fully connected mesh topology has all the computers connected to every other computer. Full Mesh is a network in which devices are organized in a mesh topology. A full mesh topology provides a great deal of redundancy, but because it can be prohibitively expensive to implement, it is usually reserved for network backbones. Even after considering the cost and the redundancy

factor of this network, its main advantage is that the network traffic can be redirected to other nodes if one of the nodes goes down. Full mesh network is used only for backbone networks.

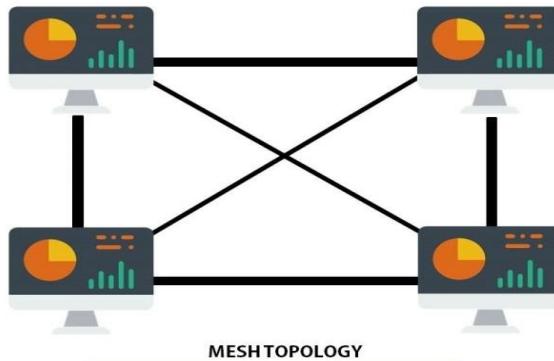


Image 3: Fully Connected Mesh Topology
Reference:https://i0.wp.com/computernetworktopology.com/wp-content/uploads/2019/03/mesh_topology.jpg?resize=768%2C748&ssl=1

2) Partial Connected Mesh Topology:

Partial Mesh topology is more practical as compared to full mesh topology. In **partially connected mesh topology**, all the nodes are not necessary to be connected with each other in a network. This partial mesh topology is less costly compared to full mesh topology and also it reduces the redundancy.

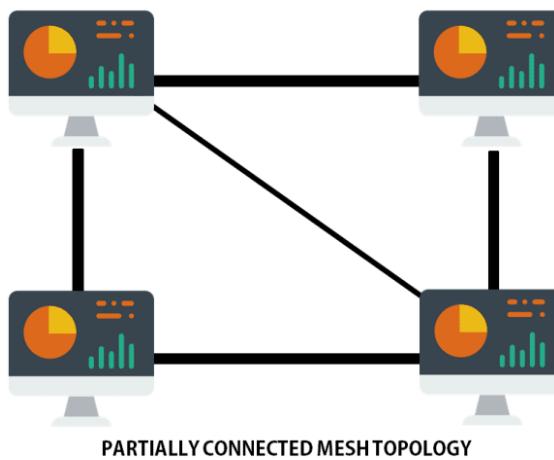


Image 4: Partially Connected Mesh Topology

References:<https://i0.wp.com/computernetworktopology.com/wp-content/uploads/2019/03/PARTIALLY-CONNECTED-MESH-TOPOLOGY.png?resize=768%2C710&ssl=1>

To find the no: of physical links in a **fully connected mesh topology** with n nodes, we first consider that each node must be connected to every other node.

n(n – 1) for half duplex communication

n(n -1) /2 for full duplex communication.

Characteristics of Mesh Topology:

- Fully connected
- Robust
- Not flexible
- Poor expandability

Advantages of Mesh Topology:

- There is no traffic problem as there are dedicated point to point links for each computer.
- It has multiple links, so if one route is blocked then other can be accessed for data communication.
- It provides high privacy and security.
- Fault identification is easy because of point-to-point connection.

Disadvantages of Mesh Topology:

- Mesh topology requires high no of cables and I/O ports for the communication.

-
- Installation is very difficult in mesh topology, as each node is connected to every node.
 - Mesh topology is costly compared to the other network topologies i.e. star, bus, point to point topology.

Synchronous Transmission

In synchronous transmission, data moves in a completely paired approach, in the form of chunks or frames. Synchronisation between the source and target is required so that the source knows where the new byte begins, since there are no spaces included between the data.

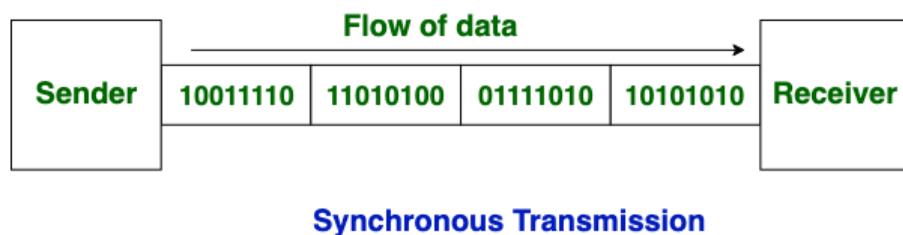


Image 5: Synchronous Transmission

Reference: <https://www.geeksforgeeks.org/difference-between-synchronous-and-asynchronous-transmission/>

Synchronous transmission is effective, dependable, and often utilized for transmitting a large amount of data. It offers real-time communication between linked devices.

An example of synchronous transmission would be the transfer of a large text file. Before the file is transmitted, it is first dissected into blocks of sentences. The blocks are then transferred over the communication link to the target location.

Because there are no beginning and end bits, the data transfer rate is quicker but there's an increased possibility of errors occurring. Over time, the clocks will get out of sync, and the target device would have the incorrect time, so some bytes could become damaged on account of lost bits. To resolve this issue, it's necessary to regularly re-synchronize the clocks, as well as to make use of check digits to ensure that the bytes are correctly received and translated.

Characteristics of Synchronous Transmission

- There are no spaces in between characters being sent.
- Timing is provided by modems or other devices at the end of the transmission.
- Special 'syn' characters goes before the data being sent.
- The syn characters are included between chunks of data for timing functions.

Examples of Synchronous Transmission

- Chatrooms
- Video conferencing
- Telephonic conversations
- Face-to-face interactions

Asynchronous Transmission

In asynchronous transmission, data moves in a half-paired approach, 1 byte or 1 character at a time. It sends the data in a constant current of bytes. The size of a character transmitted is 8 bits, with a parity bit added both at the beginning and at the end, making it a total of 10 bits. It doesn't need a clock for integration—rather, it utilises the parity bits to tell the receiver how to translate the data.

Synchronous Transmission

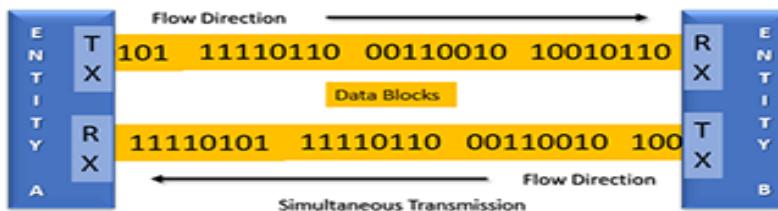


Image 6: Asynchronous Transmission

Reference: https://study.com/cimages/multimages/16/c5555ee1-ae21-409d-a2f3-24cb3d36df37_stm-350.png

It is straightforward, quick, cost-effective, and doesn't need 2-way communication to function.

Characteristics of Asynchronous Transmission

- Each character is headed by a beginning bit and concluded with one or more end bits.
- There may be gaps or spaces in between characters.

Examples of Asynchronous Transmission

- Emails
- Forums
- Letters
- Radios

-
- Televisions

Point of Comparison	Synchronous Transmission	Asynchronous Transmission
Definition	Transmits data in the form of chunks or frames	Transmits 1 byte or character at a time
Speed of Transmission	Quick	Slow
Cost	Expensive	Cost-effective
Time Interval	Constant	Random
Gaps between the data?	Yes	No
Examples	Chat Rooms, Telephonic Conversations, Video Conferencing	Email, Forums, Letters

Synchronous and Asynchronous Transmission

Synchronous vs. Asynchronous Transmission

1. In synchronous transmission data is transmitted in the form of chunks, while in asynchronous transmission data is transmitted one byte at a time.

-
2. Synchronous transmission needs a clock signal between the source and target to let the target know of the new byte. In comparison, with asynchronous transmission, a clock signal is not needed because of the parity bits that are attached to the data being transmitted, which serves as a start indicator of the new byte.
 3. The data transfer rate of synchronous transmission is faster since it transmits in chunks of data, compared to asynchronous transmission which transmits one byte at a time.
 4. Asynchronous transmission is straightforward and cost-effective, while synchronous transmission is complicated and relatively pricey.
 5. Synchronous transmission is systematic and necessitates lower overhead figures compared to asynchronous transmission.

Both synchronous and asynchronous transmission have their benefits and limitations. Asynchronous transmission is used for sending a small amount of data while synchronous transmission is used for sending bulk amounts of data. Thus, we can say that both synchronous and asynchronous transmission are essential for the overall process of data transmission.

Configure different protocol services

In this section, we will read about:

- User Authentication Strategy
- OU Structure
- User Environment
- Group Policies
- AGDLP Process
- Different types of protocols - TCP/IP,HTTP, FTP,SMTP
- OSI Model
- Media Access Method
- DNS services
- DHCP services
- WINS services
- RAS services
- Web services
- Proxy Services

User Authentication Strategy

A user authentication policy is a process in which you verify that someone who is attempting to access services and applications is who they claim to be. This can be accomplished through a variety of authentication methods, such as entering a password into your laptop or phone or a PIN number into the ATM.



Image 1: Authentication Strategies

Reference:https://www.cisco.com/c/en/us/products/security/identity-services-engine/what-is-user-authentication-policy/_jcr_content/Grid/subcategory_atl_d1dc/layout-subcategory-atl/anchor_info_6e7e/image.img.png/1568923193753.png

What is the purpose of authentication?

Authentication is used to verify that you are who you say you are. After a user's identity is confirmed, for instance with a username and password, that identity may be used in an authorization policy to determine the appropriate access privileges. Organizations today must

ensure that the right users are given access to the right resources, whether it is physical or--increasingly--digital.

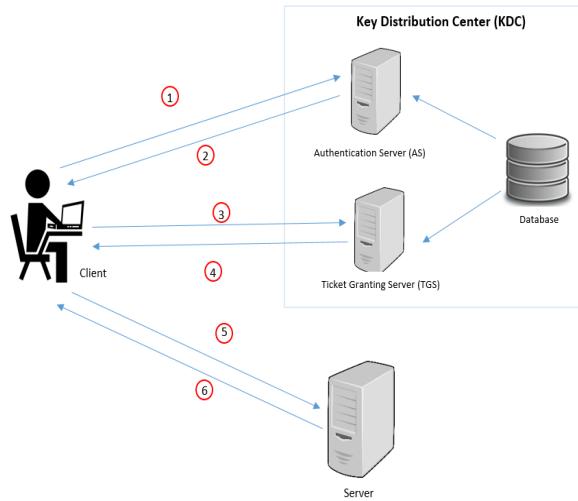


Image2: Authentication Strategy

Reference:

<https://medium.com/@dewni.matheesha/kerberos-the-computer-network-authentication-protocol-a198309339b7>

What are the different authentication protocols?

Network authentication protocols are used to help securely transfer identity credentials for authentication between the subject (user or device) and the authentication server. There are several different authentication protocols for network access control, including:

- Kerberos
- Extensible Authentication Protocol (EAP)
- IEEE 802.1X
- Remote Authentication Dial-In User Service (RADIUS)
- Terminal Access Controller Access-Control System (TACACS)

How do I benefit from a user authentication policy?

A user authentication policy may be used to help ensure that only the intended audience is accessing certain assets in your organization. User authentication policies strive to ensure that the person requesting sensitive information and data is the right person to access that information.

Types of user authentication

Two-factor authentication (2FA)

Two-factor authentication, also known as multifactor authentication (MFA), is a two-step authentication process. It combines a username and password, or PIN, with a physical or mobile token for extra security. This combination of authentication factors makes it more difficult for a potential intruder to gain access.



Image3: Two-Factor Authentication

Reference: <https://www.avatier.com/blog/defining-multi-factor-authentication-need-now/>

Three-factor authentication (3FA)

Three-factor authentication combines what you know, what you have, and what you are. Similar to a two-factor authentication, what you know and what you have typically involves usernames

and passwords and a one-time token. However, with 3FA there is an additional factor--what you are--which uses biometrics such as fingerprints to verify a user's identity.



Image 4: Three Factor Authentication

Reference: <https://www.avatier.com/blog/defining-multi-factor-authentication-need-now/>

Four-factor authentication (4FA)

Four-factor identification is another form of layered security that involves knowledge, possession, inherence, and location. As with 3FA, knowledge, possession, and inherence consist of passwords and PINs, token authentication, and biometrics. For an extra layer of security, 4FA also uses verification of a user's login to authenticate the user.



Image 5: Four Factor Authentication

Reference: <https://www.avatier.com/blog/defining-multi-factor-authentication-need-now/>

Organization Unit

The Organizational Unit (OU) is a sub-division in an Active directory into which, we can place users, groups, computers and other organizational units. Using organizational units, we can create containers within a domain that represent the hierarchical, logical structures within organization. We can manage the configuration and use of accounts and resources based on your organizational model.

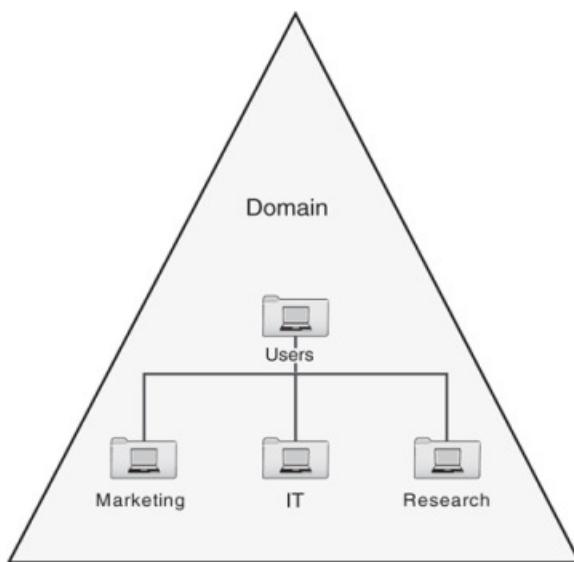


Image 6: Organization Unit for Domain

Reference:

<https://medium.com/@dewni.matheesha/kerberos-the-computer-network-authentication-protocol-a198309339b7>

An organizational unit (OU) is a container that logically organizes and groups Active Directory objects within domains. OUs are not part of the DNS namespace. They organize Active Directory objects into logical administrative groups. OUs therefore serve as containers in which users can create and manage Active Directory objects. OUs are considered the smallest unit to which an Administrator can assign permissions to resources within Active Directory.

An OU enables users to apply security policies, deploy applications, delegate administrative control for Active Directory objects, and run scripts. An important thing to understand is that OUs are not security principals. The user accounts, group accounts, and computer accounts within the OUs are security principals.

The Active Directory object types that can be located in OUs are listed below

User, group, and computer objects; shared folders, printers, applications, and other OUs from the same domain.understanding organizational units

User objects are the main security principals used in Active Directory. A user object consists of the user name, password, group membership details, and other information that define the user. A group object prevents Administrators from setting individual user permissions. A set of users can be grouped then assigned the appropriate permission to Active Directory objects. A computer object contains information on a computer that is a member of the domain. Because OUs can contain other OUs, an Administrator can hierarchically group resources and other Active Directory objects to reflect the organization's structure. The process of adding OUs to other OUs in a hierarchical manner is referred to as nesting OUs.

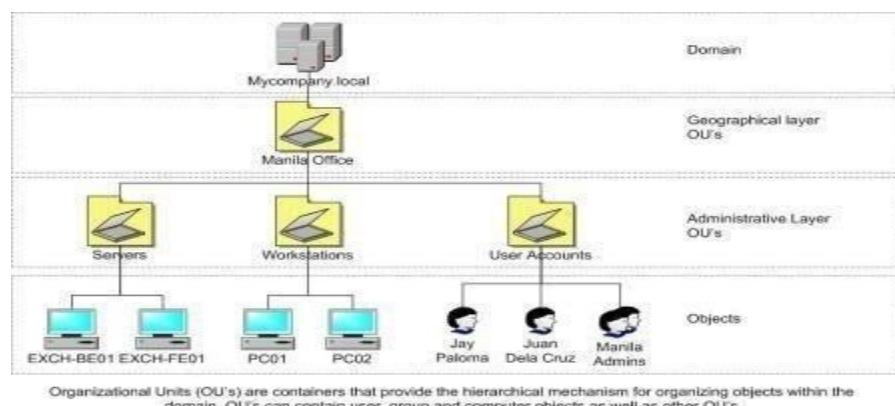


Image 7: Organization Unit

Reference: <https://www.tech-faq.com/wp-content/uploads/understanding-organizational-units.jpg>

A few benefits of OUs are summarized below

- OUs can be nested to support different hierarchy levels
- Each domain in the Active Directory environment can have its own OU structure. One domain's OU structure is independent of another domain's OU structure.
- It is fairly simple to change an OU structure. OU structures are much more flexible than domain structures.
- Objects in child OUs can inherit OU configuration settings.
- Group Policy settings can also be applied to OUs

Users can delegate administrative control of Active Directory objects through OUs

OUs typically delegate administrative control for Active Directory objects to hide Active Directory objects and to administer Group Policy. When a user delegates administrative control over an OU, he/she enables other users or groups to administer the OU. Higher level administrators usually delegate administrative control. Delegation of control over OUs enables users to transfer management tasks to various users within the organization.

The administrative tasks that are usually delegated are listed below

- Create, delete, and manage user accounts
- Create, delete, and manage groups
- Reset passwords on user accounts
- Read all user information
- Modify group membership
- Manage Group Policy links

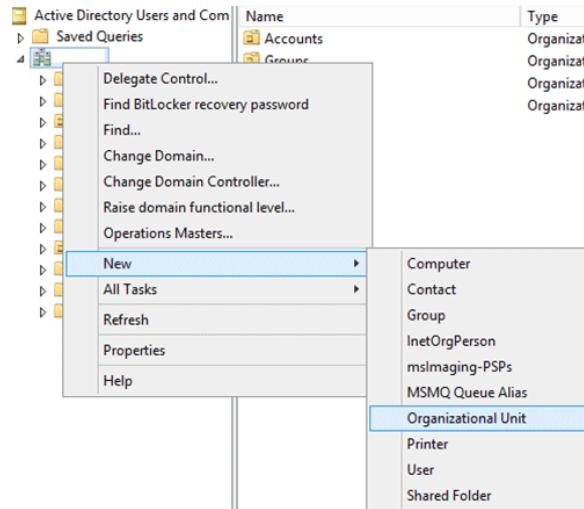


Image 8: Tasks of OU

Reference: <https://medium.com/@dewni.matheesha/kerberos-the-computer-network-authentication-protocol-a198309339b7>

Administrators that are responsible for domain management activities have full control over all Active Directory objects within the domain. This is the default configuration setting. These Administrators therefore create domain controllers, domains, and the OU for the domain. If there are units within the organization that need to manage and define their own OU structure, users can delegate the Full Control permission for an OU to these individuals. This would enable those individuals to perform all the previously mentioned management activities for the particular OU. In other instances, users might need to only delegate control for specific object classes for an OU.

As mentioned before, OU can also hide sensitive domain objects from particular users. This is done by creating an OU for those domain objects that will be hidden or that the user does not want everyone to view, then assigning only those users that should be allowed to give these objects the necessary permissions. After the appropriate permissions are configured for the OU, move the sensitive Active Directory objects to the OU.

User Environment

What is User Environment?

A user environment is a set of distributed objects that collectively, completely characterize the activity of a user in a universal system.

A user environment is then an abstraction that captures the essence of a user in a universal system and consists of:

- environment identification
- user profile
- user location
- user activity

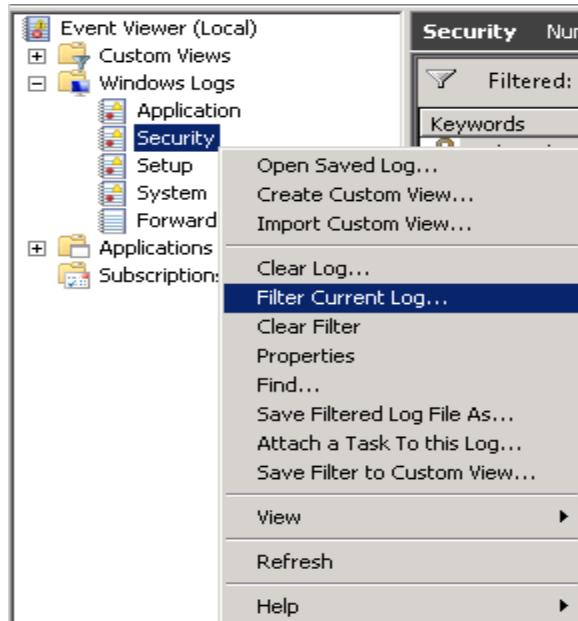


Image 9: User Environment

Reference: <https://medium.com/@dewni.matheesha/kerberos-the-computer-network-authentication-protocol-a198309339b7>

Group Policies

Group policies can be defined as a collection of permissions that users can apply to Active Directory objects. Group policy settings can be linked to sites, domains, and OUs, and can apply to user accounts, computer accounts, and group accounts. Group policy settings are applied to OUs in the form of Group Policy Objects (GPOs). The GPO contains the Group policy settings that can be applied to users and computers in an OU.

Group policy is applied in the following order

- Local computer policy
- Site policy
- Domain policy
- OU policy, commencing with the parent OU

However, Active Directory includes a No Override and Block Inheritance setting that can be used to control how policies are applied. The No Override setting can be enabled to stop a child OU's policy setting from overwriting the parent OU policy setting. The Block Inheritance setting can be enabled to prevent a child OU and any objects that it contains from inheriting group policy settings from its parent OU.

Planning an OU Structure

When planning an OU structure, identify and define the following:

- The manner in which the enterprise is managed
- The OU structure for each domain
- The OUs that need to be created
- The manner in which group policy needs to be applied.

-
- The OUs for which administrative control will be delegated and the users that control will be delegated to.
 - The sensitive Active Directory objects to be hidden from users.

The following strategy is generally recommended for an OU structure:

- Create an OU with the end result being that one group administers the Active Directory objects within the OU.
- This enables users to grant the particular group the identical rights to all Active Directory objects in the particular OU and to the OU itself. Avoid an OU structure that results in the same group needing to manage objects over many different OUs.
- This would mean that the appropriate rights would need to be individually granted in each OU.

It is also good practice to assign an owner to each OU. The OU's owner would be responsible for performing the following management tasks:

- Create, delete, and manage child OUs
- Apply group policy
- Delegate administrative control over objects in the OU

Also, separate service admin objects from the remainder of domain objects. Hiding service admin objects prevents all domain users from viewing its properties and attributes and it also enables users to effectively apply group policy so that only service admin users are able to perform certain administrative tasks.

Group Policies

Group Policies are computer or user settings that can be defined to control or secure the Windows server and client infrastructure. Understanding GPO in Windows Server 2012 before actually configuring and applying policy settings is very important. It is easy to understand GPO in Windows Server 2012. There are some **new features of GPO in Windows Server 2012**.

Understanding GPO in Windows Server 2012

Two main components of GPO are,

- GPO Object and
- GPO Policy Settings.

GPO Object: – GPO Object is an active directory object that has various group policy settings. These policy settings can be user settings or computer settings and can be applied to user or computers. GPO objects are stored in GPO container. The GPO object is stored in active directory database and each object has its own unique **GUID** (Globally Unique Identifier).

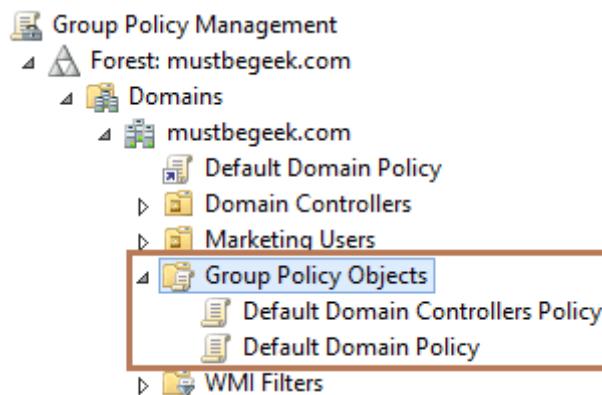


Image 11: Group Policy Object

Reference: <https://www.mustbegeek.com/understanding-gpo-in-windows-server-2012/#.Xssz3TozbIV>

GPO Policy Settings: – GPO policy settings are the real settings within GPO object that defines particular action. GPO policy settings comes from GPO templates which are stored in **SYSVOL** folder of each domain controller. For example, Prohibit Access to Control Panel is a GPO policy setting that will simply disable access to control panel. Most of the GPO settings can be enabled, disabled or not configured. The example is shown below,

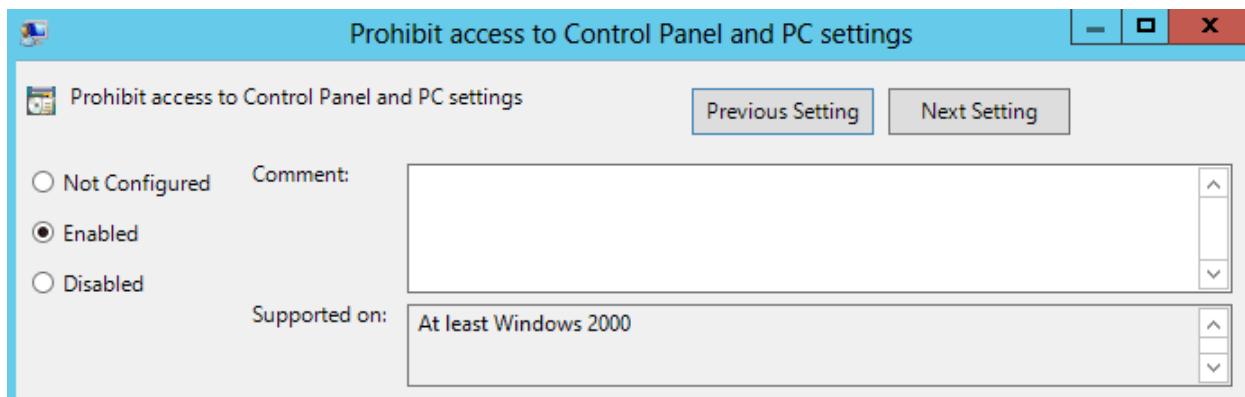


Image 12: Group Policy Settings

Reference: <https://www.mustbegeek.com/understanding-gpo-in-windows-server-2012/#.Xssz3TozbIV>

When you create a group policy, the GPO object is created and stored in GPO container in active directory and at the same time, GPO template is created and stored in **SYSVOL** folder. After creating a group policy, it can be linked to Sites, Domains and OUs.

Group policy is process in the order of LSDOU: –

1. Local Group Policy
2. Sites
3. Domains
4. Organizational OUs

There are certain things that you should remember while creating and applying GPO settings. As stated earlier there are computer settings and user settings of each GPO object. Computer settings are applied at startup of the client machine. User settings are applied at use logon.

Policies refresh can be initiated manually by using, **C:\> gpupdate /force command** or **C:\> Invoke-Gpupdate** PowerShell cmdlet.

In fresh domain controller there are two default group policy settings configured. They are: –

1. **Default Domain Policy:** – This policy is linked to the entire domain and has policies like password policies, account lockout policies and kerberos protocol policies. It is recommended that not to edit this policy. If you want to link new group policy then create new GPO and link to the domain.
2. **Default Domain Controller Policy:** – This policy setting is applied to domain controllers and is linked to domain controllers OU. This policy affects domain controllers only.

AGDLP Process

Introduction

AGDLP stands for Account, Global, Domain Local, Permission.

AGDLP is a role based strategy that is designed to provide flexible resource management using groups.

Managing those permissions and group memberships are simplified and configured to allow for multiple domains.

AGDLP - ADDLP stands for the following.

A for Accounts.

G for Global Group.

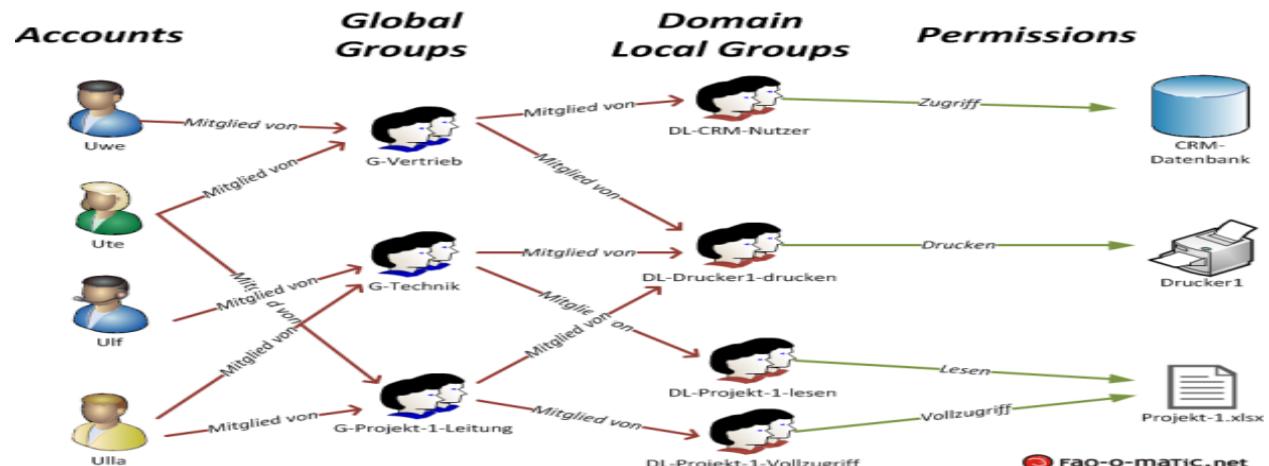


Image 1- <https://nlabs.files.wordpress.com/2020/02/windows-agdlp.png?w=620/>

Advantages

- AGDLP is a role base strategy for applying permissions, as a user changes their role in an organization.
- Looking at the users in the groups, you can quickly determine who has access to which resources in your domain.
- Domain Local Groups can only be used in the domain that the group was created in.

- Helps for auditing.

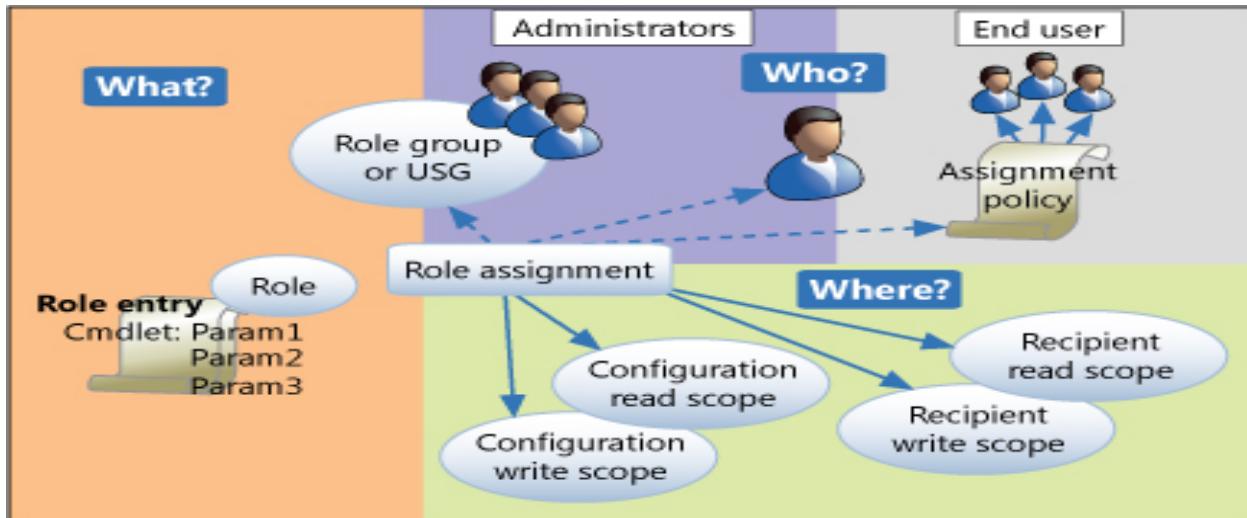


Image
2-https://www.quest.com/community/resized-image/_size/550x0/_key/communityserver-blogs-components-weblogfiles/00-00-00-00-06/Jones1011_2D00_Figure02.png

Different types of protocols

Introduction

Definition 1: A protocol is a standard set of rules that allow electronic devices to communicate with each other.

Definition 2: A protocol is a set of guidelines to govern the data transfer between the devices.

A Network Protocol is a group of rules accompanied by the network. Network protocols will be formalized requirements and plans composed of rules, procedures, and types that describe communication among a couple of devices over the network. The protocol can be described as an approach to rules that enable a couple of entities of a communication program to transfer information through any type of variety of a physical medium. The protocol identifies the rules, syntax, semantics as well as, synchronization of communication as well as, feasible error managing methods. In this article, we will discuss the different types of networking protocols. Let's discuss each of them briefly:

-
1. Transmission Control Protocol (TCP): TCP is a popular communication protocol which is used for communicating over a network. It divides any message into series of packets that are sent from source to destination and there it gets reassembled at the destination.
 2. Internet Protocol (IP): IP is designed explicitly as addressing protocol. It is mostly used with TCP. The IP addresses in packets help in routing them through different nodes in a network until it reaches the destination system. TCP/IP is the most popular protocol connecting the networks.
 3. User Datagram Protocol (UDP): UDP is a substitute communication protocol to Transmission Control Protocol implemented primarily for creating loss-tolerating and low-latency linking between different applications.
 4. Post office Protocol (POP): POP3 is designed for receiving incoming E-mails.
 5. Simple mail transport Protocol (SMTP): SMTP is designed to send and distribute outgoing E-Mail.
 6. File Transfer Protocol (FTP): FTP allows users to transfer files from one machine to another. Types of files may include program files, multimedia files, text files, and documents, etc.
 7. Hyper Text Transfer Protocol (HTTP): HTTP is designed for transferring a hypertext among two or more systems. HTML tags are used for creating links. These links may be in any form like text or images. HTTP is designed on Client-server principles which allow a client system for establishing a connection with the server machine for making a request. The server acknowledges the request initiated by the client and responds accordingly.
 8. Hyper Text Transfer Protocol Secure (HTTPS): HTTPS is abbreviated as Hyper Text Transfer Protocol Secure is a standard protocol to secure the communication among two computers one using the browser and other fetching data from web server. HTTP is used for transferring data between the client browser (request) and the web server (response) in the hypertext format, same in case of HTTPS except that the transferring of data is done in an encrypted format. So it

can be said that https thwart hackers from interpretation or modification of data throughout the transfer of packets.

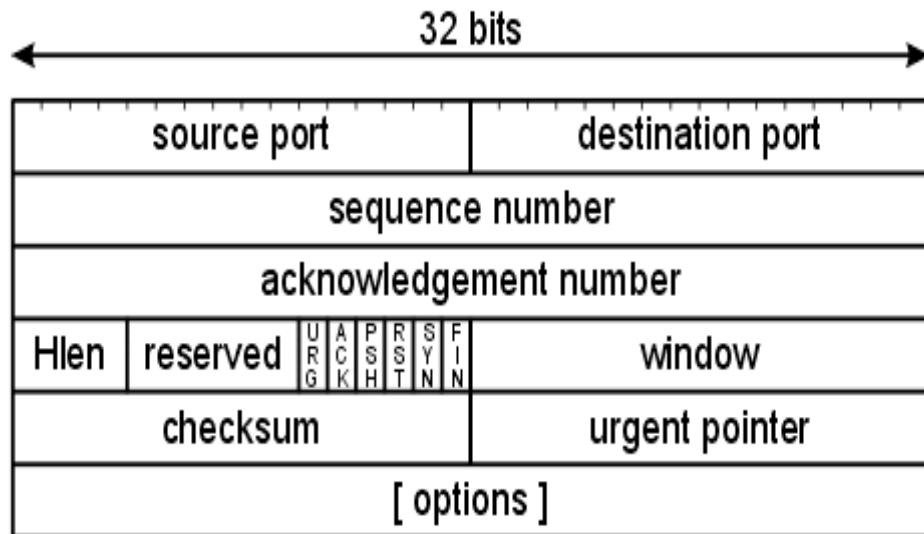
9. Telnet: Telnet is a set of rules designed for connecting one system with another. The connecting process here is termed as remote login. The system which requests for connection is the local computer, and the system which accepts the connection is the remote computer.
10. Gopher: Gopher is a collection of rules implemented for searching, retrieving as well as displaying documents from isolated sites. Gopher also works on the client/server principle.

Transmission Control Protocol

It provides a full transport layer services to applications.

TCP is a connection oriented protocol and offers end-to-end packet delivery. It acts as back bone for connection

TCP is a reliable protocol as it detects the error and retransmits the damaged frames.



Image

3-https://lh3.googleusercontent.com/proxy/MmQAe8LIPH97fO51WtYBRv6hMEL4GNj-QprSgwN8WXL_zGga4jsXDWUsZ1JCCJwoXFyY15EKcwhxis3JHKWrbDRHjGWUCd4Yt7LPpur0Uky-gvRE4j0J28RhRC6_g

- TCP is among the most widely used protocol using the internet.

-
- TCP is a two-way conversation.
 - TCP is focused on stability.
 - Packets will be instructed and numbered.
 - Packets will be error-checked.

TCP is a connection oriented protocol and offers end-to-end packet delivery. It acts as back bone for connection. It exhibits the following key features:

Transmission Control Protocol (TCP) corresponds to the Transport Layer of OSI Model.

TCP is a reliable and connection oriented protocol.

TCP offers:

- Stream Data Transfer.
- Reliability.
- Efficient Flow Control
- Full-duplex operation.
- Multiplexing.

TCP offers connection oriented end-to-end packet delivery.

TCP ensures reliability by sequencing bytes with a forwarding acknowledgement number that indicates to the destination the next byte the source expect to receive.

It retransmits the bytes not acknowledged within specified time period.

TCP Services

Stream Deliver Service

TCP protocol is stream oriented because it allows the sending process to send data as stream of bytes and the receiving process to obtain data as stream of bytes.

Sending and Receiving Buffers

It may not be possible for sending and receiving process to produce and obtain data at same speed, therefore, TCP needs buffers for storage at sending and receiving ends.

Bytes and Segments

The Transmission Control Protocol (TCP), at transport layer groups the bytes into a packet. This packet is called segment. Before transmission of these packets, these segments are encapsulated into an IP datagram.

Full Duplex Service

Transmitting the data in duplex mode means flow of data in both the directions at the same time.

Connection Oriented Service

TCP offers connection oriented service in the following manner:

TCP of process-1 informs TCP of process – 2 and gets its approval.

TCP of process – 1 and TCP of process – 2 and exchange data in both the two directions.

After completing the data exchange, when buffers on both sides are empty, the two TCP's destroy their buffers.

Reliable Service

For sake of reliability, TCP uses acknowledgement mechanism.

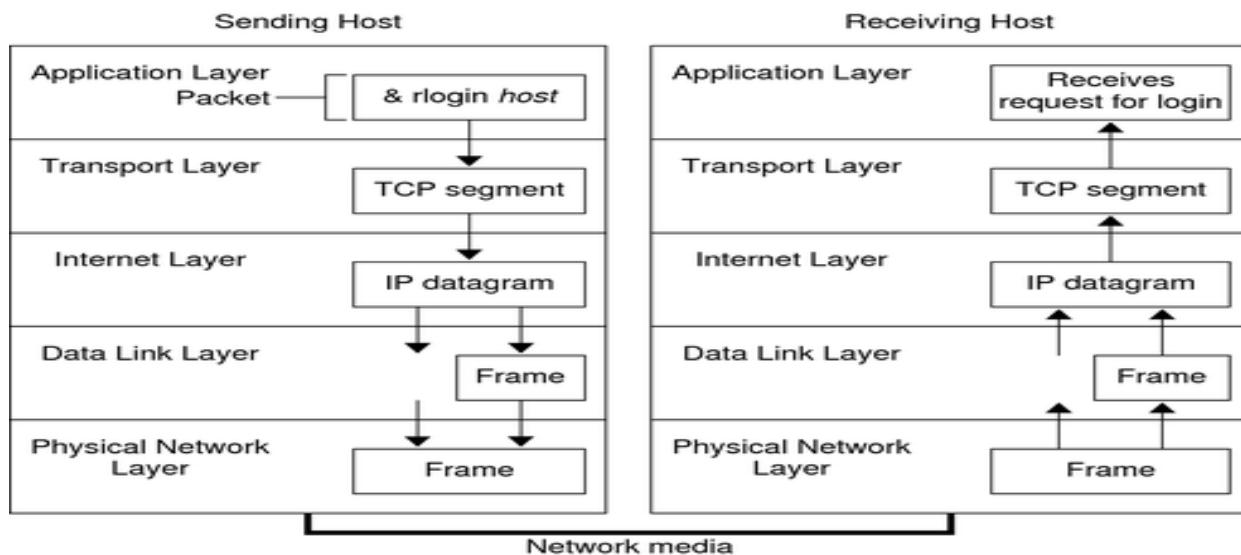


Image 4- https://docs.oracle.com/cd/E18752_01/html/816-4554/figures/ipov.fig88.png

TCP Benefits

1. It is an Open standard and is independent of hardware and software manufacturer.

-
- 2. It can send data between different computer systems running completely through Operating system.
 - 3. It is separated from the underlying hardware and it will run over Ethernet, tokens ring and even over dial-up telephones lines.
 - 4. It is a routable protocol.
 - 5. It has a reliable and efficient data-delivery mechanism.
 - 6. It uses a common addressing scheme, so any system can address any other system.

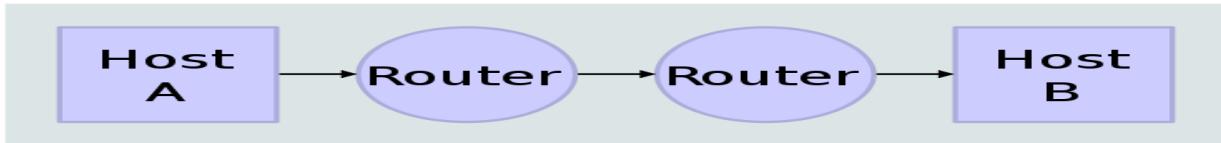
Internet Protocol

Internet Protocol is connectionless and unreliable protocol. It ensures no guarantee of successfully transmission of data.

In order to make it reliable, it must be paired with reliable protocol such as TCP at the transport layer.

The Internet protocol suite provides end-to-end data communication specifying how data should be packetized, addressed, transmitted, routed, and received. This functionality is organized into four abstraction layers, which classify all related protocols according to the scope of networking involved.[1][2] From lowest to highest, the layers are the link layer, containing communication methods for data that remains within a single network segment (link); the internet layer, providing internetworking between independent networks; the transport layer, handling host-to-host communication; and the application layer, providing process-to-process data exchange for applications.

Network Topology



Data Flow

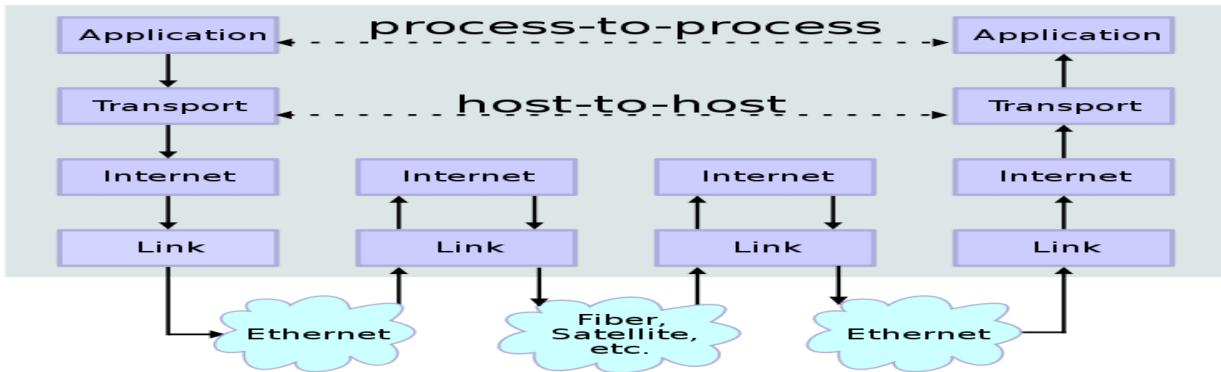


Image 5-https://upload.wikimedia.org/wikipedia/commons/thumb/c/c4/IP_stack_connections.svg/350px-IP_stack_connections.svg.png

Conceptual data flow in a simple network topology of two hosts (A and B) connected by a link between their respective routers. The application on each host executes read and write operations as if the processes were directly connected to each other by some kind of data pipe. After establishment of this pipe, most details of the communication are hidden from each process, as the underlying principles of communication are implemented in the lower protocol layers. In analogy, at the transport layer the communication appears as host-to-host, without knowledge of the application data structures and the connecting routers, while at the internetworking layer, individual network boundaries are traversed at each router.

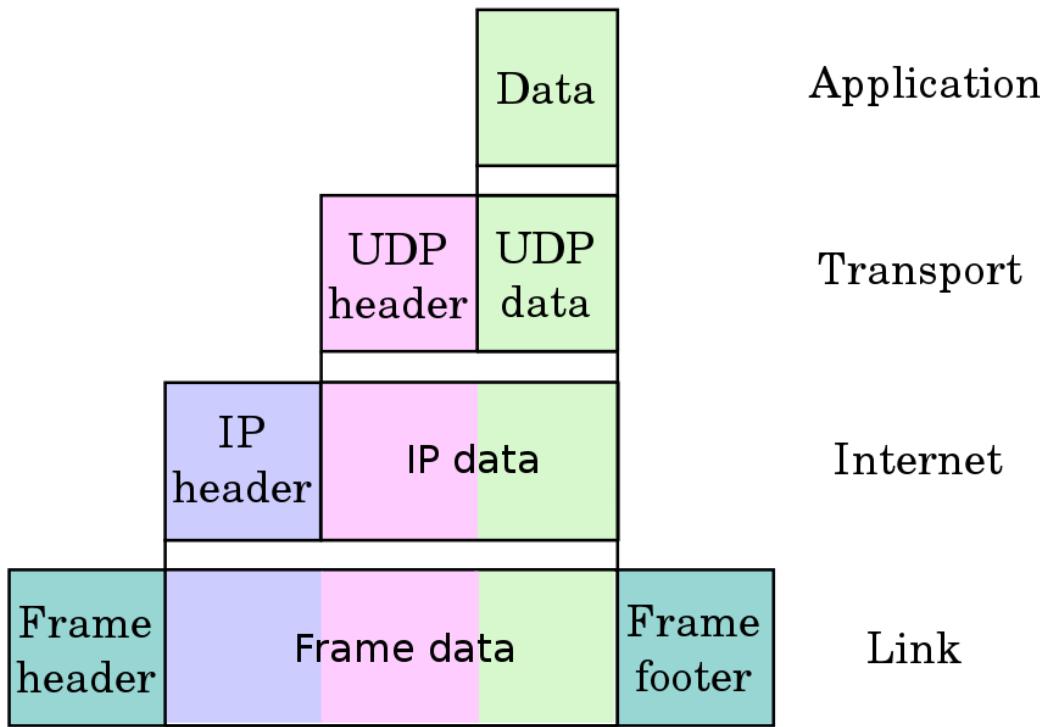


Image 6-https://upload.wikimedia.org/wikipedia/commons/thumb/3/3b/UDP_encapsulation.svg/1024px-UDP_encapsulation.svg.png

- The application layer is the scope within which applications, or processes, create user data and communicate this data to other applications on another or the same host.
- The transport layer performs host-to-host communications on either the local network or remote networks separated by routers.[33] It provides a channel for the communication needs of applications. UDP is the basic transport layer protocol, providing an unreliable connectionless datagram service. The Transmission Control Protocol provides flow-control, connection establishment, and reliable transmission of data.
- The internet layer exchanges datagrams across network boundaries. It provides a uniform networking interface that hides the actual topology (layout) of the underlying network connections. It is therefore also the layer that establishes internetworking. Indeed, it defines and establishes the Internet. This layer defines the addressing and routing structures used for the TCP/IP protocol suite. The primary protocol in this scope is the Internet Protocol, which defines IP addresses. Its function in routing is to transport datagrams to the next host, functioning as an IP router, that has the connectivity to a network closer to the final data destination.

- The link layer defines the networking methods within the scope of the local network link on which hosts communicate without intervening routers. This layer includes the protocols used to describe the local network topology and the interfaces needed to affect the transmission of Internet layer datagrams to next-neighbor hosts.

Short Information

- The application layer sends the data (to be transferred to remote destination) to the transport layer.
- The transport layer puts its header in the beginning and sends this complete packet (TCP-header + app-data) to the IP layer.
- On the same lines, The IP layer puts its header in front of the data received from TCP (Note that data received from TCP = TCP-header + app-data).
- So now the structure of IP datagram becomes IP-header + TCP-header + app-data.
- This IP datagram is passed to the Ethernet layer which on the same lines adds its own header to IP datagram and then the whole packet is transmitted over network.

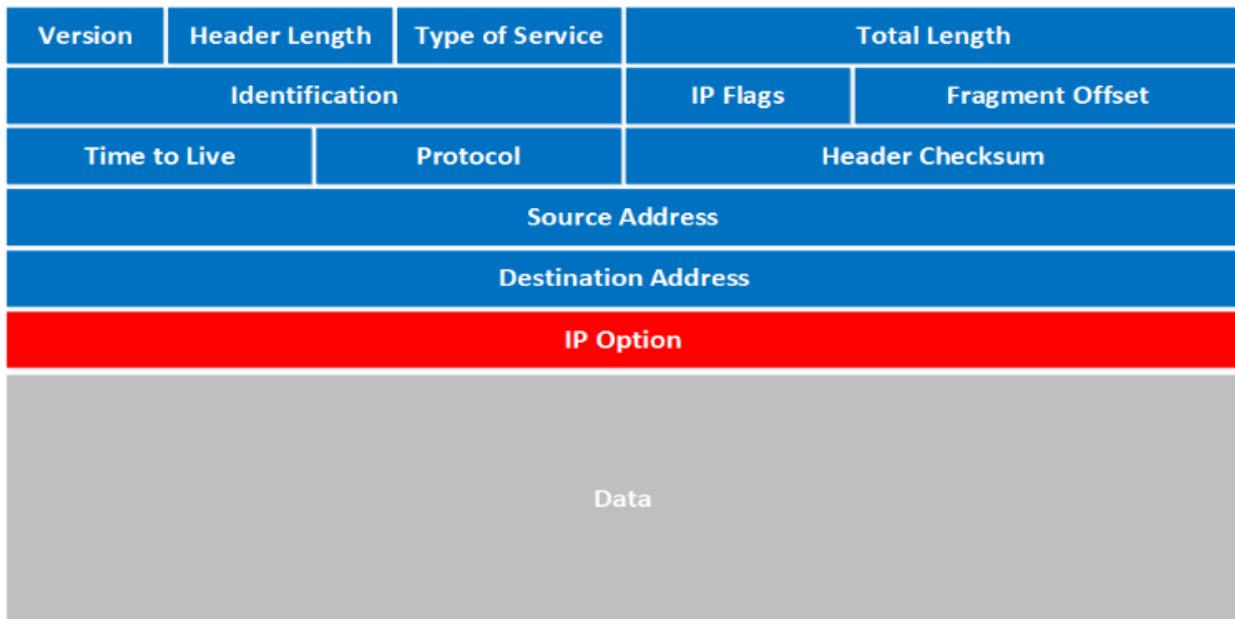


Image 7-<https://networklessons.com/cisco/ccna-routing-switching-icnd1-100-105/ipv4-packet-header>

-
- **Version:** the first field tells us which IP version we are using, only IPv4 uses this header so you will always find decimal value 4 here.
 - **Header Length:** this 4 bit field tells us the length of the IP header in 32 bit increments. The minimum length of an IP header is 20 bytes so with 32 bit increments, you would see value of 5 here. The maximum value we can create with 4 bits is 15 so with 32 bit increments, that would be a header length of 60 bytes. This field is also called the **Internet Header Length (IHL)**.
 - **Type of Service:** this is used for QoS (Quality of Service). There are 8 bits that we can use to mark the packet which we can use to give the packet a certain treatment. You can read more about this field in my IP precedence and DSCP tutorial.
 - **Total Length:** this 16-bit field indicates the entire size of the IP packet (header and data) in bytes. The minimum size is 20 bytes (if you have no data) and the maximum size is 65.535 bytes, that's the highest value you can create with 16 bits.
 - **Identification:** If the IP packet is fragmented then each fragmented packet will use the same 16 bit identification number to identify to which IP packet they belong to.
 - **IP Flags:** These 3 bits are used for fragmentation:
 - The first bit is always set to 0.
 - The second bit is called the **DF (Don't Fragment) bit** and indicates that this packet should not be fragmented.
 - The third bit is called the **MF (More Fragments)** bit and is set on all fragmented packets except the last one.
 - **Fragment Offset:** this 13 bit field specifies the position of the fragment in the original fragmented IP packet.
 - **Time to Live:** Every time an IP packet passes through a router, the time to live field is decremented by 1. Once it hits 0 the router will drop the packet and sends an ICMP time exceeded message to the sender. The time to live field has 8 bits and is used to prevent packets from looping around forever (if you have a routing loop).
 - **Protocol:** this 8 bit field tells us which protocol is encapsulated in the IP packet, for example TCP has value 6 and UDP has value 17.

- **Header Checksum:** this 16 bit field is used to store a checksum of the header. The receiver can use the checksum to check if there are any errors in the header.
- **Source Address:** here you will find the 32 bit source IP address.
- **Destination Address:** and here's the 32 bit destination IP address.
- **IP Option:** this field is not used often, is optional and has a variable length based on the options that were used. When you use this field, the value in the header length field will increase. An example of a possible option is “source route” where the sender requests for a certain routing path.

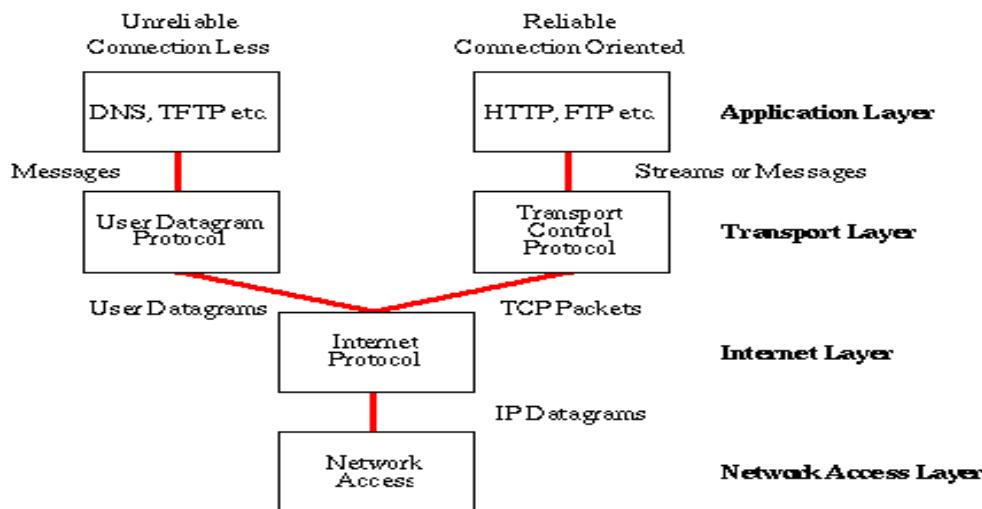


Image 8-<https://www.w3.org/People/Frystyk/thesis/tcp.gif>

- The application layer sends the data (to be transferred to remote destination) to the transport layer.
- The transport layer puts its header in the beginning and sends this complete packet (TCP-header + app-data) to the IP layer.
- On the same lines, The IP layer puts its header in front of the data received from TCP (Note that data received from TCP = TCP-header + app-data).
- So now the structure of IP datagram becomes IP-header + TCP-header + app-data.
- This IP datagram is passed to the ethernet layer which on the same lines adds its own header to IP datagram and then the whole packet is transmitted over network.

Hyper Text Transfer Protocol

HTTP is a communication protocol. It defines mechanism for communication between browser and the web server. It is also called request and response protocol because the communication between browser and server takes place in request and response pairs.

HTTP Request

HTTP request comprises of lines which contains:

Request line

Header Fields

Message body

Key Points

The first line i.e. the Request line specifies the request method i.e. Get or Post.

The second line specifies the header which indicates the domain name of the server from where index.htm is retrieved.

HTTP Response

Like HTTP request, HTTP response also has certain structure. HTTP response contains:

Status line

Headers

Message body

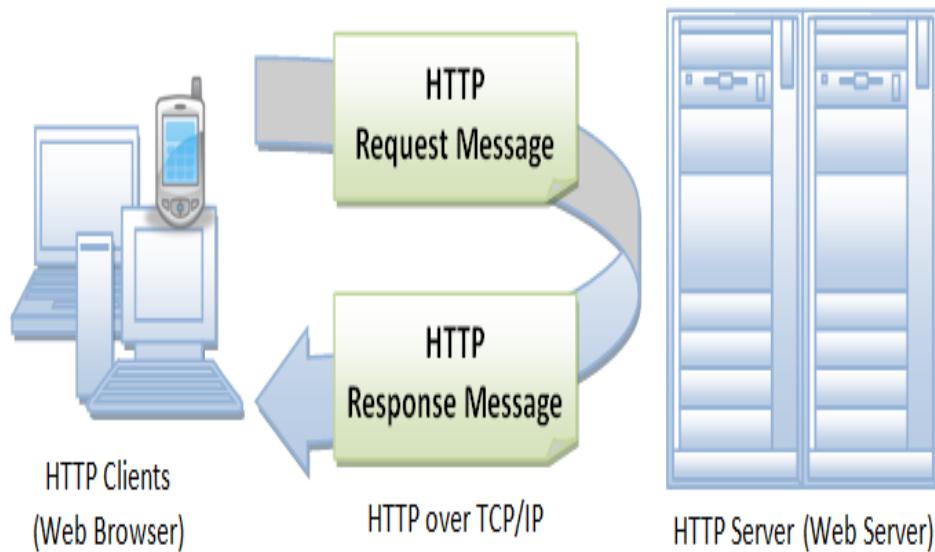


Image 9-<https://www.ntu.edu.sg/home/ehchua/programming/webprogramming/images/HTTP.png>

Hyper Text Transfer Protocol Secure

- Hypertext Transfer Protocol Secure (HTTPS) is an extension of the Hypertext Transfer Protocol (HTTP). It is used for secure communication over a computer network, and is widely used on the Internet.
- In HTTPS, the communication protocol is encrypted using Transport Layer Security (TLS) or, formerly, Secure Sockets Layer (SSL).
- The protocol is therefore also referred to as HTTP over TLS,[3] or HTTP over SSL.

Advantages

- User Data is Encrypted
- You'll Enjoy Better SEO
- Protects your website from Phishing
- Authentication of the accessed website, and protection of the privacy and integrity of the exchanged data while in transit.

-
- It protects against man-in-the-middle attacks, and the bidirectional encryption of communications between a client and server protects the communications against eavesdropping and tampering

Limitations

- SSL/TLS does not prevent the indexing of the site by a web crawler
- SSL (Secure Sockets Layer) and TLS (Transport Layer Security) encryption can be configured in two modes: simple and mutual.

From an architectural point of view

An SSL/TLS connection is managed by the first front machine that initiates the TLS connection. If, for any reasons (routing, traffic optimization, etc.), this front machine is not the application server and it has to decipher data, solutions have to be found to propagate user authentication information or certificate to the application server, which needs to know who is going to be connected.

For SSL/TLS with mutual authentication, the SSL/TLS session is managed by the first server that initiates the connection. In situations where encryption has to be propagated along chained servers, session timeOut management becomes extremely tricky to implement.

Security is maximal with mutual SSL/TLS, but on the client-side there is no way to properly end the SSL/TLS connection and disconnect the user except by waiting for the server session to expire or by closing all related client applications.

SSL/TLS does not prevent the indexing of the site by a web crawler, and in some cases the URI of the encrypted resource can be inferred by knowing only the intercepted request/response size.[33] This allows an attacker to have access to the plaintext (the publicly available static content), and the encrypted text (the encrypted version of the static content), permitting a cryptographic attack.

- SSL 1.0 – never publicly released due to security issues.
- SSL 2.0 – released in 1995. Deprecated in 2011. Has known security issues.
- SSL 3.0 – released in 1996. Deprecated in 2015. Has known security issues.
- TLS 1.0 – released in 1999 as an upgrade to SSL 3.0. Planned deprecation in 2020.

- TLS 1.1 – released in 2006. Planned deprecation in 2020.
- TLS 1.2 – released in 2008.
- TLS 1.3 – released in 2018.

File Transfer Protocol

- FTP is used to copy files from one host to another browser and the web server.
- FTP creates two processes such as Control Process and Data Transfer Process at both ends i.e. at client as well as at server.
- FTP establishes two different connections: one is for data transfer and other is for control information.
- Control connection is made between control processes while Data Connection is made between
- FTP uses port 21 for the control connection and Port 20 for the data connection.

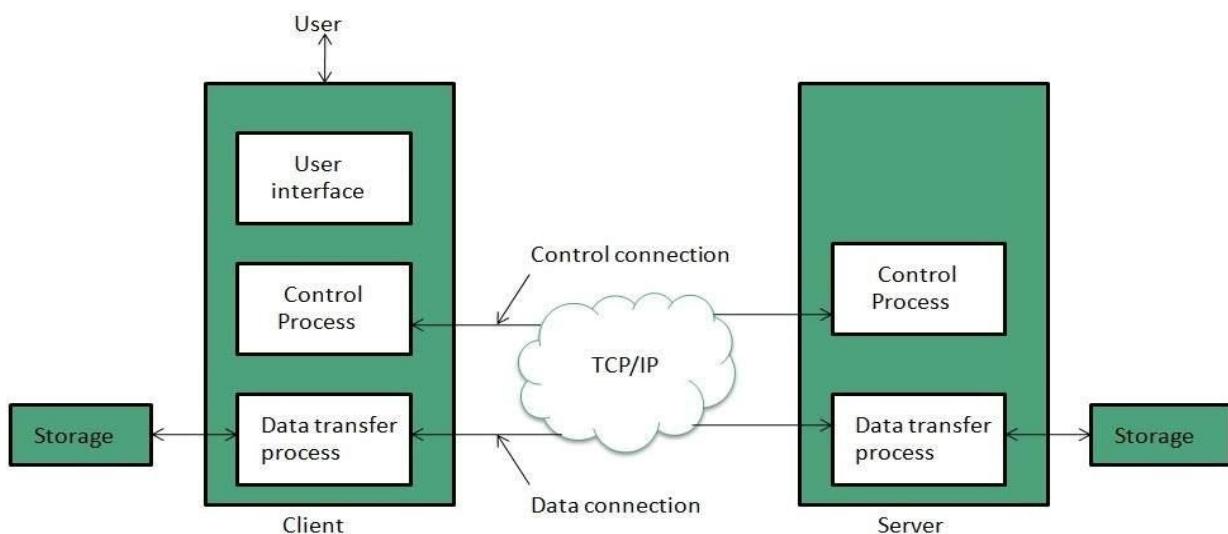


Image 10-https://www.tutorialspoint.com/internet_technologies/images/internet-ftp_model.jpg

Simple Mail Transfer Protocol

- SMTP is a set of communication guidelines that allow software to transmit an electronic mail over the internet is called Simple Mail Transfer Protocol.

- It is a program used for sending messages to other computer users based on e-mail addresses.
- It provides a mail exchange between users on the same or different computers, and it also supports:
 1. It can send a single message to one or more recipients.
 2. Sending message can include text, voice, video or graphics.
 3. It can also send the messages on networks outside the internet.

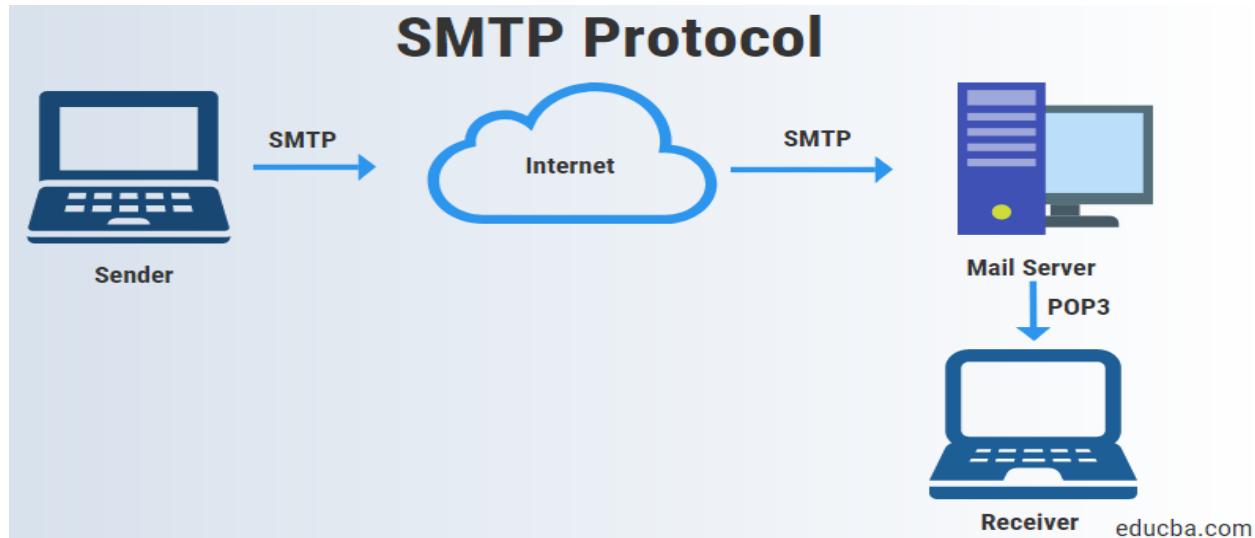


Image 11-<https://cdn.educba.com/academy/wp-content/uploads/2019/07/smtp-protocol.png>

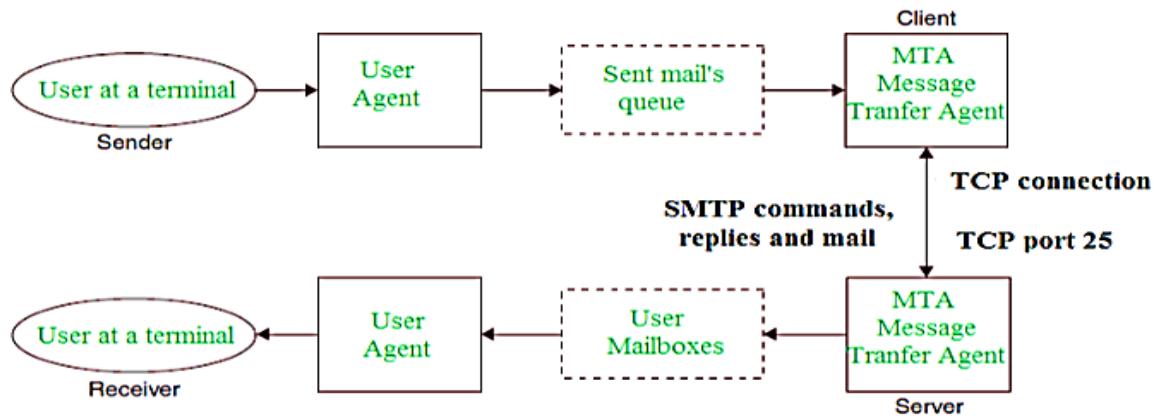


Image 12- https://media.geeksforgeeks.org/wp-content/cdn-uploads/gq/2017/02/SMTP_1.png

Some SMTP Commands:

- HELO – Identifies the client to the server, fully qualified domain name, only sent once per session
- MAIL – Initiate a message transfer, fully qualified domain of originator
- RCPT – Follows MAIL, identifies an addressee, typically the fully qualified name of the addressee and for multiple addressees use one RCPT for each addressee
- DATA – send data line by line

Open System Interconnection Model (OSI)

Introduction

- OSI stands for Open Systems Interconnection. It has been developed by ISO – ‘International Organization of Standardization’, in the year 1984.
- Designed to show the flow of moving data from one software application of one computer to another software application of another computer.
- Open Systems Interconnection (OSI) model is the virtual model which describes the Concept of a computer system with the concern of internal structure and technology.

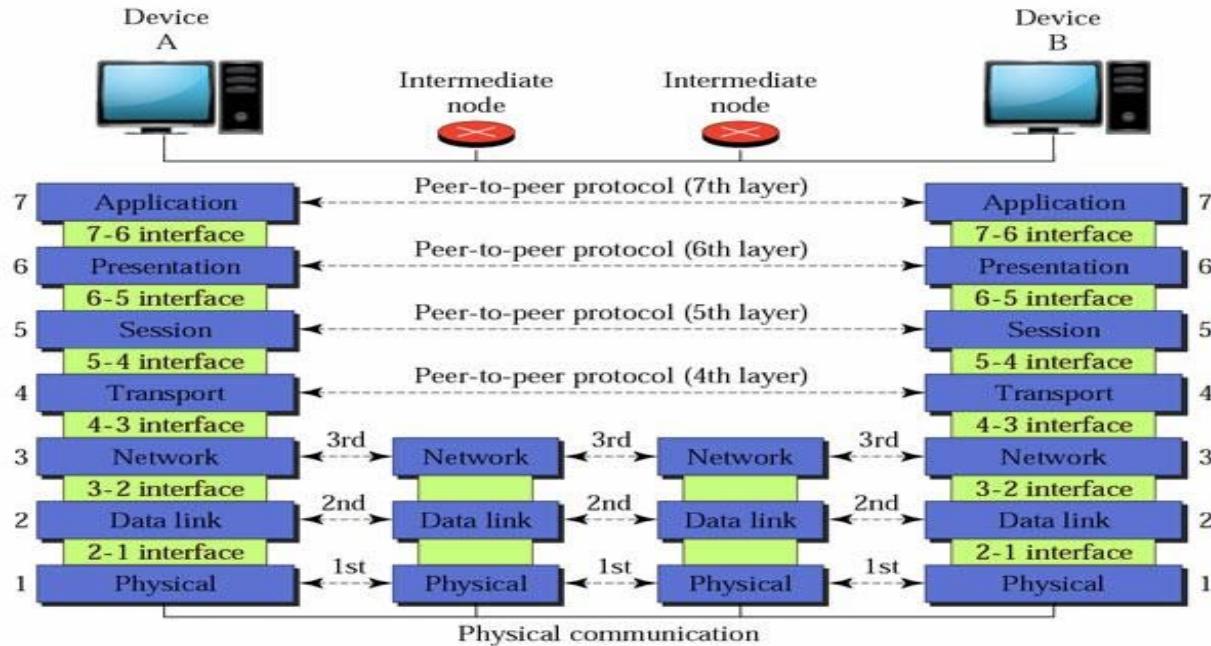


Image 13-https://cdn.educba.com/academy/wp-content/uploads/2019/05/OSI-Model1_Done.jpg

Physical Layer Functions

- The functions of the physical layer are :
- **Bit synchronization:** The physical layer provides the synchronization of the bits by providing a clock. This clock controls both sender and receiver thus providing synchronization at bit level.
- **Bit rate control:** The Physical layer also defines the transmission rate i.e. the number of bits sent per second.
- **Physical topologies:** Physical layer specifies the way in which the different, devices/nodes are arranged in a network i.e. bus, star or mesh topology.
- **Transmission mode:** Physical layer also defines the way in which the data flows between the two connected devices. The various transmission modes possible are: Simplex, half-duplex and full-duplex.

Data Link Layer Functions

- The data link layer is responsible for the node to node delivery of the message. The main function of this layer is to make sure data transfer is error-free from one node to another, over the physical layer.
 - Packet in Data Link layer is referred as Frame.
 - Data Link layer is handled by the NIC (Network Interface Card) and device drivers of host machines.
 - Switch & Bridge are Data Link Layer devices.
1. Logical Link Control (LLC) 2. Media Access Control (MAC)
1. **Framing:** Framing is a function of the data link layer. It provides a way for a sender to transmit a set of bits that are meaningful to the receiver. This can be accomplished by attaching special bit patterns to the beginning and end of the frame.
 2. **Physical addressing:** After creating frames, Data link layer adds physical addresses (MAC address) of sender and/or receiver in the header of each frame.
 3. **Error control:** Data link layer provides the mechanism of error control in which it detects and retransmits damaged or lost frames.
 4. **Flow Control:** The data rate must be constant on both sides else the data may get corrupted thus , flow control coordinates that amount of data that can be sent before receiving acknowledgement.
 5. **Access control:** When a single communication channel is shared by multiple devices, MAC sub-layer of data link layer helps to determine which device has control over the channel at a given time.

Network Layer Functions

- **Routing:** The network layer protocols determine which route is suitable from source to destination. This function of network layer is known as routing.
- **Logical Addressing:** In order to identify each device on internetwork uniquely, network layer defines an addressing scheme. The sender & receiver's IP address are placed in the

header by network layer. Such an address distinguishes each device uniquely and universally.

- Segment in Network layer is referred as Packet.
- Network layer is implemented by networking devices such as routers.

Transport Layer Functions

- **Segmentation and Reassembly:** This layer accepts the message from the (session) layer , breaks the message into smaller units . Each of the segment produced has a header associated with it. The transport layer at the destination station reassembles the message.
- **Service Point Addressing:** In order to deliver the message to correct process, transport layer header includes a type of address called service point address or port address. Thus by specifying this address, transport layer makes sure that the message is delivered to the correct process.
- The services provided by the transport layer :
- **Connection Oriented Service:** It is a three-phase process which include
 - Connection Establishment
 - Data Transfer
 - Termination / disconnectionIn this type of transmission, the receiving device sends an acknowledgement, back to the source after a packet or group of packet is received. This type of transmission is reliable and secure.
- **Connection less service:** It is a one-phase process and includes Data Transfer. In this type of transmission, the receiver does not acknowledge receipt of a packet. This approach allows for much faster communication between devices. Connection-oriented service is more reliable than connectionless Service.

Session Layer Functions

- **Session establishment, maintenance and termination:** The layer allows the two processes to establish, use and terminate a connection.
- **Synchronization :** This layer allows a process to add checkpoints which are considered as synchronization points into the data. These synchronization point help to identify the

error so that the data is re-synchronized properly, and ends of the messages are not cut prematurely and data loss is avoided.

- **Dialog Controller :** The session layer allows two systems to start communication with each other in half-duplex or full-duplex.

Presentation Layer Functions

- **Translation :** For example, ASCII to EBCDIC.
- **Encryption/ Decryption :** Data encryption translates the data into another form or code. The encrypted data is known as the cipher text and the decrypted data is known as plain text. A key value is used for encrypting as well as decrypting data.
- **Compression:** Reduces the number of bits that need to be transmitted on the network.

Application layer Functions

At the very top of the OSI Reference Model stack of layers, we find Application layer which is implemented by the network applications. These applications produce the data, which has to be transferred over the network. This layer also serves as a window for the application services to access the network and for displaying the received information to the user.

- Network Virtual Terminal
- FTAM-File transfer access and management
- Mail Services
- Directory Services

Media Access Methods

Introductions

A media access method refers to the manner in which a computer terminal on a network gains and controls access to the network's physical medium such as a cable.

The prime objective of media access is to prevent data packets from colliding when two or more computer terminals on a network try to transmit data simultaneously over a network.

Carrier Sense Multiple Access with Collision Detection (CSMA/CD)

- This is a media access method which defines how the network places data on the cable and how it takes it off.
- CSMA/CD specifies how bus topologies such as Ethernet handle transmission collisions.
- It usually operates in two modes of Carrier Sense, Multiple Access and Collision Detection.
- **Carrier Sense** means that each station on the LAN continually listens to (tests) the cable for the presence of a signal prior to transmitting.
- **Multiple Access** means that there are many computers attempting to transmit and compete for the opportunity to send data (i.e., they are in contention).
- **Collision Detection** means that when a collision is detected, the stations will stop transmitting and wait a random length of time before retransmitting the data.

CSMA/CD works best in an environment where relatively fewer, longer data frames are transmitted. This is in contrast to token passing which works best with a relatively large amount of short data frames. Because CSMA/CD works to control or manage collisions rather than prevent them, network performance can be degraded with heavy data traffic. More traffic will lead to a greater number of collisions and retransmissions in a network. CSMA/CD is used on Ethernet networks.

Carrier Sense Multiple Access with Collision Avoidance (CSMA/CA)

- CSMA/CA stands for Carrier-Sense Multiple Access with Collision Avoidance and is a media access method very similar to CSMA/CD.
- The difference is that the CD (collision detection) is changed to CA (collision avoidance).
- Instead of detecting and reacting to collisions, CSMA/CA tries to avoid them by having each computer signal its intention to transmit before actually transmitting.
- In effect, the transmitting computer gives a “Request” prior to transmitting.

Although CSMA/CA can prevent collisions, it comes with a cost in the form of the additional overhead incurred by having each workstation broadcast its intention prior to transmitting. Thus, CSMA/CA is slower than CSMA/CD. CSMA/CA is used on Apple networks

Token Passing

- Token passing is a media access method by which collisions are prevented.
- Collisions are eliminated under token passing because only a computer that possesses a free token (a small data frame) is allowed to transmit.
- The token passing method also allows different priorities to be assigned to different stations on the ring.
- Transmissions from stations with higher priority take precedence over stations with lower priority.
- Token passing works best in an environment where a relatively large number of shorter data frames are being transmitted
- There are two common error conditions that can occur on a token passing LAN:
 - a) Constant Frame Error
 - A token cannot be acknowledged and continues to be passed around the ring.
 - b) Lost Token Error
 - A token is accidentally “hung up” or removed from the ring.

Demand Priority

- Demand priority utilizes a “hub-centric approach” to media access. A “smart hub” controls access to the network. When a workstation needs to transmit, it sends a request to the hub. The hub grants permission to transmit based on network conditions and requester priority. As they are under the control of the hub, workstations or terminals do not compete for access to the network.

-
- Unlike regular Ethernet in which a transmission is transmitted to all stations, demand priority utilizes a directed transmission. The hub directs the transmission from sender to intended recipient rather than sending it to all stations.
 - With demand priority, workstations can transmit and receive at the same time. This is because demand priority uses “quartet signaling” (Transmission of data on four pairs of wires).

CSMA/CD	Token Passing
Used primarily by Ethernet LANs.	Used primarily by Token Ring LANs.
Works best in larger networks with relatively fewer, longer data frames.	Works best in small to medium size networks with many short data frames
Does not allow different priorities to be assigned to stations.	Allows different priorities to be assigned to stations.
Normally less expensive than token passing.	Normally more expensive than CSMA/CD.

Domain Name Services

- Domain Name System (DNS) is an Internet service that translates the domain names into IP addresses, which computer can understand.
- Every device connected to the internet has a unique IP address which other machines use to find the device.

HOW DNS WORKS

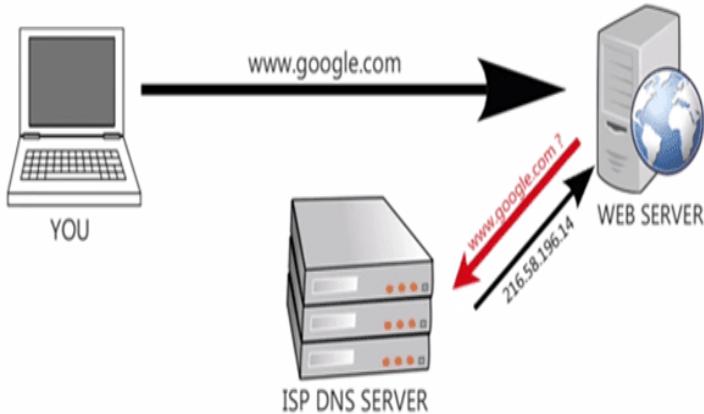


Image 14-https://www.etalsoftsolutions.com/blog/wp-content/uploads/2019/02/how_dns_works.png

DNS Records

Records	Description	Function
A	Address Record	It returns a 32bit IP addresses. This is where the actual Website is redirected towards most commonly.
CNAME	Canonical Name Record	This is an Alias. The DNS Server will continue to lookup with this new name.
DNAME	Delegation Name	This again is an alias for a name and also its subname, unlike CNAME, which is only an alias for itself. But similar to CNAME, the DNS Server tries to lookup with this new name as well.
DNSKEY	DNS KEY Record	There is another record known as KEY record which I haven't mentioned here. The format of DNSKEY is same as the KEY, and is used in DNSSEC (more in description).

LOC	Location Record	This provides the geographical location depending upon the domain name.
MX	Mail Exchange Record	This is related to the email routing which I mentioned previously. This maps the domain name with the email ID.
NS	Name Server Record	Provides a DNS ZONE to authorized name servers.
TKEY	Secret Key Record	This is the Key used with TSIG which is encrypted under Public Key.
TSIG	Transaction Signature	This is used to authenticate updates coming from an approved source or name server. It is used along with TKEY.
TXT	Text Record	This file provides machine data related to frameworks and encryption.

There are 4 DNS servers involved in loading a webpage:

The recursor can be thought of as a librarian who is asked to go find a particular book somewhere in a library. The DNS recursor is a server designed to receive queries from client machines through applications such as web browsers. Typically the recursor is then responsible for making additional requests in order to satisfy the client's DNS query.

- **Root nameserver** - The root server is the first step in translating (resolving) human readable host names into IP addresses. It can be thought of like an index in a library that points to different racks of books - typically it serves as a reference to other more specific locations.
- **TLD nameserver** - The top level domain server (TLD) can be thought of as a specific rack of books in a library. This nameserver is the next step in the search for a specific IP address, and it hosts the last portion of a hostname (In example.com, the TLD server is “com”).
- **Authoritative nameserver** - This final nameserver can be thought of as a dictionary on a rack of books, in which a specific name can be translated into its definition. The authoritative nameserver is the last stop in the nameserver query. If the authoritative name server has access to the requested record, it will return the IP address for the requested hostname back to the DNS Recursor (the librarian) that made the initial request.

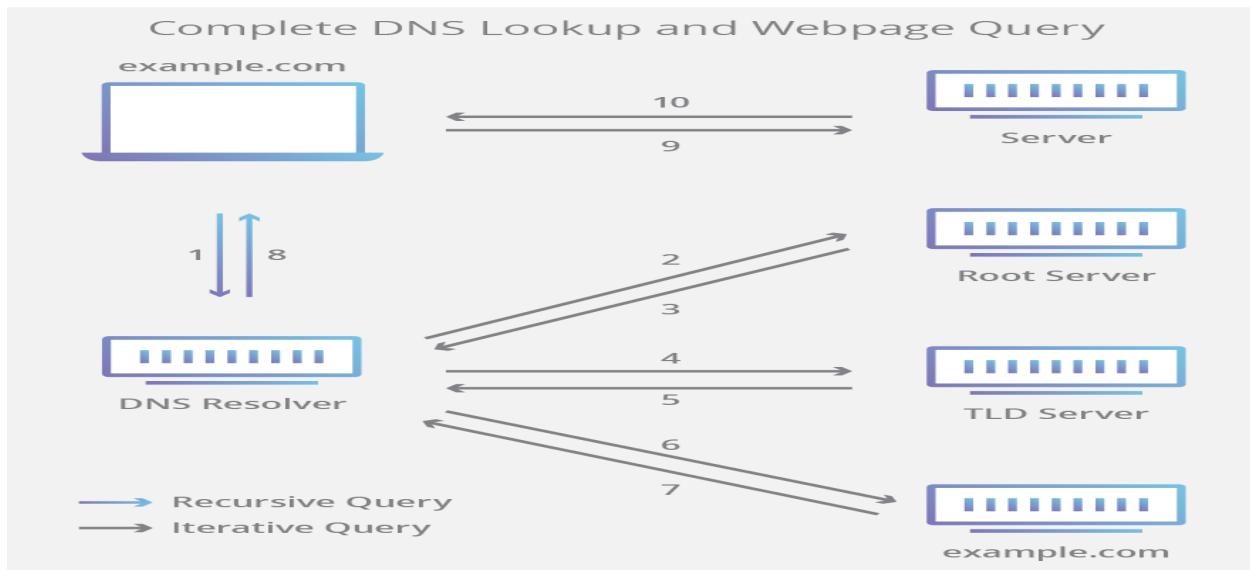


Image 15-<https://www.cloudflare.com/img/learning/dns/what-is-dns/dns-lookup-diagram.png>

Dynamic Host Configuration Protocol

- Dynamic Host Configuration Protocol (DHCP) is a network management protocol used to dynamically assign an Internet Protocol (IP) address to any device, or node, on a network so they can communicate using IP.
- The DHCP client will demand an IP address by broadcasting a DHCP Discover message to the local subnet.

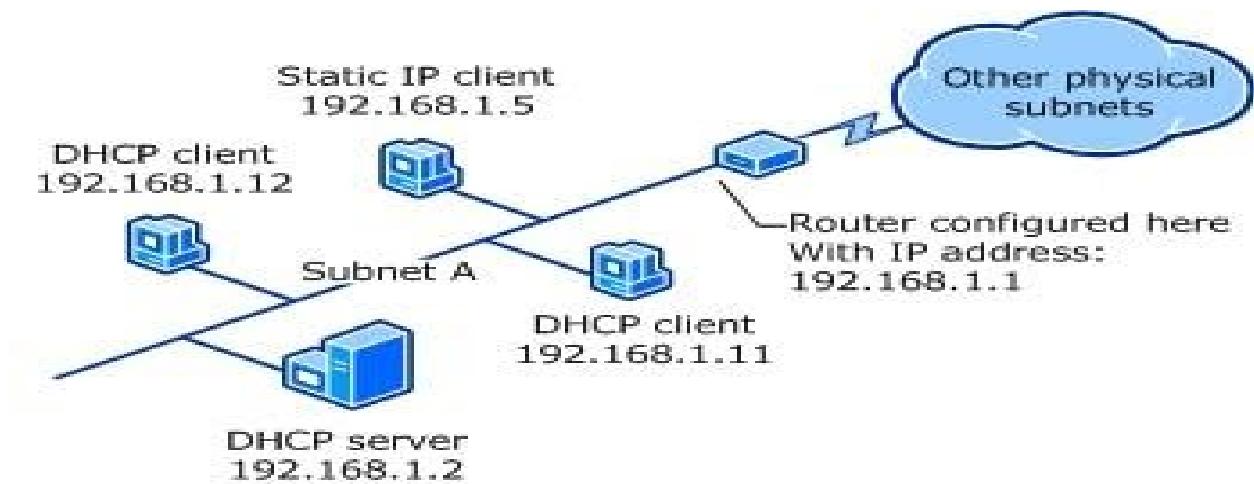


Image 16-<https://networkencyclopedia.com/wp-content/uploads/2019/08/configuring-dhcp-scope.jpg>

DHCP Process

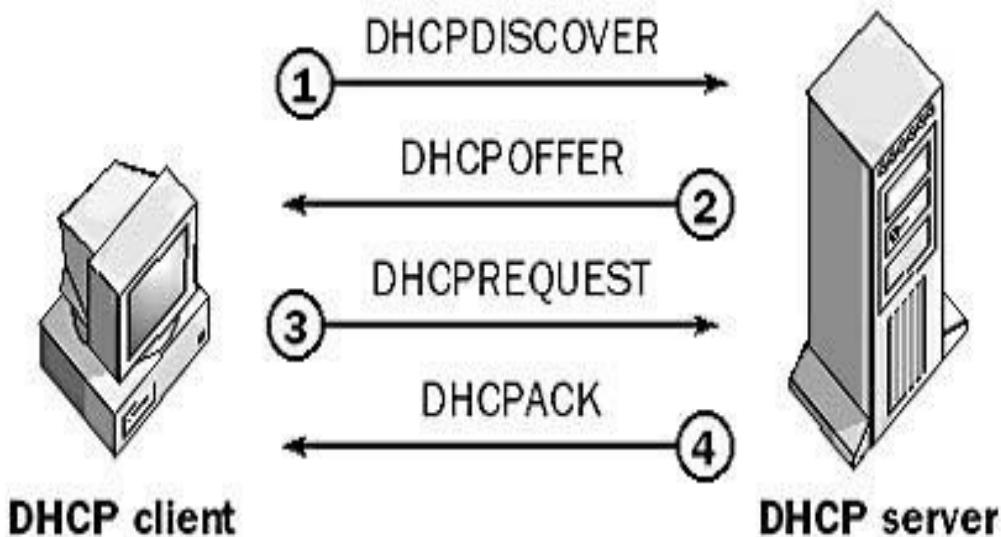


Image 17-<https://networkencyclopedia.com/wp-content/uploads/2019/08/dhcp.jpg>

1. **DHCPDISCOVER**: The client broadcasts a request for a DHCP server.
2. **DHCPOFFER**: DHCP servers on the network offer an address to the client.
3. **DHCPREQUEST**: The client broadcasts a request to lease an address from one of the offering DHCP servers.
4. **DHCPACK**: The DHCP server that the client responds to acknowledges the client, assigns it any configured DHCP options, and updates its DHCP database. The client then initializes and binds its TCP/IP protocol stack and can begin network communication.

Windows Internet Name Service

Windows Internet Name Service, or WINS, is a Microsoft Windows service that dynamically registers NetBIOS names of computers on the network.

The Windows Internet Naming Service (WINS) converts the NetBIOS host names into IP addresses.

It allows the Windows machines on a given LAN segment to recognize Windows machines on other LAN segments.

It was designed specifically to support NetBIOS over TCP/IP (NetBT)



Image 18-<https://networkencyclopedia.com/wp-content/uploads/2019/09/wins-windows-internet-name-service.jpg>

Advantages

- In order for NetBIOS hosts (servers and clients running pre-Windows 2000 versions of Microsoft Windows) to communicate on a network, their NetBIOS names must first be resolved into IP addresses. WINS servers perform this task.
- Directed traffic to WINS servers generates less network traffic than broadcasts.
- WINS provides a mechanism for browsing network resources across multiple domains and subnets.
- The WINS database of NetBIOS name to IP address mappings is dynamically maintained, eliminating the need for lmhosts files on clients.

Example

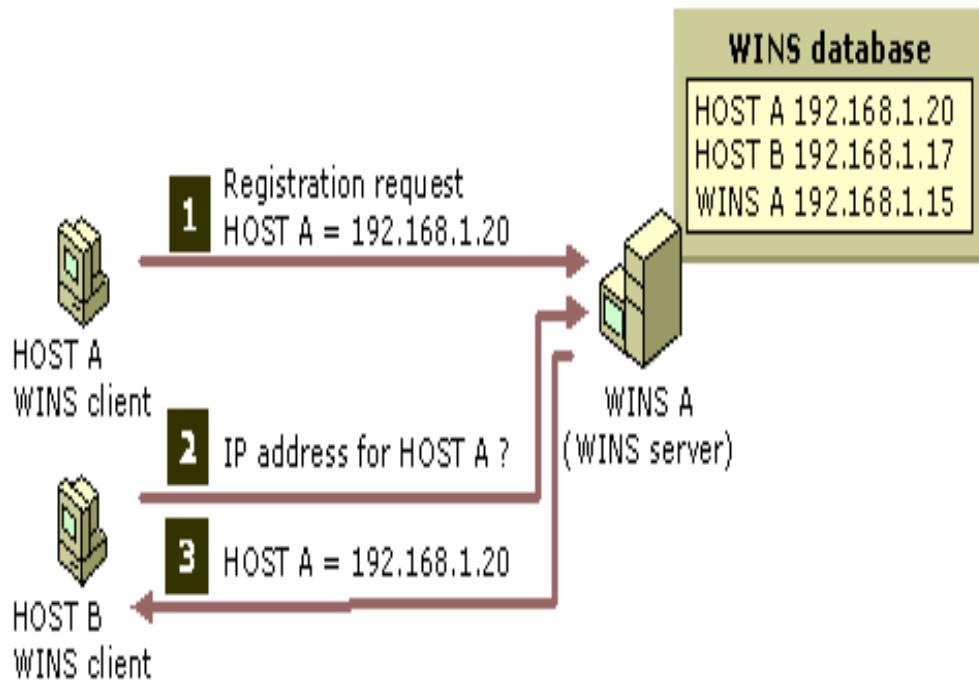


Image 19-<https://networkencyclopedia.com/wp-content/uploads/2019/09/windows-internet-name-service-wins.gif>

In this example, the following occurs:

1. A WINS client, HOST-A, registers any of its local NetBIOS names with WINS-A, its configured WINS server.
2. Another WINS client, HOST-B, queries WINS-A to locate the IP address for HOST-A on the network.
3. WINS-A replies with the IP address for HOST-A, 192.168.1.20.

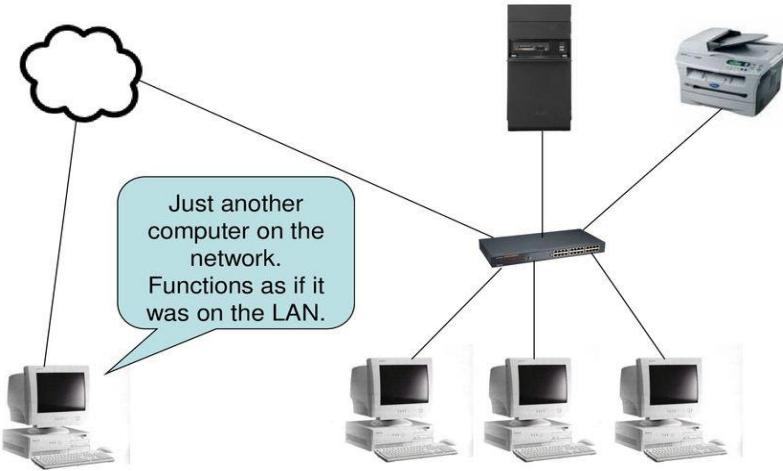
Remote Access Service

A remote access service (RAS) is any combination of hardware and software to enable the remote access tools or information that typically reside on a network of IT devices.

A remote access service connects a client to a host computer, known as a remote access server.

RAS is arranged within an organization and directly connected with the organization's internal network and systems.

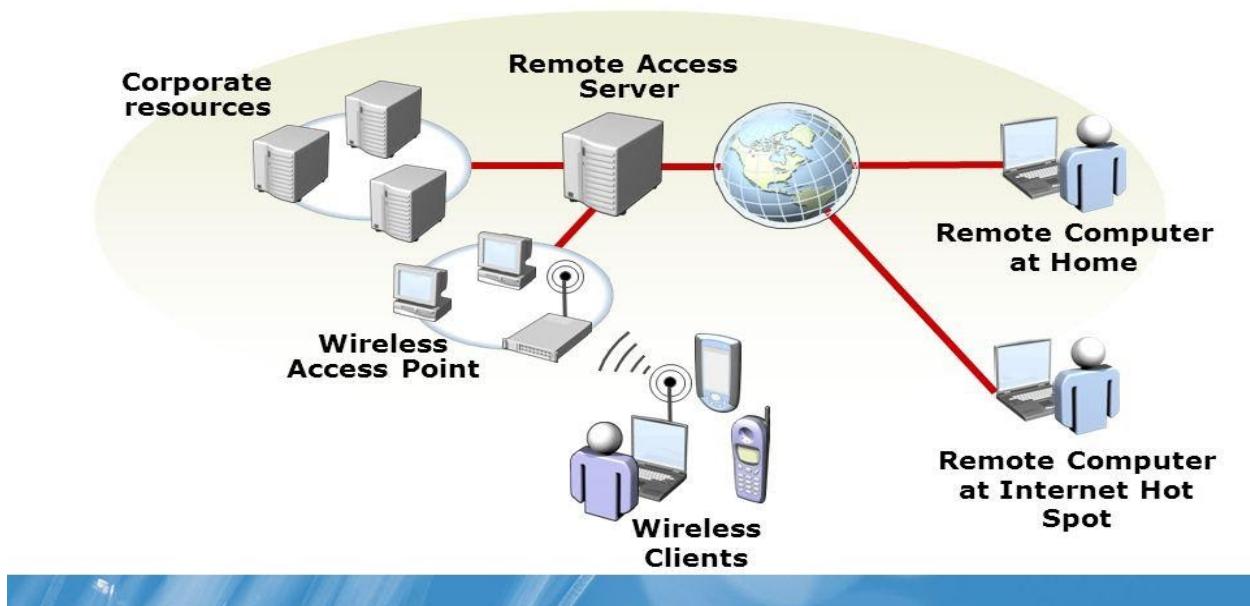
Remote Access



Image

20-<https://slideplayer.com/slide/14892336/91/images/2/Remote+Access+Just+another+computer+on+the+network.+Functions+as+if+it+was+on+the+LAN.jpg>

- A remote access server (RAS) is a type of server that provides a suite of services to remotely connected users over a network or the Internet.
- It operates as a remote gateway or central server that connects remote users with an organization's internal local area network (LAN).
- RAS is a service that allows remote clients to connect to the server over a modem using a RAS-based protocol such as the Serial Line Internet Protocol (SLIP) or the newer Point-to-Point Protocol (PPP).
- PPP can run with network protocols such as TCP/IP, IPX/SPX, and NetBEUI; SLIP only supports TCP/IP.
- Examples : Team Viewwer, Ammyy software



Image

21-<https://slideplayer.com/slide/7602148/25/images/4/Remote+Computer+at+Home+Remote+Computer+at+Internet+Hot+Spot.jpg>

Web Services

Web service is a standardized medium to circulate communication between the client and server applications on the World Wide Web.

A web service is a software module that is designed to perform a certain set of tasks.

Web Services

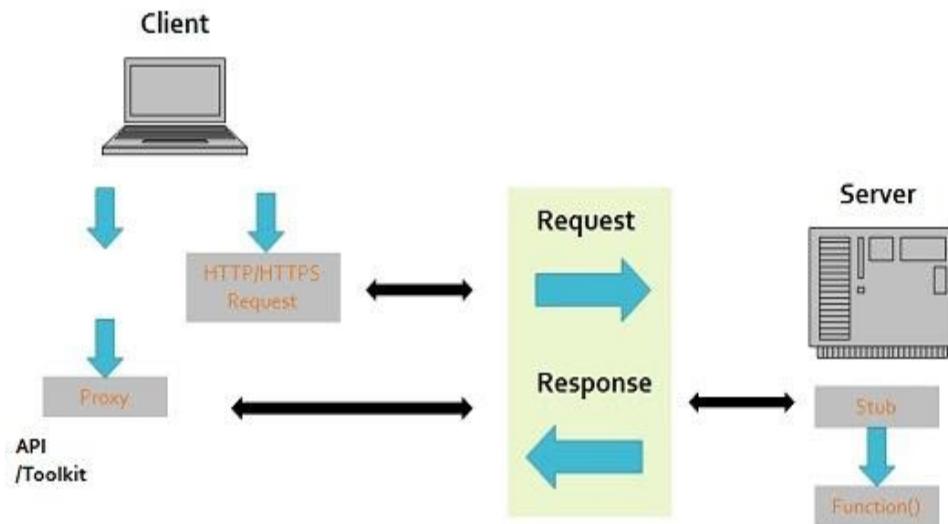


Image 22-<https://documentation.alphasoftware.com/pages/Guides/Services/Web%20Service%20Clients/images/WebServicesSimple.jpg>

A web service is a client server application or application component for communication

A web service communicate over network between two devices

It is a software system for interoperable machine to machine communication

A web service is a collection of open protocols and standards used for exchanging data between applications or systems

Web Services Architecture

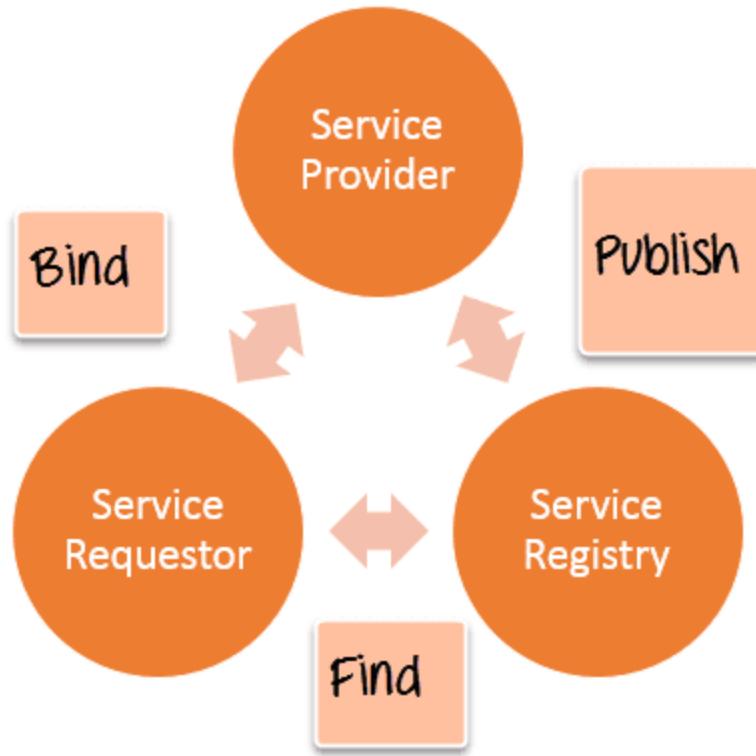


Image 23-https://www.guru99.com/images/3-2016/032316_0646_Webservicea3.png

1. **Provider** - The provider creates the web service and makes it available to client application who want to use it.
2. **Requestor** - A requestor is nothing but the client application that needs to contact a web service. The client application can be a .Net, Java, or any other language based application which looks for some sort of functionality via a web service.
3. **Broker** - The broker is nothing but the application which provides access to the UDDI. The UDDI, as discussed in the earlier topic enables the client application to locate the web service.

-
1. **Publish** - A provider informs the broker (service registry) about the existence of the web service by using the broker's publish interface to make the service accessible to clients
 2. **Find** - The requestor consults the broker to locate a published web service
 3. **Bind** - With the information it gained from the broker(service registry) about the web service, the requestor is able to bind, or invoke, the web service.

Types of Web Services

There are mainly two types of web services.

1. SOAP web services.
2. RESTful web services.

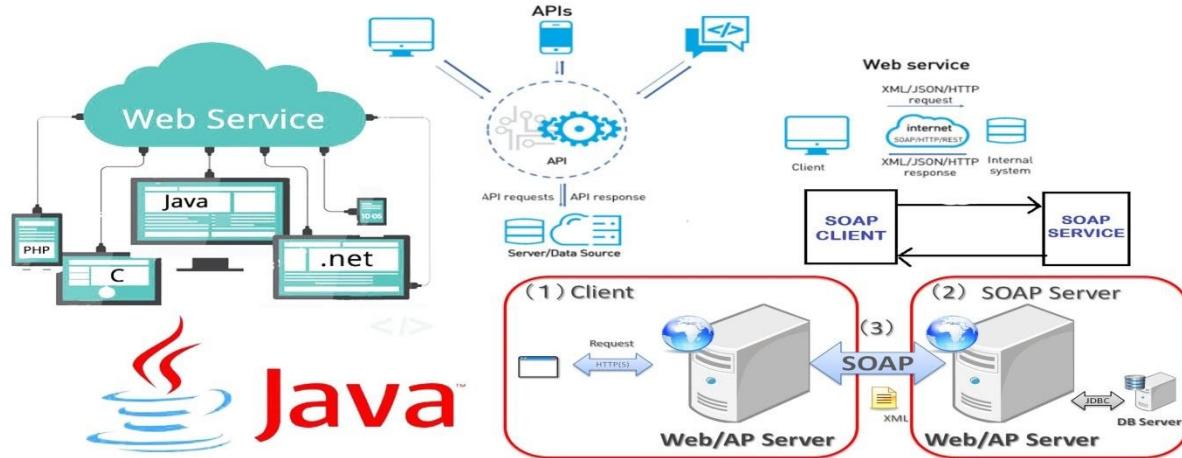
SOAP (Simple Object Access Protocol)

SOAP is known as a transport-independent messaging protocol. SOAP is based on transferring XML data as SOAP Messages. Each message has something which is known as an XML document. Only the structure of the XML document follows a specific pattern, but not the content. The best part of Web services and SOAP is that its all sent via HTTP, which is the standard web protocol.

Here is what a SOAP message consists of

- o Each SOAP document needs to have a root element known as the <Envelope> element. The root element is the first element in an XML document.
- o The "envelope" is in turn divided into 2 parts. The first is the header, and the next is the body.
- o The header contains the routing data which is basically the information which tells the XML document to which client it needs to be sent to.
- o The body will contain the actual message.

The diagram below shows a simple example of the communication via SOAP.



SOAP Web services

Image 24-https://miro.medium.com/max/7016/1*ecBXg7uI6pr1TQU9dVBNew.jpeg

Web Services Advantages

1. **Exposing Business Functionality on the network** - A web service is a unit of managed code that provides some sort of functionality to client applications or end users. This functionality can be invoked over the HTTP protocol which means that it can also be invoked over the internet. Nowadays all applications are on the internet which makes the purpose of Web services more useful. That means the web service can be anywhere on the internet and provide the necessary functionality as required.
2. **Interoperability amongst applications** - Web services allow various applications to talk to each other and share data and services among themselves. All types of applications can talk to each other. So instead of writing specific code which can only be understood by specific applications, you can now write generic code that can be understood by all applications
3. **A Standardized Protocol which everybody understands** - Web services use standardized industry protocol for the communication. All the four layers (Service Transport, XML Messaging, Service

Description, and Service Discovery layers) uses well-defined protocols in the web services protocol stack.

4. **Reduction in cost of communication** - Web services use SOAP over HTTP protocol, so you can use your existing low-cost internet for implementing web services.

REST stands for Representational State Transfer

REST is an architectural style not a protocol.

Restful Web Service is a lightweight, maintainable, and scalable service that is built on the REST architecture.

Restful Web Service, expose API from your application in a secure, uniform, stateless manner to the calling client.

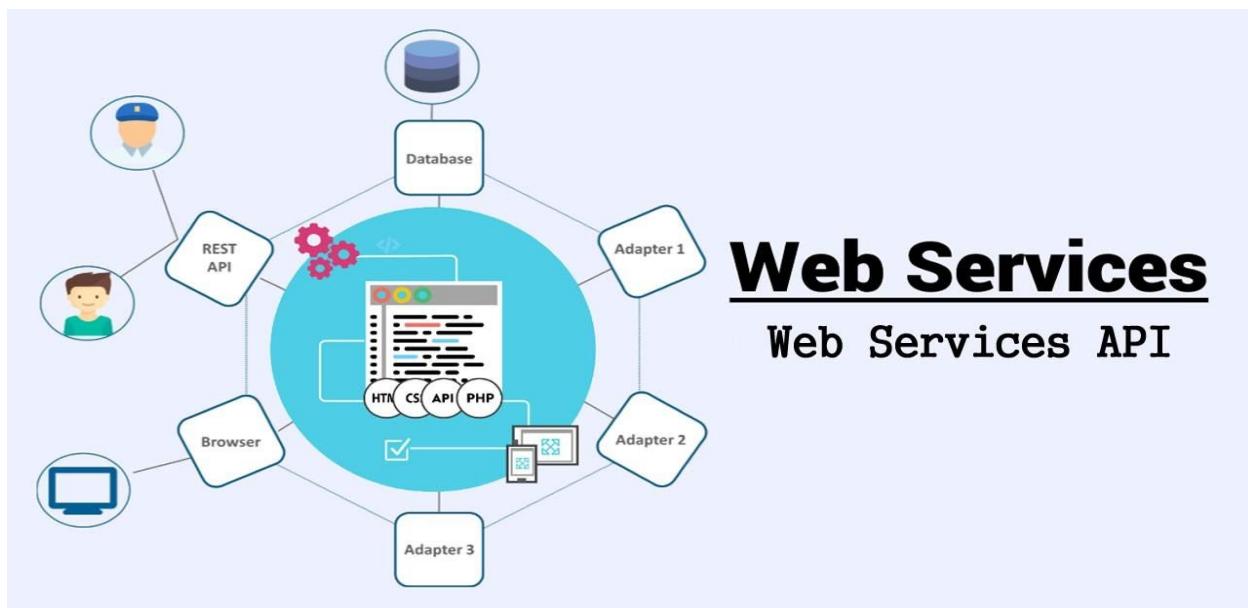


Image 25-https://miro.medium.com/max/7016/1*ecBXg7uI6pr1TQU9dVBNew.jpeg

Advantages

Type	Advantages	Description
SOAP	Security	SOAP defines its own security known as WS Security

	Language and Platform independent	SOAP web services can be written in any programming language and executed in any platform
RESTful	Fast	RESTful Web Services are fast
	Language and Platform independent	It is also language and platform independent
	Can use SOAP	RESTful web services can use SOAP web services as the implementation
	Permits different data format	RESTful web service permits different data format such as Plain Text, HTML, XML and JSON

Disadvantages

Disadvantages	Description
Slow	SOAP uses XML format that must be parsed to be read. It defines many standards that must be followed while developing the SOAP applications. So it is slow and consumes more bandwidth and resource.
WSDL Dependent	SOAP uses WSDL and doesn't have any other mechanism to discover the service

Proxy Services

A proxy server is a server (a computer system or an application) that acts as an intermediate for requests from clients looking for resources from other servers. A client connects to the proxy

server, inviting some service, such as a file, connection, web page, or another resource available from a different server and the proxy server estimates the request as a way to simplify and control its difficulty. Proxies were generated to add structure and encapsulation to circulated systems.

The main purpose of proxy service is to filter requests to ensure that no dangerous traffic creeps in by relating strict routing rules and to boost the performance of the system.

A proxy server is a server (a computer system or an application) that acts as an intermediate for requests from clients looking for resources from other servers.

Functions:

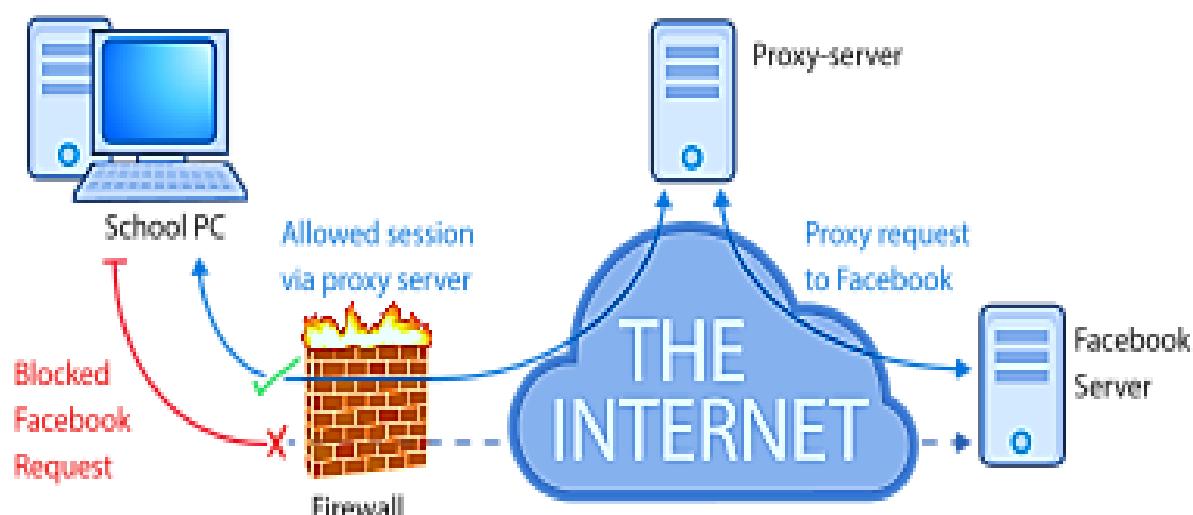
Monitoring and Filtering

Improving performance

Translation

Accessing services anonymously

Security



Image

26-https://www.google.com/url?sa=i&url=https%3A%2F%2Fen.wikipedia.org%2Fwiki%2FProxy_server&psig=AOvVaw04nu3-U1qG

BG9bFwidUYBU&ust=1589697386740000&source=images&cd=vfe&ved=2ahUKEwi5t8ix4rfpAhV23XMBHRYIDFoQr4kDegUIARCcAg

Anonymity: The web server you use can only see the IP address of the proxy and not your system.

Control: If you are the owner of a website, you can see who visits your website. You can choose who visits your website. If you have blocked someone from your website they would get a message saying something like “site unavailable”

Caching: You can save bandwidth if I cache a web site.

Malware: You can intercept unwanted things and stop junks at the proxy.

Load Balancing: Efficiently distributing incoming network traffic among servers.

Types of Proxy services

Proxy services are of two types

Forward proxy.

A forward proxy is an Internet-facing proxy that is used to retrieve a range of sources.

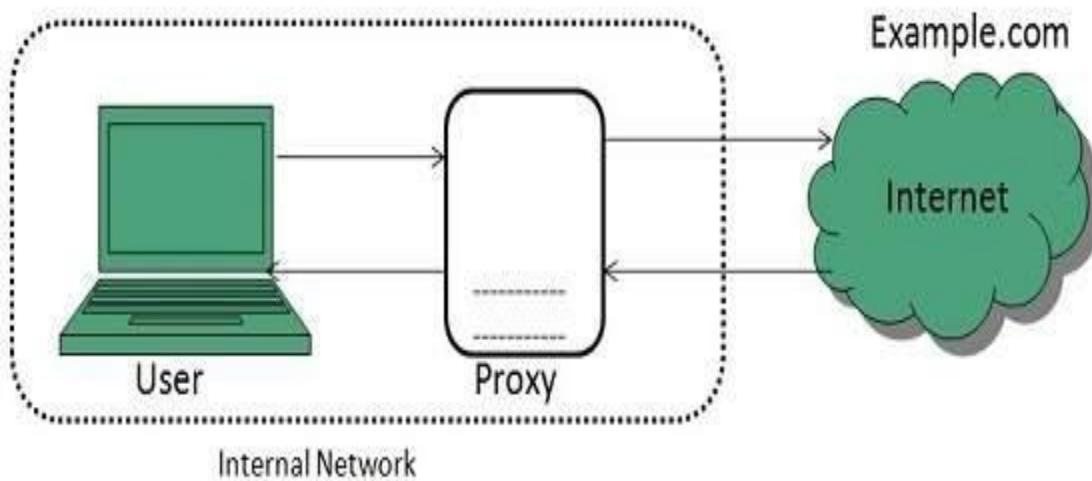


Image 27:-https://www.tutorialspoint.com/internet_technologies/images/internet-forward_proxy.jpg

Reverse proxy

A reverse proxy is particularly used for the protection and security of the server. It includes tasks like caching, authentication and decryption.

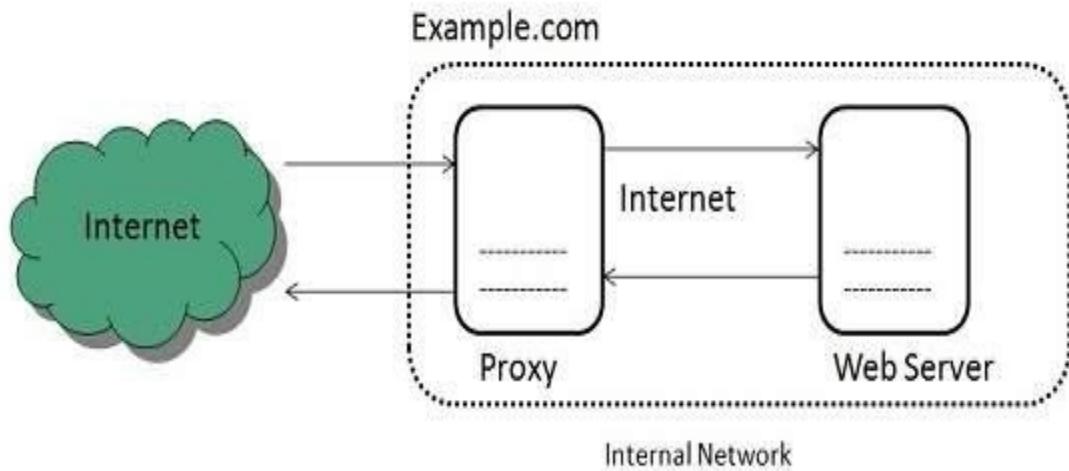


Image 28-https://www.tutorialspoint.com/internet_technologies/images/internet-reverse_proxy.jpg

Install and configure Linux server environment

In this section, we will read about:

- Configuration Plan
- Public and data directory
- Host file
- SWAT
- Password

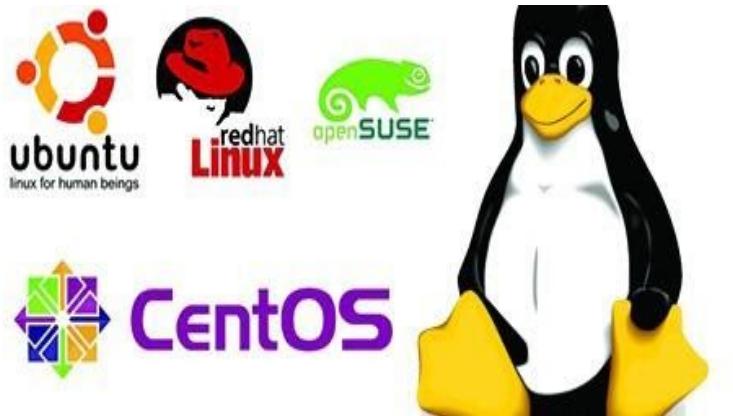


Image 1 – Linux distributions

Reference - <https://medium.com/viithiisys/10-steps-to-secure-linux-server-for-production-environment-a135109a57c5>

Configuration Plan

It is an idea to formally identify the goals, scope, and needs of a new server before beginning.

- **Server Role**

Servers will be purpose-built devices. This means that a server will run the services that are necessary to perform its role. It is the “Role-Specific” section containing guidelines for specific common server roles.

- **Vulnerable Services**

Many services have inherent security vulnerabilities, often because they do not encrypt sensitive traffic.

- **Picking a Platform**

It is time to pick a delivery of Linux. Use an advanced server-oriented system when at all possible. ITStends to use Red Hat Linux and may be able to provide licenses upon request.

- **Network and Access Control**

It is essential to plan network architecture and configuration ahead of time. Using a “least access necessary” model, plan what network sectors need access to this machine.

- **Users and Authentication**

Recognize potential users and access levels ahead of time. Decide what users need what roles and what groups will be needed to manage those roles. An “employee” group or a “managers” group may be necessary so that employees are not granted full root access just for this purpose.

Public and data directory

A public folder is a function of a software application, It is the only one that handles data of any type, that allows an operator to share files with other operators and devices within the same network or the same computer. Different features and setups depending on the application in public folder. Data directory initialization can be done automatically, after installing MySQL then will initialization data directory.

```
shell> mkdir MySQL-files
```

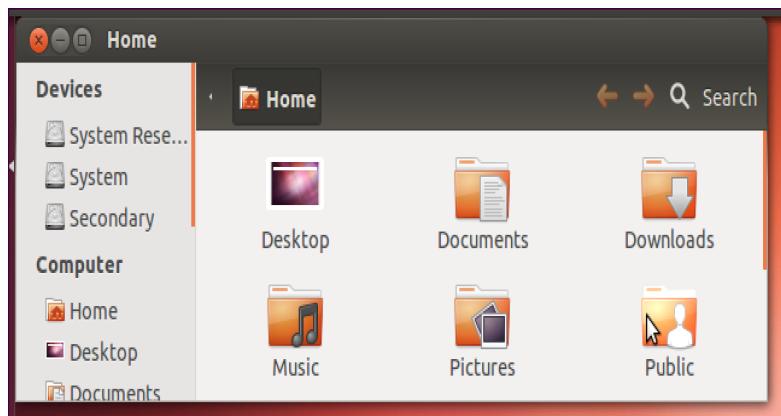


Image 2 – Public folder

Reference - <https://www.howtogeek.com/116309/use-ubuntus-public-folder-to-easily-share-files-between-computers/>

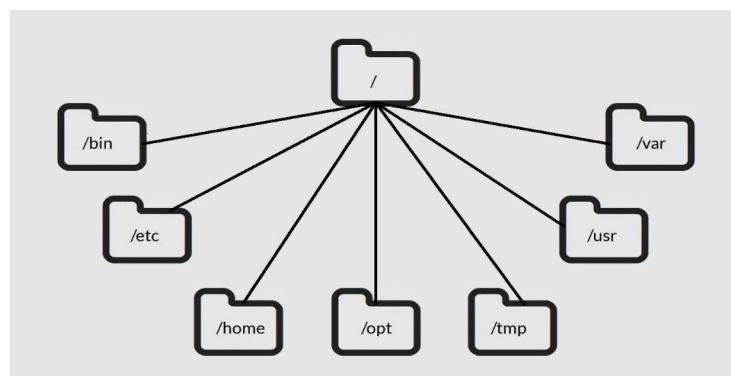


Image 3 – Data directory in Linux

Reference - <https://www.linuxtrainingacademy.com/linux-directory-structure-and-file-system-hierarchy/>

Host file

All operating systems with the support of the network have a hosts file in order to translate hostnames to IP addresses. Open a website by typing its hostname, the system will read through the host's file to a corresponding IP address. These are the simple text file located in the etc folder on Linux and Mac OS.

Application

- Block a website
- Handle an attack or resolve a prank
- Create a duplicate for locations on your local server
- Override addresses that your DNS server provides
- Control access to network traffic

SWAT

SWAT is a web-based application that helps to configure Samba. It is used to configure the settings on your samba server using GUI (graphic user interface).

Functions of SWAT

Globals

Provides access to the global parameters in smb.conf. You can work at one of two levels, which shows only the more important options listed, or Advanced, which shows every available parameter. Click on the corresponding buttons to pick your preferred level. Make any edits then click on Commit Changes to save your choices, or Reset Values to go back to the original smb.conf values.

Shares

Let's create, edit, or drop shares. Edit an existing share need to pick it from the combo box, then click on Choose Share; clicking on Delete Share will delete it.

Printers

It works like shares but works with printers instead.

Wizard

Lets you do a quick server configuration. Choice either a standalone server, a domain controller, or a domain member.

Status

Shows you which services are running, active shares, and open files. You can click on Auto Refresh so the page will refresh on its own every so many second (30 by default).

View

View the current configuration file. You can click on the View button to see it either in the normal view or the full view.

Password

It is used to create, delete, enable, or disable local Samba users and change passwords for a local or remote server.

Password

In Linux, regular operators and superoperators can access services via password authentication. By default, the root user account password is locked in Ubuntu Linux for safety reasons. As a result, you cannot log in using root user or use a command such as ‘su -’ to become a Super operator.

type passwd command is used to change your own password:

```
$ passwd
```

Output:

Changing password

(current) UNIX password:

Enter new UNIX password:

Retype new UNIX password:

passwd: password updated successfully

The -g option is used for group password change. change password for group sales:

```
# passwd -g group name
```

The current group password is not prompted for. The -r option is used with the -g option because to remove the current password group. This allows group access to all members.

The -r option is used with the -g option to restrict the named group for all operators. As a common guideline, passwords should consist of 6 to 8 characters including one or more from each of the following sets:

-
- Lowercase alphabetic
 - Uppercase alphabetic
 - Digits 0 thru 9
 - Punctuation marks

Install & configure the different types of network devices in a network

In this section, we will read about:

- Functions of NIC
- Repeaters
- Hub
- Switches
- Routers
- Bridges.
- Internet serviceprovider

Network Devices

Network devices are the devices used for consolidating a network, connecting to a network, routing the packets, strengthening the signals, interactive with others, surfing the web, sharing files on the network.

Functions of Network Interface Card (NIC)

A Network interface card (also known as a NIC, network card, or network interface controller) is an electronic device that joins a computer to a computer network, usually a LAN. It is considered a piece of computer hardware. The NIC contains the electronic circuitry required to connect using a wired connection (e.g., Ethernet) or a wireless connection (e.g., WiFi).

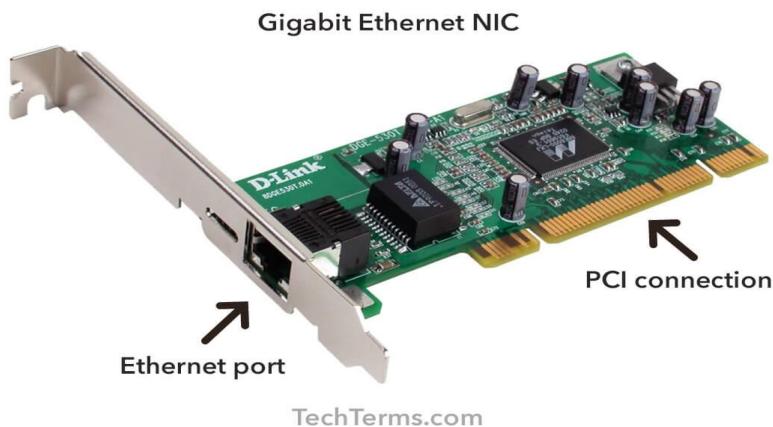


Image 4 – Gigabit Ethernet NIC
Reference - <https://techterms.com/definition/nic>

Repeaters

Repeaters receive network signals on one port, amplify them, and repeat them out the other port. Since they operate only at the Physical layer of the OSI model, repeaters can intersect

different media types but cannot convert protocols.

The repeater can do more harm than good because it propagates everything, including noise and error packets. The purpose of a repeater is to extend the maximum distance of a single network segment.

Repeater Mode

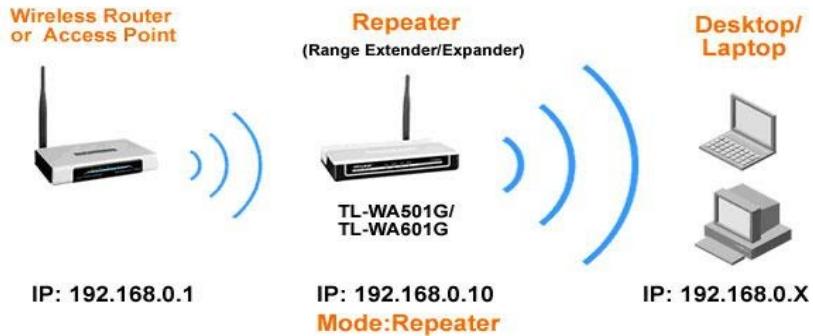


Image 5 – Repeater Mode
Reference - <https://www.tp-link.com/ae/support/faq/151/>

Hub

A hub (also called a concentrator) serves as a central joining point for several network devices. At a basic level, a hub is nothing more than a multiport repeater. A hub repeats what it obtains on one port to all other ports.

Types of hub

There are two types of Hub

Active Hub

An active hub is usually powered and amplifies and cleans up the signal it receives, thus doubling the effective segment distance limitation for the specific topology.

Active Hubs

- Need a power source
- Power added to the signal when passed through port
- Prevents weakening of signal by multiple devices being attached
- Repeats signal to all hosts connected to hub

lynda.com

Image 6 – Active Hub features

Reference - <https://www.lynda.com/Windows-Server-tutorials/Exploring-hubs/408231/435884-4.html>

Passive Hub

A passive hub typically is unpowered and makes only physical, electrical connections.

Usually, the maximum segment distance of a topology is shortened because the hub takes some power away from the signal strength in order to do its job.



2.Pассивный хаб

- Act as connection point, not as repeater.
- Do not require electricity to run.
- Inexpensive and easy to configure.

Image 7 – Passive Hub features

Reference - <https://www.slideshare.net/patelgopal1044/network-d>



Switches

What is a switch ?

Switches are key building blocks for any network. They connect multiple devices, such as computers, wireless access points, printers, and servers; on the same network within a building or campus. A switch enables connected devices to share information and talk to each other.

A switch is a data link layer networking device which connects devices in a network and uses packet switching to send and receive data over the network.

When a user accesses the internet or another computer network outside their immediate location, messages are sent through the network of transmission media. This technique of transferring the information from one computer network to another network is known as **switching**. Switching in a computer network is achieved by using switches. A switch is a small hardware device which is used to join multiple computers together with one local area network (LAN).



Image 1 -Switch

Reference - <https://www.indiamart.com/proddetail/networking-switches-dlink-and-digisol-11032831233.html>

Role of switches in networking

- Network switches operate at layer 2 (Data link layer) in the OSI model.
- Switching is transparent to the user and does not require any configuration in the home network.
- Switches are used to forward the packets based on MAC addresses.
- A Switch is used to transfer the data only to the device that has been addressed. It verifies the destination address to route the packet appropriately.
- It is operated in full duplex mode.
- Packet collision is minimum as it directly communicates between source and destination.
- It does not broadcast the message as it works with limited bandwidth.

Why is switching concept required ?

Switching concept is developed because of the following reasons:

- Bandwidth: It is defined as the maximum transfer rate of a cable. It is a very critical and expensive resource. Therefore, switching techniques are used for the effective utilization of the bandwidth of a network.
- Collision: Collision is the effect that occurs when more than one device transmits the message over the same physical media, and they collide with each other. To overcome this problem, switching technology is implemented so that packets do not collide with each other.

Types of Switches

Switches are the connectivity points of an Ethernet network. These are small devices that can receive data from multiple input ports and send it to the specific output port that takes data to its

intended destination in the network. There are different types of switches in a network. These are:

1. Unmanaged switches –

These are the switches that are mostly used in home networks and small businesses as they plug-in and instantly start doing their job and such switches do not need to be watched or configured. These require only small cable connections. It allows devices on a network to connect with each other such as a computer to a computer or a computer to a printer in one location. They are the least expensive switches among all categories.



Image2 -Unmanaged Switch

Reference - <https://www.netgear.com/business/products/switches/unmanaged/>

2. Managed switches –

These types of switches have many features like the highest levels of security, precision control and full management of the network. These are used in organisations containing a large network and can be customized to enhance the functionality of a certain network. These are the most costly option but their scalability makes them an ideal option for a network that is growing. They are achieved by setting a simple network management protocol(SNMP).

They are of two types:

a. Smart switches:

These switches offer basic management features with the ability to create some levels of security but have a simpler management interface than the other managed switches. Thus they are often called partially managed switches. These are mostly used in fast and constant LANs which support gigabit data transfer and allocations. It can accept configuration of VLANs (Virtual LAN).

b. Enterprise managed switches:

They have features like ability to fix, copy, transform and display different network configurations along with a web interface SNMP agent and command

line interface. These are also known as fully managed switches and are more expensive than the smart switches as they have more features that can be enhanced. These are used in organisations that contain a large number of ports, switches and nodes.



Image 3 -Managed Switch

Reference - <https://www.netgear.com/business/products/switches/unmanaged/>

3. LAN switches –

These are also known as Ethernet switches or data switches and are used to reduce network congestion or bottleneck by distributing a package of data only to its intended recipient. These are used to connect points on a LAN.



Image4 -LAN Switch

Reference - <https://www.netgear.com/business/products/switches/unmanaged/>

4. PoE switches –

PoE switches are used in PoE technology which stands for power over Ethernet that is a technology that integrates data and power on the same cable allowing power devices to receive data in parallel to power. Thus these switches provide greater flexibility by simplifying the cabling process.



Image5 -PoE Switch

Reference -<https://www.wifi-stock.com/details/zq-poes-8-7.html/products/switches/unmanaged/>

Advantages of Switches

- Switches increase available network bandwidth
- Switches reduce the workload on individual computers
- Switches increase network performance
- Networks that include switches experience fewer frame collisions because switches create collision domains for each connection (a process called micro segmentation)
- Switches connect directly to workstations.

Disadvantages of Switches

- A Switch is more expensive than network bridges.
- A Switch cannot determine the network connectivity issues easily.
- Proper designing and configuration of the switch are required to handle multicast packets.
- Broadcast traffic may be troublesome.
- While limiting broadcasts, they are not as good as routers.

Routers

What is a Router ?

The router is a physical or virtual internetworking device that is designed to receive, analyze, and forward data packets between computer networks. A router examines a destination IP address of a given data packet, and it uses the headers and forwarding tables to decide the best way to transfer the packets. There are some popular companies that develop routers; such are Cisco, 3Com, HP, Juniper, D-Link, Nortel, etc. Some important points of routers are given below:

- A router is used in LAN (Local Area Network) and WAN (Wide Area Network) environments. For example, it is used in offices for connectivity, and you can also establish the connection between distant networks such as from Bhopal to
- It shares information with other routers in networking.
- It uses the routing protocol to transfer the data across a network.
- Furthermore, it is more expensive than other networking devices like switches and hubs.



Image6 -Router

Reference - <https://www.lifewire.com/what-is-a-router-2618162>

A router works on the third layer of the OSI model, and it is based on the IP address of a computer. It uses protocols such as ICMP to communicate between two or more networks. It is

also known as an intelligent device as it can calculate the best route to pass the network packets from source to the destination automatically.

A virtual router is a software function or software-based framework that performs the same functions as a physical router. It may be used to increase the reliability of the network by virtual router redundancy protocol, which is done by configuring a virtual router as a default gateway. A virtual router runs on commodity servers, and it is packaged with alone or other network functions, like load balancing, firewall packet filtering, and wide area network optimization capabilities.

How does Router work ?

A router analyzes a destination IP address of a given packet header and compares it with the routing table to decide the packet's next path. The list of routing tables provides directions to transfer the data to a particular network destination. They have a set of rules that compute the best path to forward the data to the given IP address.

Routers use a modem such as a cable, fiber, or DSL modem to allow communication between other devices and the internet. Most of the routers have several ports to connect different devices to the internet at the same time. It uses the routing tables to determine where to send data and from where the traffic is coming.

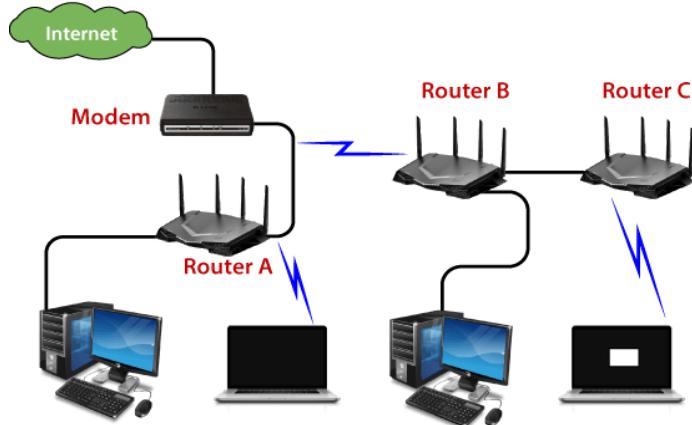


Image7 -Router working

Reference - <https://www.javatpoint.com/router>

A routing table mainly defines the default path used by the router. So, it may fail to find the best way to forward the data for a given packet. For example, the office router along a single default path instructs all networks to its internet services provider.

There are two types of tables in the router that are static and dynamic. The static routing tables are configured manually, and the dynamic routing tables are updated automatically by dynamic routers based on network activity.

What is a Routing Table in Router?

A routing table determines the path for a given packet with the help of an IP address of a device and necessary information from the table and sends the packet to the destination network. The routers have the internal memory that is known as Random Access Memory (RAM). All the information of the routing table is stored in RAM of routers.

A routing table contains the following entities:

- It contains an IP address of all routers which are required to decide the way to reach the destination network.
- It includes extrovert interface information.
- Furthermore, it also contained IP addresses and subnet masks of the destination host.

Network Element in Router

There are two types of a network element in the router which are as follows:

- Control plane: A router supports a routing table that determines which path and physical interface connection should be used to send the packet. It is done by using internal pre-configured directives, which are called static routes, or by learning routes with the help of routing protocol. A routing table stores the static and dynamic routes. Then the control-plane logic eliminates the unnecessary directives from the table and constructs a forwarding information base that is used by the forwarding plane.
- Forwarding plane: A router sends data packets between incoming and outgoing interface connections. It uses information stored in the packet header and matches it to entries in

the FIB, which is supplied by the control plane; accordingly, it forwards the data packet to the correct network type. It is also called the user plane or data plane.

Routing Protocols

Routing protocols specify a way for the router to identify other routers on the network and make dynamic decisions to send all network messages. There are several protocols, which are given below:

- Open Shortest Path First (OSPF): It is used to calculate the best route for the given packets to reach the destination, as they move via a set of connected networks. It is identified by the Internet Engineering Task Force (IETF) as Interior Gateway Protocol.
- Border Gateway Protocol (BGP): It helps manage how packets are routed on the internet via exchange of information between edge routers. It provides network stability for routers if one internet connection goes down while forwarding the packets, it can adapt another network connection quickly to send the packets.
- Interior Gateway Routing Protocol (IGRP): It specifies how routing information will be exchanged between gateways within an independent network. Then, the other network protocols can use the routing information to determine how transmissions should be routed.
- Enhanced Interior Gateway Routing Protocol (EIGRP): In this protocol, if a router is unable to find a path to a destination from the tables, it asks the route to its neighbors, and they pass the query to their neighbors until a router has found the path. When the entry of the routing table changes in one of the routers, it informs its neighbors only about the changes, but does not send the entire table.
- Exterior Gateway Protocol (EGP): It decides how routing information can be exchanged between two neighbor gateway hosts, each of which has its own router. Additionally, it is commonly used to exchange routing table information between hosts on the internet.
- Routing Information Protocol (RIP): It determines how routers can share information while transferring traffic among connected groups of local area networks. The maximum number of hops that can be allowed for RIP is 15, which restricts the size of networks that RIP can support.

Features of Router

- A router works on the 3rd layer (Network Layer) of the OSI model, and it is able to communicate with its adjacent devices with the help of IP addresses and subnet.
- A router provides high-speed internet connectivity with the different types of ports like gigabit, fast-Ethernet, and STM link port.
- It allows the users to configure the port as per their requirements in the network.
- Routers' main components are central processing unit (CPU), flash memory, RAM, Non-Volatile RAM, console, network, and interface card.
- Routers are capable of routing the traffic in a large networking system by considering the sub-network as an intact network.
- Routers filter out the unwanted interference, as well as carry out the data encapsulation and decapsulation process.
- Routers provide the redundancy as it always works in master and slave mode.
- It allows the users to connect several LAN and WAN.
- Furthermore, a router creates various paths to forward the data.

Types of Routers

There are various types of routers in networking; such are given below:

1. Wireless Router: Wireless routers are used to offer Wi-Fi connectivity to laptops, smartphones, and other devices with Wi-Fi network capabilities, and it can also provide standard ethernet routing for a small number of wired network systems.

Wireless routers are capable of generating a wireless signal in your home or office, and it allows the computers to connect with routers within a range, and use the internet. If the connection is indoors, the range of the wireless router is about 150 feet, and when the connection is outdoors, then its range is up to 300 feet.

Furthermore, you can make more secure wireless routers with a password or get your IP address. Thereafter, you can log in to your router by using a user ID and password that will come with your router.



Image8 -Wireless Router

Reference - <https://www.lifewire.com/what-is-a-router-2618162>

2. Brouter: A brouter is a combination of the bridge and a router. It allows transferring the data between networks like a bridge. And like a router, it can also route the data within a network to the individual systems. Thus, it combines these two functions of bridge and router by routing some incoming data to the correct systems while transferring the other data to another network.

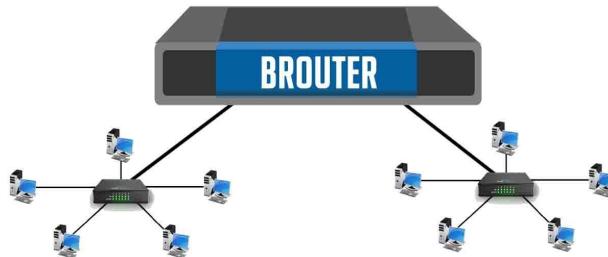


Image9 -Brouter

Reference - <https://www.lifewire.com/what-is-a-router-2618162>

3. Core router: A core router is a type of router that can route the data within a network, but it is not able to route the data between the networks. It is a computer communication system device and the backbone of networks, as it helps to link all network devices. It is used by internet service providers (ISPs), and it also provides various types of fast and powerful data communication interfaces.



Image10 -Core Router

Reference -<https://www.indiamart.com/proddetail/cisco-service-provider-core-router-17912957255.html>

4. Edge router: An edge router is a lower-capacity device that is placed at the boundary of a network. It allows an internal network to connect with the external networks. It is also called an access router. It uses an External BGP (Border Gateway Protocol) to provide connectivity with remote networks over the internet.

There are two types of edge routers in networking:

- Subscriber edge router
- Label edge router

The subscriber edge router belongs to an end-user organization, and it works in a situation where it acts on a border device.

The label edge router is used in the boundary of Multiprotocol Label Switching (MPLS) networks. It acts as a gateway between the LAN, WAN, or the internet.



Image11 -Edge Router

Reference - <https://www.technodabbler.com/edge-router-x/>

5. Broadband routers: Broadband routers are mainly used to provide high-speed internet access to computers. It is needed when you connect to the internet through phone and use voice over IP technology (VOIP).

All broadband routers have the option of three or four Ethernet ports for connecting the laptop and desktop systems. A broadband router is configured and provided by the internet service provider (ISP). It is also known as a broadband modem, asymmetric digital subscriber line (ADSL), or digital subscriber line (DSL) modem.



Image12 - Broadband Router

Reference - <https://www.technodabbler.com/edge-router-x/>

Advantages of Router

There are so many benefits of a router, which are given below:

- Security: Router provides the security, as LANs work in broadcast mode. The information is transmitted over the network and traverses the entire cable system. Although the data is available to each station, but the station which is specifically addressed reads the data.
- Performance enhancement: It enhances the performance within the individual network. For example, if a network has 14 workstations, and all generate approximately the same volume of traffic. The traffic of 14 workstations runs through the same cable in a single network. But if the network is divided into two sub-networks each with 7 workstations, then a load of traffic is reduced to half. As each of the networks has its own servers and hard disk, so fewer PCs will need the network cabling system.
- Reliability: Routers provide reliability. If one network gets down when the server has stopped, or there is a defect in the cable, then the router services, and other networks will not be affected. The routers separate the affected network, whereas the unaffected networks remain connected, without interrupting the work and any data loss.
- Networking Range: In networking, a cable is used to connect the devices, but its length cannot exceed 1000 meters. A router can overcome this limitation by performing the function of a repeater (Regenerating the signals). The physical range can be as per the requirement of a particular installation, as long as a router is installed before the maximum cable range exceeds.

Disadvantages of Router

- They operate based on routable network protocols.
- They are expensive compared to other network devices.
- Dynamic router communications can cause additional network overhead. This results into less bandwidth for user data.
- They are slower as they need to analyze data from layer-1 through layer-3.
- They require a considerable amount of initial configurations.
- They are protocol dependent devices which must understand the protocol they are forwarding.

Bridges

What is a bridge ?

A network bridge is a device that divides a network into segments. Each segment represents a separate collision domain, so the number of collisions on the network is reduced. Each collision domain has its own separate bandwidth, so a bridge also improves the network performance.

A bridge works at the Data link layer (Layer 2) of the OSI model. It inspects incoming traffic and decides whether to forward it or filter it. Each incoming Ethernet frame is inspected for the destination MAC address. If the bridge determines that the destination host is on another segment of the network, it forwards the frame to that segment.

Consider the following example network:

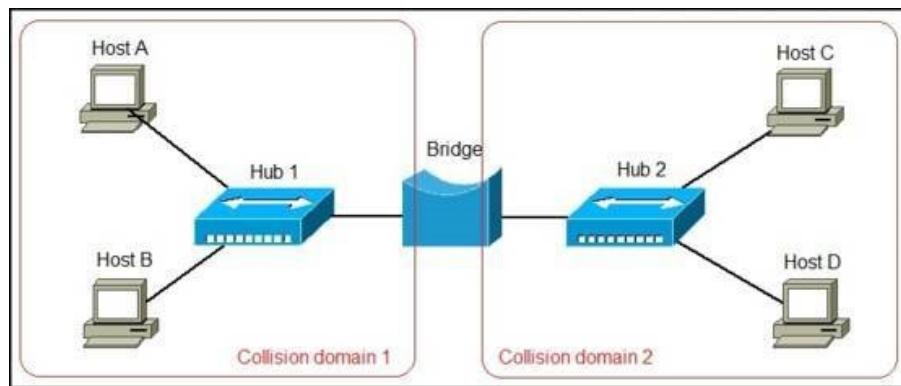


Image13 -Bridge

Reference -<https://geek-university.com/ccna/what-is-a-network-bridge/>

In the picture above we have a network of four computers. The network is divided into segments by a bridge. Each segment is a separate collision domain with its own bandwidth. Let's say that Host A wants to communicate with Host C. Host A will send the frame with the Host C's destination MAC address to the bridge. The bridge will inspect the frame and forward it to the segment of the network Host C is on.

Network bridges offer substantial improvements over network hubs, but they are not widely used anymore in modern LANs. Switches are commonly used instead.

Types of Bridges

- Transparent Bridge : As the name suggests, it is an invisible bridge in the computer network. The main function of this bridge is to block or forward the data depending on the MAC address. The other devices within the network are unaware of the existence of bridges. These types of bridges are most popular and operate in a transparent way to the entire networks which are connected to hosts. This bridge saves the addresses of MAC within a table that is similar to a routing table. This estimates the information when a packet is routed to its position. So it can also merge several bridges to check incoming traffic in a better way. These bridges are implemented mainly in Ethernet networks.
- Translational Bridge : A translational bridge plays a key role in changing a networking system from one type to another. These bridges are used to connect two different networks like token ring & Ethernet. This bridge can add or remove the data based on the traveling direction, and forward the frames of the data link layer in between LANs which uses various types of network protocols. The different network connections are Ethernet to FDDI/token ring otherwise Ethernet on UTP (unshielded twisted pair) to coax & in between FOC and copper wiring.
- Source-route Bridge : Source-route Bridge is one type of technique used for Token Ring networks and it is designed by IBM. In this bridge, the total frame route is embedded in one frame. So that it allows the bridge to make precise decisions of how the frame is forwarding using the network. By using this method, two similar network segments are connected to the data link layer. It can be done in a distributed way wherever end-stations join within the bridging algorithm.

Functions of Bridges

The main functions of bridges in a computer network include the following.

- This networking device is used for dividing local area networks into several segments.
- In the OSI model, it works under the data link layer.
- It is used to store the address of MAC in PCs used in a network and also used for diminishing the network traffic.

Advantages of Bridge

The advantages are

- It acts as a repeater to extend a network
- Network traffic on a segment can be reduced by subdividing it into network communications
- Collisions can be reduced.
- Some types of bridges connect the networks with the help of architectures & types of media.
- Bridges increase the available bandwidth to individual nodes because fewer network nodes share a collision domain
- It avoids waste BW (bandwidth)
- The length of the network can be increased.
- Connects different segments of network transmission.

Disadvantages of Bridge

The disadvantages are

-
- It is unable to read specific IP addresses because they are more troubled with the MAC addresses.
 - They cannot help while building the network between the different architectures of networks.
 - It transfers all kinds of broadcast messages, so they are incapable to stop the scope of messages.
 - These are expensive as we compare with repeaters
 - It doesn't handle more variable & complex data load which occurs from WAN.

Difference between Bridge and Router

Bridge	Router
A bridge is a networking device that is used to connect two local area networks (LANs) by using media access control addresses and transmit the data between them.	A router is also a networking device that sends the data from one network to another network with the help of their IP addresses.
A bridge is able to connect only two different LAN segments.	A router is capable of connecting the LAN and WAN.
A bridge transfers the data in the form of frames.	A router transfers the data in the form of packets.
It sends data based on the MAC address of a device.	It sends data based on the IP address of a device.
The bridge has only one port to connect the device.	The router has several ports to connect the devices.
The bridge does not use any table to forward the data.	The router uses a routing table to send the data.

Internet Service Provider

What is an Internet Service Provider ?

ISP stands for Internet Service Provider. It is a company that provides access to the internet and similar services such as Website designing and virtual hosting. For example, when you connect to the Internet, the connection between your Internet-enabled device and the internet is executed through a specific transmission technology that involves the transfer of information packets through an Internet Protocol route.

Data is transmitted through different technologies, including cable modem, dial-up, DSL, high speed interconnects. An Internet service provider is also known as an Internet access provider (IAP).



Image14 -ISP

Reference -<https://www.javatpoint.com/isp-full-form>

Why use an ISP?

Unless you have a specialized line (other than a telephone line), you cannot connect directly to the internet using your telephone line. Indeed, the telephone line was not designed for this:

- it was originally designed to transport "voice", i.e. a frequency modulation in the range of the voice tone
- telephone servers only know how to start a conversation from a telephone number
- unless you resort to a special service, generally it is not possible to have communication between more than two points...

So, the internet service provider is an intermediary (connected to the internet by specialized lines) which gives you access to the Internet, using a number which you enter using your modem, and which enables a connection to be established.

How does the ISP connect you to the Internet?

When you are connected to the Internet through your service provider, communication between you and the ISP is established using a simple protocol: PPP (Point to Point Protocol), a protocol making it possible for two remote computers to communicate without having an IP address. In fact your computer does not have an IP address. However an IP address is necessary to be able to go onto the Internet because the protocol used on the Internet is the TCP/IP protocol which makes it possible for a very large number of computers which are located by these addresses to communicate. So, communication between you and the service provider is established according to the PPP protocol which is characterised by:

- a telephone call
- initialization of communication
- verification of the user name (login or userid)
- verification of the password

Once you are "connected", the internet service provider lends you an IP address which you keep for the whole duration that you are connected to the internet. However, this address is not fixed because at the time of the next connection the service provider gives you one of its free addresses (therefore different because depending on its capacity, it may have several hundreds of thousand addresses.). Your connection is therefore a proxy connection because it is your service provider

who sends all the requests you make and the service provider who receives all the pages that you request and who returns them to you. It is for these reasons for example that when you have Internet access via an ISP, you must pick up your email on each connection because generally it is the service provider that receives your email (it is stored on one of its servers).

Types of Internet Service Providers

The connection between your Internet enabled device and the global network is executed through a specific digital data transmission technology. It represents the transfer of information packets through an Internet Protocol route.

Accordingly, based on the method of data transmission, the Internet access provided by ISPs can be divided into many types, some of which are as follows:

- Dial-up Internet access - This is the oldest method of providing access to the Internet. It uses a telephone line to perform a modem-to-modem connection. For that purpose, the user's computer is attached to a telephone line enabled modem device, which dials into the node of the ISP and starts transferring data between the servers that store websites the user wants to see and their Internet connected device. The dial-up Internet is today considered outdated in most Internet societies due to the slow connection speed it ensures (about 40-50 kbit/s.). However, the wide availability of telephone access makes this type of Internet access the only alternative for remote areas that remain off the broadband network. It is also the least expensive Internet access service and is preferred by users on a tight budget.

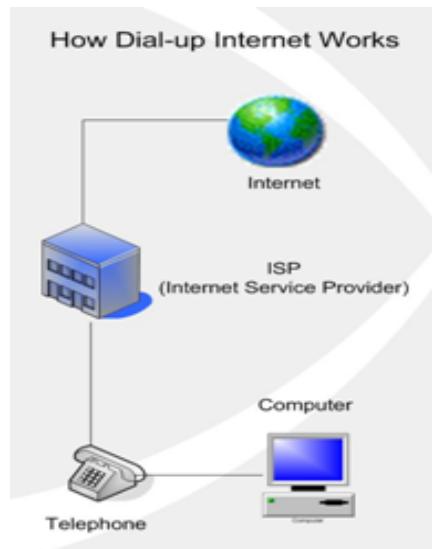


Image15 -Dial-up internet access

Reference -<https://www.highspeed-internet-providers.com/how-dialup-works.html>

- DSL - DSL, which stands for 'digital subscriber line' is an advanced version of the dial-up Internet access method. It uses high frequency to execute a connection over the telephone network and allows the internet and the phone connection to run on the same telephone line. This method offers an Asymmetric Digital Subscriber (ADSL), where the upload speed is less than the download speed, and a Symmetric Digital Subscriber Line (SDSL), which offers equal upload and download speeds. Out of these two, ADSL is more popular among users and is popularly known as DSL.

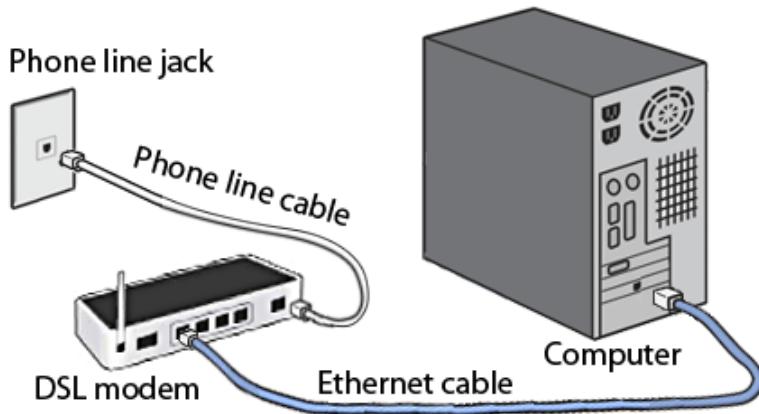


Image16 -DSL

Reference - <https://www.javatpoint.com/dsl-full-form>

- Cable Internet - The cable Internet is among the most preferred methods for providing residential Internet access. Technically speaking, it represents a broadband Internet access method, using the high-bandwidth cable television network to transmit data between the global network and the households. To use cable Internet you will need a cable modem at home that will be connected with the CMTS (Cable Modem Termination System) of your cable ISP. The cable Internet access can be offered together with a cable television subscription and separately, for customers' convenience. The second case incurs higher subscription fees due to the extra equipment installation costs.
- Wireless Broadband (WiBB): It is a modern broadband technology for Internet access. It allows high-speed wireless internet within a large area. To use this technology, you are required to place a dish on the top of your house and point it to the transmitter of your Wireless Internet Service Provider (WISP).

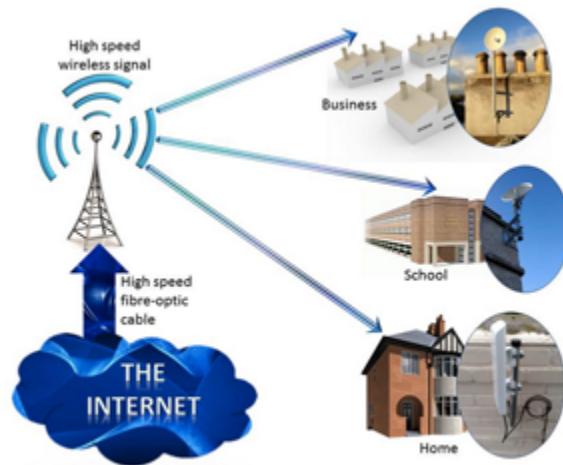


Image17 -Wireless Broadband

Reference -<https://www.wifi4india.com/broadband/wireless-broadband-service.html>

- Wi-Fi Internet - Wi-Fi (from Wireless Fidelity) has become one of the most widely distributed Internet access methods, with the growing usage of portable computers and Internet enabled mobile devices, such as smartphones, PDAs, game consoles, etc. In this sense, it is the most mobile Internet access method, since you are able to use it everywhere as long as you are located within the scope of coverage, i.e. within the range of an Internet connected wireless network. Due to its ability to serve mobile devices, Wi-Fi is used in public places such as airports, hotels and restaurants to provide Internet access to customers. There are also specialized Wi-Fi hotspots where the service is either free or paid. Some of the largest cities in the world are in the process of building Wi-Fi networks that cover all the public places in the central areas.



Image18 - WiFi

Reference -<https://www.princehotels.com/kawana/notice/information-on-internet-wifi-connection-service-in-kawana-hotel/>

- ISDN: It is a short form of Integrated Services Digital Network. It is a telephone system network which integrates a high-quality digital transmission of voice and data over the same standard phone line. It offers a fast upstream and downstream Internet connection speed and allows both voice calls and data transfer.

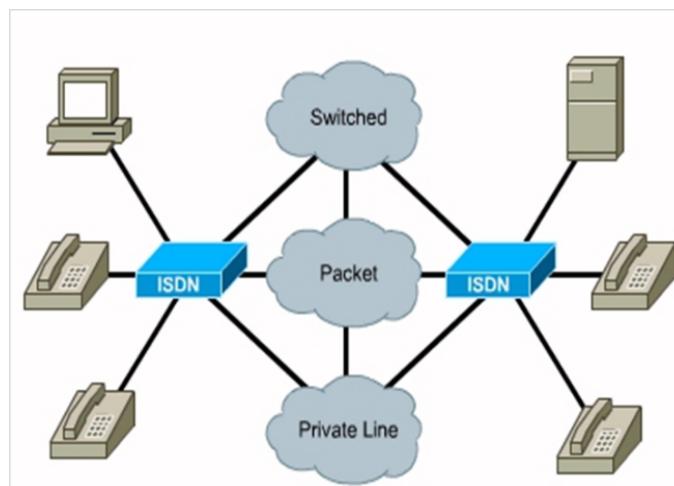


Image19 - ISDN

Reference -<http://jonapchan.blogspot.com/2012/01/isdn.html>

- Ethernet: It is a wired LAN (Local Area Network) where computers are connected within a primary physical space. It enables devices to communicate with each other via a protocol (a set of rules or common network language). It may provide different speeds such as 10 Mbps, 100 Mbps and 10 Gbps.

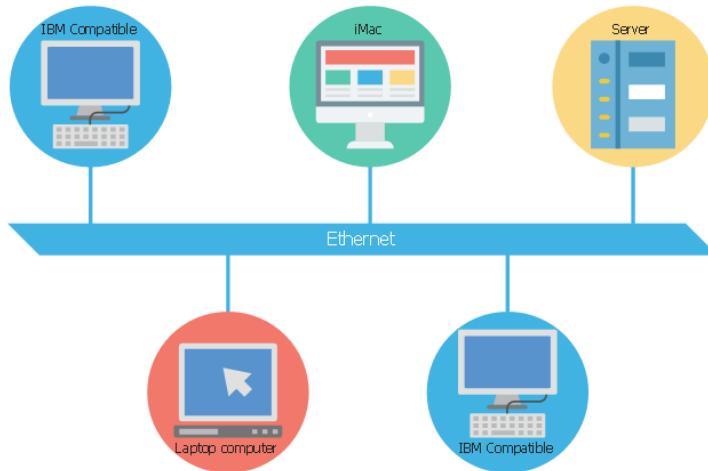


Image20 -Ethernet

Reference -<https://www.conceptdraw.com/examples/ethernet-network>

Configure and manage network security

In this section, we will read about:

- Modern Network Security
- Threats and the basics of securing a network.
- Secure Administrative Access
- LAN security considerations.
- Network Security Devices.

Modern Network Security

Why Internet security ?

Cyberspace (internet, work environment, intranet) is becoming a dangerous place for all organizations and individuals to protect their sensitive data or reputation. This is because of the numerous people and machines accessing it.

One important indicator is the IT skills of a person that wants to hack or to breach your security has decreased but the success rate of it has increased, this is because of three main factors:

- Hacking tools that can be found very easily by everyone just by googling and they are endless.
- Technology with the end-users has increased rapidly within these years, like internet bandwidth and computer processing speeds.
- Access to hacking information manuals.



Image -Internet security

Reference -<https://antivirus.comodo.com/blog/computer-safety/importance-of-internet-security/>

Cyber Security Introduction

"Cybersecurity is primarily about people, processes, and technologies working together to encompass the full range of threat reduction, vulnerability reduction, deterrence, international

engagement, incident response, resiliency, and recovery policies and activities, including computer network operations, information assurance, law enforcement, etc."

Cybersecurity is the protection of Internet-connected systems, including hardware, software, and data from cyber attacks. It is made up of two words one is cyber and other is security. Cyber is related to the technology which contains systems, network and programs or data. Whereas security related to the protection which includes systems security, network security and application and information security.

It is the body of technologies, processes, and practices designed to protect networks, devices, programs, and data from attack, theft, damage, modification or unauthorized access. It may also be referred to as information technology security.



Image -Cyber Security

Reference -<https://www.forbes.com/sites/forbesbusinesscouncil/2019/10/09/using-cyber-security-as-a-competitive-advantage/>

We can also define cybersecurity as the set of principles and practices designed to protect our computing resources and online information against threats. Due to the heavy dependency on computers in a modern industry that store and transmit an abundance of confidential and essential information about the people, cybersecurity is a critical function and needed insurance of many businesses.

Importance of Cyber Security

We live in a digital era which understands that our private information is more vulnerable than ever before. We all live in a world which is networked together, from internet banking to government infrastructure, where data is stored on computers and other devices. A portion of that data can be sensitive information, whether that be intellectual property, financial data, personal information, or other types of data for which unauthorized access or exposure could have negative consequences.

Cyber-attack is now an international concern and has given many concerns that hacks and other security attacks could endanger the global economy. Organizations transmit sensitive data across networks and to other devices in the course of doing businesses, and cybersecurity describes how to protect that information and the systems used to process or store it.

As the volume of cyber-attacks grows, companies and organizations, especially those that deal with information related to national security, health, or financial records, need to take steps to protect their sensitive business and personal information.

Specific issues that cyber security measures can help protect against include:

- Cyber-attacks : Brute force, targeted, and denial of service attacks that take your business offline or provide unauthorized access to your systems and data
- Data breaches : Exposure of sensitive business, customer, and supplier data
- Identity theft : Compromised customer data that results in the theft of logins, passwords, and other sensitive, personally identifiable data

Cyber security helps your organization stay ahead of cyber threats by providing a toolbox of approaches, tactics, and software to identify and protect against threats.

A comprehensive cyber security strategy, supported by strong policies, processes, practices, and tools can significantly reduce the risk that an organization or individual will be targeted or damaged by cyber-attacks.

Cyber Security Goals

The objective of Cybersecurity is to protect information from being stolen, compromised or attacked. Cybersecurity can be measured by at least one of three goals-

1. Protect the confidentiality of data.
2. Preserve the integrity of data.
3. Promote the availability of data for authorized users.

These goals form the confidentiality, integrity, availability (CIA) triad, the basis of all security programs. The CIA triad is a security model that is designed to guide policies for information security within the premises of an organization or company. This model is also referred to as the AIC (Availability, Integrity, and Confidentiality) triad to avoid confusion with the Central Intelligence Agency. The elements of the triad are considered the three most crucial components of security.

The CIA criteria are one that most of the organizations and companies use when they have installed a new application, creates a database or when guaranteeing access to some data. For data to be completely secure, all of these security goals must come into effect. These are security policies that all work together, and therefore it can be wrong to overlook one policy.

The CIA triad are-

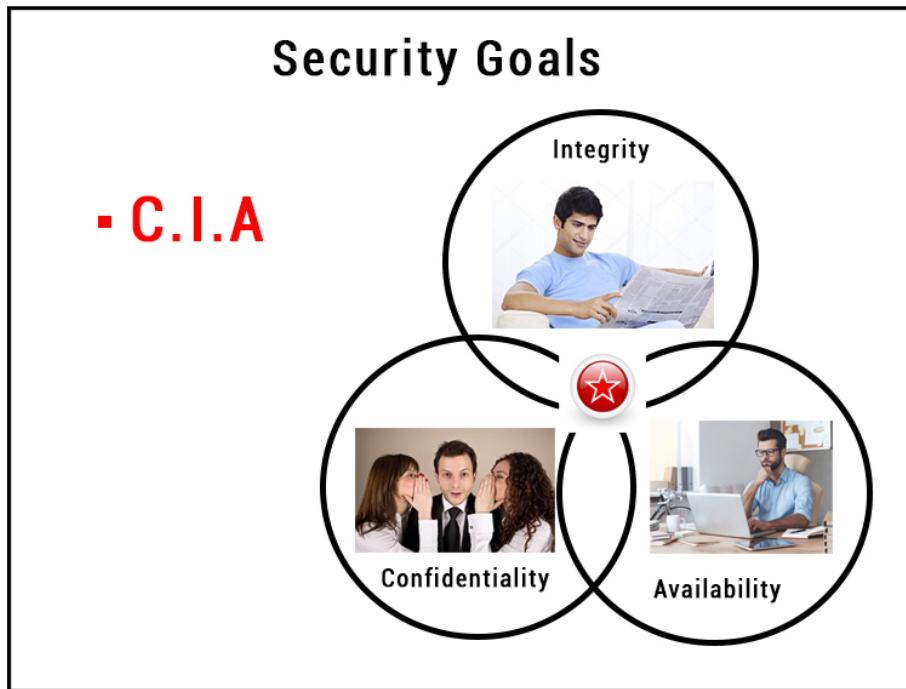


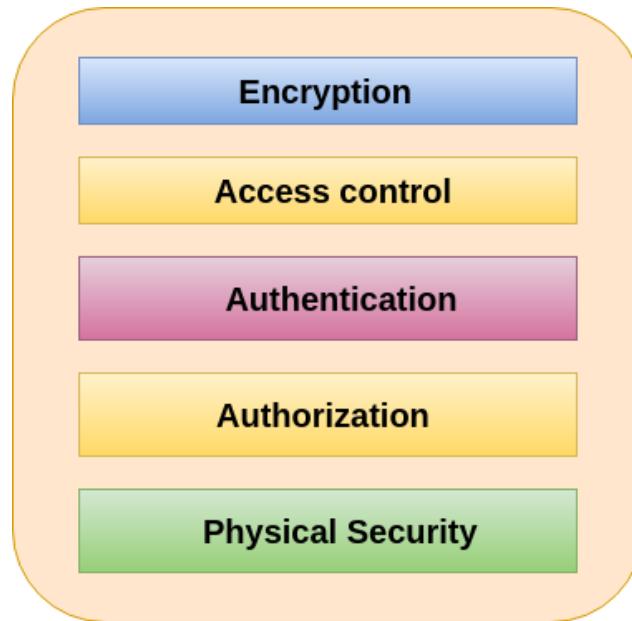
Image -Security goals(CIA)

Reference -<https://www.javatpoint.com/cyber-security-goals>

1. Confidentiality

Confidentiality is roughly equivalent to privacy and avoids the unauthorized disclosure of information. It involves the protection of data, providing access for those who are allowed to see it while disallowing others from learning anything about its content. It prevents essential information from reaching the wrong people while making sure that the right people can get it. Data encryption is a good example to ensure confidentiality.

Tools for Confidentiality



Confidentiality Tools

Image -Confidentiality tools

Reference -<https://www.javatpoint.com/cyber-security-goals>

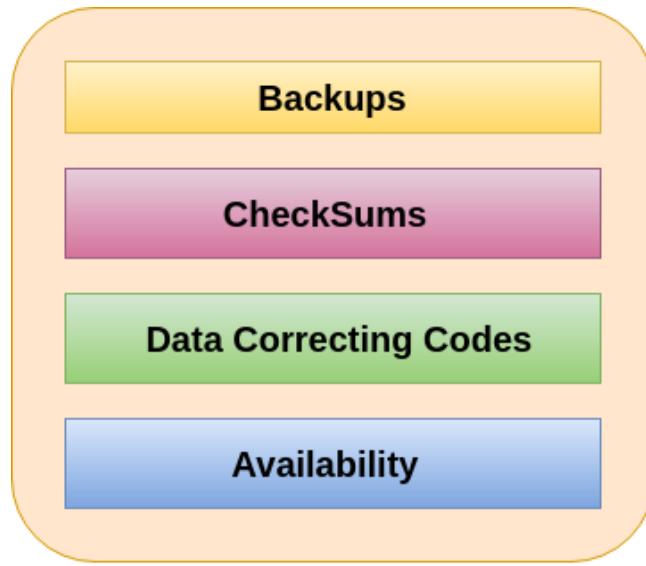
- **Encryption** : Encryption is a method of transforming information to make it unreadable for unauthorized users by using an algorithm. The transformation of data uses a secret key (an encryption key) so that the transformed data can only be read by using another secret key (decryption key). It protects sensitive data such as credit card numbers by encoding and transforming data into unreadable ciphertext. This encrypted data can only be read by decrypting it. Asymmetric-key and symmetric-key are the two primary types of encryption.
- **Access control** : Access control defines rules and policies for limiting access to a system or to physical or virtual resources. It is a process by which users are granted access and certain privileges to systems, resources or information. In access control systems, users need to present credentials before they can be granted access such as a person's name or a computer's serial number. In physical systems, these credentials may come in many forms, but credentials that can't be transferred provide the most security.
- **Authentication** : An authentication is a process that ensures and confirms a user's identity or role that someone has. It can be done in a number of different ways, but it is usually based on a combination of-

-
- something the person has (like a smart card or a radio key for storing secret keys),
 - something the person knows (like a password),
 - something the person is (like a human with a fingerprint).
 - Authentication is the necessity of every organization because it enables organizations to keep their networks secure by permitting only authenticated users to access its protected resources. These resources may include computer systems, networks, databases, websites and other network-based applications or services.
 - Authorization : Authorization is a security mechanism which gives permission to do or have something. It is used to determine whether a person or system is allowed access to resources, based on an access control policy, including computer programs, files, services, data and application features. It is normally preceded by authentication for user identity verification. System administrators are typically assigned permission levels covering all system and user resources. During authorization, a system verifies an authenticated user's access rules and either grants or refuses resource access.
 - Physical Security : Physical security describes measures designed to deny the unauthorized access of IT assets like facilities, equipment, personnel, resources and other properties from damage. It protects these assets from physical threats including theft, vandalism, fire and natural disasters.

2. Integrity

Integrity refers to the methods for ensuring that data is real, accurate and safeguarded from unauthorized user modification. It is the property that information has not been altered in an unauthorized way, and that source of the information is genuine.

Tools for Integrity



Integrity Tools

Image -Integrity tools

Reference -<https://www.javatpoint.com/cyber-security-goals>

- **Backups :** Backup is the periodic archiving of data. It is a process of making copies of data or data files to use in the event when the original data or data files are lost or destroyed. It is also used to make copies for historical purposes, such as for longitudinal studies, statistics or for historical records or to meet the requirements of a data retention policy. Many applications especially in a Windows environment, produce backup files using the .BAK file extension.
- **Checksums :** A checksum is a numerical value used to verify the integrity of a file or a data transfer. In other words, it is the computation of a function that maps the contents of a file to a numerical value. They are typically used to compare two sets of data to make sure that they are the same. A checksum function depends on the entire contents of a file. It is designed in a way that even a small change to the input file (such as flipping a single bit) likely results in different output values.
- **Data Correcting Codes :** It is a method for storing data in such a way that small changes can be easily detected and automatically corrected.

3. Availability

Availability is the property in which information is accessible and modifiable in a timely fashion by those authorized to do so. It is the guarantee of reliable and constant access to our sensitive data by authorized people.

Tools for Availability

- Physical Protections
 - Computational Redundancies
-
- Physical Protections : Physical safeguard means to keep information available even in the event of physical challenges. It ensures sensitive information and critical information technology are housed in secure areas.
 - Computational redundancies : It is applied as fault tolerant against accidental faults. It protects computers and storage devices that serve as fallbacks in the case of failures.

Cybersecurity Practice Areas

There are many different, and constantly evolving, disciplines that make up a complete cyber security approach. Here are some of the most common disciplines:

- Data security: Protecting and maintaining the integrity of business, customer, and other data.
- Application Security : Ensuring that software and other applications cannot be hacked, compromised, accessed without proper authorization, or disabled.
- Network Security : Protecting network infrastructure and software from unauthorized access.
- Operational Security : Day-to-day monitoring and security management.
- Cloud Security : Cyber security methods used across public, private, or hybrid cloud environments.

-
- Identity and Access Management (IAM) : Authenticating users and authorizing them to access specific applications, data, and other systems.
 - Privileged Access Management (PAM) : Controlling and monitoring privileged access for users, accounts, applications, and other system assets.
 - Vulnerability Management (VM) : Proactive identification (such as through scanning) and resolution (such as through patching, systems hardening, implementing new solutions, etc.) of potential threats and vulnerabilities in the IT ecosystem.
 - Enterprise Mobility Management (EMM) : This can include mobile device management (MDM) and other processes and technologies for securely enabling a mobile workforce.
 - Business Continuity (BC) and Disaster Recovery (DR) : Planning for events that cause IT disruption (whether arising from human error, equipment failure, malware or hacking attack, environmental catastrophe, etc.) and restoring IT functionality as soon as possible after such an event. BC / DR overlap with incident response, which is focused on marshaling resources to handle a security incident and also forensically investigate how the incident occurred and plan for implications (such as audit, public breach notification, etc.).
 - Security Training : Teaching employees and other users to identify and appropriately deal with common security issues like phishing, malware, or social engineering.

All of these practices are vital to keeping business systems secure and operational, and for avoiding data breaches or hacks that expose business, partner, or customer data.

Threats and the Basics of securing a network

Common Network Security Threats

Types of Cyber Attacks

A cyber-attack is an exploitation of computer systems and networks. It uses malicious code to alter computer code, logic or data and lead to cybercrimes, such as information and identity theft.

We are living in a digital era. Nowadays, most people use computers and the internet. Due to the dependency on digital things, the illegal computer activity is growing and changing like any type of crime.

Cyber-attacks can be classified into the following categories:



Classification of Cyber attacks

Image -Types of cyber Attacks

Reference -<https://www.javatpoint.com/types-of-cyber-attacks>

1. Web-based attacks

These are the attacks which occur on a website or web applications. Some of the important web-based attacks are as follows-

- Injection attacks :It is the attack in which some data will be injected into a web application to manipulate the application and fetch the required information.
Example- SQL Injection, code Injection, log Injection, XML Injection etc.
- DNS Spoofing : DNS Spoofing is a type of computer security hacking. Whereby a data is introduced into a DNS resolver's cache causing the name server to return an incorrect IP address, diverting traffic to the attacker's computer or any other computer. The DNS

spoofing attacks can go on for a long period of time without being detected and can cause serious security issues.

- Session Hijacking : It is a security attack on a user session over a protected network. Web applications create cookies to store the state and user sessions. By stealing the cookies, an attacker can have access to all of the user data.
- Phishing : Phishing is a type of attack which attempts to steal sensitive information like user login credentials and credit card number. It occurs when an attacker is masquerading as a trustworthy entity in electronic communication.
- Brute force : It is a type of attack which uses a trial and error method. This attack generates a large number of guesses and validates them to obtain actual data like user password and personal identification number. This attack may be used by criminals to crack encrypted data, or by security analysts to test an organization's network security.
- Denial of Service : It is an attack which meant to make a server or network resource unavailable to the users. It accomplishes this by flooding the target with traffic or sending it information that triggers a crash. It uses the single system and single internet connection to attack a server. It can be classified into the following-
 - Volume-based attacks- Its goal is to saturate the bandwidth of the attacked site, and is measured in bit per second.
 - Protocol attacks- It consumes actual server resources, and is measured in a packet.
 - Application layer attacks- Its goal is to crash the web server and is measured in request per second.
- Dictionary attacks : This type of attack stored the list of a commonly used password and validated them to get the original password.
- URL Interpretation : It is a type of attack where we can change the certain parts of a URL, and one can make a web server to deliver web pages for which he is not authorized to browse.
- File Inclusion attacks : It is a type of attack that allows an attacker to access unauthorized or essential files which are available on the web server or to execute malicious files on the web server by making use of the include functionality.
- Man in the middle attacks : It is a type of attack that allows an attacker to intercept the connection between client and server and acts as a bridge between them. Due to this, an attacker will be able to read, insert and modify the data in the intercepted connection.

2.System-based attacks

These are the attacks which are intended to compromise a computer or a computer network. Some of the important system-based attacks are as follows-

- Virus :It is a type of malicious software program that spread throughout the computer files without the knowledge of a user. It is a self-replicating malicious computer program that replicates by inserting copies of itself into other computer programs when executed. It can also execute instructions that cause harm to the system.
- Worm : It is a type of malware whose primary function is to replicate itself to spread to uninfected computers. It works the same as the computer virus. Worms often originate from email attachments that appear to be from trusted senders.
- Trojan horse : It is a malicious program that occurs unexpected changes to computer settings and unusual activity, even when the computer should be idle. It misleads the user of its true intent. It appears to be a normal application but when opened/executed some malicious code will run in the background.
- Backdoors : It is a method that bypasses the normal authentication process. A developer may create a backdoor so that an application or operating system can be accessed for troubleshooting or other purposes.
- Bots : A bot (short for "robot") is an automated process that interacts with other network services. Some bots programs run automatically, while others only execute commands when they receive specific input. Common examples of bots program are the crawler, chatroom bots, and malicious bots.

Cyber Security Best Practices

Cyber security involves the application of a number of tools, approaches, and best practices that can significantly reduce cyber risk.

- Audit your existing IT ecosystem : Audit every element of your networks, servers, infrastructure, operating systems, applications, and data. It is only through having a complete map of your IT systems that you can identify attack vectors and threats.

-
- Complete a gap analysis : Once you understand the potential threats to your IT security, understand the existing tools and approaches you have in place to deal with cyber security threats.
 - Use a risk-based approach to cyber security : Once you have identified potential threats, rate each one based on likelihood and impact. This will help you prioritize which risks to deal with first.
 - Take advantage of modern cyber security software : Seek out vendors and software that use modern detection techniques to identify and report on threats. Ideally, this software should be updated on a regular basis to take advantage of new learning and identified issues.
 - Implement robust identity and access management : Tools like biometrics, single sign-on, two-factor authentication, and adaptive security controls can help you ensure that you are requesting proper authentication from authorized users.
 - Use privileged access management : The principle of least privilege will ensure that you only provide the access necessary for individuals to perform their roles. This will keep the most sensitive data off-limits, available only to those who have reason to access it.
 - Employ vulnerability scanning : Vulnerability scanning and penetration testing will identify potential flaws in your IT security. This will help you create an effective patch schedule to resolve any issues.
 - Train your employees in good security practices : Employees are often the weakest link in the cyber security chain. Make sure they are educated about social engineering, phishing, malware, and other scams, and that there is proper reporting and escalation routes if they identify threats.
 - Take account of cyber security frameworks : There are a number of frameworks, best practices, and regulations you can use to guide cyber security. These include PCI DSS, ISO 27001/27002, CIS Critical Security Controls, and the NIST Cybersecurity Framework.

Network Security Models

With the rapid growth in the Internet, cybersecurity has become a major concern to organizations throughout the world. The fact that the information and tools & technologies needed to penetrate

the security of corporate organization networks are widely available has increased that security concern.

Today, the fundamental problem is that much of the security technology aims to keep the attacker out, and when that fails, the defences have failed. Every organization who uses the internet needed security technologies to cover the three primary control types - preventive, detective, and corrective as well as provide auditing and reporting. Most security is based on one of these types of things: something we have (like a key or an ID card), something we know (like a PIN or a password), or something we are (like a fingerprint).

Some of the important security technologies used in the cybersecurity are -

- (1) Firewalls
- (2) Antivirus Software
- (3) Passwords
- (4) Cryptography
- (5) Algorithms etc

1. Firewalls

Firewall is a computer network security system designed to prevent unauthorized access to or from a private network. It can be implemented as hardware, software, or a combination of both. Firewalls are used to prevent unauthorized Internet users from accessing private networks connected to the Internet. All messages are entering or leaving the intranet pass through the firewall. The firewall examines each message and blocks those that do not meet the specified security criteria.

The primary benefits of using a firewall are:

- Shield from Vulnerable Services
- Logging and Statistics on Network Usage, and misuse of it.
- Policy Enforcement

Advantages of Firewall

-
- It enforces a security policy by allowing a single point for implementing and controlling all security decisions to be made.
 - It filters monitors and logs the sessions between any two networks. As a result, our exposure to the internet is also limited.

2.VPNs

A VPN stands for virtual private network. It is a technology which creates a safe and an encrypted connection on the Internet from a device to a network. This type of connection helps to ensure our sensitive data is transmitted safely. It prevents our connection from eavesdropping on the network traffic and allows the user to access a private network securely. This technology is widely used in corporate environments.

A VPN works the same as a firewall like firewall protects data local to a device wherever VPNs protect data online. To ensure safe communication on the internet, data travels through secure tunnels, and VPNs users use an authentication method to gain access over the VPNs server. VPNs are used by remote users who need to access corporate resources, consumers who want to download files and business travellers want to access a site that is geographically restricted.

3.Authentication

Features of the authentication are –

- User identification and password.
- A signed digital certificate or even a fingerprint.
- User's voice, hand configuration, a fingerprint etc.

4. Intrusion Detection System (IDS)

An IDS is a security system which monitors the computer systems and network traffic. It analyses traffic for possible hostile attacks originating from the outsider and also for system misuse or attacks originating from the insider. A firewall does a job of filtering the incoming traffic from the internet, the IDS in a similar way compliments the firewall security. Like, the firewall protects an organization sensitive data from malicious attacks over the Internet, the

Intrusion detection system alerts the system administrator in the case when someone tries to break in the firewall security and tries to have access on any network in the trusted side.

5. Antivirus software

Anti-virus softwares is used to protect a computer from all types of malware. Antivirus software can detect viruses; worms etc. and warn the presence in the computer. It can deactivate the malware and clean the computer of different types of the malicious software.

Antivirus softwares is the utility which prevents viruses from entering our system. They can also detect and remove the virus entered in our system. There are the memory resident programs and get activated as soon as the system is started. It checks all the files in the system and if any virus is detected, it removes the virus. Also while working on the computer if some infected storage device is found, it generates the warning message and stops the data transfer.

It is an application program which is designed to detect and remove viruses, worms and Trojan horses from the computer system. Antivirus software looks for these computer threats in all the files and folders of the computer system. It looks for changes and activities in the systems that are typical in case of virus attack. Scanners that are built within the anti-virus software look for particular types of codes within programs. If a virus is detected the anti-virus tries to remove it from the system. The most popular antivirus softwares are Norton antivirus and quick heal total security.

Benefits of Antivirus software

- Scan specific files or directories.
- Allows to schedule scans to automatically run for you.
- Allows you to initiate scan of a particular file or entire computer or of a CD or flash drive at any time.
- Removes any malicious code detected.
- Show you the ‘health’ of your computer.

Basic Functions of Antivirus Engines

All antivirus engines have three components to function accordingly. It is important to have a look at these functions because it will help us for better manual cleaning of viruses in case we need.

- Scanning – When a new virus is detected in the cyberspace, antivirus producers start writing programs (updates) that scans for similar signature strings.
- Integrity Checking – This method generally checks for manipulated files in OS from the viruses.
- Interception – This method is used basically to detect Trojans and it checks the request made by the operating system for network access.

The following image shows the schema for an antivirus engines functionality.

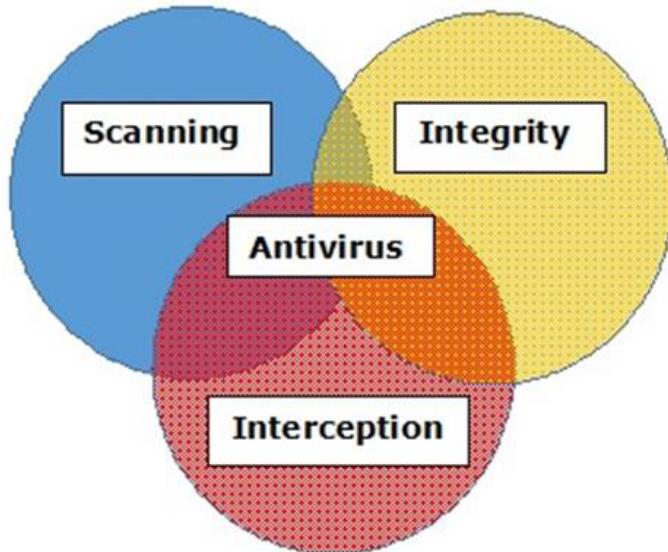


Image -Antivirus engine Functionality

Reference -https://www.tutorialspoint.com/computer_security/computer_security_antiviruses.htm

6.Cryptography

The term Cryptography means the concept of encryption and decryption together. Cryptography is the method in which the plain text message is encoded that is called ciphertext at the transmitter's end, which is then conveyed to the receiver. The receiver then decrypts to get the original message back. Cryptography is also termed as an art or method to achieve protected communication between the communicating parties by encoding the message between them such

that no third party can gain anything useful out of interception. Various techniques are utilized for this purpose of cryptography.

Broadly these techniques fall into two categories.

- Symmetric key Cryptography: In this the significant component used is the equal for the both encoding and decoding.
- Asymmetric key Cryptography: In this the key element used is unlike for both encryption as well as decryption.

7.Encryption

Encryption is a transformed type of genuine information where only the authorized parties know how to read it, so in the worst case scenario if somebody has access to these files they would still not be able to understand the message in it.

Secure Administrative Access

Techniques for secure administrative access

One of the fundamental requirements in protecting the network is to secure the administrative access to any network device. With Cisco devices, administrative access to the device could allow someone to reconfigure features or even possibly use that device to launch attempts on other devices. Some of the basic techniques for securing administrative access would include the following:

- Setting User mode passwords
- Setting Privilege mode passwords
- Encrypting passwords in the configuration files
- Setting an MOTD banner to advise about the security restrictions
- Setting access privilege levels

-
- Restricting Telnet access to the device
 - Restricting web browser access to the device
 - Restricting SNMP access to the device

User Mode Passwords

The User level on a Cisco router often has three potential access points. They include the following:

- Console (con) port Access for the console cable. Figure 2-2 shows a typical console port on a router.
- Auxiliary (AUX) port A console-like access that can be attached to an external modem for a dial-up connection.
- Virtual terminal (vty) ports The access points for Telnet sessions.

The default configuration for each of these interfaces, doesn't include a password. Since the release of version 12.0 of the IOS, the virtual terminals and AUX ports require that a password is set. If none is set, the user will be rejected with the message "password required, but none set." The console port doesn't have this requirement, so it's a good idea to always set a password to prevent anyone with a laptop and a console cable from accessing the device.

The basic password configuration for each is the same. The password is defined with the password command and the login command. Passwords can be 1 to 25 characters, and can include uppercase and lowercase letters, as well as numbers, to comply with complex password requirements in the password policy.

Privilege Mode Passwords

Access security for the Privilege mode involves being prompted for a password only if an enabled password or enable secret password has been previously defined in Global Configuration mode. If neither is set, no security allowing any user to view and/or change the device configuration exists for the Privilege mode. Someone could even set a password and lock out other users.

The older enable password command followed by the desired password creates a cleartext entry in the running configuration that could be viewed by anyone seeing the configuration. The more secure enable secret command followed by the desired password creates an encrypted entry in the running configuration that can't be understood by anyone just seeing the configuration. If both enable password and enable secret are configured, only the enable secret is used. The enable password is ignored.

Password Encryption

You can secure the passwords in Global Configuration mode by typing the service password-encryption command. This permanently encrypts all passwords, so make sure you know what they are.

Typing no service password-encryption won't cause the passwords to revert to cleartext. The system will no longer encrypt new passwords, but the existing ones remain encrypted. Make sure you know a password before you encrypt it.

Message of the Day Banner (MOTD)

It's possible and prudent to create a message that will appear to everyone logging in to the User mode. This message should be a polite warning of company security policies for unauthorized access. Some courts have held that if this isn't explicitly stated—telling people to stay out, then it's an implicit invitation to come in and raise havoc.

To configure this message, use the banner motd command in the Global Configuration mode. The syntax is a little unusual in that you type the command, followed by a character you don't plan to include in the message. This character becomes a delimiter, in that everything you type after it until the character appears again will be part of the message. An example would be banner motd *No Unauthorized Access* where the asterisks indicate the beginning and the end of the message. The asterisks won't appear in the message.

You can make multiple-line messages by using SHIFT-ENTER at the end of the line and ignoring the warning message that appears the first time you try it. Typing a new MOTD replaces any existing one.

Privilege Levels

Cisco devices numbered 0 through 15 have 16 privilege levels. By default, any user who can furnish the user-level password or user name/password combination can gain User exec mode access to the device, which is privilege level 1. From there, if the user knows the enable secret password, they can access the Privilege exec mode, or privilege level 15. The three predefined privilege levels on Cisco devices include the following:

- 1 User exec mode only (prompt is router>), the default level for login
- 15 Privileged exec mode (prompt is router#), the Enable mode
- 0 Seldom used, but includes five commands: disable, enable, exit, help, and logout

The Syntax is

privilege mode {level level command | reset command}, where

mode	Indicates the configuration level being assigned. This includes all router configuration modes, including exec, configure, and interface.
level	Indicates the level being defined.
command	Indicates the command to be included. If you specify exec mode, then the command must be an exec mode command.
reset	Resets the privilege level of the command to the default privilege level.

Cyber security policies

Security policies are a formal set of rules which is issued by an organization to ensure that the users who are authorized to access company technology and information assets comply with rules and guidelines related to the security of information. It is a written document in the organization which is responsible for how to protect the organizations from threats and how to handle them when they occur. A security policy also considered to be a "living document" which means that the document is never finished, but it is continuously updated as requirements of the technology and employee changes.

Need of Security policies-

- It increases efficiency : The best thing about having a policy is being able to increase the level of consistency which saves time, money and resources. The policy should inform the employees about their individual duties, and tell them what they can do and what they cannot do with the organization's sensitive information.
- It upholds discipline and accountability : When any human mistake will occur, and system security is compromised, then the security policy of the organization will back up any disciplinary action and also support a case in a court of law. The organization policies act as a contract which proves that an organization has taken steps to protect its intellectual property, as well as its customers and clients.
- It can make or break a business deal : It is not necessary for companies to provide a copy of their information security policy to other vendors during a business deal that involves the transference of their sensitive information. It is true in a case of bigger businesses which ensures their own security interests are protected when dealing with smaller businesses which have less high-end security systems in place.
- It helps to educate employees on security literacy : A well-written security policy can also be seen as an educational document which informs the readers about their importance of responsibility in protecting the organization's sensitive data. It involves choosing the right passwords, providing guidelines for file transfers and data storage which increases employee's overall awareness of security and how it can be strengthened.

We use security policies to manage our network security. Most types of security policies are automatically created during the installation. We can also customize policies to suit our specific environment. There are some important cybersecurity policies recommendations describe below-

1. Virus and Spyware Protection policy :This policy provides the following protection:

- It helps to detect, removes, and repairs the side effects of viruses and security risks by using signatures.
- It helps to detect the threats in the files which the users try to download by using reputation data from Download Insight.

-
- It helps to detect the applications that exhibit suspicious behaviour by using SONAR heuristics and reputation data.

2. Firewall Policy : This policy provides the following protection:

- It blocks the unauthorized users from accessing the systems and networks that connect to the Internet.
- It detects the attacks by cybercriminals.
- It removes the unwanted sources of network traffic.

3. Intrusion Prevention policy : This policy automatically detects and blocks the network attacks and browser attacks. It also protects applications from vulnerabilities. It checks the contents of one or more data packages and detects malware which is coming through legal ways.

4. LiveUpdate policy : This policy can be categorized into two types one is LiveUpdate Content policy, and another is LiveUpdate Setting Policy. The LiveUpdate policy contains the setting which determines when and how client computers download the content updates from LiveUpdate. We can define the computer that clients contact to check for updates and schedule when and how often clients computer check for updates.

5. Application and Device Control : This policy protects a system's resources from applications and manages the peripheral devices that can attach to a system. The device control policy applies to both Windows and Mac computers whereas application control policy can be applied only to Windows clients.

6. Exceptions policy : This policy provides the ability to exclude applications and processes from detection by the virus and spyware scans.

7. Host Integrity policy : This policy provides the ability to define, enforce, and restore the security of client computers to keep enterprise networks and data secure. We use this policy to ensure that the client's computers who access our network are protected and compliant with companies' securities policies. This policy requires that the client system must have installed antivirus.



LAN Security Considerations

Understand Types of Network Devices

To build a strong network and defend it, you need to understand the devices that comprise it. Here are the main types of network devices:

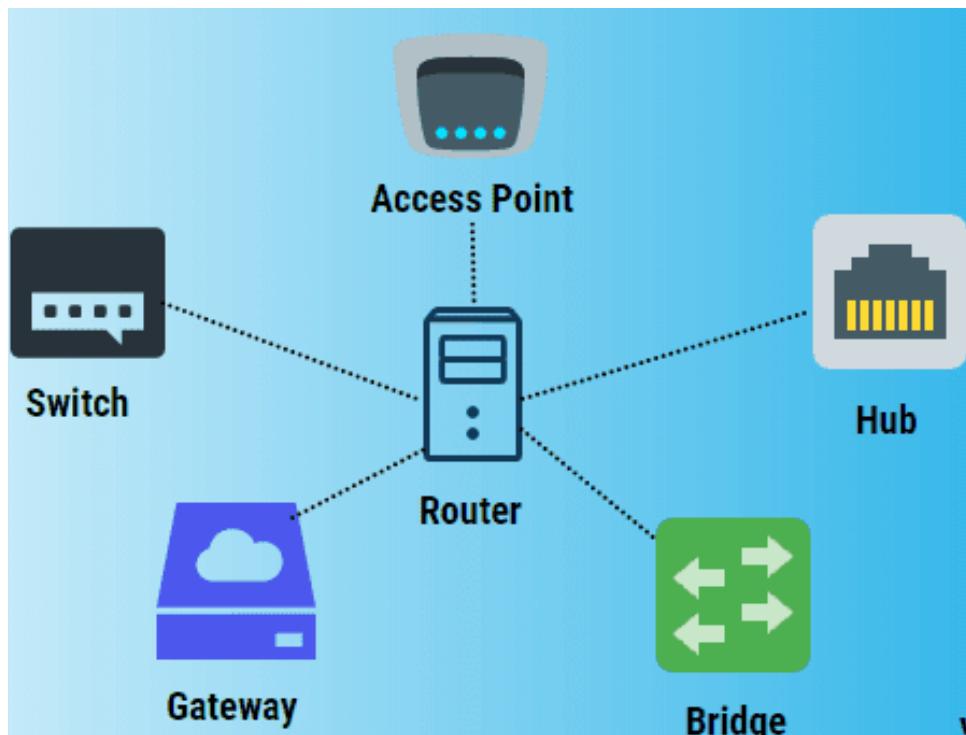


Image 1: LAN Devices

Reference: <https://cdn.educba.com/academy/wp-content/uploads/2019/10/Types-of-Network-Devices.png>

Hub

Hubs connect multiple local area network (LAN) devices together. A hub also acts as a repeater in that it amplifies signals that deteriorate after traveling long distances over connecting cables. Hubs do not perform packet filtering or addressing functions. Hubs operate at the Physical layer.

Switch

Switches generally have a more intelligent role than hubs. Strands of LANs, are usually connected using switches. Mainly working at the Data Link layer, they read the packet headers

and process the packets appropriately. Generally, switches can read the hardware addresses of incoming packets to transmit them to the appropriate destination.

Router

Routers help transmit packets to their destinations by charting a path through the sea of interconnected network devices. They remove the packets from the incoming frames, analyze them individually and assign IP addresses. Routers normally work at the Network layer of the OSI model.

Bridge

Bridges are used to connect two or more hosts or network segments together. The basic role of bridges in network architecture is storing and forwarding frames between the different segments that the bridge connects. They use hardware Media Access Control (MAC) addresses for transferring frames. Bridges work only at the Physical and Data Link layers of the OSI model.

Gateway

Gateways normally work at the Transport and Session layers of the OSI model. At the Transport layer and above, there are numerous protocols and standards from different vendors; gateways are used to deal with them.

Know Your Network Defenses

Using the proper devices and solutions can help you defend your network. Here are the most common ones you should know about:

Firewall

One of the first lines of defense in a network, a firewall isolates one network from another. Firewalls either can be standalone systems or included in other devices, such as routers or servers. You can find both hardware and software firewall solutions; some firewalls are available as appliances that serve as the primary device separating two networks.

Intrusion Detection System (IDS)

An IDS enhances cybersecurity by spotting a hacker or malicious software on a network so you can remove it promptly to prevent a breach or other problems, and use the data logged about the

event to better defend against similar intrusion incidents in the future. Investing in an IDS that enables you respond to attacks quickly can be far less costly than rectifying the damage from an attack and dealing with the subsequent legal issues.

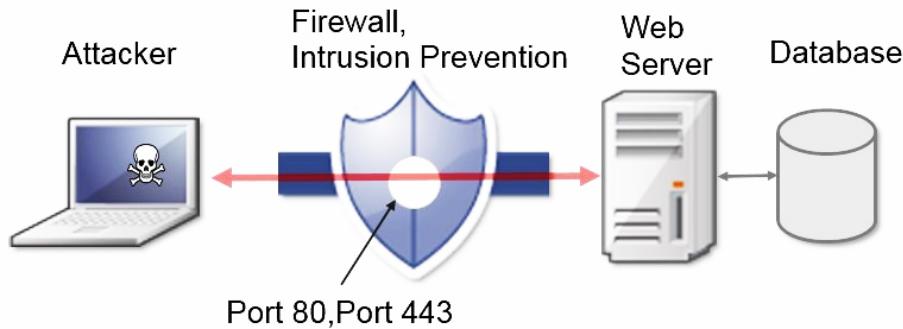


Image 2: Network Defences
Reference: <https://securityintelligence.com/wp-content/uploads/2015/04/application.jpg>

Intrusion Prevention System (IPS)

An IPS is a network security solution that can not only detect intruders, but also prevent them from successfully launching any known attack. Intrusion prevention systems combine the abilities of firewalls and intrusion detection systems. However, implementing an IPS on an effective scale can be costly, so businesses should carefully assess their IT risks before making the investment. Moreover, some intrusion prevention systems are not as fast and robust as some firewalls and intrusion detection systems, so it might not be an appropriate solution when speed is an absolute requirement.

Network Access Control (NAC)

Network access control (NAC) involves restricting the availability of network resources to endpoint devices that comply with your security policy. Some NAC solutions can automatically fix non-compliant nodes to ensure it is secure before access is allowed. NAC is most useful when the user environment is fairly static and can be rigidly controlled, such as enterprises and government agencies. It can be less practical in settings with a diverse set of users and devices that are frequently changing, which are common in the education and healthcare sectors.

Web Filter

Web filters are solutions that by preventing users' browsers from loading certain pages from particular websites. There are different web filters designed for individual, family, institutional and enterprise use.

Proxy Server

Proxy servers act as negotiators for requests from client software seeking resources from other servers. A client connects to the proxy server, requesting some service (for example, a website); the proxy server evaluates the request and then allows or denies it. In organizations, proxy servers are usually used for traffic filtering and performance improvement.

Anti-DDoS

Anti-DDoS devices detect distributed denial of service (DDoS) attacks in their early stages, absorb the volume of traffic and identify the source of the attack.

Load Balancer

Load balancers are physical units that direct computers to individual servers in a network based on factors such as server processor utilization, number of connections to a server or overall server performance. Organizations use load balancers to minimize the chance that any particular server will be overwhelmed and to optimize the bandwidth available to each computer in the network.

Spam Filter

Spam filters detect unwanted email and prevent it from getting to a user's mailbox. Spam filters judge emails based on policies or patterns designed by an organization or vendor. More sophisticated filters use a heuristic approach that attempts to identify spam through suspicious word patterns or word frequency.

Segregate Your Network

Network segmentation involves segregating the network into logical or functional units called zones. For example, you might have a zone for sales, a zone for technical support and another zone for research, each of which has different technical needs. You can separate them using

routers or switches or using virtual local area networks (VLANs), which you create by configuring a set of ports on a switch to behave like a separate network.

Segmentation limits the potential damage of a compromise to whatever is in that one zone. Essentially, it divides one target into many, leaving attackers with two choices: Treat each segment as a separate network, or compromise one and attempt to jump the divide. Neither choice is appealing. Treating each segment as a separate network creates a great deal of additional work, since the attacker must compromise each segment individually; this approach also dramatically increases the attacker's exposure to being discovered. Attempting to jump from a compromised zone to other zones is difficult. If the segments are designed well, then the network traffic between them can be restricted. There are always exceptions that must be allowed through, such as communication with domain servers for centralized account management, but this limited traffic is easier to characterize.

Segmentation is also useful in data classification and data protection. Each segment can be assigned different data classification rules and then set to an appropriate level of security and monitored accordingly.

An extreme example of segmentation is the air gap one or more systems are literally not connected to a network. Obviously, this can reduce the usefulness of many systems, so it is not the right solution for every situation. In some cases, however, a system can be sensitive enough that it needs to not be connected to a network; for example, having an air-gapped backup server is often a good idea. This approach is one certain way of preventing malware infections on a system.

Virtualization is another way to segment a network. Keep in mind that it is much easier to segment virtual systems than it is to segment physical systems. As one simple example, consider a virtual machine on your workstation. You can easily configure it so that the virtual machine is completely isolated from the workstation it does not share a clipboard, common folders or drives, and literally operates as an isolated system.

Types of Network Segments

Network segments can be classified into the following categories:

Public Networks

Public Networks allow accessibility to everyone. The internet is a perfect example of a public network. There is a huge amount of trivial and unsecured data on public networks. Security controls on these networks are weak.

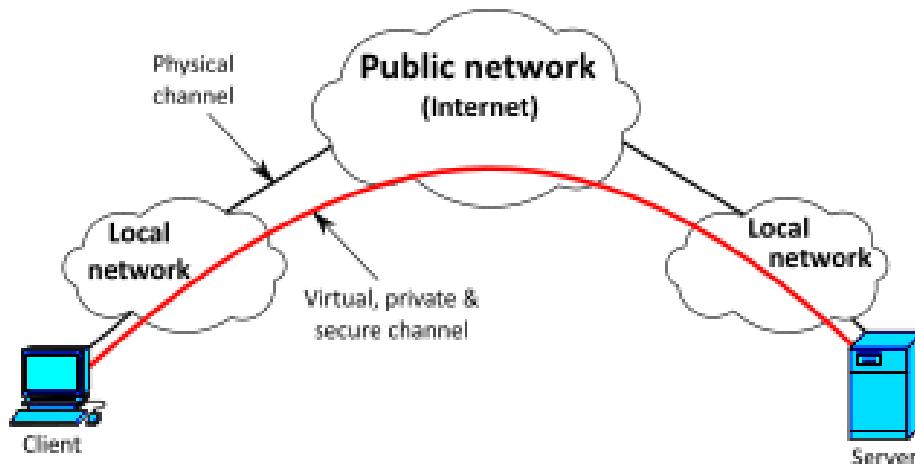


Image 3: Network Segmentation

Reference: https://upload.wikimedia.org/wikipedia/commons/thumb/e/e8/VPN_overview-en.svg/330px-VPN_overview-en.svg.png

Semi-Private Networks

Semi-Private Networks sit between public networks and private networks. From a security standpoint, a semi-private network may carry confidential information but under some regulations.

Private Networks

Private Networks are organizational networks that handle confidential and proprietary data. Each organization can own one or more private networks. If the organization is spread over vast geographical distances, the private networks at each location may be interconnected through the internet or other public networks.

Demilitarized Zone (DMZ)

Demilitarized Zone (DMZ) is a noncritical yet secure region at the periphery of a private network, separated from the public network by a firewall; it might also be separated from the private network by a second firewall. Organizations often use a DMZ as an area where they can

place a public server for access by people they might not trust. By isolating a server in a DMZ, you can hide or remove access to other areas of your network. You can still access the server using your network, but others aren't able to access further network resources.

Software-Defined Networking (SDN)

Software-Defined Networking (SDN) is a relatively recent trend that can be useful both in placing security devices and in segmenting the network. Essentially, in an SDN, the entire network is virtualized, which enables relatively easy segmentation of the network. It also allows administrators to place virtualized security devices wherever they want.

Place Your Security Devices Correctly

As you design your network segregation strategy, you need to determine where to place all your devices. The easiest device to place is the firewall: You should place a firewall at every junction of a network zone. Each segment of your network should be protected by a firewall. This is actually easier to do than you might think. All modern switches and routers have firewall capabilities. These capabilities just need to be turned on and properly configured. Another device that obviously belongs on the perimeter is an anti-DDoS device so you can stop DDoS attacks before they affect the entire network. Behind the main firewall that faces public network, you should have a web filter proxy.

To determine where to place other devices, you need to consider the rest of your network configuration. For example, consider load balancers. If we have a cluster of web servers in a DMZ, then the load balancer needs to be in the DMZ as well. However, if we have a cluster of database servers in a private network segment, then the load balancer must be placed with that cluster. Port mirroring will also be placed wherever your network demands it. This is often done throughout network switches so that traffic from a given network segment is also copied to another segment. This can be done to ensure that all network traffic is copied to an IDS or IPS; in that case, there must be collectors or sensors in every network segment, or else the IDS or IPS will be blind to activity in that segment.

Network aggregation switches are another device for which there is no definitive placement advice. These switches aggregate multiple streams of bandwidth into one. One example would be to use an aggregation switch to maximize bandwidth to and from a network cluster.

Use NAT

Network address translation (NAT) enables organizations to compensate for the address deficiency of IPv4 networking. NAT translates private addresses (internal to a particular organization) into routable addresses on public networks such as the internet. In particular, NAT is a method of connecting multiple computers to the internet (or any other IP network) using one IP address.

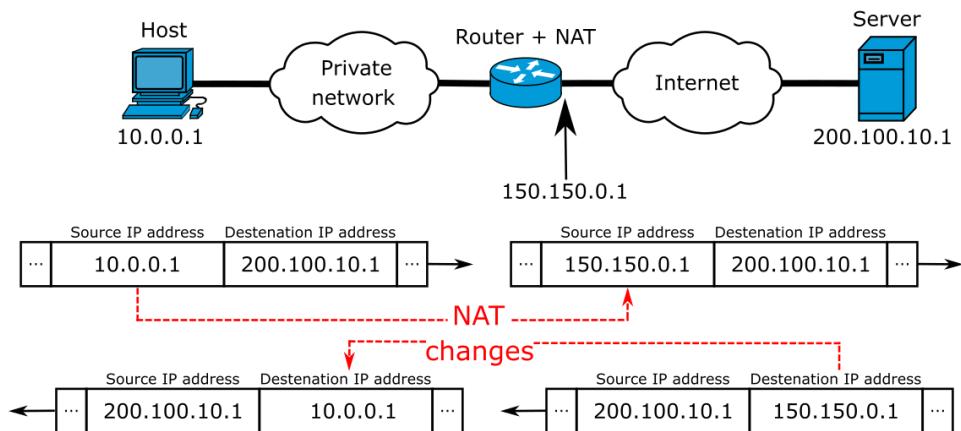


Image 4: NAT Translation

Reference: https://upload.wikimedia.org/wikipedia/commons/thumb/c/c7/NAT_Concept-en.svg/1200px-NAT_Concept-en.svg.png

NAT complements firewalls to provide an extra measure of security for an organization's internal network. Usually, hosts from inside the protected networks, which have private addresses, are able to communicate with the outside world, but systems that are located outside the protected network have to go through the NAT boxes to reach internal networks. Moreover, NAT enables an organization to use fewer IP addresses, which helps confusing attackers about which particular host they are targeting.

Don't Disable Personal Firewall

Personal firewalls are software-based firewalls installed on each computer in the network. They work in much the same way as larger border firewalls — they filter out certain packets to prevent them from leaving or reaching your system. The need for personal firewalls is often questioned, especially in corporate networks, which have large dedicated firewalls that keep potentially harmful traffic from reaching internal computers. However, that firewall can't do anything to prevent internal attacks, which are quite common and often very different from the ones from the internet; attacks that originate within a private network are usually carried out by viruses. So,

instead of disabling personal firewalls, simply configure a standard personal firewall according to your organization's needs and export those settings to the other personal firewalls.

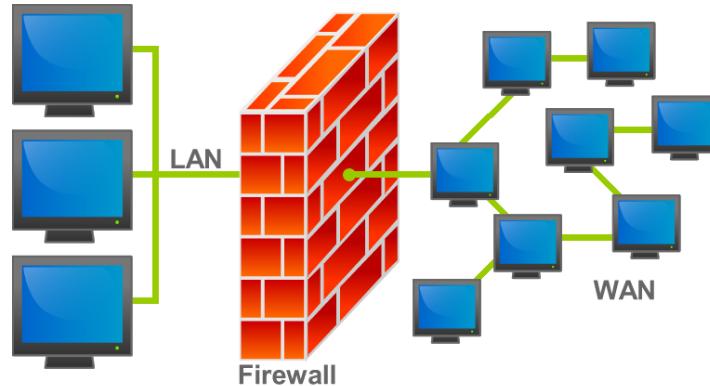


Image 5: Firewall at Local LAN

Reference: <https://anydifferencebetween.com/wp-content/uploads/2016/09/Difference-Between-Personal-Firewall-and-Network-Firewall.png>

Use Centralized Loggings

Record suspicious logins and other computer events and look for anomalies. This best practice will help you reconstruct what happened during an attack so you can take steps to improve your threat detection process and quickly block attacks in the future. However, remember that attackers are clever and will try to avoid detection and logging. They will attack a sacrificial computer, perform different actions and monitor what happens in order to learn how your systems work and what thresholds they need to stay below to avoid triggering alerts.

Use Web Domain Whitelisting

Limiting users to browsing only the websites you've explicitly approved helps in two ways. First, it limits your attack surface. If users cannot go to untrusted websites, they are less vulnerable. It's a solid solution for stopping initial access via the web. Second, whitelisting limits hackers' options for communication after they compromise a system. The hacker must use a different protocol, compromise an upstream router, or directly attack the whitelisting mechanism to communicate. Web domain whitelisting can be implemented using a web filter that can make web access policies and perform web site monitoring.

Route through Proxy

All outbound web access should be routed through an authenticating server where access can be controlled and monitored. Using a web proxy helps ensure that an actual person, not an unknown

program, is driving the outbound connection. There can be up-front work required to reconfigure the network into this architecture, but once done, it requires few resources to maintain. It has practically no impact on the user base and therefore is unlikely to generate any pushback. It raises the level of operational security since there is a single point device that can be easily monitored.

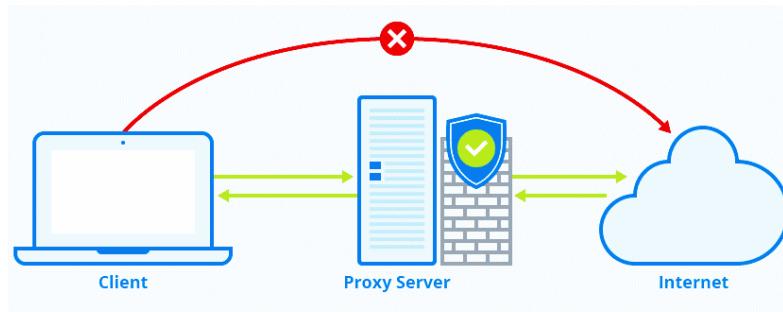


Image 6: Proxy Routing
Reference: <https://www.seobility.net/en/wiki/images/8/8a/Proxy-Server.png>

Use Honeypots and Honeynets

A honeypot is a separate system that appears to be an attractive target but is in reality a trap for attackers (internal or external). For example, you might set up a server that appears to be a financial database but actually has only fake records. Using a honeypot accomplishes two important goals. First, attackers who believe they have found what they are looking for will leave your other systems alone, at least for a while. Second, since honeypots are not real systems, no legitimate users ever access it and therefore you can turn on extremely detailed monitoring and logging there. When an attacker does access it, you'll be gathering an impressive amount of evidence to aid in your investigation.

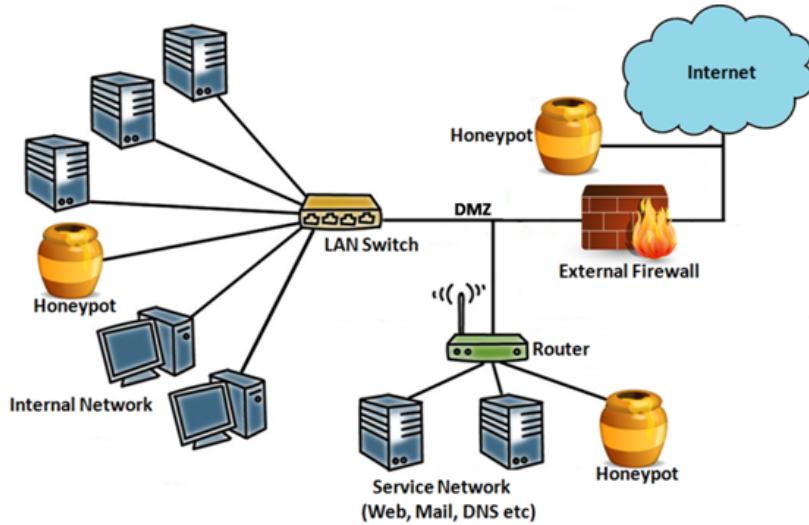


Image 7: Honeypots and Honeynets
Reference: https://www.umangsoftware.com/wp-content/uploads/2019/08/honeypot_2.png

A Honeynet is the next logical extension of a honeypot, it is a fake network segment that appears to be a very enticing target. Some organizations set up fake wireless access points for just this purpose.

Protect From Insider Threat

To deal with insider threats, you need both prevention and detection strategies. The most important preventive measure is to establish and enforce the least-privilege principle for access management and access control. Giving users the least amount of access they need to do their jobs enhances data security, because it limits what they can accidentally or deliberately access and ensures that if their password is compromised, the hacker doesn't have all keys to the kingdom. Other preventative measures include system hardening, anti-sniffing networks and strong authentication. Detection strategies include monitoring users and networks and using both network- and host-based intrusion detection systems, which are typically based on signatures, anomalies, behavior or heuristics.

End users also need to be trained in how to deal with the security threats they face, such as phishing emails and attachments. The best security in the world can be undermined by end users who fail to follow security policies. However, they cannot really be expected to follow those policies without adequate training.

Monitor & Baseline Protocols

You should monitor the use of different protocol types on your network to establish baselines both the organization level and a user level. Protocol baselining includes both wired and wireless networks. Data for the baseline should be obtained from routers, switches, firewalls, wireless APs, sniffers and dedicated collectors. Protocol deviations could indicate tunneling information or the use of unauthorized software to transmit data to unknown destinations.

Use VPNs

A virtual private network (VPN) is a secure private network connection across a public network. For example, VPNs can be used to connect LANs together across the internet. With a VPN, the remote end appears to be connected to the network as if it were connected locally. A VPN requires either special hardware or VPN software to be installed on servers and workstations. VPNs typically use a tunneling protocol, such as Layer 2 Tunneling Protocol, IPSec or Point-to-Point Tunneling Protocol (PPTP). To improve security, VPNs usually encrypt data, which can make them slower than normal network environments.

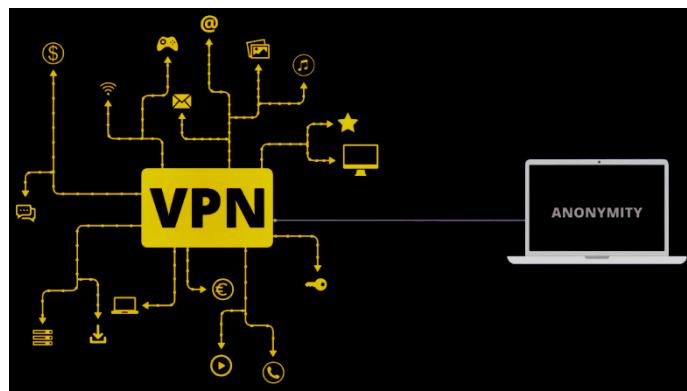


Image 8: VPN for Anonymity

Reference: https://embed-fastly.wistia.com/deliveries/d108d6daa05c480eacf817179f39db37f4c118c.webp?image_crop_resized=1280x720

Use Multiple Vendors

In addition to diversity of controls, you should strive for diversity of vendors. For example, to defend against malware, you should have antimalware software on each of your computers, as well as on the network and at the firewall — and use software from different vendors for each of these places. Because each vendor uses the same malware detection algorithms in all its products, if your workstation, network and firewall antimalware solutions all come from vendor A, then anything missed by one product will be missed by all three. The best approach is to use

vendor A for the firewall antimalware, vendor B for the network solution, and vendor C to protect individual computers. The probability of all three products, created by different vendors and using different detection algorithms, missing a specific piece of malware is far lower than any one of them alone missing it.

Use IDS Properly

An IDS can be an important and valuable part of your network security strategy. To get the most value from your IDS, take advantage of both ways it can detect potentially malicious activities:

Anomaly detection

Most systems maintain a certain baseline of activity on their networks and sensitive hosts. An IDS can record that baseline and scan for abnormal activity. If something unusual happens, such as a spike in activity that could indicate a ransomware or SQL injection attack, it sends an alert so the administrator can analyze the event and take action as soon as possible.

Misuse detection

The IDS will also compare activities with attack signatures, which are sets of characteristic features common to a specific attack or pattern of attacks. This helps them spot attacks even if they don't generate activity that violates your organization's baseline.

Automate Response to Attack

Many network devices and software solutions can be configured to automatically take action when an alarm is triggered, which dramatically reduces response time. Here are the actions you can often configure:

Block IP Address

The IDS or firewall can block the IP address from which the attack originated. This option is very effective against spam and denial-of-service attacks. However, some attackers spoof the source IP address during attacks, so the wrong address will be blocked.

Terminate Connections

Routers and firewalls can be configured to disrupt the connections that an intruder maintains with the compromised system by targeting RESET TCP packets at the attacker.

Acquire Additional Information

Another option is to collect information on intruders by observing them over a period of time. By analyzing the information you gather, you can find patterns and make your defense against the attack more robust. In particular, you can:

Look For the Point of Initial Access

How the intruders spread and what data was compromised. Reverse-engineer every piece of malicious software you find and learn how it works. Then clean up the affected systems and close the vulnerability that allowed initial access.

Determine How Malicious Software Was Deployed

Were administrative accounts used? Were they used after hours or in another anomalous manner? Then determine what awareness systems you could put in place to detect similar incidents in the future.

Physically Secure Network Equipment

Physical controls should be established and security personnel should ensure that equipment and data do not leave the building. Moreover, direct access to network equipment should be prohibited for unauthorized personnel.

Network Security Devices

Using the proper devices and solutions can help you defend your network. Here are the most common ones you should know about:

Firewall

One of the first lines of defense in a network, a firewall isolates one network from another. Firewalls either can be standalone systems or included in other devices, such as routers or servers. You can find both hardware and software firewall solutions; some firewalls are available as appliances that serve as the primary device separating two networks.

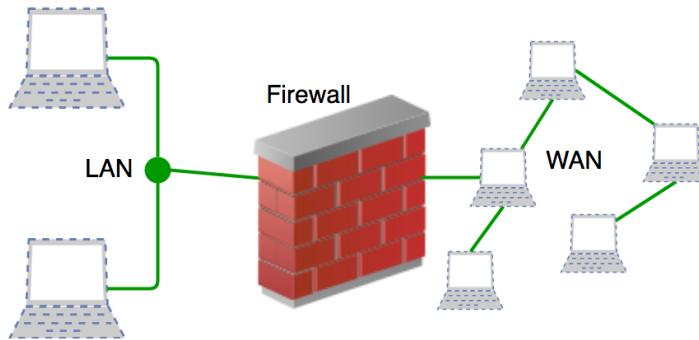


Image 9: Network Firewall

Reference: https://m.media-amazon.com/images/I/31ZROS8moRL._SR500,500_.jpg



Image 10: Firewall hardware

Reference: https://m.media-amazon.com/images/I/31ZROS8moRL._SR500,500_.jpg

Intrusion detection system (IDS)

An IDS enhances cybersecurity by spotting a hacker or malicious software on a network so you can remove it promptly to prevent a breach or other problems, and use the data logged about the event to better defend against similar intrusion incidents in the future. Investing in an IDS that enables you respond to attacks quickly can be far less costly than rectifying the damage from an attack and dealing with the subsequent legal issues.

Intrusion prevention system (IPS)

An IPS is a network security solution that can not only detect intruders, but also prevent them from successfully launching any known attack. Intrusion prevention systems combine the abilities of firewalls and intrusion detection systems. However, implementing an IPS on an effective scale can be costly, so businesses should carefully assess their IT risks before making the investment. Moreover, some intrusion prevention systems are not as fast and robust as some firewalls and intrusion detection systems, so it might not be an appropriate solution when speed is an absolute requirement.

Network access control (NAC)

It involves restricting the availability of network resources to endpoint devices that comply with your security policy. Some NAC solutions can automatically fix non-compliant nodes to ensure it is secure before access is allowed. NAC is most useful when the user environment is fairly static and can be rigidly controlled, such as enterprises and government agencies. It can be less practical in settings with a diverse set of users and devices that are frequently changing, which are common in the education and healthcare sectors.

Proxy Server

Proxy servers act as negotiators for requests from client software seeking resources from other servers. A client connects to the proxy server, requesting some service (for example, a website); the proxy server evaluates the request and then allows or denies it. In organizations, proxy servers are usually used for traffic filtering and performance improvement.

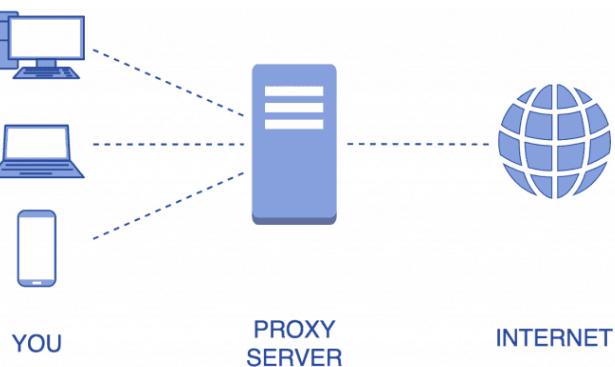


Image 11: Proxy Server

Reference: <https://s3.amazonaws.com/lintel-blogs-static-files/wp-content/uploads/2019/12/24050525/word-image-3.png>

Web Filters

Web filters are solutions that by preventing users' browsers from loading certain pages from particular websites. There are different web filters designed for individual, family, institutional and enterprise use.

Anti DDoS

Anti-DDoS devices detect distributed denial of service (DDoS) attacks in their early stages, absorb the volume of traffic and identify the source of the attack.



Image 12: Anti DDoS Protection
Reference: <https://www.accuwebhosting.com/blog/wp-content/uploads/2017/10/anti-ddos-attacks.jpg>

Load Balancer

Load balancers are physical units that direct computers to individual servers in a network based on factors such as server processor utilization, number of connections to a server or overall server performance. Organizations use load balancers to minimize the chance that any particular server will be overwhelmed and to optimize the bandwidth available to each computer in the network.

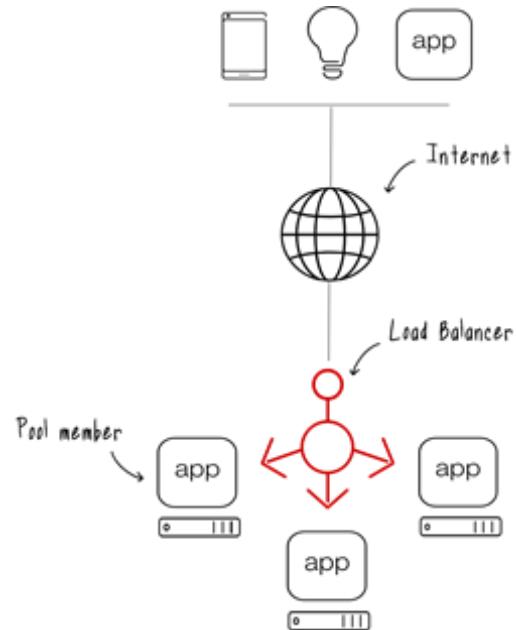


Image 13: Load Balancer for Web Apps

Reference: <https://www.f5.com/content/dam/f5-com/page-assets-en/home-en/resources/glossary/what%20is%20load%20balancing.png>

Spam Filters

Spam filters detect unwanted email and prevent it from getting to a user's mailbox. Spam filters judge emails based on policies or patterns designed by an organization or vendor. More sophisticated filters use a heuristic approach that attempts to identify spam through suspicious word patterns or word frequency.

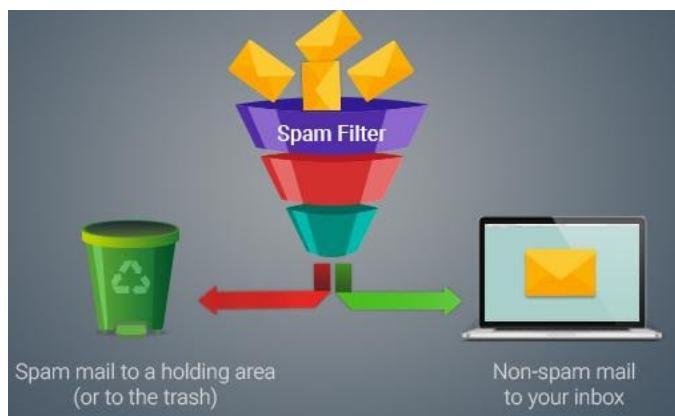


Image 14: Spam Filters

Reference: <https://blog.comodo.com/wp-content/uploads/anti-spam-filtering-techniques.jpg>

Configure and perform remote accessing & routing

In this section, we will read about:

- Overview of RemoteAccess
- VPN Concepts.
- Remote Access Authentication Protocol
- TCP/IPRouting

Overview of Remote Access

Introduction

Remote access is the ability for an authorized person to access a computer or a network from a geographical distance through a network connection. Remote access enables users to connect to the systems they need when they are physically far away. This is especially important for employees who work at branch offices, are traveling or telecommute to work.

Remote access enables remote users to access files and other system resources on any devices or servers that are connected to the network at any time, increasing employee productivity and enabling them to better collaborate with colleagues around the world.

A remote access strategy also gives organizations the flexibility to hire the best talent regardless of location, remove silos and promote collaboration between teams, offices and locations.



Image 1: Remote Access Scenario

Reference: <https://cdn.lynda.com/course/459485/459485-637199605440641228-16x9.jpg>

Technical support professionals also use remote access to connect to users' computers from remote locations to help them resolve issues with their systems or software.

One common method of providing remote access is via a remote access VPN connection. A VPN creates a safe and encrypted connection over a less secure network, such as the internet. VPN

technology was developed as a way to enable remote users and branch offices to securely log into corporate applications and other resources.

How Remote Access Works

Remote access is usually accomplished with a combination of software, hardware and network connectivity. For example, traditional remote access before the wide availability of internet connectivity was accomplished using terminal emulation software that controlled access over a hardware modem connected to a telephone network. Now, remote access is more commonly accomplished using a secure software solution like a VPN -- software -- by connecting hosts through a hard-wired network interface or Wi-Fi network interface -- hardware -- or by connecting via the internet -- network.

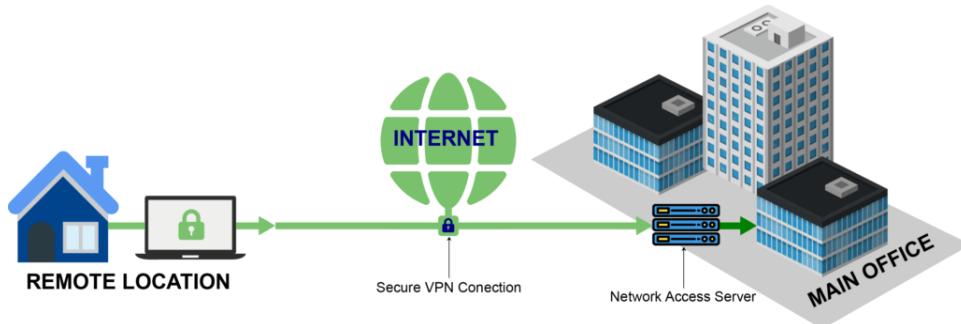


Image 2: Remote Access Working

Reference: <https://www.greyson.com/wp-content/uploads/2020/03/remote-access-vpn-1-1030x346.png>

Remote access VPNs are used to connect individual users to private networks. With a remote access VPN, each user needs a VPN client capable of connecting to the private network's VPN server.

When a user is connected to the network via a VPN client, the software encrypts the traffic before it delivers it over the internet. The VPN server, or gateway, is located at the edge of the targeted network and decrypts the data and sends it to the appropriate host inside the private network.

A computer must have software that enables it to connect and communicate with a system or resource hosted by the organization's remote access service. Once the user's computer is connected to the remote host, it can display a window with the target computer's desktop.

Enterprises can also use remote desktops to enable users to connect to their applications and networks remotely. Remote desktops use application software -- sometimes incorporated into the

remote host's operating system -- that enables apps to run remotely on a network server and be displayed locally at the same time.

Users can securely access on-premises and cloud applications and servers from anywhere, on any device with a variety of authentication methods, including remote single sign-on, which gives users easy and secure access to the apps they need without configuring VPNs or modifying firewall policies.

In addition, organizations can use multifactor authentication to verify a user's identity by combining multiple credentials unique to one person.

Types of Remote Access

Traditionally, enterprises use modems and dial-up technologies to allow employees to connect to office networks via telephone networks connected to remote access servers. Devices connected to dial-up networks use analog modems to call assigned telephone numbers to make connections and send or receive messages.

Broadband

Broadband provides remote users with high-speed connection options to business networks and to the internet. There are several types of broadband, including the following:

Cable Broadband

Cable broadband shares bandwidth across many users and, as a result, upstream data rates can be slow during high-usage hours in areas with many subscribers.

DSL (Digital Subscriber Line)

DSL broadband provides high-speed networking over a telephone network using broadband modem tech. However, DSL only works over a limited physical distance and may not be available in some areas if the local telephone infrastructure doesn't support DSL technology.

Cellular Internet

Cellular internet services can be accessed by mobile devices via a wireless connection from any location where a cellular network is available.

Satellite Internet

Satellite internet services use telecommunications satellites to provide users with internet access in areas where land-based internet access isn't available, as well as for temporary mobile installations.

Fiber Optics

Fiber optics broadband technology enables users to transfer large amounts of data quickly and seamlessly.

Remote Access Protocols

Common remote access and VPN protocols include the following:

Point-to-Point Protocol (PPP)

Point-to-Point Protocol (PPP) enables hosts to set up a direct connection between two endpoints.

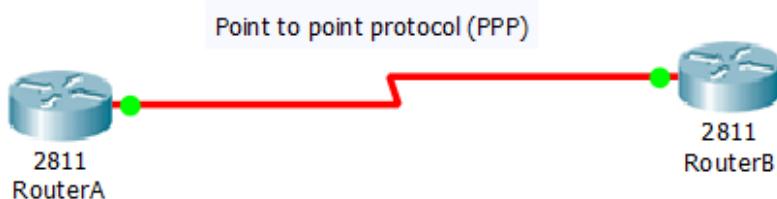


Image 3: PPP Protocol

Reference: <https://www.timigate.com/wp-content/uploads/2018/05/ppp.png>

IPSec

Internet Protocol Security is a set of security protocols used to enable authentication and encryption services to secure the transfer of IP packets over the internet.

IPSec Modes

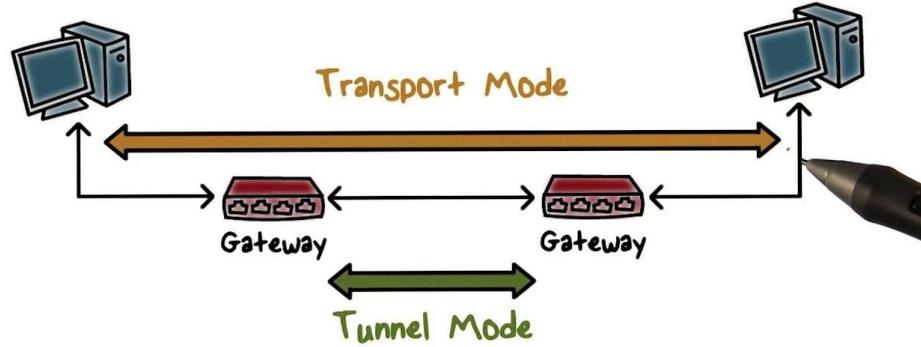


Image 4: IPSec Modes

Reference: <https://i.ytimg.com/vi/oNmadn4gwWU/maxresdefault.jpg>

Point-to-Point Tunneling (PPTP)

Point-to-Point Tunneling (PPTP) is one of the oldest protocols for implementing virtual private networks. However, over the years, it has proven to be vulnerable to many types of attack. Although PPTP is not very secure, it persists in some cases

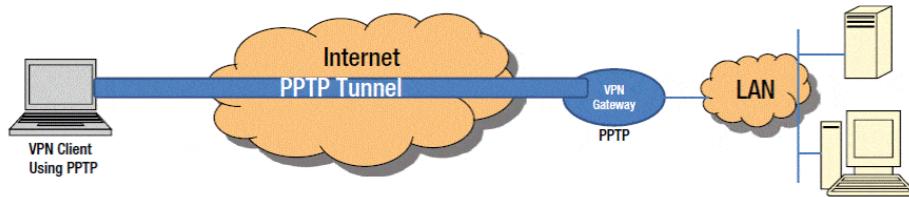


Image 5: PPTP Tunneling

Reference: <https://networkencyclopedia.com/wp-content/uploads/2019/09/point-to-point-tunneling-protocol-pptp.gif>

Layer Two Tunneling Protocol (L2TP)

Layer Two Tunneling Protocol (L2TP) is a VPN protocol that does not offer encryption or cryptographic authentication for the traffic that passes through the connection. As a result, it is usually paired with IPsec, which provides those services.

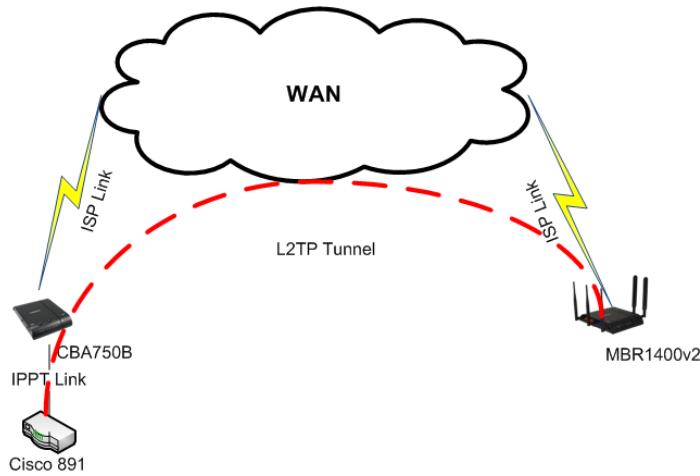


Image 6: L2TP Tunnel

Reference: <https://customer.cradlepoint.com/servlet/rtaImage?eid=ka938000000L2j8&feoid=00N38000003lF9E&refid=0EM50000000DHm4>

Remote Authentication Dial-In User Service (RADIUS)

Remote Authentication Dial-In User Service (RADIUS) is a protocol developed in 1991 and published as an Internet Standard track specification in 2000 to enable remote access servers to communicate with a central server to authenticate dial-in users and authorize their access to the requested system or service.

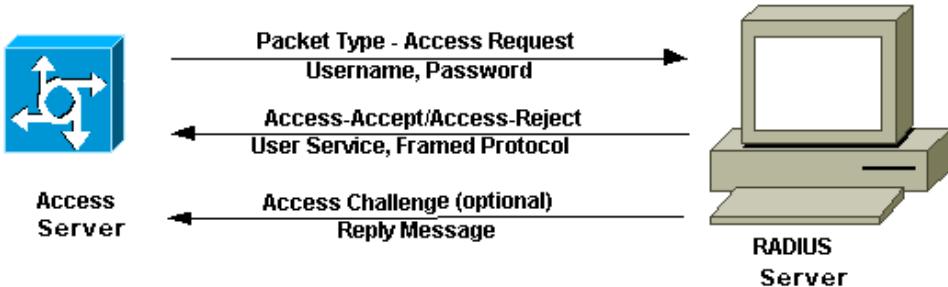


Image 7: RADIUS Authentication

Reference: <https://www.cisco.com/c/dam/en/us/support/docs/security-vpn/remote-authentication-dial-user-service-radius/12433-32b.gif>

Terminal Access Controller Access Control System (TACACS)

Terminal Access Controller Access Control System (TACACS) is a remote authentication protocol that was originally common to UNIX networks that enables a remote access server to forward a user's password to an authentication server to determine whether access to a given system should be allowed. TACACS+ is a separate protocol designed to handle authentication

and authorization, and to account for administrator access to network devices, such as routers and switches.

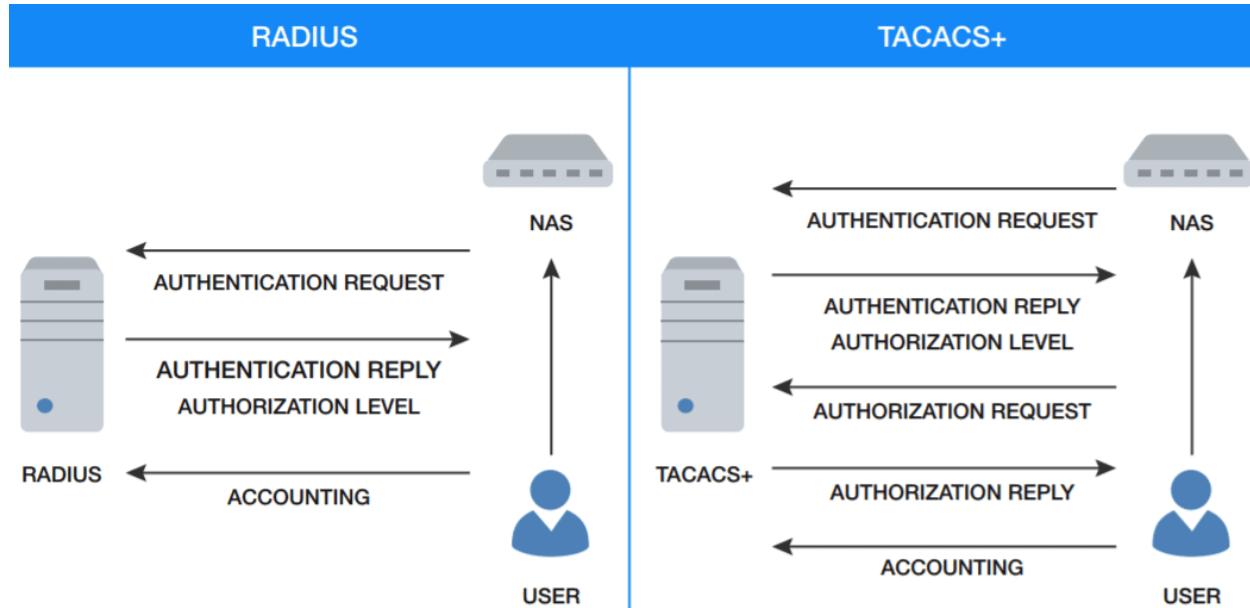


Image 8: RADIUS & TACACS Comparison

Reference:

<https://i0.wp.com/www.networkhunt.com/wp-content/uploads/2017/10/RADIUS-VS-TACACS-packet-flow.png?fit=1101%2C579&ssl=1>

VPN Concepts

Introduction

A VPN is a private network that uses a public network (usually the internet) to connect remote sites or users together. The VPN uses "virtual" connections routed through the internet from the business's private network or a third-party VPN service to the remote site or person. VPNs help ensure security — anyone intercepting the encrypted data can't read it.

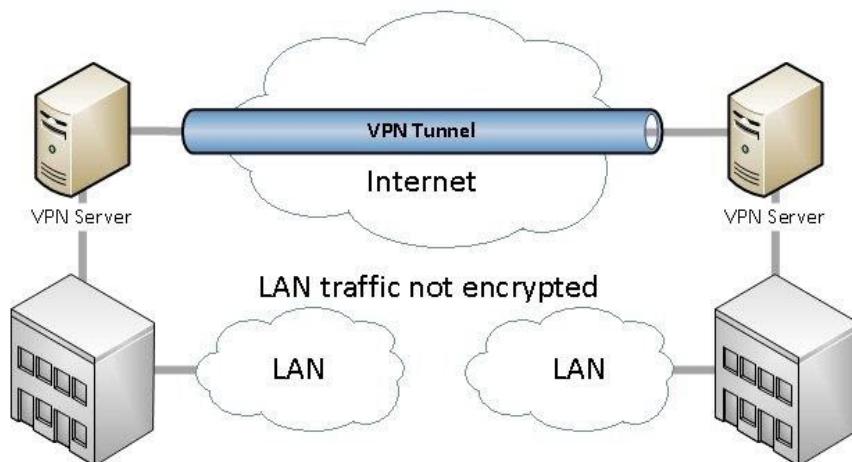


Image 9: VPN Scenario
Reference: <https://computer.howstuffworks.com/vpn.htm>

A VPN's purpose is providing a secure and reliable private connection between computer networks over an existing public network, typically the internet. Before looking at the technology that makes a VPN possible, let's consider all the benefits and features someone should expect in a VPN.

VPN Benefits

A well-designed VPN provides the following benefits:

- Extended connections across multiple geographic locations without using a leased line
- Improved security for exchanging data
- Flexibility for remote offices and employees to use the business intranet over an existing internet connection as if they're directly connected to the network

- Savings in time and expense for employees to commute if they work from virtual workplaces
- Improved productivity for remote employees

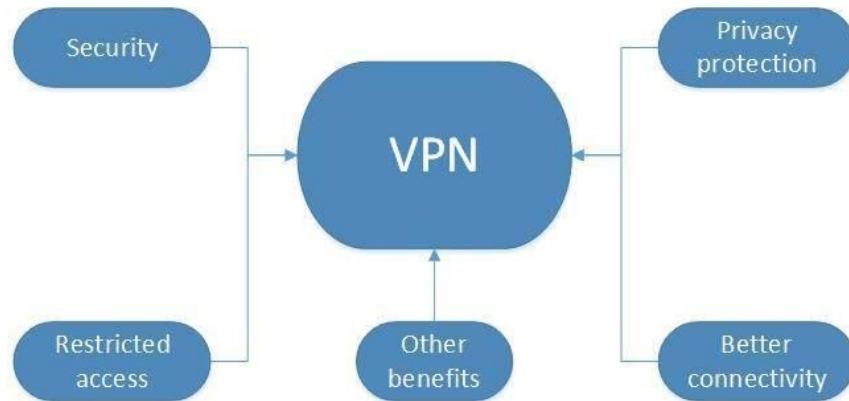


Image 10: VPN benefits

Reference:

<https://www.facebook.com/RidhitechIndia/posts/top-five-vpn-advantages-and-benefitsvpn-is-a-technology-which-creates-a-virtual-/78561680157287/>

Desired VPN Features

A company might not require all these benefits from its business VPN, but it should demand the following essential VPN features:

Security

The VPN should protect data while it's traveling on the public network. If intruders attempt to capture the data, they should be unable to read or use it.

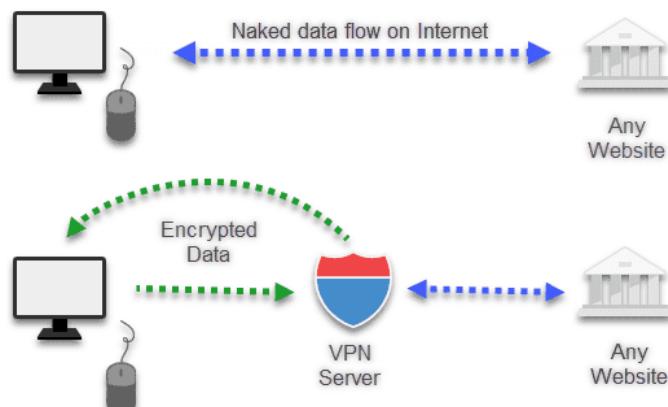


Image 11: VPN Security
Reference: <https://www.phoneswiki.com/wp-content/uploads/2019/08/how-a-VPN-works.png>

Reliability

Employees and remote offices should be able to connect to the VPN with no trouble at any time (unless hours are restricted), and the VPN should provide the same quality of connection for each user even when it is handling its maximum number of simultaneous connections.

Scalability

As a business grows, it should be able to extend its VPN services to handle that growth without replacing the VPN technology altogether.

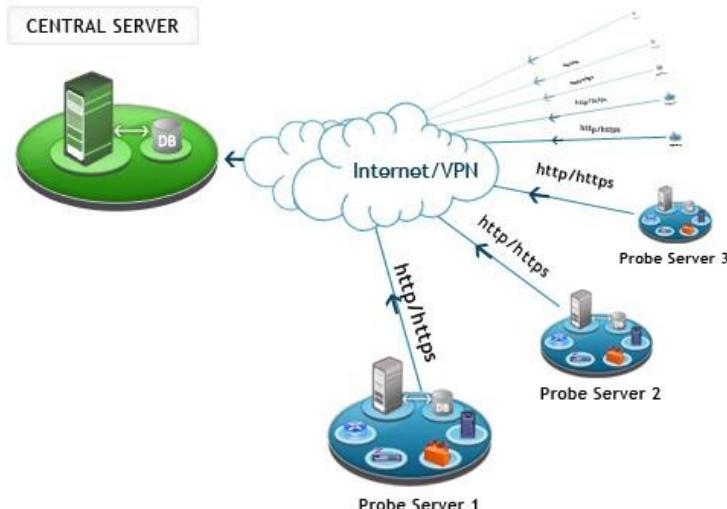


Image 12: VPN Scalability
Reference: <https://www.manageengine.com/network-monitoring/images/server-multi-probes.jpg>

VPN Types

Public VPN

Public VPN providers are often evaluated on whether they capture information about their users and the number of countries in which they have remote servers. Because a VPN privatizes information about the user, he or she can use a VPN connection to mask the location they're

connecting from, which may permit access to geographically restricted information, such as a TV service limited to access from a certain country.

One interesting thing to note about VPNs is that there are no standards about how to set them up. This article covers network, authentication and security protocols that provide the features and benefits listed above. It also describes how a VPN's components work together. If you're establishing your own VPN, though, it's up to you to decide which protocols and components to use and to understand how they work together.

Remote-Access VPN

A remote-access VPN allows individual users to establish secure connections with a remote computer network. Those users can access the secure resources on that network as if they were directly plugged in to the network's servers. An example of a company that needs a remote-access VPN is a large firm with hundreds of salespeople in the field. Another name for this type of VPN is virtual private dial-up network (VPDN), acknowledging that in its earliest form, a remote-access VPN required dialing in to a server using an analog telephone system.

There are two components required in a remote-access VPN. The first is a network access server (NAS, usually pronounced "nazz" conversationally), also called a media gateway or a remote-access server (RAS). (Note: IT professionals also use NAS to mean network-attached storage.) A NAS might be a dedicated server, or it might be one of multiple software applications running on a shared server. It's a NAS that a user connects to from the internet in order to use a VPN. The NAS requires that user to provide valid credentials to sign in to the VPN. To authenticate the user's credentials, the NAS uses either its own authentication process or a separate authentication server running on the network.

The other required component of remote-access VPNs is client software. In other words, employees who want to use the VPN from their computers require software on those computers that can establish and maintain a connection to the VPN. Most operating systems today have built-in software that can connect to remote-access VPNs, though some VPNs might require users to install a specific application instead. The client software sets up the tunneled connection to a NAS, which the user indicates by its internet address. The software also manages the encryption required to keep the connection secure. You can read more about tunneling and encryption later in this article.

Large corporations or businesses with knowledgeable IT staff typically purchase, deploy and maintain their own remote-access VPNs. Businesses can also choose to outsource their

remote-access VPN services through an enterprise service provider (ESP). The ESP sets up a NAS for the business and keeps that NAS running smoothly.

A remote-access VPN is great for individual employees, but what about entire branch offices with dozens or even hundreds of employees? Next, we'll look at another type of VPN used to keep businesses connected LAN-to-LAN.

Site-to-Site VPN

A site-to-site VPN allows offices in multiple fixed locations to establish secure connections with each other over a public network such as the internet. Site-to-site VPN extends the company's network, making computer resources from one location available to employees at other locations.

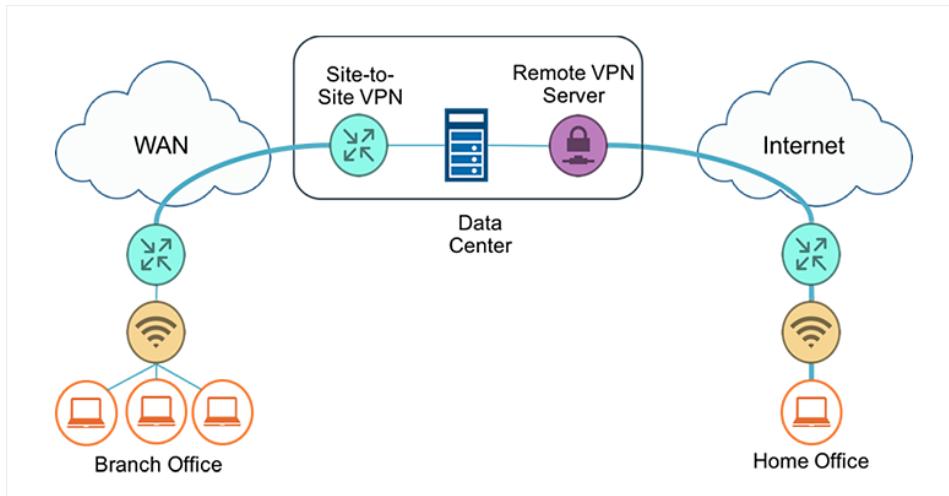


Image 13: Site to Site VPN
Reference: https://miro.medium.com/proxy/1*9IKvQ2l0ls7_P6fEfMGOdg.png

An example of a company that needs a site-to-site VPN is a growing corporation with dozens of branch offices around the world.

There are two types of site-to-site VPNs:

1. **Intranet-based:** If a company has one or more remote locations that they wish to join in a single private network, they can create an intranet VPN to connect each separate LAN to a single WAN.
2. **Extranet-based:** When a company has a close relationship with another company (such as a partner, supplier or customer), it can build an extranet VPN that connects those

companies' LANs. This extranet VPN allows the companies to work together in a secure, shared network environment while preventing access to their separate intranets.

Even though the purpose of a site-to-site VPN is different from that of a remote-access VPN, it could use some of the same software and equipment. Ideally, though, a site-to-site VPN should eliminate the need for each computer to run VPN client software as if it were on a remote-access VPN. Dedicated VPN client equipment, described later in this article, can accomplish this goal in a site-to-site VPN.

VPN Tunneling

Most VPNs rely on tunneling to create a private network that reaches across the internet. In our article "How does the internet work?" we describe how each data file is broken into a series of packets to be sent and received by computers connected to the internet. Tunneling is the process of placing an entire packet within another packet before it's transported over the internet. That outer packet protects the contents from public view and ensures that the packet moves within a virtual tunnel.

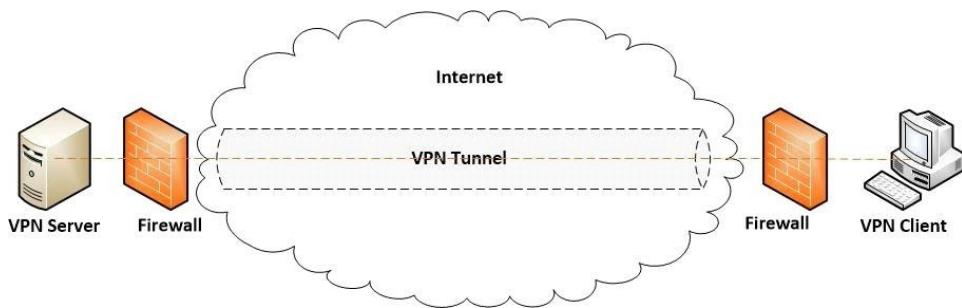


Image 14: VPN Tunneling
Reference: <https://www.vpnmentor.com/wp-content/uploads/2018/08/vpn-tunneling-diagram.jpg>

This layering of packets is called encapsulation. Computers or other network devices at both ends of the tunnel, called tunnel interfaces, can encapsulate outgoing packets and reopen incoming packets. Users (at one end of the tunnel) and IT personnel (at one or both ends of the tunnel) configure the tunnel interfaces they're responsible for to use a tunneling protocol. Also called an encapsulation protocol, a tunneling protocol is a standardized way to encapsulate packets [source: Microsoft]. Later in this article, you can read about the different tunneling protocols used by VPNs.

The purpose of the tunneling protocol is to add a layer of security that protects each packet on its journey over the internet. The packet is traveling with the same transport protocol it would have

used without the tunnel; this protocol defines how each computer sends and receives data over its ISP. Each inner packet still maintains the passenger protocol, such as internet protocol (IP), which defines how it travels on the LANs at each end of the tunnel. (See the sidebar for more about how computers use common network protocols to communicate.) The tunneling protocol used for encapsulation adds a layer of security to protect the packet on its journey over the internet.

To better understand the relationships between protocols, think of tunneling as having a computer delivered to you by a shipping company. The vendor who is sending you the computer packs the computer (passenger protocol) in a box (tunneling protocol). Shippers then place that box on a shipping truck (transport protocol) at the vendor's warehouse (one tunnel interface). The truck (transport protocol) travels over the highways (internet) to your home (the other tunnel interface) and delivers the computer. You open the box (tunneling protocol) and remove the computer (passenger protocol).

Some VPNs, such as ExpressVPN have a split tunneling feature. This means you can choose which apps send data through the VPN and which use your regular, local connection.

Equipment Used For VPN

When planning or extending a VPN, though, you should consider the following equipment:

Network access server

As previously described, a NAS is responsible for setting up and maintaining each tunnel in a remote-access VPN.

Firewall

A firewall provides a strong barrier between your private network and the internet. IT staff can set firewalls to restrict what type of traffic can pass through from the internet onto a LAN, and on what TCP and UDP ports. Even without a VPN, a LAN should include a firewall to help protect against malicious internet traffic.

AAA Server

The acronym stands for the server's three responsibilities: authentication, authorization and accounting. For each VPN connection, the AAA server confirms who you are (authentication),

identifies what you're allowed to access over the connection (authorization) and tracks what you do while you're logged in (accounting).

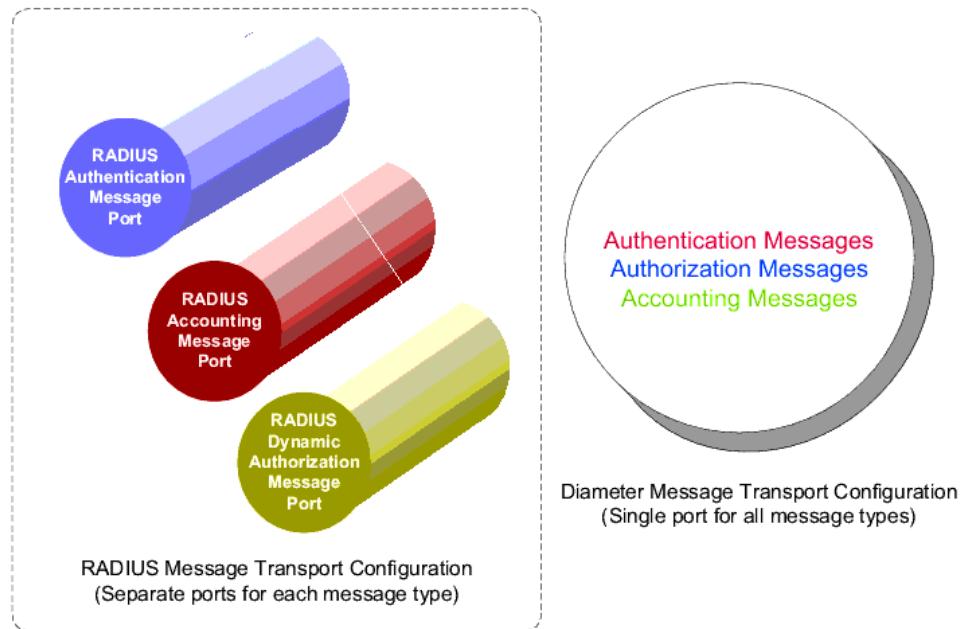


Image 15: AAA Server

Reference: https://www.juniper.net/documentation/software/aaa_802/imsaaa11/sw-imsaaa-admin/html/RAD%26Dia%20Ports5.gif

VPN Concentrator

This device replaces an AAA server installed on a generic server. The hardware and software work together to establish VPN tunnels and handle large numbers of simultaneous connections.

VPN-enabled/VPN-optimized Router

This is a typical router that delegates traffic on a network, but with the added feature of routing traffic using protocols specific to VPNs.

VPN-enabled Firewall

This is a conventional firewall protecting traffic between networks, but with the added feature of managing traffic using protocols specific to VPNs.

VPN Client

This is software running on a dedicated device that acts as the tunnel interface for multiple connections. This setup spares each computer from having to run its own VPN client software.

VPN Security

Encryption is the process of encoding data so that only a computer with the right decoder will be able to read and use it. You could use encryption to protect files on your computer or e-mails you send to friends or colleagues. An encryption key tells the computer what computations to perform on data in order to encrypt or decrypt it. The most common forms of encryption are symmetric-key encryption or public-key encryption:

In symmetric-key encryption, all computers (or users) share the same key used to both encrypt and decrypt a message. In public-key encryption, each computer (or user) has a public-private key pair. One computer uses its private key to encrypt a message, and another computer uses the corresponding public key to decrypt that message.

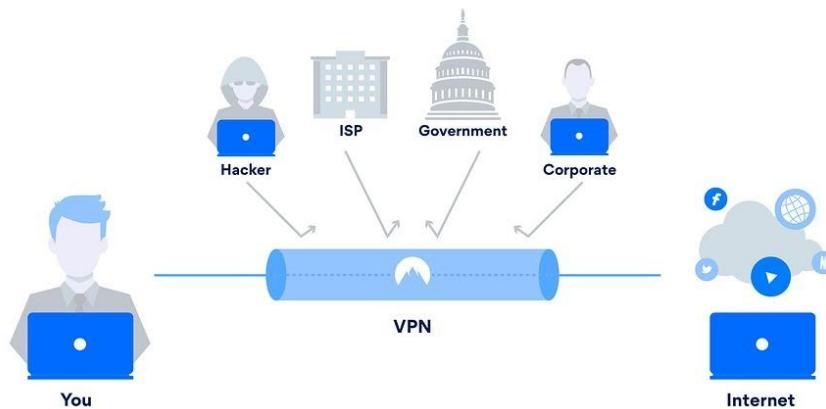


Image 16: VPN Security

Reference: <https://cdn-cybersecurity.att.com/blog-content/Blog-Images/vpn.jpg>

In a VPN, the computers at each end of the tunnel encrypt the data entering the tunnel and decrypt it at the other end. However, a VPN needs more than just a pair of keys to apply encryption. That's where protocols come in. A site-to-site VPN could use either internet protocol security protocol (IPSec) or generic routing encapsulation (GRE). GRE provides the framework for how to package the passenger protocol for transport over the internet protocol (IP). This

framework includes information on what type of packet you're encapsulating and the connection between sender and receiver.

IPSec is a widely used protocol for securing traffic on IP networks, including the internet. IPSec can encrypt data between various devices, including router to router, firewall to router, desktop to router, and desktop to server. IPSec consists of two sub-protocols which provide the instructions a VPN needs to secure its packets:

Encapsulated Security Payload (ESP) encrypts the packet's payload (the data it's transporting) with a symmetric key.

Authentication Header (AH) uses a hashing operation on the packet header to help hide certain packet information (like the sender's identity) until it gets to its destination.

Networked devices can use IPSec in one of two encryption modes. In transport mode, devices encrypt the data traveling between them. In tunnel mode, the devices build a virtual tunnel between two networks. As you might guess, VPNs use IPSec in tunnel mode with IPSec ESP and IPSec AH working together.

In a remote-access VPN, tunneling typically relies on Point-to-point Protocol (PPP) which is part of the native protocols used by the internet. More accurately, though, remote-access VPNs use one of three protocols based on PPP:

L2F (Layer 2 Forwarding)

L2F (Layer 2 Forwarding) developed by Cisco; uses any authentication scheme supported by PPP.

PPTP (Point-to-point Tunneling Protocol)

PPTP (Point-to-point Tunneling Protocol) supports 40-bit and 128-bit encryption and any authentication scheme supported by PPP.

L2TP (Layer 2 Tunneling Protocol)

L2TP (Layer 2 Tunneling Protocol) combines features of PPTP and L2F and fully supports IPSec; also applicable in site-to-site VPNs

Over time, people have developed new and better technologies to use in networks, which improves the features of existing VPNs. VPN-specific technologies, though, such as tunneling

protocols, haven't changed much in that time, perhaps because current VPNs do such a good job at to keep businesses connected around the world.

Remote Access Authentication Protocol

There are simply two methods to authenticate PPP links namely Password Authentication Protocol (PAP) and Challenge Handshake Authentication Protocol (CHAP). From these two authentication protocols, PAP is less secured as the password is sent in clear text and is performed only at the initial link establishment.



- **Step 1 :** A remote user initiates a session.
- **Step 2 :** The remote computer requests connection to a remote access server.
- **Step 3 :** The remote server acknowledges the connection.
- **Step 4 :** The client is requested to authenticate itself by using a remote authentication protocol.
- **Step 5 :** A connection is established between both computers by using the agreed-upon authentication protocol and credentials.

Image 17: RAS Process

Reference: <https://slideplayer.com/slide/5781253/19/images/4/Remote+Access+Authentication+Process.jpg>

PAP

PAP is a password Authentication Protocol used by PPP links to validate users. PAP authentication requires the calling device to enter the username and password. If the credentials match with the local database of the called device or in the remote AAA database then it is allowed to access otherwise denied.

Features

Some of the features of PAP are:

- The password is sent in clear text.
- All network operating system support PAP.

-
- It uses two-way Handshake Protocol.
 - It is non-interactive.
 - PAP supports both one-way authentication (unidirectional) and two-way authentication (bidirectional).

When to use PAP

PAP is usually used in following scenarios:

- When the application doesn't support CHAP.
- Circumstances where it is necessary to send a plain text password to stimulate a login at the called device (remote host).
- When there is occurrence of incompatibilities between different vendors of CHAP.

Advantage of CHAP over PAP

Some of the advantages are:

- CHAP is more secured than PAP.
- CHAP can provide authentication periodically to recognise that the user accessing the PPP link is same or not.
- In CHAP, the real passwords are never shared on the link instead a hash value of it is calculated and transferred.

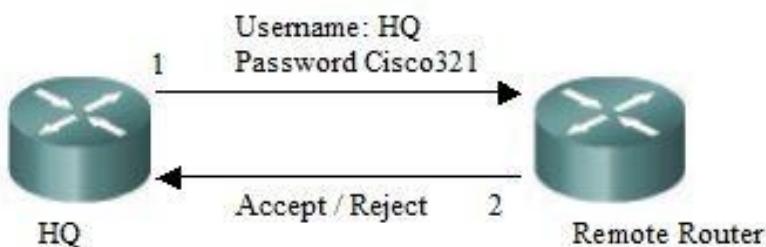


Image 17: PAP 2 Way Handshake

Reference: <https://orbit-computer-solutions.com/wp-content/uploads/2015/10/PAP-Authentication-Protocol.jpg>

Advantage of PAP over CHAP

The only advantage PAP holds over CHAP is that it is supported by all the network operating system vendors therefore it can be said that PAP is used where CHAP is not supported. But if CHAP is supported then it is recommended to use CHAP as it is more secured.

CHAP

Challenge Handshake Authentication Protocol (CHAP) is a Point-to-point protocol (PPP) authentication protocol developed by IETF (Internet Engineering Task Force). It is used at the initial startup of the link. Also, it performs periodic checkups to check if the router is still communicating with the same host.

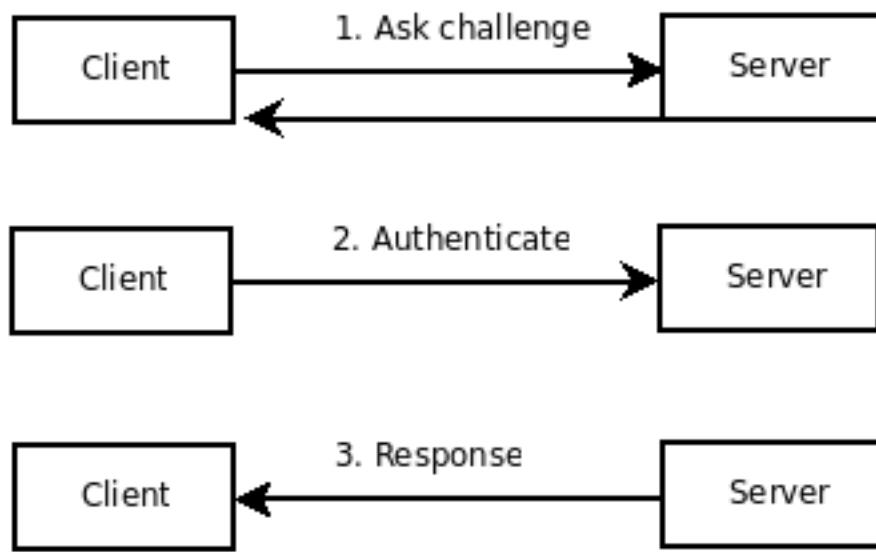


Image 18: CHAP Authentication Process

Reference: <https://lh6.googleusercontent.com/-qXnkcYTUsi8/TXi3AcRAnLI/AAAAAAAUAU/ZrDm1ttuR3A/s1600/diagram1.png>

Features

- It uses 3-way handshaking protocol (not like TCP). First, the authenticator sends a challenge packet to the peer then, the peer responds with a value using its one way hash function. The authenticator then matches the received value with its own calculated hash value. If the values match then the authentication is acknowledged otherwise, the connection will be terminated.
- It uses one-way hash function called MD5.

-
- It also authenticates periodically to check if the communication is taking place with the same device or not.
 - Also, it provides more security than PAP (Password Authentication Procedure) as the value used (find out by hash function) is changed variably.
 - CHAP requires to know the plaintext of the secret as it is never sent over the network.

CHAP Packets

There are 4 types of CHAP packets

Challenge Packet

It is a packet sent, by the authenticator to peer, at the starting of the CHAP 3-way Handshake. Challenge packet is also sent periodically to check if the connection is not altered. It contains Identifier value, value field which contains random value and also contains name field which contains name of the authenticator. The name field is used for password look up. The name field is also fed to MD5 hash generator and a one-way hash value is generated.

Response Packet

It is used to response to the challenge packet. It contains the Value field which contains one-way hash value generated, identifier value and the name field. The Name field of the Response packet is set to the hostname of the peer router. Now, the Name field of Challenge packet is looked up for the password. The router looks up for an entry that matches the username in the Name field of the Challenge packet and gets the password. Then, this password is hashed by feeding it to MD5 hash generator and one way hash value is generated. This value is inserted into the value field of response packet and sent to the authenticator.

Success Packet

Now, the authenticator also performs the same thing by looking up in name field (if it has an entry for that username) of the response packet and by using that it generates a hash value. If the value generated is same as that of peer then the success packet is send.

Failure Packet

If the generated value is different then the failure packet is send to the peer.

The Extensible Authentication Protocol (EAP)

This protocol enables extensible authentication for network access. The Extensible Authentication Protocol (EAP) enables extensible authentication for network access. EAP methods operate within the EAP framework to support a variety of authentication techniques. For example, an administrator who requires digital certificate-based authentication might deploy the EAP-TLS method. For more information, see [RFC2716].

Strong credentials such as digital certificates offer many security benefits. However, in many environments these credentials can be prohibitively expensive to send to clients. In such environments, an administrator might use a simple password-based EAP method where the client and server have shared authentication.

The Extensible Authentication Protocol Method for Microsoft Challenge Handshake Authentication Protocol (CHAP) is an EAP method that is designed to meet this need. It does so by having the client and server use MSCHAPv2 to mutually authenticate each other.

To understand the Extensible Authentication Protocol Method for Microsoft CHAP, it is necessary to understand both EAP and MSCHAPv2, as specified in [RFC3748] sections 3 and 4, and [RFC2759] section 1, respectively.

The flow for successful authentication with Extensible Authentication Protocol Method for Microsoft CHAP is as follows:

- An EAP session is established between a client (EAP peer) and an EAP server.
- The EAP server and EAP peer negotiate the EAP method to use. The Extensible Authentication Protocol Method for Microsoft CHAP is selected.
- The EAP peer and EAP server continue to exchange EAP messages with MSCHAPv2 packets encapsulated in the payload.
- After the MSCHAPv2 packets successfully authenticate the client and the server to each other, the EAP authentication finishes.

The Extensible Authentication Protocol Method for Microsoft CHAP is exposed to the same security threats as MSCHAPv2 and needs to be protected inside a secure tunnel, such as the one specified in [MS-PEAP].

The Extensible Authentication Protocol Method for Microsoft CHAP is typically deployed in an environment such as the one that is shown in the following diagram. The EAP peer mutually

authenticates with an EAP server through a network access server, for example, a Point-to-Point Protocol (PPP) dial-up server, wireless access point, or VPN gateway.

The Extensible Authentication Protocol Method for Microsoft CHAP messages are carried from the EAP peer to the network access server (NAS) over lower-layer protocols, such as PPP or 802.1X (Port-Based Network Access Control, which is an IEEE standard for local and metropolitan area networks) [IEEE802.1X].

The Extensible Authentication Protocol Method for Microsoft CHAP messages are then carried from the network access server to the EAP server over a higher-level protocol, such as Remote Authentication Dial-In User Service (RADIUS). For more information about RADIUS, see [RFC2865] and [RFC2869].

MS-CHAP

MS-CHAP is the Microsoft version of the Challenge-Handshake Authentication Protocol, CHAP. The protocol exists in two versions, MS-CHAPv1 (defined in RFC 2433) and MS-CHAPv2 (defined in RFC 2759). MS-CHAPv2 was introduced with pptp3-fix that was included in Windows NT 4.0 SP4 and was added to Windows 98 in the "Windows 98 Dial-Up Networking Security Upgrade Release"[1] and Windows 95 in the "Dial Up Networking 1.3 Performance & Security Update for MS Windows 95" upgrade. Windows Vista dropped support for MS-CHAPv1.

MS-CHAP is used as one authentication option in Microsoft's implementation of the PPTP protocol for virtual private networks. It is also used as an authentication option with RADIUS[2] servers which are used with IEEE 802.1X (e.g., WiFi security using the WPA-Enterprise protocol). It is further used as the main authentication option of the Protected Extensible Authentication Protocol (PEAP).

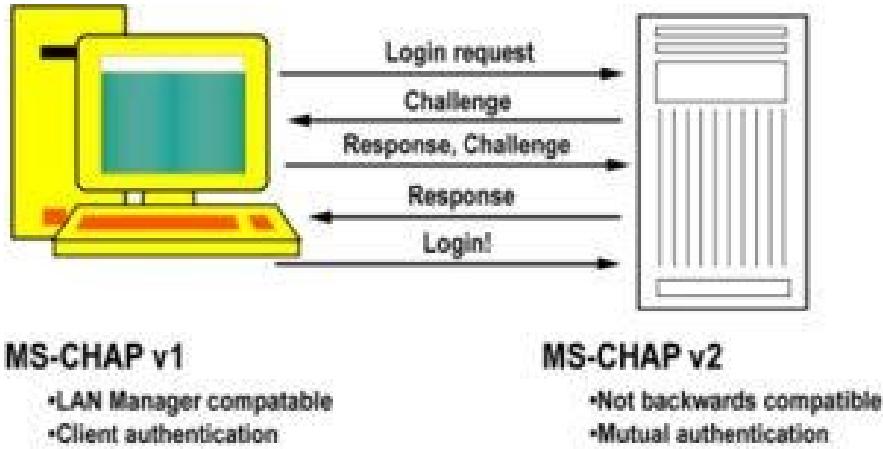


Image 19: MS-CHAP v1 and MS-CHAP v2 Comparison

Refrence:

https://lh3.googleusercontent.com/proxy/tXVHpOxZtNfImJT7ZKHeuXSklSikO1hiyxLsBmTsl4aZ1ZlzbRsMMXVDL_pkTuYyP6wd_YNhQIZA2WJqXe17D16jxipcP4uVGvwVNNMnj1Tq1sa-CgL--EhcLBzRgK5dg_3akCjyEH0UpQ-t3QigKZiMz4n2vnlKDenxBycXdZwMn5_5Cge1Cm

As compared with CHAP, MS-CHAP:

- Is enabled by negotiating CHAP Algorithm 0x80 (0x81 for MS-chapv2) in LCP option 3, Authentication Protocol
- Provides an authenticator-controlled password change mechanism
- Provides an authenticator-controlled authentication retry mechanism
- Defines failure codes returned in the Failure packet message field

MS-CHAPv2 provides mutual authentication between peers by piggybacking a peer challenge on the Response packet and an authenticator response on the Success packet.

MS-CHAP v2

MS-CHAP v2 (Microsoft Challenge Handshake Authentication Protocol version 2) is a Microsoft authentication protocol that, like CHAP, avoids sending passwords in clear-text. MS-CHAP v1 is not supported.

Steel-Belted Radius Carrier must be able to perform a digest operation similar to CHAP to support MS-CHAP v2. Therefore, it must have access to its own copy of the user's password. Native User passwords are stored in the Steel-Belted Radius Carrier database. SQL or LDAP

BindName authentication retrieves the password by means of a query to the database; the retrieved password can be used to create a digest if it is in clear-text form.

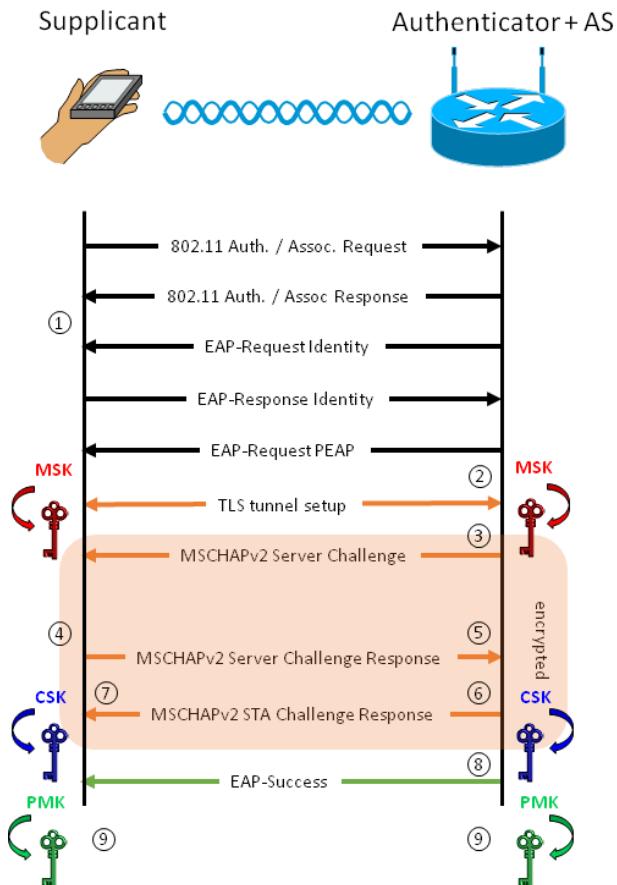


Image 20: MS-CHAP v2 Transactions
Reference: <https://i.stack.imgur.com/gOwXq.png>

MS-CHAP v2 communicates users' requests to change their passwords to a RADIUS server. Steel-Belted Radius Carrier supports this feature, although it must also be supported by whatever application the user is using to log in. For more information about MS-CHAP v2, see RFC 2433, Microsoft PPP CHAP Extensions; RFC 2548, Microsoft Vendor-specific RADIUS Attributes; and RFC 2759, Microsoft PPP CHAP Extensions, Version 2.

RADIUS

What is RADIUS?

The Remote Authentication Dial-In User Service (RADIUS) was developed in 1991 as an access server authentication and accounting protocol. It was later brought into the Internet Engineering Task Force (IETF) standards. Just about everyone uses RADIUS, since RADIUS is the underlying authentication and access protocol used by the majority of network and computing systems. RADIUS is commonly used to facilitate roaming between ISPs.

How it Works?

The user or machine sends a request to a Network Access Server (NAS) to gain access to a network resource. This request includes access credentials (such as a username and password) which are passed to the NAS device via the link-layer protocol. The request may contain other information about the user, such as network address, phone number, or physical attachment to the NAS.

The RADIUS server checks that the information is correct using an authentication protocol (ex: PAP, CHAP, EAP). The RADIUS server returns with one of three responses: Access Reject, Access Challenge, or Access Accept. Each of these responses can be passed to the user in a return webpage.

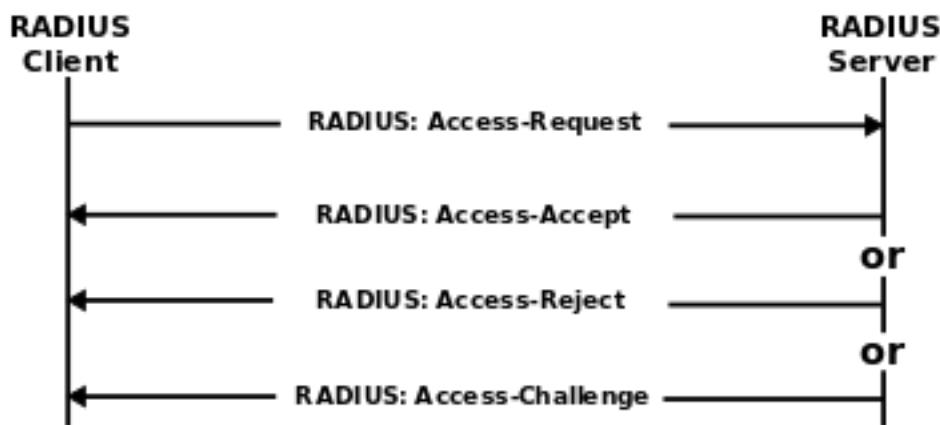


Image 21: RADIUS Connectivity Process

Reference: https://upload.wikimedia.org/wikipedia/commons/thumb/5/50/Drawing_RADIUS_1812.svg/350px-Drawing_RADIUS_1812.svg.png

Once the user is authenticated, the RADIUS server will check that the user is authorized for the specific network service.

Background Information

Communication between a network access server (NAS) and a RADIUS server is based on the User Datagram Protocol (UDP). Generally, the RADIUS protocol is considered a connectionless service. Issues related to server availability, retransmission, and timeouts are handled by the RADIUS-enabled devices rather than the transmission protocol.

RADIUS is a Client/Server Protocol

The RADIUS client is typically a NAS and the RADIUS server is usually a daemon process running on a UNIX or Windows NT machine. The client passes user information to designated RADIUS servers and acts on the response that is returned. RADIUS servers receive user connection requests, authenticate the user, and then return the configuration information necessary for the client to deliver service to the user. A RADIUS server can act as a proxy client to other RADIUS servers or other kinds of authentication servers.

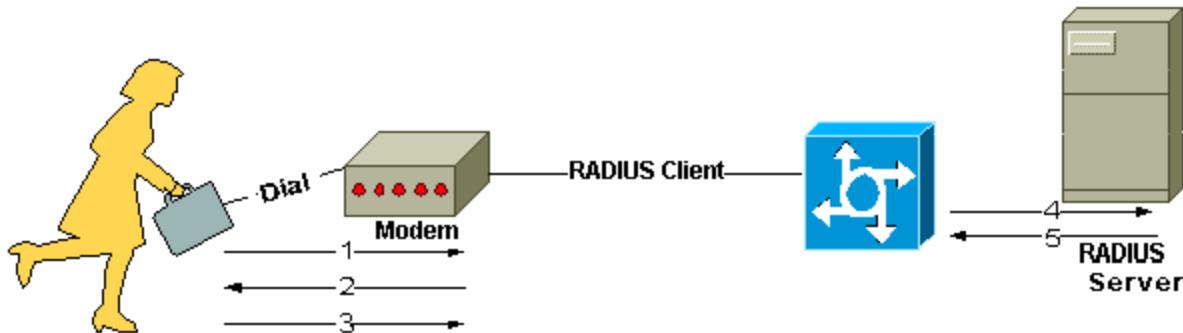


Image 22: This figure shows the interaction between a dial-in user and the RADIUS client and server.

Reference: <https://www.cisco.com/c/en/us/support/docs/security-vpn/remote-authentication-dial-user-service-radius/12433-32.html>

Connection Steps

1. User initiates PPP authentication to the NAS.
2. NAS prompts for username and password (if Password Authentication Protocol [PAP]) or challenge (if Challenge Handshake Authentication Protocol [CHAP]).
3. User replies.
4. RADIUS client sends username and encrypted password to the RADIUS server.
5. RADIUS server responds with Accept, Reject, or Challenge.
6. The RADIUS client acts upon services and services parameters bundled with Accept or Reject.

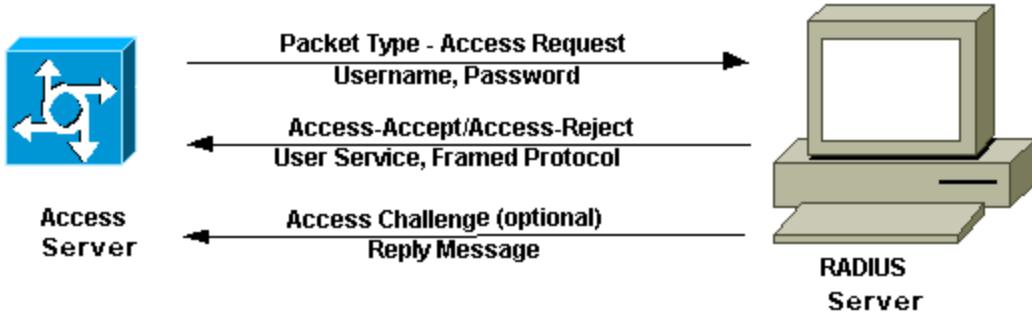


Image 23: This figure shows the interaction between a dial-in user and the RADIUS client and server.

Reference: <https://www.cisco.com/c/en/us/support/docs/security-vpn/remote-authentication-dial-user-service-radius/12433-32.html>

Authentication and Authorization

The RADIUS server can support a variety of methods to authenticate a user. When it is provided with the username and original password given by the user, it can support PPP, PAP or CHAP, UNIX login, and other authentication mechanisms.

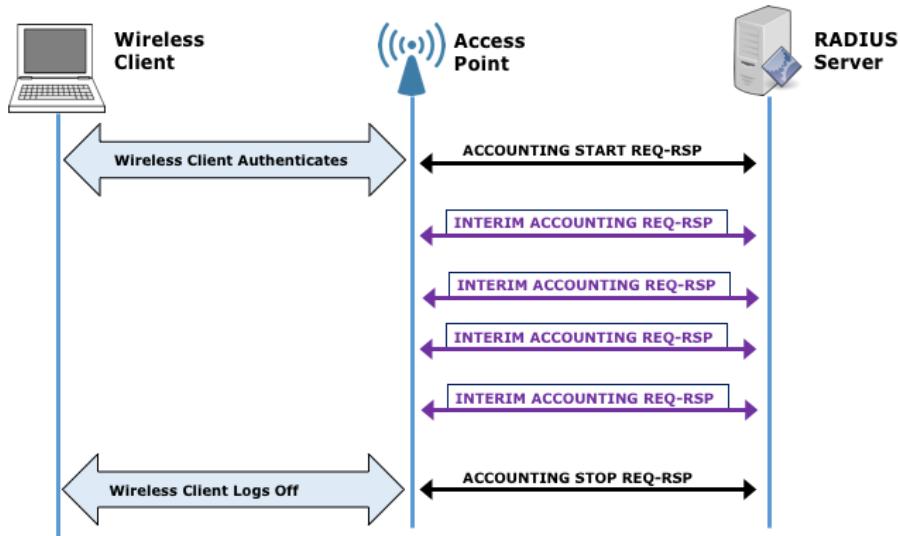


Image 24: RADIUS Handshake at Access Point

Reference: <https://community.cambiumnetworks.com/t5/image/serverpage/image-id/4125i8905BE1DA831CB3B?v=1.0>

Typically, a user login consists of a query (Access-Request) from the NAS to the RADIUS server and a corresponding response (Access-Accept or Access-Reject) from the server. The Access-Request packet contains the username, encrypted password, NAS IP address, and port. The early deployment of RADIUS was done using UDP port number 1645, which conflicts with the "datametrics" service. Because of this conflict, RFC 2865 officially assigned port number

1812 for RADIUS. Most Cisco devices and applications offer support for either set of port numbers. The format of the request also provides information about the type of session that the user wants to initiate. For example, if the query is presented in character mode, the inference is "Service-Type = Exec-User," but if the request is presented in PPP packet mode, the inference is "Service Type = Framed User" and "Framed Type = PPP."

When the RADIUS server receives the Access-Request from the NAS, it searches a database for the username listed. If the username does not exist in the database, either a default profile is loaded or the RADIUS server immediately sends an Access-Reject message. This Access-Reject message can be accompanied by a text message indicating the reason for the refusal.

In RADIUS, authentication and authorization are coupled together. If the username is found and the password is correct, the RADIUS server returns an Access-Accept response, including a list of attribute-value pairs that describe the parameters to be used for this session. Typical parameters include service type (shell or framed), protocol type, IP address to assign the user (static or dynamic), access list to apply, or a static route to install in the NAS routing table. The configuration information in the RADIUS server defines what will be installed on the NAS. The figure below illustrates the RADIUS authentication and authorization sequence.

Accounting

The accounting features of the RADIUS protocol can be used independently of RADIUS authentication or authorization. The RADIUS accounting functions allow data to be sent at the start and end of sessions, indicating the amount of resources (such as time, packets, bytes, and so on) used during the session. An Internet service provider (ISP) might use RADIUS access control and accounting software to meet special security and billing needs. The accounting port for RADIUS for most Cisco devices is 1646, but it can also be 1813 (because of the change in ports as specified in RFC 2139 leavingcisco.com).

Transactions between the client and RADIUS server are authenticated through the use of a shared secret, which is never sent over the network. In addition, user passwords are sent encrypted between the client and RADIUS server to eliminate the possibility that someone snooping on an insecure network could determine a user's password.

TCP/IP Routing

Introduction

Since TCP/IP is the protocol used for the Internet, it is a necessity that the protocol supports the immense size. TCP/IP must support routing capabilities, if not, information sent out to the Internet may never be delivered to its proper destination.

Routers use routing tables which designate where specific IP Address ranges exist. The benefit is to determine which direction the frames must be sent in order to reach their destination. It is also possible to determine which path is best if there are multiple paths to reach the same destination. Multiple destinations allow for redundancy of delivery if a path should fail. For example, look at Figure 1. Let's assume a company is made up of four buildings. Each building site is connected to two other sites through routers. Router A hosts Network 1, Router B hosts Network 2 and so on as shown in the diagram. If the connection between Router A and Router B is somehow broken, Network 1 can still communicate with Network 2 by going through Router D and Router C. Communication goes the other way as well and all four networks are still able to carry on full communications. When one connection fails, the routers can detect the failure and react appropriately to maintain communications.

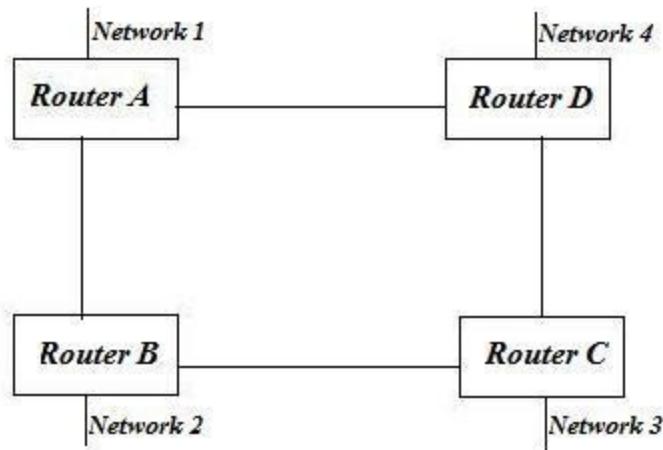


Image 25: TCP Router connections in various networks

Reference: <https://www.linux.org/threads/tcp-ip-protocol-routing-protocols.9287/>

There are five basic routing protocols to manage the routers to maintain communications for all the networks. These five routing protocols are:

-
1. Border Gateway Protocol (BGP)
 2. Routing Information Protocol (RIP)
 3. Open Shortest Path First (OSPF)
 4. Interior Gateway Routing Protocol (IGRP)
 5. Enhanced Interior Gateway Routing Protocol (EIGRP)

Setting up router tables can be done in two ways, either static or dynamic. To statically manage a number of routers can be a chore. Each routing table must be manually entered for each router. If a route is added or removed, then each routing table must be edited on all routers. For larger companies, this prospect can become a very lengthy task.

Routing tables can be dynamically modified by using one of the routing protocols. The table is updated from other routing tables which are created by the router. A router can detect other routers to communicate with to exchange information.

So, before we look at each routing protocol, let us look in more detail about the functions of the routing protocols.

We discussed static and dynamic table creation, so let's look at Single and Multipath. A Routing Protocol which handles single path can only manage a single path in the routing table. Looking back at Figure 1, this means Router B will send data to Network 1 through Router A only. Router B has no path for Network 1 through Router C. On the other hand, with a Multipath Protocol, Router B can get to Network 1 through Router A or through Router C.

The next item is dependant on whether the routers are Flat or Hierarchical. In a Flat system, all routers are equal in importance. In Figure 1, Routers A, B, C and D are all considered equal. When one router needs to send data to a specific network, it sends the data to any other router to reach the destination. This is only true in a Multipath system. With a Hierarchical setup, Routers can be designated as the Backbone as shown in Figure 2. Here, Routers A and D are the Backbone. All communication from Routers B, C, E and F go through Routers A and D. The layout is of course set up differently. In Figure 1, if Router A were connected to the Internet, it could be designated as a Backbone since it should definitely be a more used path.

Another function is the Interior or Exterior routing. If a company has routers within the company, these are usually running an Interior type protocol. The Interior type protocol allows the routers within the company to update one another. Exterior type protocols is used on the Internet to allow sharing between routers which may not be owned by the same company. Within a company, 'Domains' may be set up to keep routers separated from each other. A 'Domain' may be a department, floor, building or any separation needed. Each 'Domain' is then set as Interior

to allow the routers within that single ‘Domain’ to share routing tables with one another. Any router problems of one ‘Domain’ should not impact another unless the routers are using an Exterior type protocol.

The last item to cover in Router Protocol functions is Distance Vector and Link State. With a Distance Vector Protocol, every router sends out all or a large part of its routing table to other routers directly connected to it. With a Link State Protocol, the routing table is sent to all routers on the local network. The problem with a Distance Vector Protocol is that the routers update their tables slowly. When all routers are updated and routes are agreed on by all routers, this event is called convergence. Link State Protocols converge quickly but ultimately use more of the router’s resources.

- BGP – Dynamic, Multipath, Flat, Exterior, Distance Vector
- RIP – Dynamic, Single-path, Flat, Interior, Distance Vector
- OSPF – Dynamic, Multipath, Hierarchical, Interior, Link State
- IGRP – Dynamic, Multipath, Flat, Interior, Distance Vector
- EIGRP – Dynamic, Multipath, Flat, Interior, Distance Vector

Each router or device can be set to use a specific routing protocol that will serve the needs of the network. All routers which must communicate with one another are required to have the same protocol. Any routers with different protocols cannot communicate with one another to share information.

NOTE: Having different protocols cannot allow two devices to communicate. It is as similar as having a system running TCP/IP and another with AppleTalk. The two cannot communicate in any way without some type of intervening ‘translator’. Keep in mind that protocols are basically a set of rules which determine how information is sent over a network. A similar analogy is when two people are speaking two very different languages (we are not talking American English and British English, but English and Chinese or Russian).

Protocols Types

Although there are many types of routing protocols, three major classes are in widespread use on IP networks:

- Interior gateway protocols type 1, link-state routing protocols, such as OSPF and IS-IS
- Interior gateway protocols type 2, distance-vector routing protocols, such as Routing Information Protocol, RIPv2, IGRP.

-
- Exterior gateway protocols are routing protocols used on the Internet for exchanging routing information between Autonomous Systems, such as Border Gateway Protocol (BGP), Path Vector Routing Protocol. Exterior gateway protocols should not be confused with Exterior Gateway Protocol (EGP), an obsolete routing protocol.

There are three types of routes:

Host Route

Defines a gateway that can forward packets to a specific host or gateway on another network.

Network Route

Defines a gateway that can forward packets to any of the hosts on a specific network.

Default Route

Defines a gateway to use when a host or network route to a destination is not otherwise defined.

Routes are defined in the kernel routing table, which can hold up to 32 route definitions. These route definitions include information on networks reachable from the local host, gateways that can be used to reach remote networks, and the hop count (or distance metric) to those networks. When a gateway receives a datagram, it checks the routing tables to find out where next to send the datagram along the path to its destination.

Static & Dynamic Routing

In TCP/IP, routing can be one of two types: static or dynamic. With static routing, you maintain the routing table manually using the route command. Static routing is practical for a single network communicating with one or two other networks. However, as your network begins to communicate with more networks, the number of gateways increases, and so does the amount of time and effort required to maintain the routing table manually.

With dynamic routing, daemons update the routing table automatically. Routing daemons continuously receive information broadcast by other routing daemons, and so continuously update the routing table.

TCP/IP provides two daemons for use in dynamic routing, the routed and gated daemons. The gated daemon supports Routing Information Protocol (RIP), Routing Information Protocol Next Generation (RIPng), Exterior Gateway Protocol (EGP), Border Gateway Protocol (BGP) and

BGP4+, Defense Communications Network Local-Network Protocol (HELLO), Open Shortest Path First (OSPF), Intermediate System to Intermediate System (IS-IS), and Internet Control Message Protocol (ICMP and ICMPv6)/Router Discovery routing protocols simultaneously. In addition, the gated daemon supports the Simple Network Management Protocol (SNMP). The routed daemon only supports Routing Information Protocol.

Routing daemons can operate in one of two modes, passive or active, depending upon the options you use when starting the daemons. In active mode, routing daemons both broadcast routing information periodically about their local network to gateways and hosts, and receive routing information from hosts and gateways. In passive mode, routing daemons receive routing information from hosts and gateways, but do not attempt to keep remote gateways updated (they do not advertise their own routing information).

These two types of routing can be used not only for gateways, but for other hosts on a network as well. Static routing works the same for gateways as for other hosts. Dynamic routing daemons, however, must be run in the passive (quiet) mode when run on a host that is not a gateway.

Gateways

Gateways are a type of router. Routers connect two or more networks and provide the routing function. Some routers, for example, route at the network interface level or at the physical level.

Gateways, however, route at the network level. Gateways receive IP datagrams from other gateways for delivery to hosts on the local network, and route IP datagrams from one network to another. For example, a gateway connecting two Token-Ring networks has two Token-Ring adapter cards, each with its own Token-Ring network interface. To pass on information, the gateway receives datagrams through one network interface and sends them out through the other network interface. Gateways periodically verify their network connections through interface status messages.

Gateways route packets according to the destination network, not according to the destination host. That is, a gateway machine is not required to keep track of every possible host destination for a packet. Instead, a gateway routes packets according to the network of the destination host. The destination network then takes care of sending the packet to the destination host. Thus, a typical gateway machine requires only limited disk storage capacity (if any) and limited main memory capacity.



Image 26: Network Gateway

Reference:

https://www.bosch-mobility-solutions.com/media/global/products-and-services/passenger-cars-and-light-commercial-vehicles/connectivity-solutions/central-gateway-cgw/thumbnail_central-gateway-cgw.jpg

The distance a message must travel from originating host to destination host depends upon the number of gateway hops it must make. A gateway is zero hops from a network to which it is directly attached, one hop from a network that is reachable through one gateway, and so on. Message distance is usually expressed in the number of gateway hops required, or hop counts (also called the metric).

Interior and Exterior Gateways

Interior gateways are gateways that belong to the same autonomous system. They communicate with each other using the Routing Information Protocol (RIP), Routing Information Protocol Next Generation (RIPng), Intermediate System to Intermediate System protocol, Open Shortest Path First protocol (OSPF), or the HELLO Protocol (HELLO). Exterior gateways belong to different autonomous systems. They use the Exterior Gateway Protocol (EGP), the Border Gateway Protocol (BGP), or BGP4+.

For example, consider two autonomous systems. The first is all the networks administered by the Widget Company. The second is all the networks administered by the Gadget Company. The Widget Company has one machine, called apple, which is Widget's gateway to the Internet. The Gadget Company has one machine, called orange, which is Gadget's gateway to the Internet. Both companies have several different networks internal to the companies. The gateways

connecting the internal networks are interior gateways. But apple and orange are exterior gateways.

Each exterior gateway does not communicate with every other exterior gateway. Instead, the exterior gateway acquires a set of neighbors (other exterior gateways) with which it communicates. These neighbors are not defined by geographic proximity, but rather by their established communications with each other. The neighboring gateways, in turn, have other exterior gateway neighbors. In this way, the exterior gateways' routing tables are updated and routing information is propagated among the exterior gateways.

The routing information is sent in a pair, (N,D), where N is a network and D is a distance reflecting the cost of reaching the specified network. Each gateway advertises the networks it can reach and the costs of reaching them. The receiving gateway calculates the shortest paths to other networks and passes this information along to its neighbors. Thus, each exterior gateway is continually receiving routing information, updating its routing table and then passing that information to its exterior neighbors.

Gateway Protocols

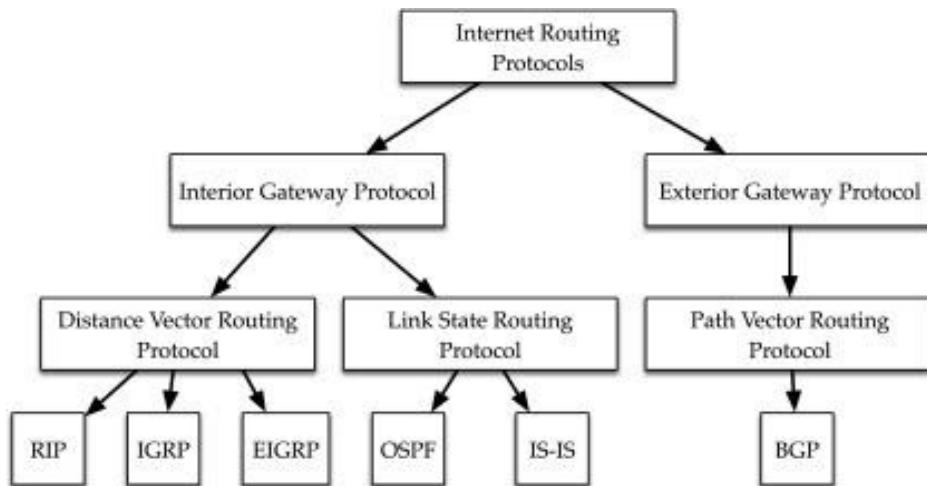


Image 27: Gateway Protocols Hierarchy

Reference: <https://ars.els-cdn.com/content/image/3-s2.0-B9780128007372000041-gr001.jpg>

HELLO Protocol (HELLO)

HELLO is one protocol that the interior gateways use to communicate among themselves. HELLO calculates the shortest path to other networks by determining the path that has the least delay time.

Routing Information Protocol (RIP)

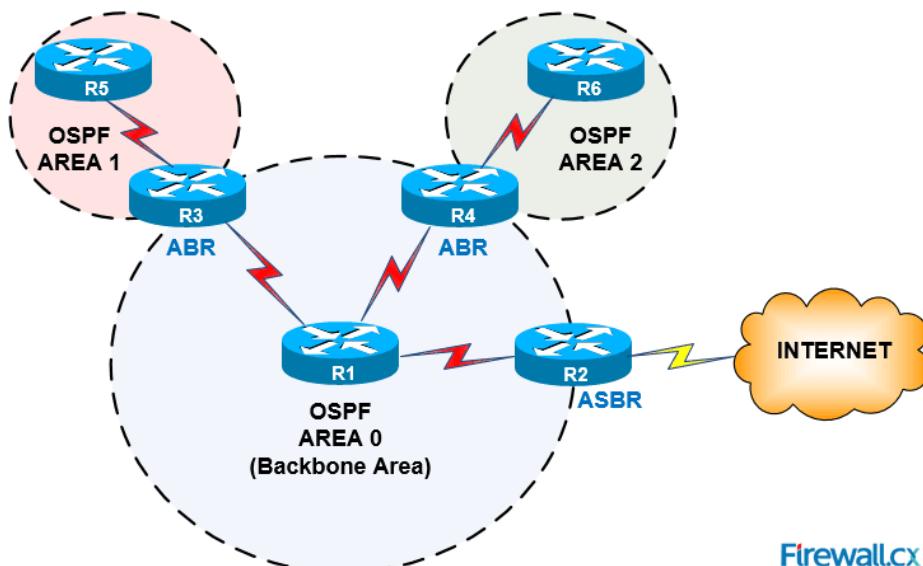
Routing Information Protocol is a protocol that the interior gateways use to communicate among themselves. Like the HELLO Protocol, RIP calculates the shortest path to other networks. Unlike HELLO, RIP estimates distance not by delay time, but by hop counts. Because the gated daemon stores all metrics internally as time delays, it converts RIP hop counts into time delays.

Routing Information Protocol Next Generation

RIPng is the RIP protocol that is enhanced to support IPv6.

Open Shortest Path First (OSPF)

OSPF is a protocol that the interior gateways use to communicate among themselves. It is a link-state protocol that is better suited than RIP for complex networks with many routers. It provides equal cost multipath routing.



Firewall.cx

Image 28: OSPF Protocol Working

Reference: <https://www.firewall.cx/images/stories/ospf-operation-basic-advanced-concepts-ospf-areas-roles-theory-overview1.png>

Exterior Gateway Protocol (EGP)

The exterior gateways can use the Exterior Gateway Protocol to communicate among themselves. The EGP does not calculate the shortest path to other networks. Instead, it merely indicates whether a particular network is reachable or not.

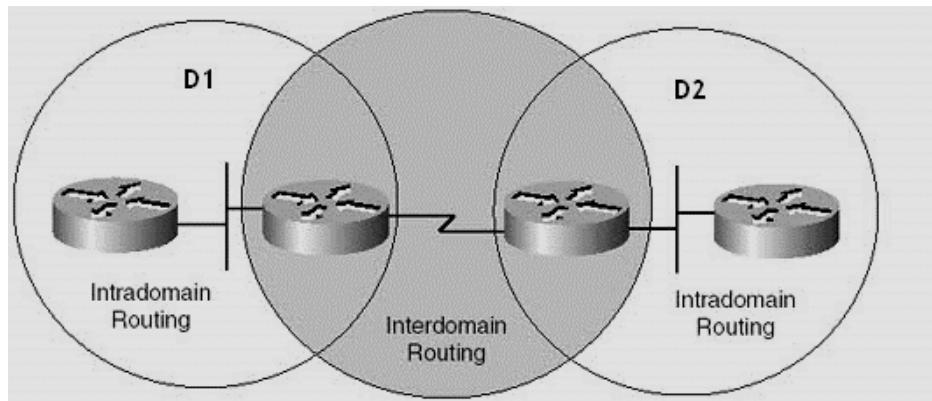


Image 29: Inter-domain routing using EGP

Reference: <https://networkencyclopedia.com/wp-content/uploads/2019/08/exterior-gateway-protocol.jpg>

Border Gateway Protocol (BGP)

The exterior gateways can use this protocol to communicate among themselves. It exchanges reachability information between autonomous systems, but provides more capabilities than EGP. BGP uses path attributes to provide more information about each route as an aid in selecting the best route.

Border Gateway Protocol 4+

BGP4+ is the BGP protocol version 4, which supports IPv6 and has other enhancements over past versions of the protocol.

Intermediate System to Intermediate System (IS-IS)

Interior gateways use IS-IS protocol to communicate among themselves. It is a link-state protocol that can route IP and ISO/CLNP packets and, like OSPF, uses a "shorter path first" algorithm to determine routes.

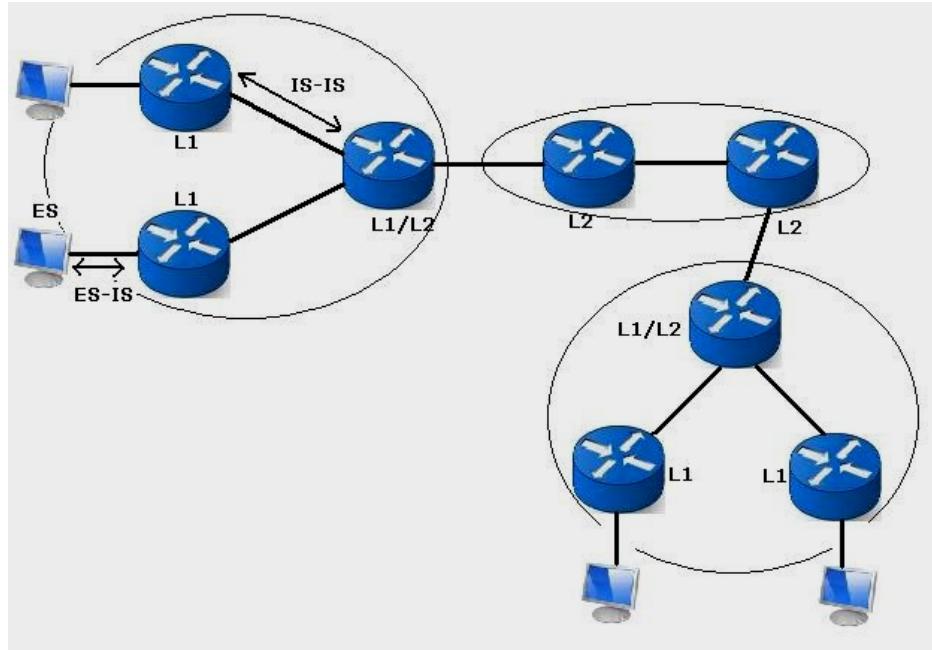


Image 30: IS-IS Protocol Location

Reference: https://sites.google.com/site/amitsciscozone/_/rsrc/1468881651863/home/is-is/is-is-terminology/IS-IS%20Terminology.JPG

Familiarize with internet and E- Commerce sites

In this section, we will read about:

- Introduction to Search Engines,
- Popular Search engines.
- Concept of Favourites Folder.
- What is an Electronic Mail.
- Email Addressing, BCC and CC, Inbox, Outbox,Addressbook,SPAM.
- Introduction to video chatting tools.
- Introduction to InternetSecurity, Threats and attacks, Malicious Software types, Internet security products and their advantages.
- IT Act & Law Introduction to Cyber Security.
- Introduction to Cyber Laws & IT Act.
- Importance of privacy and techniques to manage it.
- Definition of E commerce, Types, scope and benefits of Ecommerce.
- Difference between E commerce and traditional commerce.
- Capabilities requirements and Technology issues for E commerce.
- Types of E commerce web sites.
- Building business on the net.
- Concepts of on line Catalogues, Shopping carts, Checkoutpages.
- Payment and Order Processing, Authorization, Chargeback and other payment methods.
- Security issues and payment gateways.

Introduction to Search Engines

Introduction

Search Engine refers to a huge database of internet resources such as web pages, newsgroups, programs, images etc. It helps to locate information on the World Wide Web.

Users can search for any information by passing a query in form of keywords or phrases. It then searches for relevant information in its database and returns it to the user.



Image 1 - Search Engine

References - https://www.tutorialspoint.com/internet_technologies/search_engines.htm

Search Engine Components

Generally there are three basic components of a search engine as listed below:

1. Web Crawler
2. Database
3. Search Interfaces

Web crawler:

It is also known as spider or bots. It is a software component that traverses the web to gather information.

Database:

All the information on the web is stored in a database. It consists of huge web resources.

Search Interfaces:

This component is an interface between user and the database. It helps the user to search through the database.

Search Engine Working

Web crawler, database and the search interface are the major components of a search engine that actually makes search engines work. Search engines make use of Boolean expression AND, OR, NOT to restrict and widen the results of a search. Following are the steps that are performed by the search engine:

- The search engine looks for the keyword in the index for a predefined database instead of going directly to the web to search for the keyword.
- It then uses software to search for the information in the database. This software component is known as web crawler.

- Once a web crawler finds the pages, the search engine then shows the relevant web pages as a result. These retrieved web pages generally include title of page, size of text portion, first several sentences etc.

These search criteria may vary from one search engine to the other. The retrieved information is ranked according to various factors such as frequency of keywords, relevance of information, links etc.

- Users can click on any of the search results to open it.

Architecture

The search engine architecture comprises of the three basic layers listed below:

- Content collection and refinement.
- Search core
- User and application interfaces

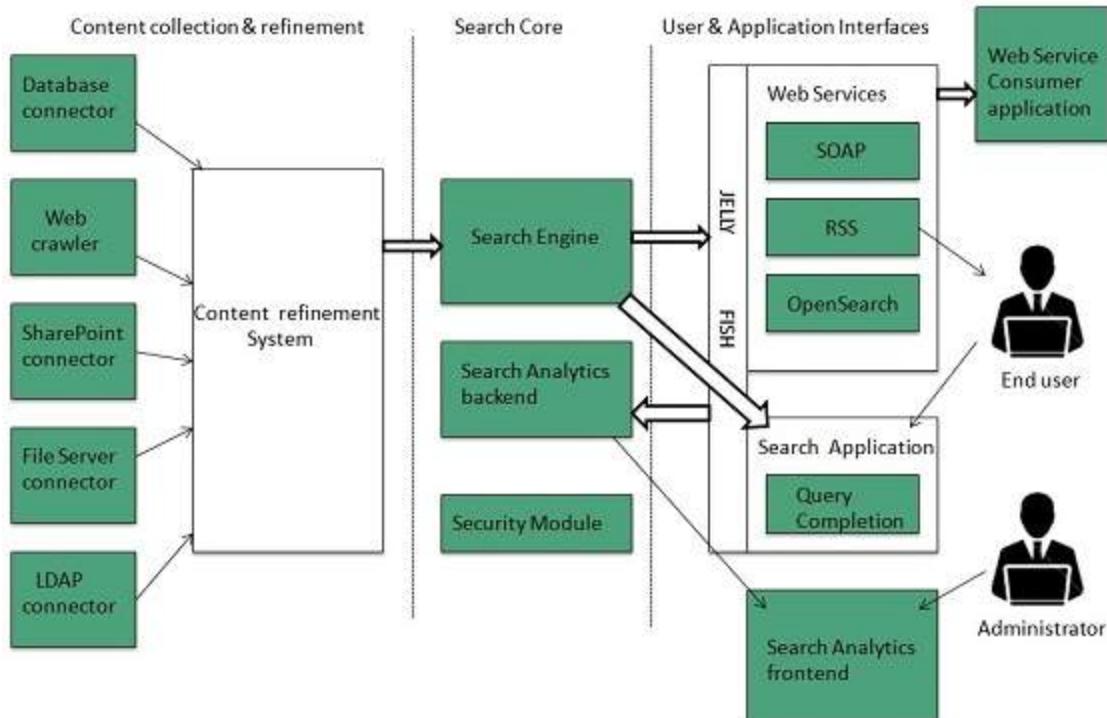


Image 2 - Search Engine Architecture.

References - https://www.tutorialspoint.com/internet_technologies/search_engines.htm

Search Engine Processing

Indexing Process

Indexing process comprises of the following three tasks:

- Text acquisition
- Text transformation
- Index creation

Text acquisition

It identifies and stores documents for indexing.

Text Transformation

It transforms documents into index terms or features.

Index Creation

It takes index terms created by text transformations and create data structures to support fast searching.

Query Process

Query process comprises of the following three tasks:

- User interaction
- Ranking
- Evaluation

User interaction

It supports creation and refinement of user query and displays the results.

Ranking

It uses query and indexes to create a ranked list of documents.

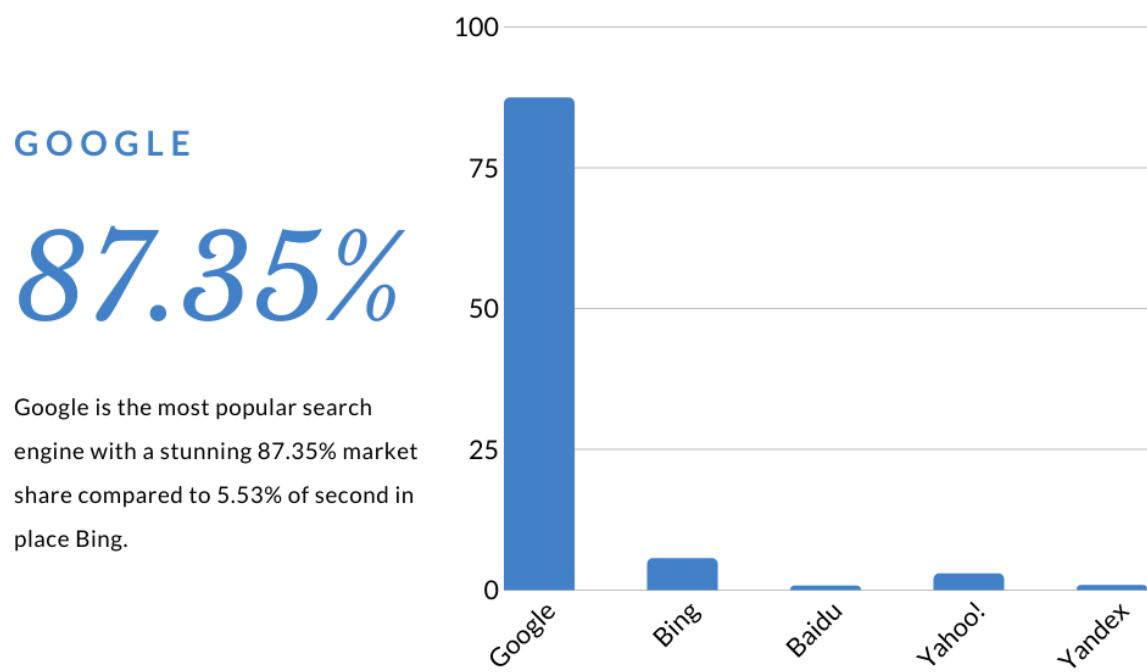
Evaluation

It monitors and measures the effectiveness and efficiency. It is done offline.

Popular Search engines

Recent statistics (updated April 2020), show that Google is the most popular search engine Worldwide with a stunning 87.35% market share.

TOP SEARCH ENGINES



GOOGLE
87.35%

Google is the most popular search engine with a stunning 87.35% market share compared to 5.53% of second in place Bing.

Nevertheless, there are other search engines worth considering, and the top 10 are presented below.

List of Top 10 Most Popular Search Engines In the World (Updated 2020)

- Google
- Bing
- Yahoo
- Baidu
- Yandex.ru
- DuckDuckGo
- Ask.com
- AOL.com
- WolframAlpha
- Internet Archive

Search Engine Market Share

According to statistics from netmarketshare, statista and statcounter, the top 5 search engines worldwide in terms of search engine market share are:

- Google
- Bing
- Yahoo
- Baidu
- Yandex

Search Engine Market Share Worldwide - April 2020

	NETMARKETSHARE	STATISTA	STATCOUNTER
GOOGLE	70.83%	87.35%	91.98%
BING	12.61%	5.53%	2.55%
BAIDU	11.83%	0.7%	1.44%
YAHOO!	2.30%	2.83%	1.66%
YANDEX	1.41%	0.76%	0.45%
DUCKDUCKGO	0.42%	N/A	N/A

RELIABLESOFT.NET

@RELIABLESOFTNET

Image 4 - Search engine market share
Reference- <https://www.reliablesoft.net/top-10-search-engines-in-the-world/#google>

Google



Image 5 - Google

References - <https://www.reliablesoft.net/top-10-search-engines-in-the-world/#google>

No need for further introductions. The search engine giant holds the first place in search with a stunning difference of 76% from second place Bing.

As you can see in the table above, Google is dominating the market in all countries on any device (desktop, mobile, and tablet).

What made Google the most popular and trusted search engine is the quality of its search results. Google is using sophisticated algorithms to present the most accurate results to the users. Google's founders Larry Page and Sergey Brin came up with the idea that websites referenced by other websites are more important than others and thus deserve a higher ranking in the search results.

Over the years the Google ranking algorithm has been enriched with hundreds of other factors (including the help of machine learning) and still remains the most reliable way to find exactly what you are looking for on the Internet.

Bing



Image 6 - Bing

Reference: <https://www.reliablesoft.net/top-10-search-engines-in-the-world/#google>

Bing is Microsoft's attempt to challenge Google in search, but despite their efforts, they still did not manage to convince users that their search engine can be a reliable alternative to Google.

Their search engine market share is constantly below 6%, even though Bing is the default search engine on Windows PCs.

Bing originated from Microsoft's previous search engines (MSN Search, Windows Live Search, Live Search) and according to Alexa rank is the #30 most visited websites on the Internet.

Yahoo



Image 7 - Yahoo

References - <https://www.reliablesoft.net/top-10-search-engines-in-the-world/#google>

Yahoo is one of the most popular email providers and its web search engine holds the third place in search with an average of 2% market share.

From October 2011 to October 2015, Yahoo search was powered exclusively by Bing. In October 2015 Yahoo agreed with Google to provide search-related services and until October 2018, the results of Yahoo were powered both by Google and Bing. As of October 2019, Yahoo! Search is once again provided exclusively by Bing.

Yahoo is also the default search engine for Firefox browsers in the United States (since 2014).

Yahoo's web portal is very popular and ranks as the 11 most visited website on the Internet (According to Alexa).

Baidu



Image 8 - Baidu

References - <https://www.reliablesoft.net/top-10-search-engines-in-the-world/#google>

Baidu was founded in 2000 and it is the most popular search engine in China. Its market share is increasing steadily and according to Wikipedia, Baidu is serving billions of search queries per month. It is currently ranked at position 4, in the Alexa Rankings.

Although Baidu is accessible worldwide, it is only available in the Chinese language.

Yandex.ru



Image 9 - Yandex

References - <https://www.reliablesoft.net/top-10-search-engines-in-the-world/#google>

According to Alexa, Yandex.ru is among the 30 most popular websites on the Internet with a ranking position of 4 in Russian.

Yandex presents itself as a technology company that builds intelligent products and services powered by machine learning. According to Wikipedia, Yandex operates the largest search engine in Russia with about 65% market share in that country.

DuckDuckGo



DuckDuckGo

Image 10 - DuckDuckGo

References - <https://www.reliablesoft.net/top-10-search-engines-in-the-world/#google>

According to DuckDuckGo traffic stats, they are serving on average 47 million searches per day but still their overall market share is constantly below 0.5%.

Unlike what most people believe, DuckDuckGo does not have a search index of their own (like Google and Bing) but they generate their search results using a variety of sources.

In other words, they don't have their own data but they depend on other sources (like Yelp, Bing, Yahoo, StackOverflow) to provide answers to users' questions.

This is a big limitation compared to Google that has a set of algorithms to determine the best results from all the websites available on the Internet.

On the positive side, DuckDuckGo has a clean interface, it does not track users and it is not fully loaded with ads.

Ask.com



Image 11 - Ask

References - <https://www.reliablesoft.net/top-10-search-engines-in-the-world/#google>

Formerly known as Ask Jeeves, Ask.com receives approximately 0.42% of the search share. ASK is based on a question/answer format where most questions are answered by other users or are in the form of polls.

It also has the general search functionality but the results returned lack quality compared to Google or even Bing and Yahoo.

AOL.com



Image 12 - Aol

References - <https://www.reliablesoft.net/top-10-search-engines-in-the-world/#google>

According to *netmarketshare* the old-time famous AOL is still in the top 10 search engines with a market share that is close to 0.05%.

The AOL network includes many popular web sites like engadget.com, techchrunch.com, and huffingtonpost.com. On June 23, 2015, AOL was acquired by Verizon Communications.

Wolframalpha



Image 13 - WolframAlpha

References - <https://www.reliablesoft.net/top-10-search-engines-in-the-world/#google>

WolframAlpha is different from all the other search engines. They market it as a *Computational Knowledge Engine* which can give you facts and data for a number of topics.

It can do all sorts of calculations, for example, if you enter “*mortgage 2000*” as input it will calculate your loan amount, interest paid, etc. based on a number of assumptions.

Internet Archive



Image 14 - Internet Archive

References - <https://www.reliablesoft.net/top-10-search-engines-in-the-world/#google>

archive.org is the internet archive search engine. You can use it to find out how a website looked since 1996. It is a very useful tool if you want to trace the history of a domain and examine how it has changed over the years.

These are the 10 best and most popular search engines on the Internet today.

The list is by no means complete and for sure many more will be created in the future but as far as the first places are concerned, Google and Bing will hold the lead positions for years to come.

Concept of Favourites Folder

While most Web browsers store saved web page locations as bookmarks, Internet Explorer saves them as favorites. Therefore, there is no difference between bookmarks and favourites. Favourites can be saved and used by the user.

For example, when you save a webpage location in Firefox, it gets stored as a bookmark. When you save one in Internet Explorer, it gets stored as a favorite. For this reason, the terms "bookmarks" and "favorites" are often used synonymously.

The following are the images showing bookmarks and favourites.

Favourites folder in Internet Explorer

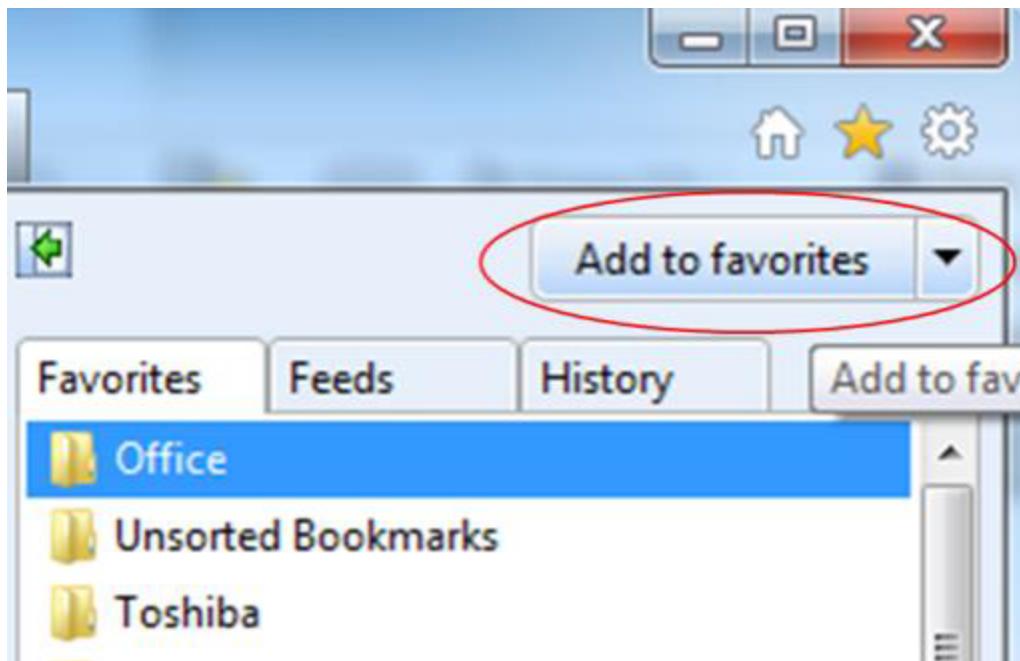


Image 15 - Favorites folder in Internet explorer
References - <https://techterms.com/definition/favorites>

Bookmarks folder in Firefox

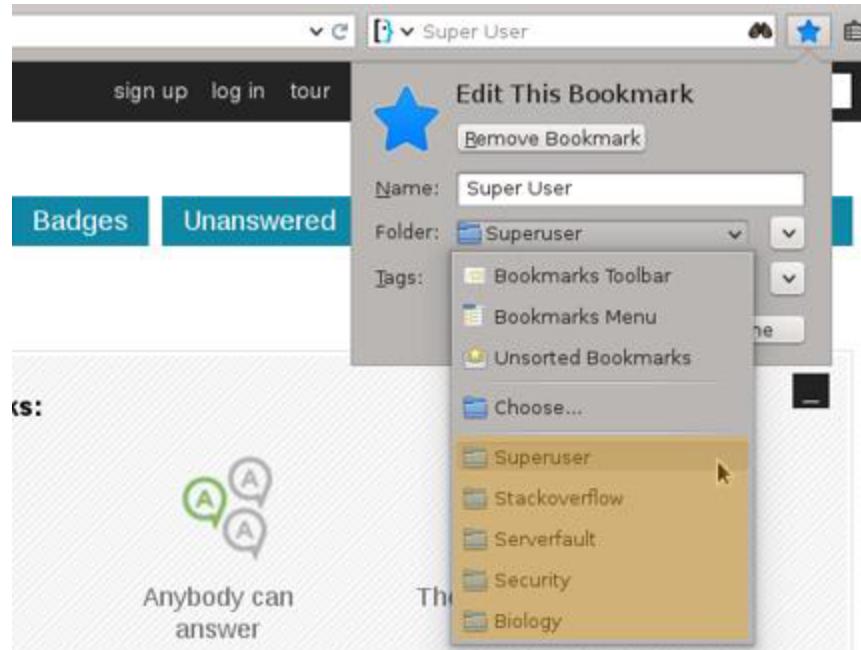


Image 15 - Bookmarks folder in FireFox
References - <https://techterms.com/definition/favorites>

Favorites are also used in other applications besides Web browsers. For example, media players often include a favorites list, which allows users to store references to favorite audio and video files in a single location. Media editing programs often include a favorites panel, which contains links to files that can be imported into projects. Mac OS X has a "Favorites" folder in which users can store aliases to frequently accessed files and folders. Windows 7 also has a "Favorites" folder, which is used to store both favorite webpages and favorite files.

You can often identify a Favorites folder by a star or heart icon. Most applications allow you to simply drag items into the Favorites folder to add them to your favorites. While "favorites" may refer to a wide variety of items, the purpose of a favorites folder is always to provide easy access to frequently used items.

What is an Electronic Mail

Definition

Email is a service which allows us to send the message in electronic mode over the internet. It offers an efficient, inexpensive and real time means of distributing information among people.

Email uses multiple protocols within the TCP/IP suite. For example, SMTP is used to send messages, while the POP or IMAP protocols are used to retrieve messages from a mail server. When you configure an email account, you must define your email address, password, and the mail servers used to send and receive messages. Fortunately, most webmail services configure your account automatically, so you only need to enter your email address and password. However, if you use an email client like Microsoft Outlook or Apple Mail, you may need to manually configure each account. Besides the email address and password, you may also have to enter the incoming and outgoing mail servers and enter the correct port numbers for each one.

The original email standard only supported plain text messages. Eventually, email evolved to support rich text with custom formatting. Today, email supports HTML, which allows emails to be formatted the same way as websites. HTML email messages can include images, links, and CSS layouts. You can also send files or "email attachments" along with messages. Most mail servers allow you to send multiple attachments with each message, but they limit the total size. In the early days of email, attachments were typically limited to one megabyte, but now many mail servers support email attachments that are 20 megabytes in size or more.

Approximately with over 2.6 billion active users and over 4.6 billion email accounts in operation, email is the most important and widely used communications medium on the internet.

History of Email

The first example of email can be found on computers at MIT in a program called "MAILBOX", all the way back in 1965.

Users of MIT computers could leave messages with this program on computers at the university for other users, who would see the messages the next time they logged on to the computer.

The system was quite effective, but only if the people wishing to communicate with each other were regularly using the same computer.

In 1969, the US Department of Defense implemented ARPANET (Advanced Research Projects Agency Network), a network connecting numerous computers across the department for the purpose of communication within the organisation.

On October 29th 1969, the first message was sent from computer to computer on ARPANET. It looked like this:

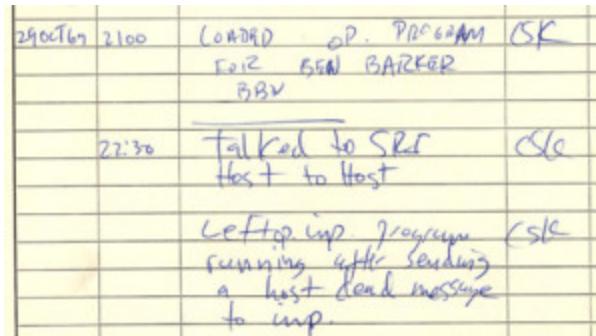


Image 16 - The first message
References - <https://phrasee.co/a-brief-history-of-email/>

It was 1971 when Ray Tomlinson invented and developed electronic mail, as we know it today, by creating ARPANET's networked email system.

The concept of nearly instantaneous communication between machines within an organisation proved to be so beneficial and practical that the concept soon began to spread.

However, with the advent of internal networks the protocols for sending messages became more complex.

When sending a message from one computer to another within a network, how would one indicate where the message was intended to go?

Ray Tomlinson had the answer:



Image 17 - Ray Tomlinson and @ symbol
References - <https://phrasee.co/a-brief-history-of-email/>

Indicating a destination for a message became as simple as addressing it: “username@name of computer”, which is essentially how email has been addressed ever since.

By 1976 75% of all ARPANET traffic was electronic mail. The medium had proved so useful that ideas were beginning to spring up about how one might be able to send an electronic mail message to a user on a computer *outside* of an internal network.

Advantages

Email has proved to be a powerful and reliable medium of communication. Here are the benefits of E-mail:

- Reliable
- Convenience
- Speed
- Inexpensive
- Printable
- Global
- Generality

Reliable

Many of the mail systems notify the sender if the e-mail message was undeliverable.

Convenience

There is no requirement of stationary and stamps. One does not have to go to the post office. But all these things are not required for sending or receiving an email.

Speed

E-mail is very fast. However, the speed also depends upon the underlying network.

Inexpensive

The cost of sending e-mail is very low.

Printable

It is easy to obtain a hardcopy of an email. Also an electronic copy of an e-mail can also be saved for records.

Global

E-mail can be sent and received by a person sitting across the globe.

Generality

It is also possible to send graphics, programs and sounds with an e-mail.

Disadvantages

Apart from several benefits of E-mail, there also exists some disadvantages as discussed below:

- Forgery
- Overload
- Misdirection
- Junk
- No response

Forgery

Email doesn't prevent forgery, that is, someone impersonating the sender, since sender is usually not authenticated in any way.

Overload

Convenience of E-mail may result in a flood of mail.

Misdirection

It is possible that you may send email to an unintended recipient.

Junk

Junk emails are undesirable and inappropriate emails. Junk emails are sometimes referred to as spam.

No Response

It may be frustrating when the recipient does not read the e-mail and respond on a regular basis.

Email Addressing, BCC and CC, Inbox, Outbox, Address book, SPAM

Email Addressing

Each user of email is assigned a unique name for his email account. This name is known as E-mail address. Different users can send and receive messages according to the email address.

E-mail is generally of the form username@domainname. For example, webmaster@tutorialspoint.com is an e-mail address where webmaster is username and tutorialspoint.com is domain name.

- The username and the domain name are separated by @ (at) symbol.
- E-mail addresses are not case sensitive.

-
- Spaces are not allowed in email addresses.

BCC and CC

BCC

BCC stands for Black Carbon Copy. It is used when we do not want one or more of the recipients to know that someone else was copied on the message.

CC

CC stands for Carbon copy. It includes those recipient addresses whom we want to keep informed but not exactly the intended recipient.

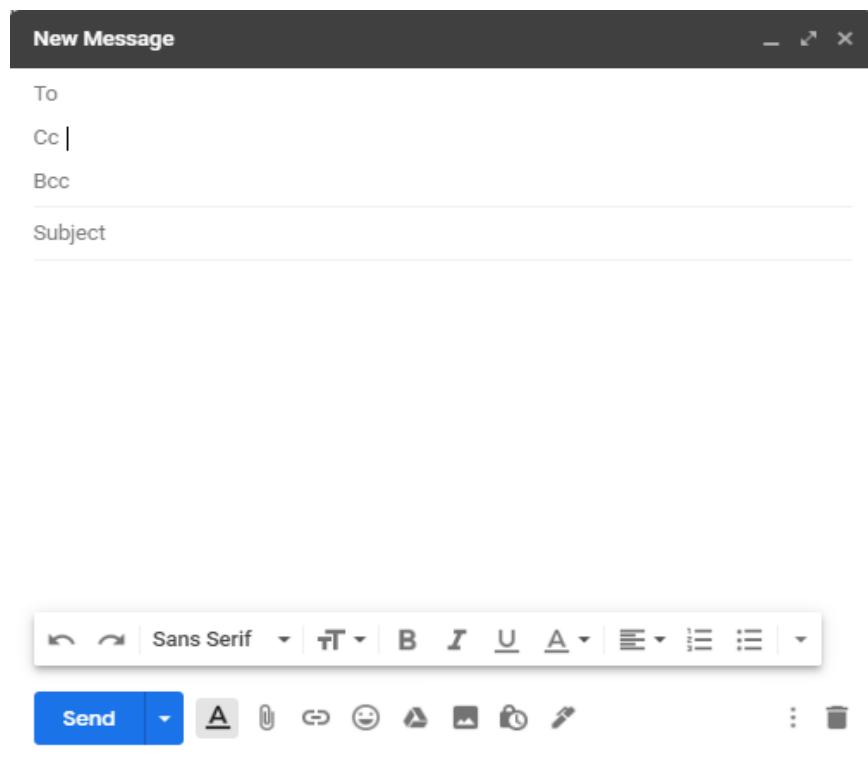


Image 18 - BCC and CC
References - https://www.tutorialspoint.com/internet_technologies/e_mail_overview.htm

Inbox

An inbox is the main folder that your incoming mail gets stored in. Whether you check your mail through a webmail interface or use a program like Outlook or Mac OS X Mail, each downloaded message gets stored in your inbox.

If you check your mail from a POP3 account using an e-mail program, the messages are downloaded to the inbox on your local hard drive. However, if you use an IMAP mail server, your inbox is created on the server and therefore your messages are stored on the server as well.

Because most people receive more mail than they can manage in one folder, it is common to create other folders to store your messages. After reading your messages, you may move them to other folders you have created (such as "Family," "Friends," "Business," etc.) or delete them by moving them to the Trash. However you decide to manage your mail, it is a good idea to keep the number of messages in your inbox from growing too large. Otherwise, you just might have to file for Email Bankruptcy.

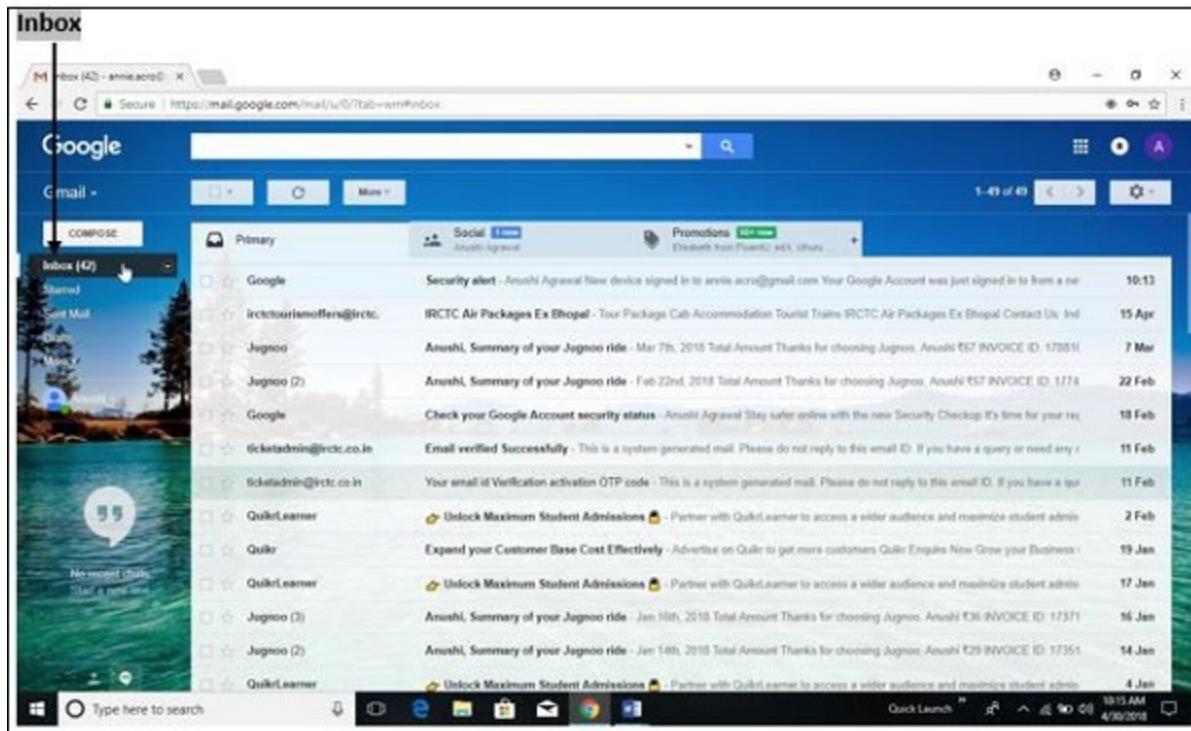


Image 19 - Inbox

References - https://www.tutorialspoint.com/computer_concepts/computer_concepts_mailbox_inbox_outbox.htm

Outbox

An outbox is where outgoing e-mail messages are temporarily stored. While you are composing a message, most mail programs automatically save a draft of your message in the outbox. The message is then stored in the outbox until it is successfully sent to the recipient. Once the message has been sent, most e-mail programs move the message to the "Sent" or "Sent Messages" folder. While the terms "Outbox" and "Sent Messages" are often used synonymously, technically they have different meanings.

Unlike the inbox, which is often overflowing with e-mail, the outbox often does not contain any messages. This is because all the messages that have been sent have already been transferred to the Sent Messages folder. You can think of an email outbox much like the outbox at an office. Mail that is to be delivered is temporarily placed in the outbox until the mailman (or the designated office mail guy) picks up the mail and brings it to the post office. However, the messages in an email outbox are typically delivered immediately (unless a connection to the outgoing SMTP mail server is not available). If only it was as easy to keep your inbox clean...

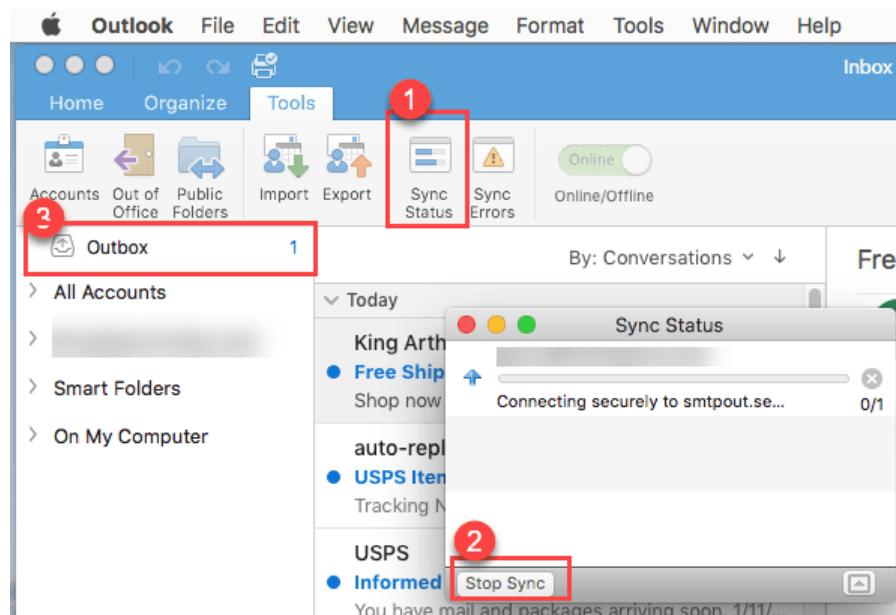


Image 19 - Outbox
References - <https://techterms.com/definition/outbox>

Address book

The Webmail Address Book is a convenient tool for storing the email addresses and other contact information of people you frequently email.

The Address Book screen displays the Name, Email Address, and Phone number of each contact, that you have added to your address book.

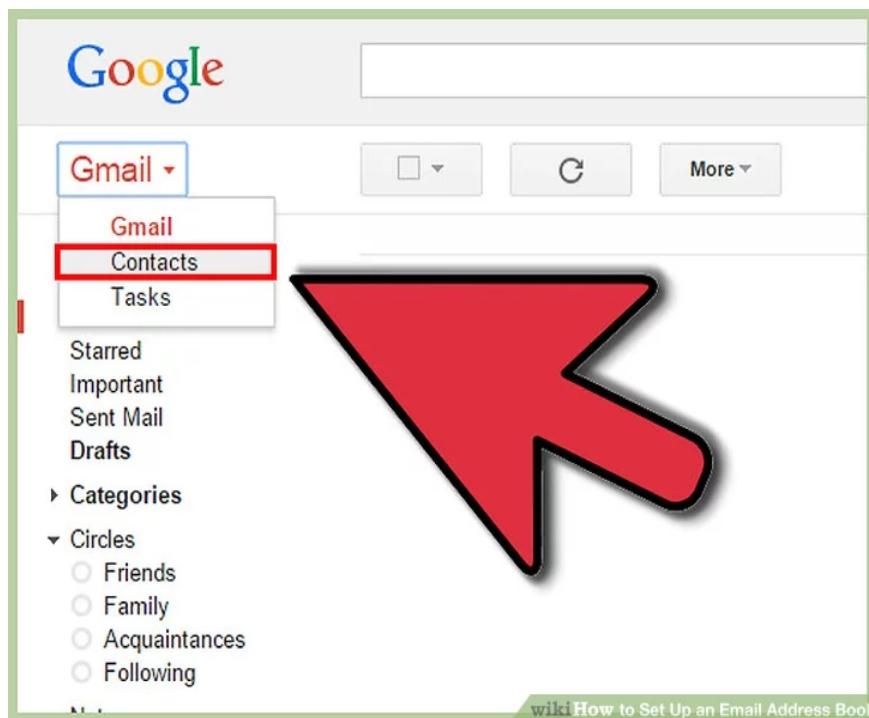


Image 20 - Address book

References - <https://www.wikihow.com/Set-Up-an-Email-Address-Book>

SPAM

Email spam, also referred to as junk email, is unsolicited messages sent in bulk by email (spamming).

The name comes from spam luncheon meat by way of a Monty Python sketch in which Spam is ubiquitous, unavoidable, and repetitive.

Subject	Sender	Date
check this out man...	Nilda Romano	Thursday 14:59:37
Help me!	(Owner MANNING)	Thursday 12:47:59
I Have Athritis pain? Then is help for you.	Crisa	Thursday 03:45:36
is down on her, and	Reagan Stacks	Wednesday 08:02:05
is natural enlargement	diane george	Tuesday 16:10:16
isn't Subject	ellen richard	Monday 10:39:58
isn't Youngest have shocking sexuality other	Karen Slapp	Monday 01:07:32
isn't serious threat	Rankin kim	06.02.2006 16:27
isn't PERSONAL	ann02005	06.02.2006 04:56
isn't We need to render the delight of having the finest	Christina Gatzung	06.02.2006 02:16
isn't Find more savings online	Kenneth draper	06.02.2006 22:30
isn't faster cheaper meds	Linda White	06.02.2006 16:37
isn't Breaking News	Geri H. (Jewished)	06.02.2006 14:49
isn't We have your wanted meds at low prices only	Isaac Hyatt	04.02.2006 08:59
isn't 100% cum enabled... 1679438	Irei Rose	03.02.2006 03:34
isn't Enjoy your wanted meds	Ingrid whalen	03.02.2006 02:28
isn't Confirm Your Washington Mutual Online Banking	Washington Mutual On...	03.02.2006 23:03
isn't our PINNACLE SYSTEM, MACROMAILDA, SYMANTEC, PC GAMES,...	Valerie been	03.02.2006 19:11
isn't Finished	Carola Fuller	03.02.2006 05:47
isn't You can save more thru ordering meds on our site.	mai swick	03.02.2006 01:21
isn't The most insane action	Katrina Jowers	31.01.2006 08:19
isn't You don't have to be fit. Noel	Kristin	28.01.2006 03:22

Image 21 - Spam
References - https://en.wikipedia.org/wiki/Email_spam

Introduction to video chatting tools

Video chat is an online face-to-face, visual communication performed with other Internet users by using a webcam and dedicated software.

The term stemmed from programs that evolved from text-based chats to incorporating two-way video interaction. Video chat is usually used when video-based communication is incorporated into a preexisting service. For instance, when Facebook incorporated Skype video-based communication in 2011, it said that it was adding a video chat.

Video chat is also known as video conferencing and video calling.

Skype popularized video chats. It lets any two people around the globe place a video call to each other. For this, all they need is a computer, the Skype application, and a good Internet connection.

Targeting the enterprise world in 2010, Skype introduced a feature that allows five people to take part in a video call. Video chat uses technology to conduct live video as well as audio interaction among users at different locations. Generally, video chats are performed by means of computers, smartphones, or tablets.



Image 22 - Skype Video call

References - <https://www.skype.com/en/features/group-video-chat/>

Although video chat mainly refers to point-to-point interaction, as with the case of FaceTime and Skype, it can also be used for multipoint (one-to-many) interactions; one typical example is Google Hangouts.

Even though video chat is frequently used interchangeably with videoconferencing, there is significant overlap between the two terms. Generally videoconferencing means multi-point, video-audio interaction set up in a business environment, with three or more participants taking part.

Skype and Apple's FaceTime video calling are two of the most popular video chat services presently available. Facebook Video Chat, ooVoo, etc., are some other examples of popular video chats. Apart from this, many websites offer video chat rooms, where users can meet face-to-face and interact.

Introduction to Internet Security, Threats and attacks, Malicious Software types, Internet security products and their advantages

Introduction to Internet Security

Internet security refers to securing communication over the internet. It includes specific security protocols such as:

- Internet Security Protocol (IPSec)
- Secure Socket Layer (SSL)

Internet Security Protocol (IPSec)

It consists of a set of protocols designed by the Internet Engineering Task Force (IETF). It provides security at the network level and helps to create authenticated and confidential packets for the IP layer.

Secure Socket Layer (SSL)

It is a security protocol developed by Netscape Communications Corporation.). It provides security at the transport layer. It addresses the following security issues:

- Privacy
- Integrity
- Authentication

Threats and attacks

Threats

Internet security threats impact the network, data security and other internet connected systems. Cyber criminals have evolved several techniques to threat privacy and integrity of bank accounts, businesses, and organizations.

Following are some of the internet security threats:

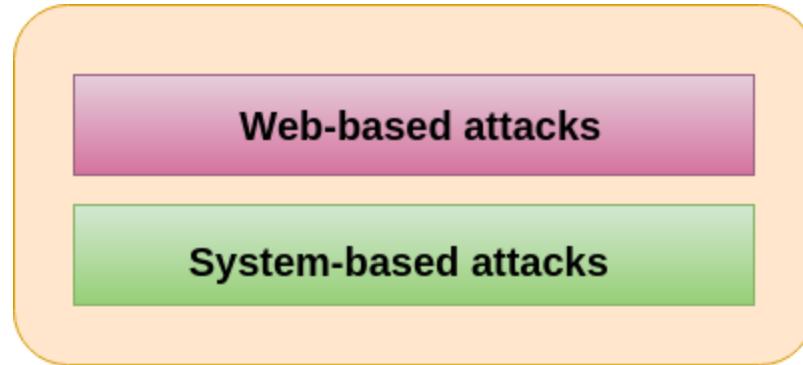
- Mobile worms
- Malware
- PC and Mobile ransomware
- Large scale attacks like Stuxnet that attempt to destroy infrastructure.
- Hacking as a Service
- Spam
- Phishing

Attacks

A cyber-attack is an exploitation of computer systems and networks. It uses malicious code to alter computer code, logic or data and lead to cybercrimes, such as information and identity theft.

We are living in a digital era. Nowadays, most people use computers and the internet. Due to the dependency on digital things, the illegal computer activity is growing and changing like any type of crime.

Cyber-attacks can be classified into the following categories:



Classification of Cyber attacks

Image 23 - Classification of cyber attacks

References - <https://www.javatpoint.com/types-of-cyber-attacks>

Web-based attacks

These are the attacks which occur on a website or web applications. Some of the important web-based attacks are as follows-

1. Injection attacks

It is the attack in which some data will be injected into a web application to manipulate the application and fetch the required information.

Example- SQL Injection, code Injection, log Injection, XML Injection etc.

2. DNS Spoofing

DNS Spoofing is a type of computer security hacking. Whereby a data is introduced into a DNS resolver's cache causing the name server to return an incorrect IP address, diverting traffic to the attacker's computer or any other computer. The DNS spoofing attacks can go on for a long period of time without being detected and can cause serious security issues.

3. Session Hijacking

It is a security attack on a user session over a protected network. Web applications create cookies to store the state and user sessions. By stealing the cookies, an attacker can have access to all of the user data.

4. Phishing

Phishing is a type of attack which attempts to steal sensitive information like user login credentials and credit card number. It occurs when an attacker is masquerading as a trustworthy entity in electronic communication.

5. Brute force

It is a type of attack which uses a trial and error method. This attack generates a large number of guesses and validates them to obtain actual data like user password and personal identification number. This attack may be used by criminals to crack encrypted data, or by security analysts to test an organization's network security.

6. Denial of Service

It is an attack which meant to make a server or network resource unavailable to the users. It accomplishes this by flooding the target with traffic or sending it information that triggers a crash. It uses the single system and single internet connection to attack a server. It can be classified into the following-

Volume-based attacks- Its goal is to saturate the bandwidth of the attacked site, and is measured in bits per second.

Protocol attacks- It consumes actual server resources, and is measured in a packet.

Application layer attacks- Its goal is to crash the web server and is measured in request per second.

7. Dictionary attacks

This type of attack stored the list of a commonly used password and validated them to get the original password.

8. URL Interpretation

It is a type of attack where we can change the certain parts of a URL, and one can make a web server to deliver web pages for which he is not authorized to browse.

9. File Inclusion attacks

It is a type of attack that allows an attacker to access unauthorized or essential files which are available on the web server or to execute malicious files on the web server by making use of the include functionality.

10. Man in the middle attacks

It is a type of attack that allows an attacker to intercept the connection between client and server and acts as a bridge between them. Due to this, an attacker will be able to read, insert and modify the data in the intercepted connection.

System-based attacks

These are the attacks which are intended to compromise a computer or a computer network. Some of the important system-based attacks are as follows-

1. Virus

It is a type of malicious software program that spread throughout the computer files without the knowledge of a user. It is a self-replicating malicious computer program that replicates by inserting copies of itself into other computer programs when executed. It can also execute instructions that cause harm to the system.

2. Worm

It is a type of malware whose primary function is to replicate itself to spread to uninfected computers. It works the same as the computer virus. Worms often originate from email attachments that appear to be from trusted senders.

3. Trojan horse

It is a malicious program that makes unexpected changes to computer setting and unusual activity, even when the computer should be idle. It misleads the user of its true intent. It appears to be a normal application but when opened/executed some malicious code will run in the background.

4. Backdoors

It is a method that bypasses the normal authentication process. A developer may create a backdoor so that an application or operating system can be accessed for troubleshooting or other purposes.

5. Bots

A bot (short for "robot") is an automated process that interacts with other network services. Some bots programs run automatically, while others only execute commands when they

receive specific input. Common examples of bots program are the crawler, chatroom bots, and malicious bots.

Malicious Software types

Malicious Software

Malicious software, commonly known as malware, is any software that brings harm to a computer system.

Malware is a program designed to gain access to computer systems, normally for the benefit of some third party, without the user's permission. Malware includes computer viruses, worms, Trojan horses, ransomware, spyware and other malicious programs.

Types of Malware:

Viruses

A Virus is a malicious executable code attached to another executable file. The virus spreads when an infected file is passed from system to system. Viruses can be harmless or they can modify or delete data. Opening a file can trigger a virus. Once a program virus is active, it will infect other programs on the computer.

Worms

Worms replicate themselves on the system, attaching themselves to different files and looking for pathways between computers, such as computer networks that share common file storage areas. Worms usually slow down networks. A virus needs a host program to run but worms can run by themselves. After a worm infects a host, it is able to spread very quickly over the network.

Spyware

Its purpose is to steal private information from a computer system for a third party. Spyware collects information and sends it to the hacker.

Trojan horse

A Trojan horse is malware that carries out malicious operations under the appearance of a desired operation such as playing an online game. A Trojan horse varies from a virus because the Trojan binds itself to non-executable files, such as image files, audio files.

Logic Bombs

A logic bomb is a malicious program that uses a trigger to activate the malicious code. The logic bomb remains non-functioning until that trigger event happens. Once triggered, a logic bomb implements a malicious code that causes harm to a computer. Cybersecurity specialists recently discovered logic bombs that attack and destroy the hardware components in a workstation or server including the cooling fans, hard drives, and power supplies. The logic bomb overdrives these devices until they overheat or fail.

Ransomware

Ransomware grasps a computer system or the data it contains until the victim makes a payment. Ransomware encrypts data in the computer with a key which is unknown to the user. The user has to pay a ransom (price) to the criminals to retrieve data. Once the amount is paid the victim can resume using his/her system.

Backdoors

A backdoor bypasses the usual authentication used to access a system. The purpose of the backdoor is to grant the cyber criminals future access to the system even if the organization fixes the original vulnerability used to attack the system.

Rootkits

A rootkit modifies the OS to make a backdoor. Attackers then use the backdoor to access the computer distantly. Most rootkits take advantage of software vulnerabilities to modify system files.

Keyloggers

Keylogger records everything the user types on his/her computer system to obtain passwords and other sensitive information and send them to the source of the keylogging program.

Internet security products and their advantages

Internet security products

1. Bitdefender Total Security
2. Kaspersky Total Security.
3. Norton 360 Deluxe.
4. Trend Micro Maximum Security.

-
- 5. Avast Ultimate
 - 6. Webroot Internet Security Plus.
 - 7. ESET Smart Security Premium.
 - 8. McAfee Total Protection Multi-Device.
 - 9. Bullguard Premium Protection.
 - 10. Panda Dome Advanced.

Advantages

Protection from viruses and their transmission.

An antivirus software mainly performs a prophylactic function. It detects any potential virus and then works to remove it. Keep in mind that all this is mostly done before the virus gets to harm the system. So, this means that most of the viruses are countered way before they get to do any harm to your systems. An antivirus may combat many viruses in a single day without your knowledge. Avast and Norton are some of the most popular antivirus software that is available in the market these days.

If a virus has attacked your system, you can potentially transfer that to your friends, family, and networks. So, if you want to protect your computer system as well as computers of your acquaintances, then consider getting an antivirus.

Block spam and ads.

If you do a quick survey on how viruses enter the computer systems of its victims, you will be amazed by the proportion of viruses that use pop up ads and websites to make their way into your computers. Pop-up ads and spam websites are one the most used gateways by the viruses to infect your computer and then damage your files.

Software such as Bullguard Internet Security works against these malicious virus-containing ads and websites by blocking their direct access to your computer network.

Defense against hackers and data thieves.

Hackers usually use a malware or virus program to access their victim's computer. They install malware into the computer without the knowledge of the victim. Hackers do so by sending malicious emails to the victims. Then the hacker can easily hack into their desired files and programs.

After that, they can use the victim's data as per their will; they can delete or damage it and steal it to demand ransom later on. Anti Malware such as Malwarebytes either put an anti

hacking lock, or they perform regular scans to detect the presence of any hacker or hacking based programs in the computer network. So, antivirus software provides full-proof protection against hackers.

Ensures protection from removable devices.

Think of the times you have transferred data to and from your computer by using removable devices such as USBs. Countless, right?

You might have suffered from slowing down your computer or a computer crash after connecting a friend's USB. Ever wondered why that happened? That is so because the USB or removable device served as a transmission device for a virus. So, should you stop using removable devices because you never know which USB might contain a virus?

No! Just get antivirus software that will scan all the removable devices for any potential viruses to make sure that no virus is transferred.

Protects your data and files.

Antivirus software keeps an eye on all the files that enter your system. All those files are put under a scan to check for any peculiarity or maliciousness. Viruses can easily be transmitted to your network via infected files, and these, in turn, can potentially harm your data and files. You may even suffer the complete loss of your precious data at the hands of such viruses. A solution from Avira software makes sure that your data and files are adequately protected.

Supercharge your PC

Think of two computers side by side.

One is suffering from the consequences of a virus attack, such as slow processing speed and frequent crashes. The other is antivirus protected. Which amongst the both will have a better speed?

The one with antivirus for sure. It is so because that computer has no problems because antivirus has stopped the virus before it can cause any real harm. Some antivirus may even delete and remove useless files from unknown sources to free up disk space, increasing the speed of the PC.

Firewall protection from spyware and phishing attacks.

A firewall, in general, monitors incoming and outgoing traffic from your computer network. When coupled with antivirus, firewall protection double checks every file or piece of data that you send or transfer from your computer via the internet to another network.

The same goes for the files and data that you receive from an external network. You can

unintentionally open a downright malicious website or email and then fall prey to a phishing attack. A phishing attack occurs when the attackers specifically aim for your login credentials, credit card information, or any other personal information/data. Such an attack can result in substantial financial loss or personal leaks. Two-Way firewall protection from antivirus software such as Avast blocks and removes any such emails or files that can harm you in any such way.

Limit the access of websites to enhance web protection.

Accessing unauthorized websites can expose your computer system to several cyber threats, including spyware, hackers, ransomware, etc. These threats can potentially risk your data and files. An antivirus software limits your web access to restrict your activities on unauthorized networks. This is done to make sure that you only access the websites that are safe and harmless for your computer system.

Keeping an eye on kids.

The biggest headache for parents in these advanced times is that their children can openly access anything using the internet, whether it be good or bad.

A parent can't always keep an eye on what their children are doing on the computer. And they can't school their kids about the good and bad web all the time because kids get annoyed easily. Antivirus software can be the solution for such worrisome parents. It can provide a monitoring tool via which you can keep tabs on the activities of your children in a safe yet efficient manner. Antivirus software provides you with proper logs of your kid's activities. ESET is one of the most prominent antivirus that offers parental control.

Protects your password.

You protect your valuable data and accounts with a password, and then you think that your data and accounts are protected.

But what if someone steals your passwords using a virus?

The password thief can, later on, blackmail you for ransom or use your password to access sensitive information. On top of using antivirus, you can also think of using a password manager for better security.

Cost-effective.

Most of the antivirus software is quite cost-effective. The monthly or yearly packages that antivirus manufacturing companies offer are inexpensive. If you consider the variety of services that come with the premium package of the antivirus, you will surely think that the cost they are offering is quite less.

In addition to that, if you are low on budget and don't want to spend money on buying the premium version of antiviruses, then you can get free antivirus.

IT Act & Law Introduction to Cyber Security

IT Act & Law

The **Information Technology Act, 2000** (also known as **ITA-2000**, or the **IT Act**) is an Act of the Indian Parliament (No 21 of 2000) notified on 17 October 2000. It is the primary law in India dealing with cybercrime and electronic commerce.

The bill was passed in the budget session of 2000 and signed by President K.R Narayanan on 9 May 2000. The bill was finalised by group of officials headed by then Minister of Information Technology Pramod Mahajan.

Offences

List of offences and the corresponding penalties:

Section	Offence	Description	Penalty

65	Tampering with computer source documents	If a person knowingly or intentionally conceals, destroys or alters or intentionally or knowingly causes another to conceal, destroy or alter any computer source code used for a computer, computer programme, computer system or computer network, when the computer source code is required to be kept or maintained by law for the time being in force.	Imprisonment up to three years, or/and with fine up to ₹200,000
66	Hacking with computer system	If a person with the intent to cause or knowing that he is likely to cause wrongful loss or damage to the public or any person destroys or deletes or alters any information residing in a computer resource or diminishes its value or utility or affects it injuriously by any means, commits hack.	Imprisonment up to three years, or/and with fine up to ₹500,000
66B	Receiving stolen computer or communication device	A person receives or retains a computer resource or communication device which is known to be stolen or the person has reason to believe is stolen.	Imprisonment up to three years, or/and with fine up to ₹100,000
66C	Using password of another person	A person fraudulently uses the password, digital signature or other unique identification of another person.	Imprisonment up to three years, or/and with fine up to ₹100,000
66D	Cheating using computer resource	If a person cheats someone using a computer resource or communication.	Imprisonment up to three years, or/and with fine up to ₹100,000

66E	Publishing private images of others	If a person captures, transmits or publishes images of a person's private parts without his/her consent or knowledge.	Imprisonment up to three years, or/and with fine up to ₹200,000
66F	Acts of cyberterrorism	If a person denies access to an authorised personnel to a computer resource, accesses a protected system or introduces contaminants into a system, with the intention of threatening the unity, integrity, sovereignty or security of India, then he commits cyberterrorism.	Imprisonment up to life.
67	Publishing information which is obscene in electronic form.	If a person publishes or transmits or causes to be published in the electronic form, any material which is lascivious or appeals to the prurient interest or if its effect is such as to tend to deprave and corrupt persons who are likely, having regard to all relevant circumstances, to read, see or hear the matter contained or embodied in it.	Imprisonment up to five years, or/and with fine up to ₹1,000,000
67A	Publishing images containing sexual acts	If a person publishes or transmits images containing a sexual explicit act or conduct.	Imprisonment up to seven years, or/and with fine up to ₹1,000,000

67B	Publishing child porn or predating children online	If a person captures, publishes or transmits images of a child in a sexually explicit act or conduct. If a person induces a child into a sexual act. A child is defined as anyone under 18.	Imprisonment up to five years, or/and with fine up to ₹1,000,000 on first conviction. Imprisonment up to seven years, or/and with fine up to ₹1,000,000 on second conviction.
67C	Failure to maintain records	Persons deemed as intermediary (such as an ISP) must maintain required records for stipulated time. Failure is an offence.	Imprisonment up to three years, or/and with fine.
68	Failure/refusal to comply with orders	The Controller may, by order, direct a Certifying Authority or any employee of such Authority to take such measures or cease carrying on such activities as specified in the order if those are necessary to ensure compliance with the provisions of this Act, rules or any regulations made thereunder. Any person who fails to comply with any such order shall be guilty of an offence.	Imprisonment up to 2 years, or/and with fine up to ₹100,000

69	Failure/refusal to decrypt data	If the Controller is satisfied that it is necessary or expedient so to do in the interest of the sovereignty or integrity of India, the security of the State, friendly relations with foreign States or public order or for preventing incitement to the commission of any cognizable offence, for reasons to be recorded in writing, by order, direct any agency of the Government to intercept any information transmitted through any computer resource. The subscriber or any person in charge of the computer resource shall, when called upon by any agency which has been directed, must extend all facilities and technical assistance to decrypt the information. The subscriber or any person who fails to assist the agency referred is deemed to have committed a crime.	Imprisonment up to seven years and possible fine.
70	Securing access or attempting to secure access to a protected system	The appropriate Government may, by notification in the Official Gazette, declare that any computer, computer system or computer network to be a protected system. The appropriate Government may, by order in writing, authorise the persons who are authorised to access protected systems. If a person who secures access or attempts to secure access to a protected system, then he is committing an offence.	Imprisonment up to ten years, or/and with fine.

71	Misrepresentation	If anyone makes any misrepresentation to, or suppresses any material fact from, the Controller or the Certifying Authority for obtaining any license or Digital Signature Certificate.	Imprisonment up to 2 years, or/and with fine up to ₹100,000
----	-------------------	--	---

Introduction to Cyber Security

Cyber security is a potential activity by which information and other communication systems are protected from and/or defended against the unauthorized use or modification or exploitation or even theft.

Likewise, cyber security is a well-designed technique to protect computers, networks, different programs, personal data, etc., from unauthorized access.

Introduction to Cyber Laws & IT Act.

Information Technology Act

In 1996, the United Nations Commission on International Trade Law (UNCITRAL) adopted the model law on electronic commerce (e-commerce) to bring uniformity in the law in different countries.

Further, the General Assembly of the United Nations recommended that all countries must consider this model law before making changes to their own laws. India became the 12th country to enable cyber law after it passed the Information Technology Act, 2000.

While the first draft was created by the Ministry of Commerce, Government of India as the ECommerce Act, 1998, it was redrafted as the ‘Information Technology Bill, 1999’, and passed in May 2000.

Objectives of the Act

The Information Technology Act, 2000 provides legal recognition to the transaction done via electronic exchange of data and other electronic means of communication or electronic commerce transactions.

This also involves the use of alternatives to a paper-based method of communication and information storage to facilitate the electronic filing of documents with the Government agencies.

Further, this act amended the Indian Penal Code 1860, the Indian Evidence Act 1872, the Bankers' Books Evidence Act 1891, and the Reserve Bank of India Act 1934. The objectives of the Act are as follows:

- Grant legal recognition to all transactions done via electronic exchange of data or other electronic means of communication or e-commerce, in place of the earlier paper-based method of communication.
- Give legal recognition to digital signatures for the authentication of any information or matters requiring legal authentication
- Facilitate the electronic filing of documents with Government agencies and also departments
- Facilitate the electronic storage of data
- Give legal sanction and also facilitate the electronic transfer of funds between banks and financial institutions
- Grant legal recognition to bankers under the Evidence Act, 1891 and the Reserve Bank of India Act, 1934, for keeping the books of accounts in electronic form.

Features of the Information Technology Act, 2000

- All electronic contracts made through secure electronic channels are legally valid.
- Legal recognition for digital signatures.
- Security measures for electronic records and also digital signatures are in place
- A procedure for the appointment of adjudicating officers for holding inquiries under the Act is finalized
- Provision for establishing a Cyber Regulatory Appellant Tribunal under the Act. Further, this tribunal will handle all appeals made against the order of the Controller or Adjudicating Officer.

-
- An appeal against the order of the Cyber Appellant Tribunal is possible only in the High Court
 - Digital Signatures will use an asymmetric cryptosystem and also a hash function
 - Provision for the appointment of the Controller of Certifying Authorities (CCA) to license and regulate the working of Certifying Authorities. The Controller to act as a repository of all digital signatures.
 - The Act applies to offences or contraventions committed outside India
 - Senior police officers and other officers can enter any public place and search and arrest without warrant
 - Provisions for the constitution of a Cyber Regulations Advisory Committee to advise the Central Government and Controller.

Cyber Security

Cyber security is the practice of defending computers, servers, mobile devices, electronic systems, networks, and data from malicious attacks. It's also known as information technology security or electronic information security. The term applies in a variety of contexts, from business to mobile computing, and can be divided into a few common categories.

- Network security is the practice of securing a computer network from intruders, whether targeted attackers or opportunistic malware.
- Application security focuses on keeping software and devices free of threats. A compromised application could provide access to the data its designed to protect. Successful security begins in the design stage, well before a program or device is deployed.
- Information security protects the integrity and privacy of data, both in storage and in transit.
- Operational security includes the processes and decisions for handling and protecting data assets. The permissions users have when accessing a network and the procedures that determine how and where data may be stored or shared all fall under this umbrella.
- Disaster recovery and business continuity define how an organization responds to a cyber-security incident or any other event that causes the loss of operations or data. Disaster recovery policies dictate how the organization restores its operations and information to return to the same operating capacity as before the event. Business continuity is the plan the organization falls back on while trying to operate without certain resources.
- End-user education addresses the most unpredictable cyber-security factor: people. Anyone can accidentally introduce a virus to an otherwise secure system

by failing to follow good security practices. Teaching users to delete suspicious email attachments, not plug in unidentified USB drives, and various other important lessons is vital for the security of any organization.

Importance of privacy and techniques to manage it

List of techniques on Importance of Privacy

1. Limit on Power

Privacy is a limit on government power, as well as the power of private sector companies. The more someone knows about us, the more power they can have over us. Personal data is used to make very important decisions in our lives. Personal data can be used to affect our reputations; and it can be used to influence our decisions and shape our behavior. It can be used as a tool to exercise control over us. And in the wrong hands, personal data can be used to cause us great harm.

2. Respect for Individuals

Privacy is about respecting individuals. If a person has a reasonable desire to keep something private, it is disrespectful to ignore that person's wishes without a compelling reason to do so. Of course, the desire for privacy can conflict with important values, so privacy may not always win out in the balance. Sometimes people's desires for privacy are just brushed aside because of a view that the harm in doing so is trivial. Even if this doesn't cause major injury, it demonstrates a lack of respect for that person. In a sense it is saying: "I care about my interests, but I don't care about yours."

3. Reputation Management

Privacy enables people to manage their reputations. How we are judged by others affects our opportunities, friendships, and overall well-being. Although we can't have complete control over

our reputations, we must have some ability to protect our reputations from being unfairly harmed. Protecting reputation depends on protecting against not only falsehoods but also certain truths. Knowing private details about people's lives doesn't necessarily lead to more accurate judgment about people. People judge badly, they judge in haste, they judge out of context, they judge without hearing the whole story, and they judge with hypocrisy. Privacy helps people protect themselves from these troublesome judgments.

4. Maintaining Appropriate Social Boundaries

People establish boundaries from others in society. These boundaries are both physical and informational. We need places of solitude to retreat to, places where we are free of the gaze of others in order to relax and feel at ease. We also establish informational boundaries, and we have an elaborate set of these boundaries for the many different relationships we have. Privacy helps people manage these boundaries. Breaches of these boundaries can create awkward social situations and damage our relationships. Privacy is also helpful to reduce the social friction we encounter in life. Most people don't want everybody to know everything about them – hence the phrase "none of your business." And sometimes we don't want to know everything about other people — hence the phrase "too much information."

5. Trust

In relationships, whether personal, professional, governmental, or commercial, we depend upon trusting the other party. Breaches of confidentiality are breaches of that trust. In professional relationships such as our relationships with doctors and lawyers, this trust is key to maintaining candor in the relationship. Likewise, we trust other people we interact with as well as the companies we do business with. When trust is breached in one relationship, that could make us more reluctant to trust in other relationships.

6. Control Over One's Life

Personal data is essential to so many decisions made about us, from whether we get a loan, a license or a job to our personal and professional reputations. Personal data is used to determine whether we are investigated by the government, or searched at the airport, or denied the ability to fly. Indeed, personal data affects nearly everything, including what messages and content we see on the Internet. Without having knowledge of what data is being used, how it is being used, the ability to correct and amend it, we are virtually helpless in today's world. Moreover, we are helpless without the ability to have a say in how our data is used or the ability to object and have legitimate grievances be heard when data uses can harm us. One of the hallmarks of freedom is having autonomy and control over our lives, and we can't have that if so many important decisions about us are being made in secret without our awareness or participation.

7. Freedom of Thought and Speech

Privacy is key to freedom of thought. A watchful eye over everything we read or watch can chill us from exploring ideas outside the mainstream. Privacy is also key to protecting speaking unpopular messages. And privacy doesn't just protect fringe activities. We may want to criticize people we know to others yet not share that criticism with the world. A person might want to explore ideas that their family or friends or colleagues dislike.

8. Freedom of Social and Political Activities

Privacy helps protect our ability to associate with other people and engage in political activity. A key component of freedom of political association is the ability to do so with privacy if one chooses. We protect privacy at the ballot because of the concern that failing to do so would chill people's voting their true conscience. Privacy of the associations and activities that lead up to going to the voting booth matters as well, because this is how we form and discuss our political beliefs. The watchful eye can disrupt and unduly influence these activities.

9. Ability to Change and Have Second Chances

Many people are not static; they change and grow throughout their lives. There is a great value in the ability to have a second chance, to be able to move beyond a mistake, to be able to reinvent oneself. Privacy nurtures this ability. It allows people to grow and mature without being shackled with all the foolish things they might have done in the past. Certainly, not all misdeeds should be shielded, but some should be, because we want to encourage and facilitate growth and improvement.

10. Not Having to Explain or Justify Oneself

An important reason why privacy matters is not having to explain or justify oneself. We may do a lot of things which, if judged from afar by others lacking complete knowledge or understanding, may seem odd or embarrassing or worse. It can be a heavy burden if we constantly have to wonder how everything we do will be perceived by others and have to be ready to explain.

E commerce

Definition of E-Commerce

Ecommerce, also known as electronic commerce or internet commerce, refers to the buying and selling of goods or services using the internet, and the transfer of money and data to execute these transactions. Ecommerce is often used to refer to the sale of physical products online, but it can also describe any kind of commercial transaction that is facilitated through the internet.

Whereas e-business refers to all aspects of operating an online business, ecommerce refers specifically to the transaction of goods and services.

The history of ecommerce begins with the first ever online sale: on August 11, 1994 a man sold a CD by the band Sting to his friend through his website NetMarket, an American retail platform. This is the first example of a consumer purchasing a product from a business through the World Wide Web—or “ecommerce” as we commonly know it today.

Since then, ecommerce has evolved to make products easier to discover and purchase through online retailers and marketplaces. Independent freelancers, small businesses, and large corporations have all benefited from ecommerce, which enables them to sell their goods and services at a scale that was not possible with traditional offline retail.

Examples of Ecommerce

Ecommerce can take on a variety of forms involving different transactional relationships between businesses and consumers, as well as different objects being exchanged as part of these transactions.

-
- 1. Retail:** The sale of a product by a business directly to a customer without any intermediary.
 - 2. Wholesale:** The sale of products in bulk, often to a retailer that then sells them directly to consumers.
 - 3. Dropshipping:** The sale of a product, which is manufactured and shipped to the consumer by a third party.
 - 4. Crowdfunding:** The collection of money from consumers in advance of a product being available in order to raise the startup capital necessary to bring it to market.
 - 5. Subscription:** The automatic recurring purchase of a product or service on a regular basis until the subscriber chooses to cancel.
 - 6. Physical products:** Any tangible good that requires inventory to be replenished and orders to be physically shipped to customers as sales are made.
 - 7. Digital products:** Downloadable digital goods, templates, and courses, or media that must be purchased for consumption or licensed for use.
 - 8. Services:** A skill or set of skills provided in exchange for compensation. The service provider's time can be purchased for a fee.

Types of E-Commerce

Business-to-Business (B2B)

As the title suggests, a B2B transaction is where one business is selling to another business. These transactions often involve customizing an order on a rolling basis. B2B transactions can include bulk pricing, larger quantity orders, or specialty products that an average consumer would never need on a day to day basis. B2B transactions create powerful and long-lasting relationships between each side when orchestrated correctly. Typical products that are involved in B2B transactions include office supplies, gasoline and oil, medical equipment, airplanes, ships, and military equipment. These items are large in physical size or quantities needed which would be overwhelming for an average consumer to purchase on their own.

B2B transactions occur in many forms and take place globally. A popular derivative of the B2B model occurs between business and an administration of some sort (B2A). B2A transactions occur between companies and bodies of public administration such as the government. Also, the B2A model is sometimes referred to as B2G (business-to-government). As the world becomes increasingly reliant upon the internet, so have governments. Many processes are becoming optimized through digitalization and many administrations and governing bodies have implemented third-party technologies to assist in the process. In order to win business, marketing may occur targeted at decision makers within the government or authoritative body. These efforts would fall under the B2A model. Other B2A transactions include social security, employment contracting, financial measuring, and other online payment options.

Business-to-Consumer (B2C)

The most traditional transaction type from a consumer's point of view is the B2C model. This model mimics a purchase that is made in-store at a brick and mortar location but occurs entirely online. Businesses sell goods straight to consumers through their website. The internet serves as a marketplace in itself and the eCommerce store serves as the portal between businesses and consumer shopping online. Online stores are able to list multiple products and SKUs which gives customers many options to pick and choose from during their buying experience. This allows for more options for a customer to research and find the perfect fit. Clothing, electronics, and outdoor recreational equipment are just a few of the products that effectively sold online in the B2C. The B2C transaction is not limited to products, but services are quite often distributed in

this fashion as well. Businesses may offer services like financial advising, tutoring, subscription memberships, and others to grow their presence online.

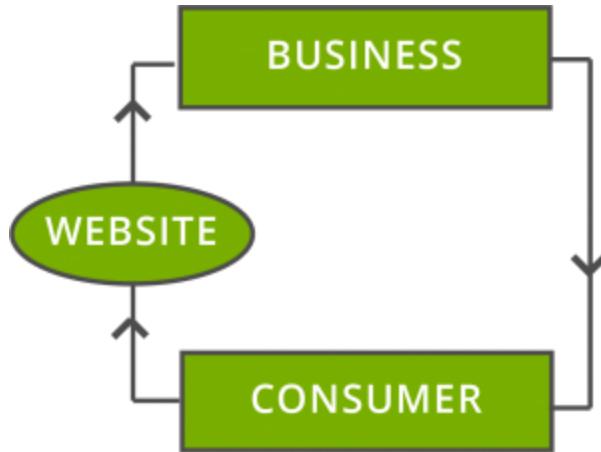


Image 1:B2C-Business to Consumer.
Reference: <https://trellis.co/wp-content/uploads/2019/01/ebook-asset-4-300x224.png>

Consumer-to-Consumer (C2C)

With the rise of eCommerce, much innovation has taken place in many forms. The internet itself is a powerful marketplace in and of itself. Other marketplaces have come to fruition to offer consumers shopping options and pathways to obtain desired products. Platforms like eBay, Craigslist, Grailed, and even parts of Amazon allow consumers to sell to consumers. This bridge allows men and women to sell goods without setting up a personalized store. This results in fast and easy individual transactions allowing for niche items, used goods, and individual listings to be sold online.

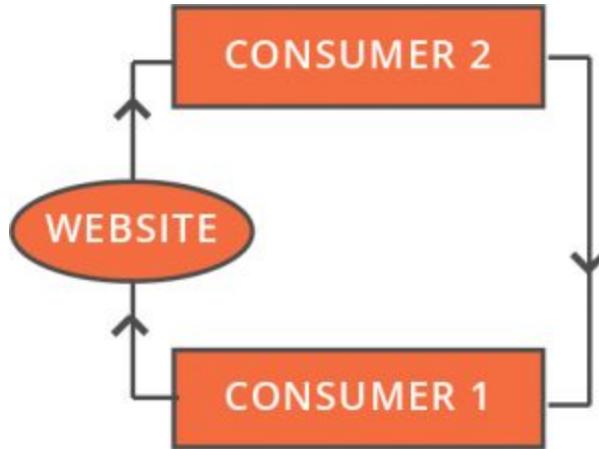


Image 2:C2C- Consumer to Consumer.

Reference:<https://trellis.co/wp-content/uploads/2019/01/ebook-asset-3@2x-100-300x223.jpg>

In the C2C model, the platform itself does not own or sell any products. rather, it serves as the bridge between the consumer selling and consumer buying. They act as a third party to oversee and authorize the transaction to ensure it goes smoothly. Popular platforms became successful due to a high amount of users and traffic while offering a solution to get rid of goods with little cost and overhead. Selling an item on these sites can be as simple as opening the app or site, creating an account, listing the item, and waiting for another consumer to purchase. No additional marketing is needed which leaves more profit in the lister's pockets.

This type of model is becoming increasingly prominent with the inception of different marketplaces looking to gain a share of the market opportunity. C2C opportunities increase consumer buying power by eliminating many steps of the buying process.

Consumer-to-Business (C2B)

On the other side of the spectrum, the C2B model allows businesses to receive value from consumers when it is traditionally the other way around. Consumers are able to provide a service to businesses to augment their existing business through a reverse auction system. Consumers can act like contractors bidding on certain projects which allows them to bring value back to the business. This name your price option allows businesses to reach different parts of a community

that may have been previously untapped. For example, popular bloggers can charge a fee to businesses wishing to have their item or idea listed in order to receive exposure. The consumer is setting the price and has leverage over the transaction since they are providing the service.

Scope of E-Commerce

The scope of eCommerce Business in India is undoubtedly going to increase year after year. A recent report by the Internet and Mobile Association of India shows that a fast-paced growth of around 50% is to be expected in the coming five years.

The primary attribute of this growth is undoubtedly the rise of 3G/4G mobile internet users and a large number of smartphone users because the same mobile commerce is expected to change how business transactions happen in India.

The scope of eCommerce business is turning out to be more famous day-after-day according to the market demand. And this requirement is generating innovations worldwide focused on delivery time, ease of transactions and several features served by eCommerce businesses, for example, drone delivery or artificial intelligence.

This article is focused on scope, future, application and various critical factors for the growth of the eCommerce business scope in India.

Key factors for the growth of eCommerce Business Scope in India:

- Reduction in the cost of broadband internet facilities to ensure more people come online.
- Encouraging more domain registrations and letting e-commerce websites maintain them at cheaper rates (at least till they make substantial profits).
- Encouraging innovative schemes such as the COD (Cash on Delivery) in a country where credit card use is not prominent shows how we have eased into this particular niche. A lot of the major e-commerce websites are based in India and the consistency, and reliability of these sites have shown the people how hassle-free, shopping and availing services are.
- Bringing internet facilities to the rural areas in India as it remains a largely untapped resource and the possibilities are endless for a major boom in the e-commerce industry, as India's Internet penetration is 0.5% of the population. If these e-commerce businesses can reach these regions, their net value can only increase from the current values.

-
- E-commerce can also spread to newer disciplines such as health services in these remote areas in India and help in offering health solutions to people who do not have the luxury of hospitals in their vicinity. This will certainly help once the rural areas are provided with internet facilities and will be a potential business prospect shortly.

Benefits of E-Commerce:

1) Low costs

An important benefit of ecommerce is that starting a website is anytime less expensive than a physical outlet. You do not have to furnish your outlet, no need to pay rent and hire several employees to work in it. The cost of marketing and promotional strategies is also low.

One of its main Benefits Of Ecommerce is the absence of middlemen that reduces the cost price to a greater degree. As a direct link is established between buyer and seller the portal is able to create an effective supply chain.

Moreover, the online portal is computerized and automated saving a crucial amount of money. Yes, you will need to shed a small amount if you are interested in a customized website but you already have a customer base that is a compulsive online shopper.

2) Flexibility and speed

An individual or a company can easily open an online store within a few days whereas a physical outlet needs space, commercial leasing procedure as well as ample construction and decoration time for its opening. It is possible to change displays and product offerings within minutes in an e-commerce site whereas you need proper planning and ample time and manpower to do so in physical stores.

In terms of flexibility and speed e-commerce sites beat retail outlets by a long margin and this feature is considered one of the main benefits of ecommerce. The entrepreneur is able to handle all the operations from the comfort of his home without renting office space.

He just needs an internet connection and a device to handle all the transactions effectively.

3) Speeds up the buying process

Earlier a customer had to pre-plan his shopping trip even if he wanted to buy a specific thing. It would mean rearranging his schedule and going to the outlet to make the purchase. One of the main benefits of ecommerce is that it speeds up the buying process.

A visit to the outlet which is very far from your home and will waste nearly two to three hours of your time is no longer necessary. Just sit back in the comfort of your home or even your office, search for the product and make a purchase.

Moreover, the online stores are open 24*7 hence you can use it as per your convenience. E-commerce helps the customer to buy a particular product easily without wasting his time by giving him access to a wide range of choices. You are also saving traveling time as the product is being delivered at the destination of your choice.

4) A comprehensive description of products

Customers are on the look-out for a comprehensive description of the products they want to buy and it is one of the major benefits of ecommerce. An e-commerce portal offers its customers a product catalog that has data sheets featuring all the useful information about its products and services.

The characteristics, its usefulness, and specifications are listed in a detailed manner. Even the colors of some of the products like mobile phones are mentioned so that you can make a choice according to personal preference. The customers can read about the ingredients of edible products and collect background information which is not possible in retail outlets or physical stores.

Armed with the knowledge at their fingertips it becomes easier for the consumers to buy products they desire. The online websites also include the ratings and the customer feedback which tell the customers about the likeability of a product in the market.

The portal offers warranty information along with other relevant terms and conditions pertinent to the product that later prove useful for a consumer.

5) Keep an eye on buyer's habit

Information about the likes and dislikes of a customer is very important and an online store is able to record and analyze the frequency with which the buyer has purchased items or viewed other items in his portal. This is not possible in physical stores. One of the benefits of ecommerce is that the traders can keep a direct and indirect eye on the behavior of its customers and customize its offerings to suit their individuality.

The past browsing history is utilized to tempt consumers with related or same products. The online portals keep a ready stock of the items that are being pursued and purchased to satisfy its customers.

6) Easy availability through search engines

There is a huge difference between the physical and online stores if you are looking for benefits of ecommerce. The first thrives because of its branding and the second on the large traffic from search engines.

With the advent of the internet, the consumer has become more street smart and advanced. He realizes the importance of online shopping and has been using search engines to find products and services at his convenience. A physical store is in most cases limited to a single area whereas the search engines allow the worldwide audience in its portal.

In order to utilize the concept of search engines remember more often than not the consumers appear only on the first page hence make it as visible as you can so that they are tempted to visit the next pages. This enables the portal to get maximum customers, revenues and coverage for its business.

7) Technology at its best

An important benefit of ecommerce is that it is using technology for its own advantage. As the systems are computerized it becomes easy to maintain its working order without the tension of getting tired or becoming slow by the end of the day.

Technology helps to make viable comparisons of the products and their rates and specifications which is not possible in physical outlets hence the use of technology make online portals accurate, effective and efficient in their dealings with their customers.

8) Reduce the cost of managing inventory

If you are looking for one of the benefits of ecommerce then it can easily save time and reduce its inventory cost when compared with physical stores. The online portal offers features and facilities that automate several responsibilities.

It introduces a web-based system through which the website can automate and manage inventory by itself and thus reduce the operating cost.

9) Encourages impulse to buy

An online site has information on the buying habits of its customers. It knows that there are several products that the consumer is interested in buying but is unable to do so. One of the benefits of e-commerce portal is that it can keep its eyes on these potential targets and offer several schemes and discounts that prompt the customers to make an impulse buy.

The website makes its products more attractive with color options and images so that the customer is tempted to make a purchase.

10) Retarget your customers

If you are looking for benefits of e-commerce then one of the main ones is its ability to retarget its customers. The portal has information about the individuals that visit its site and has made purchases.

It uses this information through several techniques to maintain the interest of the consumers like sharing a coupon and sending emails for cross-selling purposes. It is possible when a customer visits a certain page in a particular time period.

11) Availability of reviews

Online sites encourage reviews from its customers to know about customer satisfaction and what problems they are facing while using the products and services. One of the benefits of e-commerce is the availability of these reviews on its online sites so that potential customers can read about it and understand whether the product is suitable for their particular needs.

Earlier we did not have such a facility for physical stores and had to rely on our acquaintances who had used the products to get viable information about it. Now a customer can sit in the privacy of his home and can read the reviews and make a decision according to his needs without asking friends and relatives about the product.

12) Quick and affordable marketing

Physical stores spend crore of rupees on its promotional policies and hence their product cost, as well as the ultimate cost, is higher. If compared online websites use online marketing to promote its products and it is way cheaper than the offline marketing costs of retail outlets.

If you are looking for benefits of ecommerce then quick and affordable marketing options are one of them. A portal has the option of tying up with other portals, launching marketing videos, taking help of social networking sites, DIY infographics, and digital marketing to promote the products at a very low cost.

13) No geographical limitations

A physical store is located in a particular place and in most cases the people who live nearby come and visit it. One of the benefits of e-commerce stores is that it is not bound by geographical boundaries.

A customer can access the portal from anywhere in the world with the help of an internet connection and a device to operate it. The platform is available 24*7 to all its customers in any part of the world and offers information where it is able to send the products and within how many days.

You can also keep track of your product and know about its availability in any store.

14) Offers eco-friendly services

An important benefit of an e-commerce portal is that it reduces paper waste when compared with physical stores. When we visit a store product purchase involves receiving coupons, receipts, and bills whereas online stores are computerized and do not offer paper receipts.

15) Bigger profit margin

The actual cost of setting up an e-commerce store and running it is minimal compared to the physical outlets. Moreover, you also save on marketing, labor, and overhead costs. This gives the portal an additional advantage as it is able to sell its products at a reasonable rate.

When compared these rates are anytime lower than the rates levied by the physical outlets. The online stores are open day and night and are able to sell products at a greater pace.

Customers are flocking to online sites to purchase the required items instead of the retail outlets. Higher sales figures and reduced costs have helped the portals to gain a bigger profit margin and have turned out to be an important benefit of an e-commerce site.

16) Scalability

In a physical outlet if there is a surge of customers it becomes very difficult to handle them as you have a limited staff. An important benefit of e-commerce is the scalability factor. You can sell a product to one or thousands of customers at the same time without any problem.

There is no limit to the number of clients you can handle on your website as it is fully computerized and is able to tackle all the operations successfully without any problem.

17) Effective customer service

If you are looking for benefits of e-commerce then effective customer service is one of them. You can call it any time of the day and night as it is open 24*7. Online platforms have paid special attention to the customer services as they want to help the customers in their queries.

The websites offer regular updates on their sites in relation to product information or related services. Quick delivery of the products is another point in its favor and the portals also offer information to the customer so that they can keep a track of their products online.

The popularity of e-commerce platforms is on the rise as more and more people are leaning towards this mode of the electronic transaction as well as online retail. It has taken nearly a decade to see the explosive growth in the online sector.

Although at the onset people were skeptical of its success the facts and figures have proved everyone wrong as it is considered one of the most successful ventures of the current decade.

Difference between E commerce and traditional commerce.

1. Cost effective

E-commerce is very cost effective when compared to traditional commerce. In traditional commerce, cost has to be incurred for the role of middlemen to sell the company's product. The cost incurred on middlemen is eliminated in e-commerce as there is a direct link between the business and the customer. The total overhead cost required to run e-business is comparatively less, compared to traditional business.

For example, in running an e-business, only a head office is required. Whereas in traditional method, a head office with several branches are required to cater to the needs of customers situated in different places. The cost incurred on labour, maintenance, office rent can be substituted by hosting a website in e-business method.

2. Time saving

It takes a lot of time to complete a transaction in traditional commerce. E-commerce saves a lot of valuable time for both the consumers and business. A product can be ordered and the transaction can be completed in a few minutes through the internet.

3. Convenience

E-commerce provides convenience to both the customers and the business. Customers can browse through a whole directory of catalogues, compare prices between products and choose a desired product anytime and anywhere in the world without any necessity to move away from their home or work place.

E-commerce provides better connectivity for its prospective and potential customers as the organization's website can be accessed virtually from anywhere, any time through the internet. It is not necessary to move away from their workplace or home to locate and purchase a desired product.

4. Geographical accessibility

In traditional commerce, it may be easy to expand the size of the market from regional to national level. Business organizations have to incur a lot of expenses on investment to enter the international market. In e-commerce it is easy to expand the size of the market from regional to international level.

By hosting a website, by placing advertisements on the internet and satisfying certain legal norms, a business can penetrate into the global market. It is quite easy to attract customers from global markets at a marginal cost.

5. Introduction of new products

In traditional commerce, it takes a lot of time and money to introduce a new product and analyze the response of the customers. Initially, cost has to be incurred to carry out pilot surveys to understand the taste of the customers.

In e-commerce, it is easy to introduce a product on the website and get the immediate feedback of the customers. Based on the response, the products can be redefined and modified for a successful launch.

6. Profit

E-commerce helps to increase the sales of the organization. It helps the organization to enjoy greater profits by increasing sales, cutting cost and streamlining operating processes.

The cost incurred on the middlemen, overhead, inventory and limited sales pulls down the profit of the organization in traditional commerce.

7. Physical inspection

E-commerce does not allow physical inspection of goods. In purchasing goods in e-commerce, customers have to rely on electronic images whereas in traditional commerce, it is possible to physically inspect the goods before the purchase.

8. Time accessibility

Business is open only for a limited time in traditional commerce. Round the clock (24 x 7) service is available in e-commerce.

9. Product suitability

E-commerce is not suitable for perishable goods and high valuable items such as jewellery and antiques. It is mostly suitable for purchasing tickets, books, music and software. Traditional commerce is suitable for perishables and touch and feel items. Purchasing software, music in traditional commerce may appear expensive,

10. Human resource

To operate in an electronic environment, an organization requires technically qualified staff with an aptitude to update themselves in the ever changing world. E-business has difficulty in recruiting and retaining talented people.

Traditional commerce does not have such problems associated with human resource in non electronic environments.

11. Customer interaction

In traditional commerce, the interaction between the business and the consumer is a “face-to-face”.

In electronic commerce, the interaction between the business and the consumer is “screen-to-face”. Since there is no personal touch in e-business, companies need to have intimate relationships with customers to win over their loyalty.

12. Process

There is an automated processing of business transactions in electronic commerce. It helps to minimize the clerical errors.

There is manual processing of business transactions in traditional commerce. There are chances of clerical errors to occur as human intervention takes place.

13. Business relationship

The business relationship in traditional commerce is vertical or linear, whereas in electronic commerce the business relationship is characterized by end-to-end.

14. Fraud

Lot of cyber frauds take place in electronic commerce transactions. People generally fear to give credit card information. Lack of physical presence in markets and unclear legal issues give loopholes for frauds to take place in e-business transactions.

Fraud in traditional commerce is comparatively less as there is personal interaction between the buyer and the seller.

Capabilities requirements and Technology issues for E commerce.

1. Real-time, customer specific pricing

Individual pricing lists need to be available to your customers across all buying channels, in real time. This means having a system that supports continual price changes at an individual SKU level that could be different for each customer accessing the system.

2. Quick order & reorder/auto-replenishment

Due to the high frequency of component ordering, your customers frequently know exactly what they want and increasingly depend on eCommerce to quickly locate and purchase the products they need. These customers need to be able to easily enter in a long list of items they want to purchase, but also to be able to bulk order items they have recently ordered.

3. Bundle and tiered pricing

Many products offered by electrical wholesalers are very low cost and often it isn't worth listing or selling products unless they are grouped into larger bundles or tiers of packs. The B2B commerce platform therefore needs to allow the business to group and price products in a way where they can be easily marketed, merchandised and purchased.

4. Future stock availability

Visibility of overall stock and Available To Promise rules are critical in managing the supply chain. Without this, customers may decide to abandon their shopping journeys or not come back to shop at all, even though the

the wholesaler is about to receive stock imminently.

5. Customer self-service and administration

Corporate buyers will often have customer hierarchies for approval workflows and processes. Ensure your system has the capabilities to empower customers to build and configure their own users, cost centre hierarchy and workflow. This means they can administer the buying limits and approvals themselves, reducing administration and overall costs for you.

6. Invoice and credit reporting

B2B customers have lots of needs related to reporting on order invoicing, returns and credits. The cost to manually gather and send this data to your customers can be high. Make sure that the system automates the sending of reports and allows customers to access the data themselves.

7. Procurement integration

As digital transformation continues to occur across the electrical wholesale sector, businesses will need to provide technical integration support to their customers to be able to facilitate the use of their own procurement

systems in the purchase process. Those that offer this facility earlier than their competition will capitalise on acquiring new large account customers.

8. Personalization

The top priority of B2B retailers is to create a unique and personalised experience through innovation in technologies. Delivering tailored experiences have been shown to have a direct impact on conversion rates and customer loyalty.

9. Contextual assistance

Providing support to a customer base during their buying process is a key expectation of electrical wholesalers. Enabling your representatives to login to the same system as the customer and share the completion of their basket, giving them the same experience the customer is having, will help resolve issues much more effectively and quickly.

10. Cloud

Your focus should be on driving revenue and reducing costs, rather than producing and managing technical infrastructure. Harnessing cloud-based systems provides cost savings and flexibility to the business.

Types of E commerce web sites

Different eCommerce websites are labeled or referred to differently, based on the function they fulfill.

- Business-to-Business (B2B): Electronic transactions of goods and services between companies. Example: A business sells SAS products to other businesses.
- Business-to-Consumer (B2C): Electronic transactions of goods and services between companies and consumers. Example: You buy a new t-shirt from an online store.
- Consumer-to-Consumer (C2C): Electronic transactions of goods and services between consumers, mostly through a third party. Example: You sell your old smartphone on eBay or Olx to another consumer.
- Consumer-to-Business (C2B): Electronic transactions of goods and services where individuals offer products or services to companies. Example: A Social media influencer offers exposure to their online audience in exchange for a fee.

Building business on the net.

Step 1: Start a business that fills a need.

Most people who are just starting out make the mistake of looking for a product first, and a market second.

To boost your chances of success, start with a market. The trick is to find a group of people who are searching for a solution to a problem, but not finding many results. The internet makes this kind of market research easy:

- Visit online forums to see what questions people ask and what problems they're trying to solve.
- Do keyword research to find keywords that a lot of people are searching, but don't have a ton of competition with other sites.
- Check out your potential competitors by visiting their sites and taking note of what they're doing to fill the demand. Then you can use what you've learned and create a product for a market that already exists -- and do it better than the competition.

Step 2: Write a copy that sells.

There's a proven sales copy formula that takes visitors through the selling process from the moment they arrive to the moment they make a purchase:

1. Arouse interest with a compelling headline.
2. Describe the problem your product solves.
3. Establish your credibility as a solver of this problem.
4. Add testimonials from people who have used your product.
5. Talk about the product and how it benefits the user.
6. Make an offer.
7. Make a strong guarantee.
8. Create urgency.

9. Ask for the sale.

Throughout your copy, you need to focus on how your product or service is uniquely able to solve people's problems or make their lives better. Think like a customer and ask "What's in it for me?"

Step 3: Design and build your website.

Once you've got your market and product, and you've nailed down your selling process, now you're ready for your small-business web design. Remember to keep it simple. You have fewer than five seconds to grab someone's attention -- otherwise, they're gone, never to be seen again. Some important tips to keep in mind:

- Choose one or two plain fonts on a white background.
- Make your navigation clear and simple, and the same on every page.
- Only use graphics, audio or video if they enhance your message.
- Include an opt-in offer so you can collect e-mail addresses.
- Make it easy to buy -- no more than two clicks between potential customers and checkout.
- Your website is your online storefront, so make it customer-friendly.

Step 4: Use search engines to drive targeted buyers to your site.

Pay-per-click advertising is the easiest way to get traffic to a brand-new site. It has two advantages over waiting for the traffic to come to you organically. First, PPC ads show up on the search pages immediately, and second, PPC ads allow you to test different keywords, as well as headlines, prices and selling approaches. Not only do you get immediate traffic, but you can also use PPC ads to discover your best, highest-converting keywords. Then you can distribute the keywords throughout your site in your copy and code, which will help your rankings in the organic search results.

Step 5: Establish an expert reputation for yourself.

People use the internet to find information. Provide that information for free to other sites, and you'll see more traffic and better search engine rankings. The secret is to always include a link to your site with each tidbit of information.

- Give away free, expert content. Create articles, videos or any other content that people will find useful. Distribute that content through online article directories or social media sites.
- Include "send to a friend" links on valuable content on your website.
- Become an active expert in industry forums and social networking sites where your target market hangs out.

Step 6: Use the power of email marketing to turn visitors into buyers.

When you build an opt-in list, you're creating one of the most valuable assets of your online business. Your customers and subscribers have given you permission to send them an email. That means:

- You're giving them something they've asked for.
- You're developing lifetime relationships with them.
- The response is 100 percent measurable.
- Email marketing is cheaper and more effective than print, TV or radio because it's highly targeted.

Anyone who visits your site and opts into your list is a very hot lead. And there's no better tool than email for following up with those leads.

Step 7: Increase your income through back-end sales and upselling.

One of the most important internet marketing strategies is to develop every customer's lifetime value. At least 36 percent of people who have purchased from you once will buy from you again if you follow up with them. Closing that first sale is by far the most difficult part -- not to mention the most expensive. So use back-end selling and upselling to get them to buy again:

- Offer products that complement their original purchase.
- Send out electronic loyalty coupons they can redeem on their next visit.

-
- Offer related products on your "Thank You" page after they purchase.

Reward your customers for their loyalty and they'll become even more loyal.

Concepts of online Catalogues, Shopping carts, Checkout pages.

Online catalogues

An online product catalog is an important cornerstone for eCommerce retailers. Creating an immersive, information-rich experience helps eCommerce businesses build interest amongst online visitors and is key to converting potential customers into loyal shoppers.

One of the disadvantages that online shopping must accept is that potential buyers don't get an opportunity to feel the product in their hands before they purchase. A comprehensive online product catalog can dispel this shortcoming by instead providing more detailed information and a plethora of product images that help shoppers make up their mind without the need for touch. Along with using persuasive communication techniques, a detailed product catalog can be an important stimulus to encourage visitors to buy.

For many online vendors, your product range and selection is part of your unique selling position: the products you have curated for sale are part of your business identity and are what sets you apart from your e-tail peers. Making this point of difference clear through an intuitive product catalog that highlights the best of your online offerings can help you build a consistent brand identity that your shoppers will value and trust.

There are generally two ways you can create a product catalog for your eCommerce website:

- By selecting a complete eCommerce platform, you will have access to readymade templates and online tools specifically designed to help you create and maintain a product catalog for your online retail business.
- If you have an existing website with a strong identity that is more than a web-based storefront, you may be looking for plug-ins and widgets that let you devote a section of your website to selling products online.

Shopping Carts

A shopping cart on an online retailer's site is a piece of software that facilitates the purchase of a product or service. It accepts the customer's payment and organizes the distribution of that information to the merchant, payment processor and other parties.

Why shopping carts are important

Shopping carts bridge the gap between shopping and buying, so having the best shopping cart software is extremely important on your website.

It's likely that those just starting out in the market may be unfamiliar with the concept. Most people, especially those in the ecommerce industry, have likely made a purchase online at some point in their lives. That said, most consumers don't fully realize the need and capability that shopping carts have (besides leading a customer to checkout). A cart typically has three common aspects:

1. It stores product information
2. It's a gateway for order, catalog and customer management
3. It renders product data, categories and site information for user display

Another way to look at things is as follows: The online shopping cart is similar to the tangible ones we use at the supermarket, but it wears many more hats. It's also the shelves, the building, the clearance sign, the cash register and often the credit card machine relaying information back to the bank.

What options are there?

For those seriously considering the ecommerce platform route, it's important to know that there are two basic types of carts:

- Hosted shopping carts: A third-party firm "hosts" the solution and is responsible for server backups, maintenance and upgrades. The beauty of a hosted solution is that hosting comes free, which means it doesn't cost anything for the third party to keep your

site functional on the Web. The main drawback with hosted solutions is that customers will be directed to another domain for payment processing.

- Licensed shopping carts: This type of solution allows business owners to build their own type of cart and customize it to their specific needs. There is much greater flexibility in changing features and functionality, as well as in adding third-party tools if need be. However, the upfront costs are often higher and require more hands-on expertise for troubleshooting issues and technical support.

Checkout Pages

A checkout page refers to any website pages shown to a customer during the step-by-step checkout process. Think of checkout pages as the online version of a physical checkout counter in a grocery store. Checkout pages come in two types: one-page checkout and multi-page checkout.

One-page Checkout vs. Multi-page Checkout

As the terms imply, checkout pages can be built as single-page solutions or as step-by-step processes. Although the one-page checkout option is rapidly gaining popularity among online retailers due to its perceived benefits of being faster and more user-friendly, various case studies demonstrate that conversion-optimized multi-page checkouts can be just as effective, and both options have their pros and cons.

One-page Checkout: Pros

- It's faster. Despite the fact that the number of form fields to fill are pretty much the same between single-page and multi-page checkouts, it still takes less time to complete the one-page checkout because shoppers don't need to wait for the multiple pages to load or refresh.
- It has a psychological advantage. The fact that shoppers can see exactly how far along the process they are, and how many steps they have left to complete the purchase, acts like a psychological booster motivating them to finish what they've started.
- It has no navigation. Since all the fields are on the same page, customers don't need to navigate between different pages if they want to edit or change the information they

entered. It eliminates the possibility of shoppers dropping off if they need to re-enter the same details every time they go back in the browser.

One-page Checkout: Cons

- It's a nightmare to design. Depending on the amount of data you're trying to gather, one-page checkouts can be difficult to design. When crammed into one page, the number of forms and fields required can cause the layout design to look cluttered and off-putting, which would most likely lead to shopping cart abandonment.

Multi-page Checkout: Pros

- It's easier to collect data. By splitting your checkout process into multiple steps, you have a better chance of capturing customer data even if they abandon the cart at a later stage. For example, if you ask for the shopper's email address first and they end up abandoning the checkout after proceeding to the next step, you still have their email address and can follow up with an abandoned cart email.
- It's simpler to design. When you spread the forms across several pages, it is much easier to create a clean, minimalistic layout design, which also gives the impression of the checkout process being simple and fast.

Multi-page Checkout: Cons

- It can be disheartening. If the checkout progress bar is showing four more steps to go until the order is complete after the initial page, a customer might find the process too long and tedious and abandon the purchase altogether.

Choosing between the two options will ultimately boil down to the type of business you're running and your customer base. The important thing to remember is that selecting the type of checkout page is just the first step, next, you should look at ways to optimize it.

Cart > Customer information > Shipping Method > Payment method

Contact information

Email

Keep me up to date on news and exclusive offers

Shipping address

First name Last name

Company (optional)

Address

Apartment, suite, etc. (optional)

City

Country
Germany

Postal code

Phone (optional)

< Return to cart Continue to shipping method

Lotus Orange T-Shirt
Adult Unisex MD \$25.00

Gift card or discount code Apply

Subtotal \$25.00
Shipping -

Total USD \$25.00

Image3: Check out page.
Reference:<https://wp-en.oberlo.com/wp-content/uploads/2018/06/shopify-checkout-2-1024x611.jpg>

Payment and Order Processing, Authorization, Chargeback and other payment methods.

Payment & Order Processing

Once you set up your new online store in place, the very next step for you is to think about how to receive the payments from your customers online. Having a seamless and easy to process payment method helps you improve your conversion ratio.

To understand how this process of online payment works in eCommerce, let's take a look at the different components that make this online transaction of money possible.

There are two things that you need to complete an online payment process successfully:

- Merchant Account
- Payment Gateway

What Is A Merchant Account

A merchant account is a type of bank account which can accept payments via credit cards, debit cards, net banking, third-party payment applications, etc. You or your company sign a contract with a bank to open a merchant account for your online business so that all payments derived from online sales are directly transferred to your business bank account.

For this purpose, the bank asks you to fill out an application with all the details regarding your business which includes what products/services you sell online, to whom do you sell, different currencies in which you accept payments, estimated sales you would be making in a time period, etc.

Once the application gets approved by the bank, your business would be assigned a unique ID (merchant ID) along with your business bank account.

You also need to understand that there are different types of charges that are imposed by these banks, such as monthly charges, transaction fee, etc, on such merchant accounts. Having an understanding of these banking charges will help you to make sure you don't make losses at the end of an online sale.

What Is A Payment Gateway

A payment gateway is a software that is required to connect your merchant account to your online store. It's responsible for taking details from the online buyers regarding their payment mode, like credit/debit card details, net banking details etc, It is also responsible to process that payment so that it reaches your bank account safely and securely.

A payment gateway is of two types – direct and redirected. In a direct way, the buyer/customer doesn't leave the eCommerce website to make the payment. In a redirected way, the buyer/customer is redirected to the payment gateway to make the payment and is redirected back to the eCommerce store once the payment is done.

Here are the steps involved in the process of making online payments successfully:

- The customer/online buyer shares their card details with the payment gateway.
- Payment gateway then verifies the details with the associated bank and then encrypts the details.
- After the verification, the payment gateway processes the payment which is transferred to the merchant's bank account with the help of a unique merchant ID.
- As a result, the payment reaches the online seller/merchant.

Authorization

Authorization is a security mechanism to determine access levels or user/client privileges related to system resources including files, services, computer programs, data and application features. This is the process of granting or denying access to a network resource which allows the user access to various resources based on the user's identity.

Description: Most web security systems are based on a two-step process. The first step is authentication, which ensures about the user identity and the second stage is authorization, which allows the user to access the various resources based on the user's identity. Modern operating systems depend on effectively designed authorization processes to facilitate application deployment and management. Key factors contain user type, number and credentials, requiring verification and related actions and roles.

Access control in computer systems and networks relies on access policies and it is divided into two phases:

- 1) Policy definition phase where access is authorized.
- 2) Policy enforcement phase where access requests are permitted or not permitted.

Thus authorization is the function of the policy definition phase which precedes the policy enforcement phase where access requests are permitted or not permitted based on the previously defined authorizations. Access control also uses authentication to check the identity of consumers. When a consumer attempts to access a resource, the access control process investigates that the consumer has been authorized to use that resource. Authorization services are implemented by the Security Server which can control access at the level of individual files or programs.

Chargeback & Other Payment Methods

What does Chargeback mean?

A Chargeback, in ordinary terms, means a reversal. It's more of a buyer protection measure. The customer gets their money back. Take for instance, if the products they receive are faulty, a chargeback is always the feasible remedy. In usual circumstances, this is the last thing a merchant wants to come across. It brings on board lots of frustrations, more precisely to the retailer.

On the other hand, it's more of a protracted battle between the buyer and seller. It often seems like the buyer takes the edge since chargebacks come into play as a means to resolve

unauthorized transactions. Regrettably, the seller risks high chances of incurring huge losses if more customers keep on filing chargebacks.

What is a Chargeback and How does it Work?

The chargeback resolution process involves three parties. The customer, merchant and the issuing bank. The cardholder (customer) usually contacts the issuing bank to request a chargeback.

Once a chargeback claim is filed, the issuing bank initiates the procedure. It will communicate this information to the Merchant. The bank explains in detail the reason for a chargeback claim. To enhance a fair outcome, there is a window period(7days in most cases) which gives the merchant ample time to respond. This usually via a reason code. It's important to note that all credit card brands have their own chargeback reason codes. This includes brands like;

1. Mastercard
2. Visa
3. American Express
4. Discover

What follows is a reply from the merchant to either acknowledge the chargeback or contest the action. Consequently, if I'm to challenge a chargeback, I need to back my arguments with proper documents to serve as evidence. If my grounds aren't convincing, then a chargeback takes effect.

In spite of that, it's highly recommended that merchants take steps to acquaint themselves with these procedures. It really helps with future chargeback experiences.

What Amounts to a Chargeback?

Chargebacks happen due to the disputes raised by buyers in relation to a purchase. In the event where a buyer receives a defective product, they're actually allowed to raise a claim. The other common reason for a chargeback is where a buyer pays for goods but the seller fails to ship the item.

Also, customers are prone to credit card theft. If their information gets stolen and is used fraudulently to purchase goods, then this highly attracts a chargeback claim. And this is where a

Chargeback comes to enforce consumer protection rights. Unfortunately, this isn't quite impressive for any business owner. And the reason is pretty obvious. It's all at my expense as a seller.

The amount is withdrawn from my account. A chargeback is effected on payment transactions made via credit cards, debit cards, and bank transfers.

And here's why most customers demand a chargeback.

Whenever customers detect any discrepancies with their orders, they often contact their credit card issuers and file a claim. Remember, the procedure varies from one credit card company to another since they all have different rules and regulations. What appears staggering for most business entities is that it's pretty difficult to avoid chargebacks. Quite frustrating, right?

To ease the burden, I must be wary and meticulous on the product quality. In particular, if I operate an online retail business I mustn't leave any loopholes for inaccuracies. More importantly, I need to handle my business transactions with lots of precision. This helps me to ultimately mitigate all forms of liability mainly if I accept credit card payments.

As a matter of fact, if I want to analyze all potential risks which come with business transactions, I need to think of all possibilities which might bring about future chargebacks. Quite annoying how chargebacks are always part of the equation in a business setup.

Credit Card Related Chargebacks

This often happens to merchants who receive transactions via a telephone call or mail. Customers will claim a chargeback on grounds that they didn't authorize the process.

To avoid such risks, always gather requisite information from the customer before you fulfill an order. In furtherance of that, be keen to capture the correct CVV(Card verification number) of the customer's credit card. Also, you need to confirm their address. However, there are untrustworthy merchants who want to charge a customer twice for the same transactions.

This might sound a bit trivial but it's so imperative.

Make sure that your systems are up-to-date. This helps a retailer detect if the credit card has expired or if it's invalid. But wait, there's more. A customer might press the Pay button twice. If this happens, it results in two transactions simultaneously. Definitely, this attracts a chargeback.

Security issues and payment gateways

Security Issues

E-Commerce is defined as the buying and selling of products or services over electronic systems such as the Internet and to a lesser extent, other computer networks. It is generally regarded as the sales and commercial function of eBusiness. There has been a massive increase in the level of trade conducted electronically since the widespread penetration of the Internet. A wide variety of commerce is conducted via eCommerce, including electronic funds transfer, supply chain management, Internet marketing, online transaction processing, electronic data interchange (EDI), inventory management systems, and automated data collection systems. US online retail

sales reached \$175 billion in 2007 and are projected to grow to \$335 billion by 2012 (Mulpuru, 2008).

This massive increase in the uptake of eCommerce has led to a new generation of associated security threats, but any eCommerce system must meet four integral requirements:

- privacy – information exchanged must be kept from unauthorized parties
- integrity – the exchanged information must not be altered or tampered with
- authentication – both sender and recipient must prove their identities to each other and
- non-repudiation – proof is required that the exchanged information was indeed received (Holcombe, 2007).

These basic maxims of eCommerce are fundamental to the conduct of secure business online. Further to the fundamental maxims of eCommerce above, eCommerce providers must also protect against a number of different external security threats, most notably Denial of Service (DoS). These are where an attempt is made to make a computer resource unavailable to its intended users though a variety of mechanisms discussed below. The financial services sector still bears the brunt of e-crime, accounting for 72% of all attacks. But the sector that experienced the greatest increase in the number of attacks was eCommerce. Attacks in this sector have risen by 15% from 2006 to 2007 (Symantec, 2007).

Privacy

Privacy has become a major concern for consumers with the rise of identity theft and impersonation, and any concern for consumers must be treated as a major concern for eCommerce providers. According to Consumer Reports Money Adviser (Perrotta, 2008), the US Attorney General has announced multiple indictments relating to a massive international security breach involving nine major retailers and more than 40 million credit- and debit-card numbers. US attorneys think that this may be the largest hacking and identity-theft case ever prosecuted by the justice department. Both EU and US legislation at both the federal and state levels mandates certain organizations to inform customers about information uses and disclosures. Such disclosures are typically accomplished through privacy policies, both online and offline (Vail et al., 2008).

Integrity, Authentication & Non-Repudiation

In any e-commerce system the factors of data integrity, customer & client authentication and non-repudiation are critical to the success of any online business. Data integrity is the assurance

that data transmitted is consistent and correct, that is, it has not been tampered or altered in any way during transmission. Authentication is a means by which both parties in an online transaction can be confident that they are who they say they are and non-repudiation is the idea that no party can dispute that an actual event online took place. Proof of data integrity is typically the easiest of these factors to successfully accomplish. A data hash or checksum, such as MD5 or CRC, is usually sufficient to establish that the likelihood of data being undetectably changed is extremely low (Schlaeger and Pernul, 2005). Notwithstanding these security measures, it is still possible to compromise data in transit through techniques such as phishing or man-in-the-middle attacks (Desmedt, 2005). These flaws have led to the need for the development of strong verification and security measurements such as digital signatures and public key infrastructures (PKI).

One of the key developments in e-commerce security and one which has led to the widespread growth of e-commerce is the introduction of digital signatures as a means of verification of data integrity and authentication. In 1995, Utah became the first jurisdiction in the world to enact an electronic signature law. An electronic signature may be defined as “any letters, characters, or symbols manifested by electronic or similar means and executed or adopted by a party with the intent to authenticate a writing” (Blythe, 2006). In order for a digital signature to attain the same legal status as an ink-on-paper signature, asymmetric key cryptology must have been employed in its production (Blythe, 2006). Such a system employs double keys; one key is used to encrypt the message by the sender, and a different, albeit mathematically related, key is used by the recipient to decrypt the message (Antoniou et al., 2008). This is a very good system for electronic transactions, since two stranger-parties, perhaps living far apart, can confirm each other’s identity and thereby reduce the likelihood of fraud in the transaction. Non-repudiation techniques prevent the sender of a message from subsequently denying that they sent the message. Digital Signatures using public-key cryptography and hash functions are the generally accepted means of providing non-repudiation of communications.

Payment gateway

With the high percentage of people in the world on the internet today, online businesses are becoming more popular. When people do their transaction online the use of payment gateways come forward. Payment gateway is an essential part when considering online transactions because it act as the intermediate between merchant and the bank. Since when customers do their payment through payment gateway they have to enter sensitive transaction information. With the rapid growth of online transactions threats of security also increased. That is the major issue for online transactions and gateway has the high responsibility for protection of these information

over hackers and fraudsters. So the security features of payment gateway become more important. With using various standards, protocols and encryption mechanisms gateways try to provide more secure and confident service to their customers. In this paper I will be discussing a few technologies and mechanisms that are used by payment gateways to make online transactions more secure.

The evaluation of business runs from the barter system through bank notes, payment orders, checks, credit cards and now electronic payment systems and mobile payment systems. High percentage of people in the world are on the internet today. The Internet has become the preferred environment for different e-services like e-commerce, e-banking, e-voting, e-government, etc. Every company is trying to move into e-businesses. It makes online shopping easier and beneficial. It allows customers to sit in their homes and buy goods from all over the world. And also merchants can sell their products to all over the world very easily. So, online payment has become a very popular payment method in the world because of efficiency and effectiveness of online payments. Mobile Payments are also becoming a more important payment system with the increase of wireless services.

When most of the companies are moving into e-businesses, use of payment gateways to do online payments is needed. Payment gateway is a service

References

1. https://www.tutorialspoint.com/computer_fundamentals/computer_networking.htm
2. <https://beginnersbook.com/2019/03/computer-network-components/>
3. <https://www.networkstraining.com/different-types-of-networks/>
4. <https://www.javatpoint.com/intranet>
5. <https://www.educative.io/edpresso/what-are-p2p-and-clientserver-networks>
6. <https://afteracademy.com/blog/what-is-a-network-interface-card>
7. <https://incentre.net/ethernet-cable-color-coding-diagram/>
8. <https://whatis.techtarget.com/definition/server>
9. <https://www.computerhope.com/jargon/s/server.htm>
10. <https://www.promax.com/blog/top-5-types-of-servers>
11. <http://ecomputernotes.com/computernetworkingnotes/computer-network/what-are-the-different-types-of-servers>
12. <https://www.techopedia.com/definition/30262/server-architecture>
13. <https://searchwindowsserver.techtarget.com/definition/Microsoft-Windows-Server-OS-operating-system>
14. <https://searchdatacenter.techtarget.com/definition/Linux-operating-system>
15. <https://www.computerhope.com/jargon/n/netware.htm>
16. <https://www.probrand.co.uk/it-services/cloud-server>
17. <https://www.ibm.com/cloud/learn/cloud-server>
18. <https://www.techopedia.com/definition/437/client>
19. <https://sites.google.com/site/clientserverarchitecture/clients-and-their-types>
20. <https://www.brianmadden.com/feature/Types-of-Client-Devices-Terminal-Services-for-Windows-Server-2003>
21. <https://www.lifewire.com/what-is-a-node-4155598>
22. <https://www.webopedia.com/TERM/S/segment.html>
23. http://www.linfo.org/network_segment.html
24. <https://www.geeksforgeeks.org/types-and-uses-of-backbone-networks/>
25. <https://searchnetworking.techtarget.com/definition/host>
26. <https://www.ntchosting.com/encyclopedia/hosting/host/>
27. <https://www.informit.com/articles/article.aspx?p=24687&seqNum=5>
28. https://www.tutorialspoint.com/data_communication_computer_network/analog_transmission.htm
29. https://www.diffen.com/difference/Analog_vs_Digital
30. <https://www.techopedia.com/definition/14153/shielded-twisted-pair-stp>
31. <https://networkencyclopedia.com/shielded-twisted-pair-stp-cabling/>
32. <https://fcit.usf.edu/network/chap5/chap5.htm>
33. <https://www.computernetworkingnotes.com/>
34. <https://sewelldirect.com/blogs/learning-center/what-is-the-difference-between-rg59-and-r>

g6

35. <https://www.engineersgarage.com/tutorials/introduction-to-usb-advantages-disadvantages-and-architecture-part-1-6/>
36. <http://www.firewall.cx/networking-topics.html>
37. https://www.tutorialspoint.com/communication_technologies/communication_technologies_network_topologies.htm
38. <https://computernetworktopology.com/what-is-mesh-topology-advantages-disadvantages/>
39. <https://teachcomputerscience.com/synchronous-and-asynchronous/>
40. https://www.tutorialspoint.com/communication_technologies/communication_technologies_network_topologies.htm
41. <https://computernetworktopology.com/what-is-mesh-topology-advantages-disadvantages/>
42. <https://teachcomputerscience.com/synchronous-and-asynchronous/>
43. <https://www.cisco.com/c/en/us/products/security/identity-services-engine/what-is-user-authentication-policy.html>
44. <https://www.tech-faq.com/understanding-organizational-units.html>
45. <https://www.mustbegeek.com/understanding-gpo-in-windows-server-2012/#.Xssz3TozbIV>
46. [https://www.tutorialspoint.com/internet_technologies/internet_overview.htm/](https://www.tutorialspoint.com/internet_technologies/internet_overview.htm)
47. <https://www.educba.com/types-of-networking-protocols/>
48. <https://www.w3schools.in/types-of-network-protocols-and-their-uses/>
49. <https://www.w3.org/People/Frystyk/thesis/TcpIp.html#IP>
50. https://www.tutorialspoint.com/internet_technologies/internet_protocols.htm
51. https://en.wikipedia.org/wiki/Internet_protocol_suite
52. <https://en.wikipedia.org/wiki/HTTPS#Security>
53. <https://www.geeksforgeeks.org/layers-of-osi-model/>
54. <https://www.educba.com/what-is-osi-model/>
55. <https://www.mysolutionguru.com/ps/media-access-methods/112>
56. <https://www.mysolutionguru.com/ps/media-access-methods/112>
57. <https://www.cloudflare.com/learning/dns/what-is-dns/>
58. <https://www.educba.com/what-is-web-services/>
59. https://www.tutorialspoint.com/internet_technologies/web_servers.htm
60. <https://www.guru99.com/web-service-architecture.html>
61. <https://www.guru99.com/web-service-architecture.html#7>
62. <https://www.tutorialspoint.com/what-are-hub-and-switch-in-computer-network>
63. https://www.cisco.com/c/en_in/solutions/small-business/resource-center/networking/network-switch-how.html
64. <https://www.javatpoint.com/computer-network-switching>
65. <https://geek-university.com/ccna/what-is-a-network-bridge/>
66. <https://www.elprocus.com/what-is-a-bridge-in-computer-network-working-types-its-functions/>
67. http://www.idc-online.com/technical_references/pdfs/data_communications/ISP_Internet_service_providers.pdf

-
68. <https://www.ntchosting.com/encyclopedia/internet/isp/>
 69. <https://www.javatpoint.com/cyber-security-introduction>
 70. https://www.tutorialspoint.com/computer_security/computer_security_tutorial.pdf
 71. <https://www.beyondtrust.com/resources/glossary/cyber-security>
 72. https://shodhganga.inflibnet.ac.in/bitstream/10603/73828/9/09_chapter%202%20overvie w%20of%20networking,threats%20and%20security%20measures.pdf
 73. <http://etutorials.org/Networking/Cisco+Certified+Security+Professional+Certification/Part+I+Introduction+to+Network+Security/Chapter+2+Securing+the+Network/Securing+N etwork+Devices/>
 74. https://www.netwrix.com/network_security_best_practices.html
 75. https://www.netwrix.com/network_security_best_practices.html
 76. <https://searchsecurity.techtarget.com/definition/remote-access>
 77. <https://computer.howstuffworks.com/vpn.htm>
 78. <https://www.geeksforgeeks.org/password-authentication-protocol-pap/>
 79. <https://www.geeksforgeeks.org/challenge-handshake-authentication-protocol-chap/>
 80. https://docs.microsoft.com/en-us/openspecs/windows_protocols/ms-chap/4740bf05-db7e-4542-998f-5a4478768438
 81. <https://en.wikipedia.org/wiki/MS-CHAP>
 82. https://docs.microsoft.com/en-us/openspecs/windows_protocols/ms-chap/4740bf05-db7e-4542-998f-5a4478768438
 83. https://www.juniper.net/documentation/en_US/sbr-carrier8.4.1/information-products/topic-collections/sbr-admin-guide-10/id-34608.html
<https://www.extrahop.com/resources/protocols/radius/>
 84. <https://www.extrahop.com/resources/protocols/radius/>
 85. <https://www.linux.org/threads/tcp-ip-protocol-routing-protocols.9287/>
 86. https://en.wikipedia.org/wiki/Routing_protocol
 87. https://sites.ualberta.ca/dept/chemeng/AIX-43/share/man/info/en_US/a_doc_lib/aixbman/commadmn/tcp_route.htm
 - 88.