BROADBAND TECHNICIAN

CATALOG INFORMATION
(కాటలాగ్ సమాచారం)

Book Title : Broadband Technician / TEL/Q0102

Product No : SMTPL-110

Version No : 1.0

Date of release: November-2016

LIMITS OF LIABILITY AND

DISCLAIMER OF WARRANTY

వారెంటీ యొక్క నిరాకరణ

The author of this book, have put their best efforts in preparing this course material and the content. These efforts include development, research and verification to check the effectiveness.

ఈ పుస్తక రచయిత, ఈ కోర్సు విషయం మరియు కంటెంట్ను తయారుచేయడంలో వారి ఉత్తమ ప్రయత్నాలను చేశాడు.
ఈ ప్రయత్నాలు అభివృద్ధి, పరిశోధన మరియు సమర్థతను తనిఖీ చేయడానికి ధ్రువీకరణ ఉన్నాయి.

The authors make no warranty of any kind expressed or implied with regard to these programs, concepts, or the documentation contained in this book. The authors shall not be liable in any event for incidental or consequential damages in connection with, or arising out of, the furnishing, performance or use of these programs and documentation.

రచయితలు ఈ పుస్తకంలో ఉన్న ఈ కార్యక్రమాలు, భావనలు, లేదా డాక్యుమెంటేషన్కు సంబంధించి వ్యక్తీకరించిన లేదా సూచించిన ఏ విధమైన వారంటీని తయారు చేయరు. ఈ కార్యక్రమాల మరియు పత్రాల యొక్క ఫర్నిషింగ్, పనితీరు లేదా వినియోగంతో సంబంధం లేకుండా, లేదా సంభవించేటప్పుడు, సంభవించే లేదా సంభవించే నష్టాలకు సంబంధించి రచయితలు ఎటువంటి సందర్భాలలో బాధ్యత వహించరు.

Table of Contents

Introduction to Broadband Technician

Broadband Technician Job Description:

Typically, working in the telecommunications industry, a broadband technician installs or maintains Cable, Internet and telephone services delivered to a client's home or business. It is most common for these technicians to perform on-site installation and repairs, traveling to client residences or commercial locations.

బ్రాడ్బ్యాండ్ టెక్నీషియన్ ఉద్యోగ వివరణ:

సాధారణంగా, టెలీకమ్యూనికేషన్స్ పరిశ్రమలో పనిచేస్తున్న, ఒక బ్రాడ్బ్యాండ్ సాంకేతిక నిపుణుడు సంస్థాపిస్తాడు లేదా నిర్వహిస్తాడు కేబుల్, ఇంటర్నెట్ మరియు టెలిఫోన్ సేవలు క్లయింట్ యొక్క ఇంటికి లేదా వ్యాపారానికి పంపిణీ చేయబడతాయి. ఈ సాంకేతిక నిపుణులు క్లయింట్ రెసిడెన్స్ లేదా వాణిజ్య స్థానాలకు ప్రయాణించే ఆన్-సైట్ ఇన్స్టాలేషన్ మరియు మరమత్తులు నిర్వహించడానికి చాలా సాధారణం.

What Is a Broadband Technician?

Broadband technicians install and repair telephone and broadband service lines for businesses and homes, typically offering services at all hours of the day. They will travel directly to their clients in order to perform their work, servicing and installing broadband connections and making accurate and thorough records of what they do and use during the course of their jobs. These professionals may work for a variety of employers, such as telecommunication companies or electronic service centers, and typically have to perform duties outside in different weather conditions.

ఒక బ్రాడ్బ్యాండ్ టెక్నీషియన్ అంటే ఏమిటి?

బ్రాడ్బ్యాండ్ యాక్సెస్ కోసం CPE (మోడెమ్, రౌటర్లు మరియు స్విచ్లు) యొక్క సంస్థాపన, ఆకృతీకరణ మరియు పరీక్షలకి వ్యక్తి బాధ్యత వహిస్తాడు. కస్టమర్ ప్రాంగణంలో CPE మరియు తుది వినియోగదారు పరికరం (CPU, ల్యాప్టాప్, టాబ్లెట్లు, స్మార్ట్ / IP టివి మొదలైనవి) మధ్య అనుసంధానాన్ని కూడా ఏర్పాటు చేస్తుంది మరియు సమన్వయంతో కేబుల్, కనెక్టివిటీ మరియు పరికర లోపాలను గుర్తించడం, స్థానీకరించడం మరియు సవరించడం కోసం ప్రాథమిక సమస్య-షూటింగ్ను నిర్వహిస్తుంది.

Objective of the Course:

The person is responsible for installation, configuration and testing of CPE (modem, routers, and Switches) for broadband access. He also establishes connectivity between CPE and end-user device (CPU, Laptop, tablets, Smart/IP TV etc.) at customer premises and carries out basic trouble-shooting for identifying, localizing & rectifying cable, connectivity and equipment fault in coordination with NOC.

కోర్సు యొక్క లక్ష్యం:

బ్రాడ్బ్యాండ్ యాక్సెస్ కోసం CPE (మోడెమ్, రౌటర్లు మరియు స్విచ్లు) యొక్క సంస్థాపన, ఆకృతీకరణ మరియు పరీక్షలకి వ్యక్తి బాధ్యత వహిస్తాడు. కస్టమర్ ప్రాంగణంలో CPE మరియు తుది వినియోగదారు పరికరం (CPU, ల్యాప్టాప్, టాబ్లెట్లు, స్మార్ట్ / IP టివి మొదలైనవి) మధ్య అనుసంధానాన్ని కూడా ఏర్పాటు చేస్తుంది మరియు సమన్వయంతో కేబుల్, కనెక్టివిటీ మరియు పరికర లోపాలను గుర్తించడం, స్థానీకరించడం మరియు సవరించడం కోసం ప్రాథమిక సమస్య-షూటింగ్ను నిర్వహిస్తుంది.

Broadband

In general, broadband refers to telecommunication in which a wide band of frequencies is available to transmit information. Because a wide band of frequencies is available, information can be multiplexed and sent on many different frequencies or channels within the band concurrently, allowing more information to be transmitted in a given amount of time (much as more lanes on a highway allow more cars to travel on it at the same time).

బ్రాడ్బ్యాండ్

సాధారణంగా, బ్రాడ్బ్యాండ్ టెలికమ్యూనికేషన్ను సూచిస్తుంది, దీనిలో విస్తృత బ్యాండ్ల ఫ్రీక్వెన్సీ సమాచారం ప్రసారం చేయడానికి అందుబాటులో ఉంటుంది. పౌనఃపున్యాల విస్తృత బ్యాండ్ అందుబాటులో ఉన్నందున, సమాచారము బహుళస్థాయిలో ప్రసారం . మరియు బృందం పరిధిలో ఉన్న అనేక పౌనఃపున్యాలపై లేదా ఛానళ్ళ ద్వారా పంపబడుతుంది, ఇది ఎక్కువ సమయం కేటాయించిన సమయం లో ఎక్కువ సమాచారాన్ని పంపటానికి అనుమతిస్తుంది (ఎక్కువ మార్గంలో ఎక్కువ మార్గాలు అదే సమయంలో ప్రయాణించండి).

Broadband is a type of high-speed internet connection that has surpassed dial-up as the standard way to connect to the internet. Broadband packages come in all shapes and sizes, from ADSL broadband to cable broadband and 3G and 4G mobile broadband.

బ్రాడ్బ్యాండ్ అనేది హై-స్పీడ్ ఇంటర్నెట్ కనెక్షన్, ఇది డయల్-అప్ను ఇంటర్నెట్కి కనెక్ట్ చేయడానికి ప్రామాణిక మార్గంగా అధిగమించింది. బ్రాడ్బ్యాండ్ ప్యాకేజీలు ADSL బ్రాడ్బ్యాండ్ నుండి కేబుల్ బ్రాడ్బ్యాండ్ మరియు 3G మరియు 4G మొబైల్ బ్రాడ్బ్యాండ్ వరకు అన్ని ఆకారాలు మరియు పరిమాణాలలో లభిస్తాయి.

Types of Broadband Connections:

బ్రాడ్బ్యాండ్ కనెక్షన్ల రకాలు:

Broadband includes several high-speed transmission technologies such as:

బ్రాడ్బ్యాండ్ కనెక్షన్ల రకాలు: బ్రాడ్బ్యాండ్లో పలు హై స్పీడ్ ట్రాన్స్మిషన్ టెక్నాలజీలు ఉన్నాయి:

Digital Subscriber Line (DSL)

- డిజిటల్ సబ్స్క్రయిబర్ లైన్ (DSL)
- Cable Modem (కేబుల్ మోడెమ్)
- Fiber(ఫైబర్)
- Wireless (వైర్లెస్)
- Satellite (ఉపగ్రహ)
- Broadband over Powerlines((BPL) పవర్లైన్స్ (BPL) పై బ్రాడ్బ్యాండ్)

The broadband technology you choose will depend on a number of factors. These may include whether you are located in an urban or rural area, how broadband Internet access is packaged with other services (such as voice telephone and home entertainment), price, and availability.

మీరు ఎంచుకున్న బ్రాడ్బ్యాండ్ టెక్నాలజీ అనేక అంశాలపై ఆధారపడి ఉంటుంది. మీరు పట్టణ లేదా గ్రామీణ ప్రాంతాల్లో ఉన్నవారైనా, బ్రాడ్బ్యాండ్ ఇంటర్నెట్ సదుపాయం ఇతర సేవలతో (వాయిస్ టెలిఫోన్ మరియు గృహ వినోదం వంటివి), ధర మరియు లభ్యతతో ఎలా ప్యాక్ చేయబడినా కూడా వీటిలో మీరు ఉండవచ్చు.

Digital Subscriber Line (DSL)

DSL is a wireline transmission technology that transmits data faster over traditional copper telephone lines already installed to homes and businesses. DSL-based broadband provides transmission speeds ranging from several hundred Kbps to millions of bits per second (Mbps). The availability and speed of your DSL service may depend on the distance from your home or business to the closest telephone company facility.

డిజిటల్ సబ్స్క్రయిబర్ లైన్ (DSL)

DSL అనేది ఒక వైర్లైన్ ట్రాన్స్మిషన్ టెక్నాలజీ, ఇంతకు ముందు గృహాలు మరియు వ్యాపారాలకు ఇప్పటికే సాంప్రదాయిక రాగి టెలిఫోన్ లైన్లను ఇన్స్టాల్ చేయడంలో సమాచారాన్ని వేగంగా ప్రసారం చేస్తుంది. DSL- ఆధారిత బ్రాడ్బ్యాండ్ అనేక వందల Kbps నుండి సెకనుకు లక్షల బిట్స్ వరకు (Mbps) వరకు ప్రసార వేగం అందిస్తుంది. మీ DSL సేవ యొక్క లభ్యత మరియు వేగాన్ని మీ హోమ్ లేదా వ్యాపార దూరం నుండి సమీప టెలిఫోన్ కంపెనీ సదుపాయంలో ఆధారపడి ఉండవచ్చు.

The following are types of DSL transmission technologies:

DSL ప్రసార సాంకేతిక రకాలు:

Asymmetrical Digital Subscriber Line (ADSL) – Used primarily by residential customers, such as Internet surfers, who receive a lot of data but do not send much. ADSL typically provides faster speed in the downstream direction than the upstream direction. ADSL allows faster downstream data transmission over the same line used to provide voice service, without disrupting regular telephone calls on that line.

అసమాన డిజిటల్ సబ్స్క్రయిబర్ లైన్ (ADSL) - ప్రాధమికంగా గృహ వినియోగదారులచే వాడబడిన ఇంటర్నెట్ సర్ఫర్లు, చాలా డేటాని అందుకుంటారు కాని చాలా ఎక్కువ పంపించవు. అప్స్ట్రీమ్ దిశ కంటే దిగువ దిశలో ADSL వేగంగా వేగవంతమైన వేగం అందిస్తుంది. ADSL వాయిస్ సేవను అందించడానికి ఉపయోగించిన అదే రేఖపై వేగవంతమైన దిగువ స్థాయి డేటా బదిలీని అనుమతిస్తుంది, ఆ లైన్లో సాధారణ టెలిఫోన్ కాల్స్ను భంగం చేయకుండా.

Symmetrical Digital Subscriber Line (SDSL) – Used typically by businesses for services such as video conferencing, which need significant bandwidth both upstream and downstream.

Faster forms of DSL typically available to businesses include:

సిమెమెట్రిక్ డిజిటల్ సబ్స్క్రయిబర్ లైన్ (SDSL) - సాధారణంగా వీడియో కాన్ఫరెన్సింగ్ వంటి సేవల ద్వారా వాడతారు, ఇది అప్స్ట్రీమ్ మరియు దిగువ స్థాయికి గణనీయమైన బ్యాండ్విడ్త్ అవసరమవుతుంది. DSL యొక్క వేగవంతమైన రూపాలు సాధారణంగా అందుబాటులో ఉంటాయి:

- High data rate Digital Subscriber Line (HDSL); and
- హై డేటా రేట్ డిజిటల్ సబ్స్క్రయిబర్ లైన్ (HDSL); మరియు
- Very High data rate Digital Subscriber Line (VDSL).
- అధిక డేటా రేట్ డిజిటల్ సబ్స్క్రయిబర్ లైన్ (VDSL).

Cable Modem
కేబుల్ మోడెమ్

Cable modem service enables cable operators to provide broadband using the same coaxial cables that deliver pictures and sound to your TV set.
కేబుల్ మోడెమ్ సేవ కేబుల్ ఆపరేటర్లను బ్రాడ్బ్యాండ్ ను అదే ఏకాక్షక తంతులు ఉపయోగించి చిత్రాలను మరియు మీ టీవీ సెట్కు ధ్వనిని అందించడానికి అనుమతిస్తుంది.

Most cable modems are external devices that have two connections: one to the cable wall outlet, the other to a computer. They provide transmission speeds of 1.5 Mbps or more.
చాలా కేబుల్ మోడెములు బాహ్య పరికరాలు రెండు కనెక్షన్లను కలిగి ఉంటాయి: ఒక కేబుల్ వాల్ స్టీట్ కు ఒకదానిని, మరొకదానికి కంప్యూటర్. వారు 1.5 Mbps లేదా అంతకంటే ఎక్కువ ప్రసార వేగాలను అందిస్తాయి.

Subscribers can access their cable modem service by simply turning on their computers, without dialing-up an ISP. You can still watch cable TV while using it. Transmission speeds vary depending on the type of cable modem, cable network, and traffic load. Speeds are comparable to DSL.

చందాదార్లు వారి కేబుల్ మోడెమ్ సేవను తమ ISP లను డయల్ చేయకుండానే తమ కంప్యూటర్లలో తిరగడం ద్వారా పొందవచ్చు. మీరు దీనిని ఉపయోగిస్తున్నప్పుడు కేబుల్ టీవీని చూడవచ్చు. ట్రాన్స్మిషన్ వేగాలు కేబుల్ మోడెమ్, కేబుల్ నెట్వర్క్ మరియు ట్రాఫిక్ లోడ్ల రకాన్ని బట్టి మారుతుంటాయి. వేగం DSL తో పోల్చవచ్చు.

Fiber (ఫైబర్)

Fiber optic technology converts electrical signals carrying data to light and sends the light through transparent glass fibers about the diameter of a human hair. Fiber transmits data at speeds far exceeding current DSL or cable modem speeds, typically by tens or even hundreds of Mbps.

The actual speed you experience will vary depending on a variety of factors, such as how close to your computer the service provider brings the fiber and how the service provider configures the service, including the amount of bandwidth used. The same fiber providing your broadband can also simultaneously deliver voice (VoIP) and video services, including video-on-demand.

ఫైబర్ ఆప్టిక్ టెక్నాలజీ డేటాను మోస్తున్న ఎలక్ట్రికల్ సిగ్నల్స్ వెలుగులోకి మారుస్తుంది మరియు మానవ జుట్టు యొక్క వ్యాసం గురించి పారదర్శక గాజు ఫైబర్స్ ద్వారా కాంతిని పంపుతుంది . ఫైబర్ ప్రస్తుత DSL లేదా కేబుల్ మోడెమ్ వేగం కంటే ఎక్కువ వేగంతో డేటాను బదిలీ చేస్తుంది , సాధారణంగా పదుల లేదా వందల Mbps ద్వారా. మీరు అందించే వాస్తవ వేగం వివిధ రకాలైన కారకాలపై ఆధారపడి మారుతుంది, సేవా ప్రదాత అందించే ఫైబర్ను మరియు సేవ ప్రొవైడర్ సేవను ఏ విధంగా బ్యాండ్విడ్త్తో సహా , కాన్ఫిగర్ చేస్తుందో మీ కంప్యూటర్కు దగ్గరగా ఉంటుంది . మీ బ్రాడ్బ్యాండ్ అందించే ఫైబర్ కూడా ఒకే సమయంలో వాయిస్ (VoIP) మరియు వీడియో సేవలను అందిస్తుంది, ఇందులో వీడియో-ఆన్-డిమాండ్ ఉంటుంది.

Telecommunications providers sometimes offer fiber broadband in limited areas and have announced plans to expand their fiber networks and offer bundled voice, Internet access, and video services.
టెలికమ్యూనికేషన్స్ ప్రొవైడర్లు కొన్నిసార్లు పరిమిత ప్రాంతాలలో ఫైబర్ బ్రాడ్బ్యాండ్ను అందిస్తారు మరియు వారి ఫైబర్ నెట్వర్క్లను విస్తరించడానికి మరియు కొట్టబడిన వాయిస్, ఇంటర్నెట్ యాక్సెస్ మరియు వీడియో సేవలను అందించే ప్రణాళికలను ప్రకటించారు.

Variations of the technology run the fiber all the way to the customer's home or business, to the curb outside, or to a location somewhere between the provider's facilities and the customer.
టెక్నాలజీ యొక్క వైవిధ్యాలు కస్టమర్ యొక్క ఇంటికి లేదా వ్యాపారంకు ఫైబర్ను బయటికి కలుపుతాయి, బయట కాలిబాటకు లేదా ఎక్కడో ప్రొవైడర్ యొక్క సౌకర్యాలు మరియు కస్టమర్ల మధ్య ఒక ప్రదేశానికి నడుస్తాయి.

Wireless (వైర్లెస్)

Wireless broadband connects a home or business to the Internet using a radio link between the customer's location and the service provider's facility. Wireless broadband can be mobile or fixed.
టెలికమ్యూనికేషన్స్ ప్రొవైడర్లు కొన్నిసార్లు పరిమిత ప్రాంతాలలో ఫైబర్ బ్రాడ్బ్యాండ్ను అందిస్తారు మరియు వారి ఫైబర్ నెట్వర్క్లను విస్తరించడానికి మరియు కొట్టబడిన వాయిస్, ఇంటర్నెట్ యాక్సెస్ మరియు వీడియో సేవలను అందించే ప్రణాళికలను ప్రకటించారు.

Wireless technologies using longer-range directional equipment provide broadband service in remote or sparsely populated areas where DSL or cable modem service would be costly to provide. Speeds are generally comparable to DSL and cable modem. An external antenna is usually required.
వైర్లెస్ టెక్నాలజీలు సుదూర లేదా తక్కువ జనాభా కలిగిన ప్రాంతాల్లో డిఎస్ఎల్ లేదా కేబుల్ మోడెమ్ సేవ అందించడానికి ఖరీదైనవిగా ఉండే అధిక-పరిధి డైరెక్షనల్ పరికరాలను బ్రాడ్బ్యాండ్ సేవలను అందిస్తాయి. వేగం DSL మరియు కేబుల్ మోడెమ్ కు సమానంగా ఉంటుంది. ఒక బాహ్య యాంటెన్నా సాధారణంగా అవసరం.

Wireless broadband Internet access services offered over fixed networks allow consumers to access the Internet from a fixed point while stationary and often require a direct line-of-sight between the wireless transmitter and receiver. These services have been offered using both licensed spectrum and unlicensed devices. For example, thousands of small Wireless Internet Services Providers (WISPs) provide such wireless broadband at speeds of around one Mbps using unlicensed devices, often in rural areas not served by cable or wire line broadband networks.

ఫిక్స్డ్ నెట్వర్క్లపై అందించే వైర్లెస్ బ్రాడ్బ్యాండ్ ఇంటర్నెట్ యాక్సెస్ సేవలు వినియోగదారులను ఇంటర్నెట్ను ఒక స్థిర బిందువు నుండి యాక్సెస్ చేయడానికి అనుమతిస్తుంది, అయితే స్టేషనరీ మరియు తరచూ వైర్లెస్ ట్రాన్స్మిటర్ మరియు రిసీవర్ మధ్య ప్రత్యక్ష లైన్-ఆఫ్-సైట్ అవసరమవుతుంది. ఈ సేవలు లైసెన్స్డ్ స్పెక్ట్రం మరియు లైసెన్స్ లేని పరికరాలను ఉపయోగించి అందివ్వబడ్డాయి. ఉదాహరణకు, వేలాది చిన్న వైర్లెస్ ఇంటర్నెట్ సర్వీసు ప్రొవైడర్స్ (WISP లు) ఒక వైర్లెస్ బ్రాడ్బ్యాండ్ ను ఒక Mbps చుట్టూ లైసెన్స్ లేని పరికరాలను ఉపయోగించి, కేబుల్ లేదా వైర్ లైన్ బ్రాడ్బ్యాండ్ నెట్వర్క్ ద్వారా గ్రామీణ ప్రాంతాలలో తరచుగా అందించబడతాయి.

Wireless Local Area Networks (WLANs) provide wireless broadband access over shorter distances and are often used to extend the reach of a "last-mile" Wireline or fixed wireless broadband connection within a home, building, or campus environment. Wi-Fi networks use unlicensed devices and can be designed for private access within a home or business, or be used for public Internet access at "hot spots" such as restaurants, coffee shops, hotels, airports, convention Centers, and city parks.
వైర్లెస్ లోకల్ ఏరియా నెట్వర్క్స్ (WLAN లు) తక్కువ దూరాలకు పైగా వైర్లెస్ బ్రాడ్బ్యాండ్ యాక్సెస్ను అందిస్తాయి మరియు గృహ, భవన లేదా క్యాంపస్ పర్యావరణంలో "చివరి-మైలు" వైర్లైన్ లేదా స్థిర వైర్లెస్ బ్రాడ్బ్యాండ్ కనెక్షన్ యొక్క విస్తరణకు తరచుగా ఉపయోగిస్తారు. Wi-Fi నెట్వర్క్లు లైసెన్స్ లేని పరికరాలను ఉపయోగిస్తాయి మరియు గృహాలు లేదా వ్యాపారం లోపల ప్రైవేట్ యాక్సెస్ కోసం రూపొందించబడతాయి లేదా రెస్టారెంట్లు, కాఫీ దుకాణాలు, హోటళ్ళు, విమానాశ్రయాలు, కన్వెన్షన్ సెంటర్స్ మరియు నగర

పార్కులు వంటి "హాట్ స్పాట్స్" వద్ద పబ్లిక్ ఇంటర్నెట్ యాక్సెస్ కోసం ఉపయోగించవచ్చు.

Mobile wireless broadband services are also becoming available from mobile telephone service providers and others. These services are generally appropriate for highly-mobile customers and require a special PC card with a built in antenna that plugs into a user's laptop computer. Generally, they provide lower speeds, in the range of several hundred Kbps.

మొబైల్ వైర్లెస్ బ్రాడ్బ్యాండ్ సేవలు మొబైల్ టెలిఫోన్ సర్వీసు ప్రొవైడర్లు మరియు ఇతరుల నుండి కూడా అందుబాటులోకి వచ్చాయి. ఈ సేవలు సాధారణంగా అధిక-మొబైల్ వినియోగదారులకి తగినవి మరియు ఒక ప్రత్యేక ల్యాప్టాప్ కంప్యూటర్లో ప్లగ్ ఇన్ చేసే యాంటెన్నాలో నిర్మించిన ప్రత్యేక PC కార్డ్ అవసరం. సాధారణంగా, వారు అనేక వందల Kbps పరిధిలో, తక్కువ వేగం అందిస్తాయి.

Satellite

ఉపగ్రహ

Just as satellites orbiting the earth provide necessary links for telephone and television service, they can also provide links for broadband. Satellite broadband is another form of wireless broadband, and is also useful for serving remote or sparsely populated areas.

భూమిని కక్ష్యలో ఉన్న ఉపగ్రహాలు టెలిఫోన్ మరియు టెలివిజన్ సర్వీసులకు అవసరమైన లింకులను అందిస్తాయి, వీరు బ్రాడ్బ్యాండ్కు లింక్లను కూడా అందిస్తారు. ఉపగ్రహ బ్రాడ్బ్యాండ్ వైర్లెస్ బ్రాడ్బ్యాండ్ యొక్క మరొక రూపం, మరియు రిమోట్ లేదా తక్కువ జనసాంద్రత గల ప్రాంతాల్లో పనిచేయడానికి కూడా ఉపయోగపడుతుంది .

Downstream and upstream speeds for satellite broadband depend on several factors, including the provider and service package purchased the consumer's line of sight to the orbiting satellite, and the weather. Typically a consumer can expect to receive (download) at a speed of about 500 Kbps and send (upload) at a speed of about 80 Kbps. These speeds may be slower than DSL and cable modem, but they are about 10 times faster than the download speed with dial-up Internet access. Service can be disrupted in extreme weather conditions.

శాటిలైట్ బ్రాడ్బ్యాండ్ కొరకు దిగువ మరియు దిగువ స్థాయి వేగం అనేక కారణాలపై ఆధారపడివుంటుంది, వీటిలో కొనుగోలుదారు మరియు సేవా ప్యాకేజీ, కన్స్యూమర్ యొక్క కక్ష్య కక్ష్య, మరియు వాతావరణం యొక్క కక్ష్య లైన్. సాధారణంగా వినియోగదారుడు సుమారు 500 Kbps వేగంతో (డౌన్ లోడ్ చేసుకోవచ్చు) మరియు 80 Kbps వేగంతో (అప్లోడ్) పంపవచ్చు. ఈ వేగం DSL మరియు కేబుల్ మోడెమ్ కన్నా నెమ్మదిగా ఉండవచ్చు, కానీ అవి డయల్-అప్ ఇంటర్నెట్ యాక్సెస్తో డౌన్లోడ్ వేగం కంటే 10 రెట్లు వేగంగా ఉంటాయి. విపరీతమైన వాతావరణ పరిస్థితుల్లో సేవను భంగపరచవచ్చు.

Broadband over Powerline (BPL)

BPL is the delivery of broadband over the existing low- and medium-voltage electric power distribution network. BPL speeds are comparable to DSL and cable modem speeds. BPL can be provided to homes using existing electrical connections and outlets. BPL is an emerging technology that is available in very limited areas. It has significant potential because power lines are installed virtually everywhere, alleviating the need to build new broadband facilities for every customer.

పవర్లైన్ పై బ్రాడ్బ్యాండ్ (BPL)

BPL అనేది ప్రస్తుతమున్న తక్కువ- మరియు మధ్యస్థ-వోల్టేజ్ ఎలెక్ట్రిక్ పవర్ ట్రాన్స్మిషన్ నెట్వర్క్పై బ్రాడ్బ్యాండ్ పంపిణీ. BPL వేగాలు DSL మరియు కేబుల్ మోడెమ్ వేగాలతో పోల్చవచ్చు. ఇప్పటికే ఉన్న విద్యుత్ కనెక్షన్లు మరియు అవుట్లెట్లను ఉపయోగించి గృహాలకు BPL ను ఇవ్వవచ్చు. BPL అనేది చాలా పరిమిత ప్రాంతాలలో లభించే సాంకేతిక

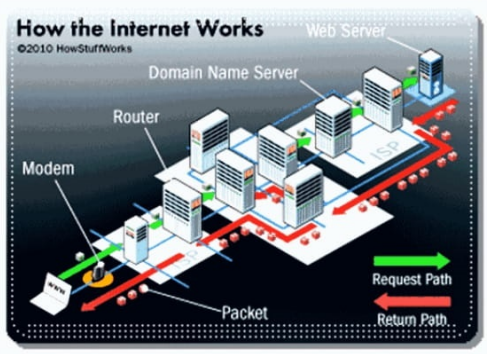
పరిజ్ఞానం. ప్రతి కస్టమర్లకు కొత్త బ్రాడ్బ్యాండ్ సౌకర్యాలను నిర్మించాల్సిన అవసరాన్ని తగ్గించడంతో, ప్రతిచోటా విద్యుత్తు పంక్తులు వ్యవస్థాపించబడుతుండటంతో ఇది గణనీయమైన శక్తిని కలిగి ఉంది.

Fiber BroadBand Some Internet Service Providers

ఫైబర్ బ్రాడ్బ్యాండ్ కొన్ని ఇంటర్నెట్ సర్వీస్ ప్రొవైడర్స్

ACT Fibernet, Bharat Fibernet, Airtel, Excitel, Fibertel, Hi Reach Broadband, Netrun Broadband, RVR Net, YOU Broadband, Airtel

ACT ఫిబెర్నెట్, భారత్ ఫిబెర్నెట్, ఎయిర్టెల్, ఎక్సిటెల్, ఫైబెర్టెల్, హాయ్ రీచ్ బ్రాడ్బ్యాండ్, నెట్రన్ బ్రాడ్బ్యాండ్, RVR నెట్, యు బ్రాడ్ బ్యాండ్, ఎయిర్టెల్



COMPUTERHARDWARE
కంప్యూటర్ హార్డ్వేర్)

Computer hardware is the physical and tangible components of a *computer*, such as the monitor, keyboard, *computer* data storage, graphic card, sound card and motherboard.

Examples of Hardware are the following –

కంప్యూటర్ హార్డ్వేర్ అనేది మానిటర్, కీబోర్డ్, కంప్యూటర్ డేటా నిల్వ, గ్రాఫిక్ కార్డు, సౌండ్ కార్డ్ మరియు మదర్బోర్డు వంటి కంప్యూటర్ యొక్క భౌతిక మరియు ప్రత్యక్ష భాగాలు.

హార్డువేర్కు ఉదాహరణలు క్రిందివి –

Input devices – keyboard, mouse, etc.
Output devices – printer, monitor, etc.
Secondary storage devices – Hard disk, CD, DVD, etc.
Internal components – CPU, motherboard, RAM, etc.

.

Computer – Generations
కంప్యూటర్ – తరాలు

Generation in computer terminology is a change in technology a computer is/was being used. Initially, the generation term was used to distinguish between varying hardware technologies. Nowadays, generation includes both hardware and software, which together make up an entire computer system.

కంప్యూటర్ పరిభాషలో తరం సాంకేతిక పరిజ్ఞానంలో ఒక మార్పు / ఉపయోగించబడుతోంది. ప్రారంభంలో, హార్డ్వేర్ టెక్నాలజీల మధ్య తేడాను గుర్తించడానికి తరం పదం ఉపయోగించబడింది. ఈ రోజుల్లో, తరం హార్డ్వేర్ మరియు సాఫ్ట్వేర్ రెండింటినీ కలిపి మొత్తం కంప్యూటర్ వ్యవస్థను తయారు చేస్తుంది.

There are five computer generations known till date. Each generation has been discussed in detail along with their time period and characteristics. In the following table, approximate dates against each generation has been mentioned, which are normally accepted.

తేదీ వరకు తెలిసిన ఐదు కంప్యూటర్ తరాల ఉన్నాయి. ప్రతి తరం వారి సమయ వ్యవధి మరియు లక్షణాలతో పాటు వివరంగా చర్చించబడింది. కింది పట్టికలో, ప్రతి తరానికి వ్యతిరేకంగా సుమారుగా పేర్కొన్న తేదీలు ప్రస్తావించబడ్డాయి, ఇవి సాధారణంగా ఆమోదించబడతాయి .

Following are the main five generations of computers.

కంప్యూటర్ల ప్రధాన ఐదు తరాల తర్వాత ఇవి అనుసరిస్తాయి.

S.No	Generation & Description
1	First Generation The period of first generation: 1946-1959. Vacuum tube based. మొదటి తరం మొదటి తరం కాలం: 1946-1959. వాక్యూమ్ ట్యూబ్ ఆధారిత.
2	Second Generation The period of second generation: 1959-1965. Transistor based. రెండవ తరం రెండవ తరం కాలం: 1959-1965. ట్రాన్సిస్టర్ ఆధారిత.
3	Third Generation The period of third generation: 1965-1971. Integrated Circuit based. మూడవ తరం మూడవ తరం కాలం: 1965-1971. ఇంటిగ్రేటెడ్ సర్క్యూట్ ఆధారిత.
4	Fourth Generation The period of fourth generation: 1971-1980. VLSI microprocessor based. నాల్గవ తరం నాల్గవ తరపు కాలం: 1971-1980. VLSI మైక్రోప్రాసెసర్ ఆధారిత.
5	Fifth Generation The period of fifth generation: 1980-onwards. ULSI microprocessor based. ఐదవ తరం ఐదవ తరం యొక్క కాలం: 1980-ప్రారంభంలో. ULSI మైక్రోప్రాసెసర్ ఆధారిత.

Computer - Types

Computers can be broadly classified by their speed and computing power.

కంప్యూటర్లు వారి వేగం మరియు కంప్యూటింగ్ శక్తి ద్వారా విస్తృతంగా వర్గీకరించబడతాయి.

S.No	Type	Specifications
	PC (Personal Computer)	It is a single user computer system having moderately powerful microprocess ఇది ఒక ఏకైక కంప్యూటర్ వ్యవస్థ శక్తివంతమైన మైక్రోప్రాసెస
	Workstation	It is also a single user computer system, similar to personal computer however has a more powerful microprocessor. ఇది ఒక యూజర్ కంప్యూటర్ వ్యవస్థ, వ్యక్తిగత పోలి కంప్యూటర్లో మరింత శక్తివంతమైన మైక్రోప్రాసెసర్ ఉంది.
	Mini Computer	It is a multi-user computer system, capable of supporting hundreds of users simultaneously. ఇది బహుళ-వినియోగదారు కంప్యూటర్ వ్యవస్థ, ఇది మద్దతునిచ్చే సామర్థ్యం వందలాది వినియోగదారులు ఒకేసారి.
	Main Frame	It is a multi-user computer system, capable of supporting hundreds of users simultaneously. Software technology is different from minicomputer. ఇది బహుళ-వినియోగదారు కంప్యూటర్ వ్యవస్థ, ఇది మద్దతునిచ్చే సామర్థ్యం వందలాది వినియోగదారులు ఒకేసారి. సాఫ్ట్వేర్ టెక్నాలజీ మినికోమ్ప్యూటర్ నుండి భిన్నంగా ఉంటుంది.
	Supercomputer	It is an extremely fast computer, which can execute hundreds of millions of instructions per second. ఇది అత్యంత వేగవంతమైన కంప్యూటర్, ఇది అమలు చేయగలదు వందల మిలియన్ల సూచనలను సెకనుకు.

Input Unit

This unit contains devices with the help of which we enter data into the computer. This unit creates a link between the user and the computer. The input devices translate the information into a form understandable by the computer.

ఈ యూనిట్ మేము కంప్యూటర్లోకి డేటాను నమోదు చేసే సహాయంతో పరికరాలను కలిగి ఉంటుంది. ఈ యూనిట్ యూజర్ మరియు కంప్యూటర్ మధ్య లింక్ను సృష్టిస్తుంది. ఇన్పుట్ పరికరాలు కంప్యూటర్ ద్వారా సమాచారాన్ని అర్థమయ్యేలా ఒక రూపంలోకి అనువదిస్తాయి.

CPU (Central Processing Unit)

CPU (సెంట్రల్ ప్రాసెసింగ్ యూనిట్)

CPU is considered as the brain of the computer. CPU performs all types of data processing operations. It stores data, intermediate results, and instructions (program). It controls the operation of all parts of the computer.

CPU కంప్యూటర్ యొక్క మెదడుగా పరిగణించబడుతుంది. అన్ని రకాల డేటా ప్రాసెసింగ్ కార్యకలాపాలను CPU నిర్వహిస్తుంది. ఇది డేటా, ఇంటర్మీడియట్ ఫలితాలు మరియు సూచనలను (ప్రోగ్రామ్) నిల్వ చేస్తుంది. ఇది కంప్యూటర్ యొక్క అన్ని భాగాల ఆపరేషన్ను నియంత్రిస్తుంది.

CPU itself has the following three components –
CPU కి కూడా ఈ క్రింది మూడు భాగాలుంటాయి

- ALU (Arithmetic Logic Unit)
- Memory Unit
- Control Unit

Output Unit
అవుట్ పుట్

యూనిట్

The output unit consists of devices with the help of which we get the information from the computer. This unit is a link between the computer and the users. Output devices translate the computer's output into a form understandable by the users.
అవుట్పుట్ విభాగంలో కంప్యూటర్ నుండి సమాచారాన్ని మేము పొందుతున్న సహాయంతో ఉంటుంది. ఈ యూనిట్ కంప్యూటర్ మరియు వినియోగదారుల మధ్య ఒక లింక్. అవుట్పుట్ పరికరములు కంప్యూటరు అవుట్పుట్ వినియోగదారులకు అర్థమయ్యేలా ఒక రూపంలోకి అనువదిస్తాయి.

Central Processing Unit (CPU) consists of the following features –
సెంట్రల్ ప్రాసెసింగ్ యూనిట్ (CPU) క్రింది వాటిని కలిగి ఉంటుంది

- CPU is considered as the brain of the computer.
- CPU కంప్యూటర్ యొక్క మెదడుగా పరిగణించబడుతుంది .
- CPU performs all types of data processing operations.
- అన్ని రకాల డేటా ప్రాసెసింగ్ కార్యకలాపాలను CPU నిర్వహిస్తుంది .
- It stores data, intermediate results, and instructions (program).
- అన్ని రకాల డేటా ప్రాసెసింగ్ కార్యకలాపాలను CPU నిర్వహిస్తుంది.
- It controls the operation of all parts of the computer.
- ఇది కంప్యూటర్ యొక్క అన్ని భాగాల ఆపరేషన్ను నియంత్రిస్తుంది .
- CPU itself has following three components.
- CPU కూడా మూడు భాగాలను అనుసరిస్తోంది .
- Memory or Storage Unit
- Control Unit
- ALU(Arithmetic Logic Unit)

Memory or Storage Unit
మెమరీ లేదా నిల్వ యూనిట్

This unit can store instructions, data, and intermediate results. This unit supplies information to other units of the computer when needed. It is also known as internal storage unit or the main memory or the primary storage or Random Access Memory (RAM).

ఈ యూనిట్ సూచనలు, డేటా మరియు ఇంటర్మీడియట్ ఫలితాలు నిల్వ చేయవచ్చు. అవసరమైతే ఈ యూనిట్ కంప్యూటర్ యొక్క యూనిట్లకు సమాచారాన్ని అందిస్తుంది. ఇది అంతర్గత నిల్వ యూనిట్ లేదా ప్రధాన మెమరీ లేదా ప్రాథమిక నిల్వ లేదా రాండమ్ యాక్సెస్ మెమరీ (RAM) గా కూడా పిలువబడుతుంది .

Its size affects speed, power, and capability. Primary memory and secondary memory are two types of memories in the computer. Functions of the memory unit are −

దీని పరిమాణం వేగం, శక్తి మరియు సామర్థ్యంపై ప్రభావం చూపుతుంది. ప్రాథమిక మెమరీ మరియు ద్వితీయ స్మృతి కంప్యూటర్లో రెండు రకాల జ్ఞాపకాలు. మెమరీ యూనిట్ విధులు -

- It stores all the data and the instructions required for processing.
- ఇది అన్ని డేటా మరియు ప్రాసెసింగ్ కోసం అవసరమైన సూచనలను నిల్వ చేస్తుంది .
- It stores intermediate results of processing.
- ఇది ప్రాసెస్ యొక్క ఇంటర్మీడియట్ ఫలితాలను నిల్వ చేస్తుంది .
- It stores the final results of processing before these results are released to an output device.
- ఈ ఫలితాలను అవుట్పుట్ పరికరానికి విడుదల చేయడానికి ముందు ప్రాసెసింగ్ తుది ఫలితాలను ఇది నిల్వ చేస్తుంది .
- All inputs and outputs are transmitted through the main memory.
- అన్ని ఇన్పుట్లను మరియు అవుట్పుట్లను ప్రధాన మెమరీ ద్వారా బదిలీ చేయబడతాయి .

Control Unit

This unit controls the operations of all parts of the computer but does not carry out any actual data processing operations.

ఈ యూనిట్ కంప్యూటర్ యొక్క అన్ని భాగాల కార్యకలాపాలను నియంత్రిస్తుంది కానీ అసలు డేటా ప్రాసెసింగ్ కార్యకలాపాలను అమలు చేయదు .

Functions of this unit are −

- It is responsible for controlling the transfer of data and instructions among other units of a computer.
- కంప్యూటర్ యొక్క ఇతర విభాగాల మధ్య డేటా మరియు సూచనలను బదిలీ చేయడానికి ఇది బాధ్యత వహిస్తుంది.
- It manages and coordinates all the units of the computer.
- ఇది కంప్యూటర్ యొక్క అన్ని యూనిట్లను నిర్వహిస్తుంది మరియు సమన్వయపరుస్తుంది.
- It obtains the instructions from the memory, interprets them, and directs the operation of the computer.
- ఇది మెమరీ నుండి సూచనలను పొందుతుంది, వాటిని వివరించేది మరియు కంప్యూటర్ యొక్క ఆపరేషన్ను నిర్దేశిస్తుంది.
- It communicates with Input/Output devices for transfer of data or results from storage.
- డేటాను బదిలీ చేయడానికి లేదా ఇన్పుట్ / అవుట్పుట్ పరికరాలతో సమాచార మార్పిడికి లేదా ఫలితాల నుండి సమాచార మార్పిడి.
- It does not process or store data.
- ఇది డేటాను ప్రాసెస్ చేయదు లేదా నిల్వ చేయదు.

ALU (Arithmetic Logic Unit)
ALU (అర్థమెటిక్ లాజిక్ యూనిట్)

This unit consists of two subsections namely,
ఈ విభాగంలో రెండు ఉపవిభాగాలు ఉన్నాయి

- Arithmetic Section
- Logic Section

Arithmetic Section

Function of arithmetic section is to perform arithmetic operations like addition, subtraction, multiplication, and division. All complex operations are done by making repetitive use of the above operations.
గణిత విభాగం ఫంక్షన్ అదనంగా, తీసివేత, గుణకారం మరియు విభజన వంటి అంకగణిత చర్యలను నిర్వహించడం. పైన ఆపరేషన్ల పునరావృత ఉపయోగం ద్వారా అన్ని క్లిష్టమైన కార్యకలాపాలు జరుగుతాయి.

Logic Section

Function of logic section is to perform logic operations such as comparing, selecting, matching, and merging of data.
లాజికల్ విభాగం యొక్క ఫంక్షన్, డేటాను పోల్చడం, ఎంచుకోవడం, సరిపోల్చడం మరియు విలీనం చేయడం వంటి లాజిక్ చర్యలను నిర్వహించడం.

Following are some of the important input devices which are used in a computer

కంప్యూటర్లో ఉపయోగించిన కొన్ని ముఖ్యమైన ఇన్పుట్ పరికరాలను అనుసరిస్తున్నారు
Keyboard, Mouse, Joy Stick, Light pen, Track Ball, Scanner, Graphic Tablet, Microphone

కీబోర్డు, మౌస్, జాయ్ స్టిక్, లైట్ పెన్, ట్రాక్ బాల్, స్కానర్, గ్రాఫిక్ టాబ్లెట్, మైక్రోఫోన్ Magnetic Ink Card

Reader(MICR), Optical Character Reader(OCR), Bar Code Reader Optical Mark

కంప్యూటర్లో కీబోర్డు, మౌస్, జాయ్ స్టిక్, లైట్ పెన్, ట్రాక్ బాల్, స్కానర్, గ్రాఫిక్ టాబ్లెట్, మైక్రోఫోన్ మాగ్నటిక్ ఇంక్ కార్డ్ రీడర్ (MICR), ఆప్టికల్ క్యారెక్టర్ రీడర్ (OCR), బార్ కోడ్ రీడర్ ఆప్టికల్ మార్క్ రీడర్ (OMR)

Following are some of the important output devices used in a computer.
కంప్యూటర్లో ఉపయోగించిన కొన్ని ముఖ్యమైన అవుట్పుట్ పరికరాలను అనుసరిస్తున్నారు.

- Monitors (మానిటర్లు)
- Graphic Plotter(• గ్రాఫిక్ ప్లాటర్)
- Printer(• ప్రింటర్)

A memory is just like a human brain. It is used to store data and instructions. Computer memory is the storage space in the computer, where data is to be processed and instructions required for processing are stored. The memory is divided into large number of small parts called cells. Each location or cell has a

unique address, which varies from zero to memory size minus one. For example, if the computer has 64k words, then this memory unit has 64 * 1024 = 65536 memory locations. The address of these locations varies from 0 to 65535.

ఒక మెమరీ కేవలం మానవ మెదడు వంటిది. డేటా మరియు సూచనలను నిల్వ చేయడానికి ఇది ఉపయోగించబడుతుంది. కంప్యూటర్ మెమరీ డేటా నిల్వ ప్రాసెస్ మరియు ప్రాసెసింగ్ కోసం అవసరమైన సూచనలను నిల్వ ఉన్న కంప్యూటర్లో నిల్వ స్థలం. ఈ కణాలు పెద్ద సంఖ్యలో చిన్న భాగాలు అని పిలువబడతాయి. ప్రతి ప్రదేశం లేదా సెల్కు ప్రత్యేకమైన చిరునామా ఉంటుంది, ఇది సున్నా నుంచి మెమరీ పరిమాణం మైనస్ ఒకటి వరకు ఉంటుంది. ఉదాహరణకు, కంప్యూటర్ 64k పదాలను కలిగి ఉంటే, అప్పుడు ఈ మెమరీ యూనిట్ 64 * 1024 = 65536 మెమొరీ స్థానాలను కలిగి ఉంది. ఈ స్థానాల చిరునామా 0 నుండి 65535 వరకు ఉంటుంది.

Memory is primarily of three types –
మెమరీ ప్రధానంగా మూడు రకాలు

- Cache Memory
- Primary Memory/Main Memory
- కాష్ మెమరీ
- ప్రాథమిక మెమరీ / మెయిన్ మెమరీ
- Secondary Memory
- సెకండరీ మెమరీ

- Cache Memory (కాష్ మెమరీ)

Cache memory is a very high speed semiconductor memory which can speed up the CPU. It acts as a buffer between the CPU and the main memory. It is used to hold those parts of data and program which are most frequently used by the CPU. The parts of data and programs are transferred from the disk to cache memory by the operating system, from where the CPU can access them.

కాష్ మెమరీ Cache మెమరీ అనేది CPU ను వేగవంతం చేయగల చాలా వేగవంతమైన సెమీకండక్టర్ మెమరీ. ఇది CPU మరియు ప్రధాన మెమరీ మధ్య బఫర్గా పనిచేస్తుంది. ఇది చాలా తరచుగా CPU చేత ఉపయోగించబడే డేటా మరియు ప్రోగ్రామ్ యొక్క ఆ భాగాలను కలిగి ఉంచుతుంది. డేటా మరియు ప్రోగ్రామ్ల భాగాలు డిస్క్ నుండి ఆపరేటింగ్ సిస్టమ్ ద్వారా మెమరీని కాష్కు బదిలీ చేస్తాయి, ఇక్కడ CPU వాటిని ప్రాప్తి చేయగలదు.

Advantages (ప్రయోజనాలు)

The advantages of cache memory are as follows –
ప్రయోజనాలు కాష్ మెమరీ ప్రయోజనాలు క్రింది విధంగా ఉన్నాయి

- Cache memory is faster than main memory.
- ప్రధాన మెమరీ కంటే క్యాషీ మెమరీ వేగంగా ఉంటుంది. వినియోగిస్తుంది.
- It consumes less access time as compared to main memory.
- ప్రధాన మెమరీతో పోలిస్తే ఇది తక్కువ ప్రాప్యత సమయాన్ని
- It stores the program that can be executed within a short period of time.
- ఇది కొంతకాలం వ్యవధిలో అమలు చేయగల కార్యక్రమంను నిల్వ చేస్తుంది
- It stores data for temporary use.

. • ఇది తాత్కాలిక ఉపయోగం కోసం డేటాను నిల్వ చేస్తుంది.

Disadvantages (ప్రతికూలతలు)

The disadvantages of cache memory are as follows −
ప్రతికూలతలు కచేరి మెమరీ యొక్క ప్రతికూలతలు క్రింది విధంగా ఉన్నాయి −

- Cache memory has limited capacity.
- కాష్ మెమరీ పరిమిత సామర్థ్యం ఉంది.
- It is very expensive.
- ఇది చాలా ఖరీదైనది.

Primary Memory (Main Memory)
ప్రాథమిక మెమరీ (ప్రధాన మెమరీ)

Memory is primarily of three types −
మెమరీ ప్రధానంగా మూడు రకాలు −

- Cache Memory(కాష్ మెమరీ)
- Primary Memory/Main Memory
- ప్రాథమిక మెమరీ / మెయిన్ మెమరీ
- Secondary Memory (• **సెకండరీ మెమరీ)**

Computer-Memory

కంప్యూటర్ - మెమరీ

Primary memory holds only those data and instructions on which the computer is currently working. It has a limited capacity and data is lost when power is switched off. It is generally made up of semiconductor device. These memories are not as fast as registers. The data and instruction required to be processed resides in the main memory. It is divided into two subcategories RAM and ROM.

ప్రాథమిక స్మృతి కంప్యూటర్ మరియు ప్రస్తుతం పని చేస్తున్న ఆ సమాచారాన్ని మాత్రమే కలిగి ఉంటుంది. ఇది పరిమిత సామర్థ్యం కలిగి ఉంటుంది మరియు శక్తి స్విచ్ ఆఫ్ చేసినప్పుడు డేటా కోల్పోతుంది. ఇది సాధారణంగా సెమీకండక్టర్ పరికరంతో రూపొందించబడింది. ఈ జ్ఞాపకాలు రిజిస్టర్లలో అంత వేగంగా లేవు. ప్రాసెస్ చేయడానికి అవసరమైన డేటా మరియు సూచన ప్రధాన మెమరీలో ఉంటుంది. ఇది రెండు ఉపవర్గాలు RAM మరియు ROM గా విభజించబడింది.

Characteristics of Main Memory
ప్రధాన మెమరీ యొక్క లక్షణాలు

- These are semiconductor memories. (ఈ సెమీకండక్టర్ జ్ఞాపకాలు).
- It is known as the main memory. (ఇది ప్రధాన స్మృతిగా పిలువబడుతుంది.)
- Usually volatile memory. (సాధారణంగా అస్థిర మెమరీ.)
- Data is lost in case power is switched off (పవర్ ఆఫ్ స్విచ్ అయినప్పుడు డేటా కోల్పోతుంది.)
- It is the working memory of the computer. (ఇది కంప్యూటర్ యొక్క పని జ్ఞాపకం.)
- Faster than secondary memories. (ద్వితీయ జ్ఞాపకాలను కంటే వేగంగా.)
- A computer cannot run without the primary memory.(ఒక కంప్యూటర్ ప్రాథమిక మెమరీ లేకుండా అమలు కాదు.

Secondary Memory
సెకండరీ మెమరీ)

This type of memory is also known as external memory or non-volatile. It is slower than the main memory. These are used for storing data/information permanently. CPU directly does not access these memories; instead they are accessed via input-output routines. The contents of secondary memories are

first transferred to the main memory, and then the CPU can access it. For example, disk, CD-ROM, DVD, etc.

ఈ రకమైన మెమరీ బాహ్య మెమరీ లేదా అస్థిరత అని కూడా పిలుస్తారు. ఇది ప్రధాన మెమరీ కంటే నెమ్మదిగా ఉంటుంది. ఈ డేటా / సమాచారం నిల్వ కోసం శాశ్వతంగా నిల్వ చేయడానికి ఉపయోగిస్తారు. CPU నేరుగా ఈ జ్ఞాపకాలను యాక్సెస్ చేయదు, బదులుగా అవి ఇన్పుట్-అవుట్పుట్ నిత్యప్రయాణాల ద్వారా ప్రాప్తి చేయబడతాయి. సెకండరీ జ్ఞాపకాలను ఉన్న విషయాలు మొదటి ప్రధాన మెమరీకి బదిలీ చేయబడి, ఆపై CPU దీన్ని ప్రాప్తి చేయగలదు. ఉదాహరణకు, డిస్క్, CD-ROM, DVD, మొదలైనవి.

Characteristics of Secondary Memory
సెకండరీ మెమరీ లక్షణాలు

- These are magnetic and optical memories. (ఇవి అయస్కాంత మరియు ఆప్టికల్ జ్ఞాపకాలు.)
- It is known as the backup memory. (ఇది బ్యాకప్ మెమరీ అని పిలుస్తారు.)
- It is a non-volatile memory.(ఇది అస్థిర జ్ఞాపకం)
- Data is permanently stored even if power is switched off (పవర్ ఆఫ్ స్విచ్ అయినప్పటికీ డేటా శాశ్వతంగా నిల్వ చేయబడుతుంది.)
- It is used for storage of data in a computer.(కంప్యూటర్లో డేటాను నిల్వ చేయడానికి ఇది ఉపయోగించబడుతుంది.)
- Computer may run without the secondary memory.(ద్వితీయ స్మృతి లేకుండా కంప్యూటర్ అమలు కావచ్చు.)
- Slower than primary memories.(ప్రాధమిక జ్ఞాపకాలను కంటే నెమ్మదిగా)

Random Access Memory
రాండమ్ యాక్సెస్ మెమరీ

RAM (Random Access Memory) is the internal memory of the CPU for storing data, program, and program result. It is a read/write memory which stores data until the machine is working. As soon as the machine is switched off, data is erased.

RAM (రాండమ్ యాక్సెస్ మెమరీ) అనేది డేటా, ప్రోగ్రామ్, మరియు ప్రోగ్రామ్ ఫలితాల నిల్వ కోసం CPU యొక్క అంతర్గత మెమరీ. యంత్రం పనిచేసే వరకు డేటాను నిల్వచేసే ఒక చదివే / వ్రాసే మెమరీ. యంత్రం స్విచ్ ఆఫ్ అయిన వెంటనే, డేటా తొలగించబడుతుంది.

Access time in RAM is independent of the address, that is, each storage location inside the memory is as easy to reach as other locations and takes the same amount of time. Data in the RAM can be accessed randomly but it is very expensive.

RAM లో ప్రాప్యత సమయం చిరునామాకు స్వతంత్రం, అనగా మెమరీలోని ప్రతి నిల్వ స్థానం ఇతర ప్రాంతాలకు చేరుకోవడానికి చాలా సులభం మరియు అదే సమయాన్ని తీసుకుంటుంది. RAM లో డేటా యాదృచ్ఛికంగా ప్రాప్తి చేయవచ్చు కానీ చాలా ఖరీదైనది .

RAM is volatile, i.e. data stored in it is lost when we switch off the computer or if there is a power failure. Hence, a backup Uninterruptible Power System (UPS) is often used with computers. RAM is small, both in terms of its physical size and in the amount of data it can hold.

RAM అస్థిరమయినది, అనగా మనము కంప్యూటర్ను ఆపివేసినప్పుడు లేదా శక్తి వైఫల్యం ఉన్నట్లయితే అది నిల్వవున్న సమాచారం కోల్పోతుంది. అందువల్ల, ఒక బ్యాకప్ నిరంతర శక్తి వ్యవస్థ (UPS) తరచుగా కంప్యూటర్లతో ఉపయోగిస్తారు. RAM దాని భౌతిక పరిమాణం పరంగా మరియు అది పట్టుకోగల డాటా మొత్తంలో, చిన్నది.

RAM is of two types –
RAM రెండు రకాలు -

- Static RAM (SRAM) • (స్టాటిక్ RAM (SRAM))
- Dynamic RAM (DRAM)(డైనమిక్ RAM (DR)AM)

The word static indicates that the memory retains its contents as long as power is being supplied. However, data is lost when the power gets down due to volatile nature. SRAM chips use a matrix of 6-transistors and no capacitors. Transistors do not require power to prevent leakage, so SRAM need not be refreshed on a regular basis.

స్టాటిక్ పదం శక్తి సరఫరా చేయబడుతున్నంతకాలం మెమరీ దాని కంటెంట్లను కలిగి ఉందని సూచిస్తుంది . అయినప్పటికీ, అస్థిర

స్వభావం కారణంగా శక్తి తగ్గిపోయినప్పుడు డేటా కోల్పోతుంది . SRAM చిప్లు 6 ట్రాన్సిస్టర్లు మరియు ఏ కెపాసిటర్లు మాత్రికను ఉపయోగిస్తాయి. ట్రాన్సిస్టర్లు లీకేజ్ను నివారించడానికి అధికారం అవసరం లేదు, కాబట్టి SRAM నిరంతరం రిఫ్రెష్ చేయరాదు.

There is extra space in the matrix, hence SRAM uses more chips than DRAM for the same amount of storage space, making the manufacturing costs higher. SRAM is thus used as cache memory and has very fast access.

మాత్రికలో అదనపు ఖాళీ ఉంది, అందువల్ల SRAM అదే స్థలంలో నిల్వ స్థలంలో DRAM కంటే ఎక్కువ చిప్లను ఉపయోగిస్తుంది, దీనితో తయారీ ఖర్చు ఎక్కువగా ఉంటుంది. అందువలన SRAM క్యాషీ మెమరీగా వాడబడుతుంది మరియు చాలా వేగవంతమైన ప్రాప్యతను కలిగి ఉంది.

Characteristic of Static RAM

స్టాటిక్ RAM యొక్క లక్షణం

- Long life(చిరకాలం)
- No need to refresh (రిఫ్రెష్ అవసరం లేదు)
- Faster(వేగంగా)
- Used as cache memory(కాష్ మెమరీ వలె ఉపయోగిస్తారు)
- Large size(పెద్ద పరిమాణం)
- Expensive(ఖరీదైన)
- High power consumption(అధిక శక్తి వినియోగం)
- Dynamic RAM (DRAM)(డైనమిక్ RAM (DRAM)

RAM, unlike SRAM, must be continually refreshed in order to maintain the data. This is done by placing the memory on a refresh circuit that rewrites the data several hundred times per second. DRAM is used for most system memory as it is cheap and small. All DRAMs are made up of memory cells, which are composed of one capacitor and one transistor.

SRAM కాకుండా, డేటాను నిర్వహించడానికి నిరంతరం రిఫ్రెష్ చేయాలి. ఇది ఒక రిఫ్రెష్ సర్క్యూట్లో మెమరీని ఉంచడం ద్వారా జరుగుతుంది, ఇది సెకనుకు అనేక వందల సార్లు డేటాను తిరిగి వ్రాస్తుంది. చాలా తక్కువగా మెమరీ మెమరీ కోసం DRAM ఉపయోగించబడుతుంది, ఎందుకంటే అది చౌకగా మరియు చిన్నదిగా ఉంటుంది. అన్ని D RAM లు మెమొరీ సెల్స్తో తయారు చేయబడతాయి, ఇవి ఒక కెపాసిటర్ మరియు ఒక ట్రాన్సిస్టర్తో కూడి ఉంటాయి.

Characteristics of Dynamic RAM

డైనమిక్ RAM యొక్క లక్షణాలు

- Short data lifetime(చిన్న డేటా జీవితకాలం)
- Needs to be refreshed continuously(నిరంతరంగా రిఫ్రెష్ చేయవలసిన అవసరం ఉంది)
- Slower as compared to SRAM(SRAM పోలిస్తే నెమ్మదిగా)
- Used as RAM(RAM గా ఉపయోగించబడుతుంది)
- Smaller in size(పరిమాణంలో చిన్నది)
- Less expensive(తక్కువ ఖరీదైన)

- Less power consumption(తక్కువ విద్యుత్ వినియోగం)

Read Only Memory (మెమరీని మాత్రమే చదవండి)

ROM stands for Read Only Memory. The memory from which we can only read but cannot write on it. This type of memory is non-volatile. The information is stored permanently in such memories during manufacture. A ROM stores such instructions that are required to start a computer. This operation is referred to as bootstrap. ROM chips are not only used in the computer but also in other electronic items like washing machine and microwave oven.

ROM చదవడానికి మాత్రమే మెమరీ. మనము చదివిన జ్ఞాపకము మాత్రమే దానిలో రాయలేదు. ఈ రకమైన జ్ఞాపకశక్తి అస్థిరత. సమాచారం తయారీ సమయంలో ఇటువంటి జ్ఞాపకాలలో శాశ్వతంగా నిల్వ చేయబడుతుంది. ఒక కంప్యూటర్ను ప్రారంభించడానికి అవసరమైన సూచనలను ఒక ROM నిల్వ చేస్తుంది. ఈ ఆపరేషన్ను బూట్స్ట్రాప్గా సూచిస్తారు. ROM చిప్స్ కంప్యూటర్లో మరియు వాషింగ్ మెషీన్ మరియు మైక్రోవేవ్ ఓవెన్ వంటి ఇతర ఎలక్ట్రానిక్ వస్తువులలో మాత్రమే ఉపయోగించబడవు.

Let us now discuss the various types of ROMs and their characteristics.
ఇప్పుడు వివిధ రకాలైన ROM లు మరియు వారి లక్షణాలు గురించి చర్చించండి.

MROM (Masked ROM)

The very first ROMs were hard-wired devices that contained a pre-programmed set of data or instructions. These kind of ROMs are known as masked ROMs, which are inexpensive.
మొట్టమొదటి ROM లు హార్డ్-వైర్డు పరికరాలను కలిగి ఉన్నాయి, ఇవి ముందుగా ప్రోగ్రామ్ చేయబడిన డేటా లేదా సూచనలు కలిగి ఉన్నాయి. ఈ విధమైన ROM లు మాస్క్డ్ ROM లుగా పిలువబడతాయి, ఇవి చవకైనవి.

PROM (Programmable Read Only Memory)

PROM (ప్రోగ్రామబుల్ రీడ్ ఓన్లీ మెమరీ)

PROM is read-only memory that can be modified only once by a user. The user buys a blank PROM and enters the desired contents using a PROM program. Inside the PROM chip, there are small fuses which are burnt open during programming. It can be programmed only once and is not erasable.

PROM రీడ్-ఓన్లీ మెమొరీ మాత్రమే వినియోగదారుడు ఒకసారి మాత్రమే సవరించబడుతుంది. వినియోగదారు PROM కార్యక్రమంని ఉపయోగించి ఖాళీ PROM ను కొనుగోలు చేసి కావలసిన కంటెంట్లను ప్రవేశిస్తాడు. PROM చిప్ లోపల, ప్రోగ్రామింగ్ సమయంలో తెరిచిన చిన్న ఫ్యూజులు ఉన్నాయి. ఇది ఒక్కసారి మాత్రమే ప్రోగ్రామ్ చేయబడుతుంది మరియు తొలగించబడదు .

EPROM (Erasable and Programmable Read Only Memory)

EPROM (Erasable మరియు ప్రోగ్రామబుల్ రీడ్ ఓన్లీ మెమరీ)

EPROM can be erased by exposing it to ultra-violet light for duration of up to 40 minutes. Usually, an EPROM eraser achieves this function. During programming, an electrical charge is trapped in an insulated gate region. The charge is retained for more than 10 years because the charge has no leakage path. For erasing this charge, ultra-violet light is passed through a quartz crystal window (lid). This exposure to ultra-violet light dissipates the charge. During normal use, the quartz lid is sealed with a sticker.

EPROM ను 40 నిమిషాల పాటు అల్ట్రా-వైలెట్ లైట్కు వెల్లడించడం ద్వారా తొలగించవచ్చు. సాధారణంగా, ఒక EPROM eraser ఈ ఫంక్షన్

సాధిస్తుంది. ప్రోగ్రామింగ్ సమయంలో, ఒక విద్యుత్ ఛార్జ్ ఒక ఇన్సులేట్ గేట్ ప్రాంతంలో చిక్కుకున్న. చార్జ్ ఏ లీకేజ్ మార్గం లేదు ఎందుకంటే ఛార్జ్ కంటే ఎక్కువ 10 సంవత్సరాలు నిలుపుకుంది. ఈ ఛార్జ్ను తొలగించడం కోసం, ఆల్ట్రా-వైలెట్ కాంతిని క్వార్ట్జ్ క్రిస్టల్ విండో (మూత) ద్వారా పంపబడుతుంది. అల్ట్రా-వైలెట్ కాంతిని ఈ ఎక్స్పోజర్ ఛార్జ్ వెదజల్లుతుంది. సాధారణ ఉపయోగంలో, క్వార్ట్జ్ మూత స్టికర్తో మూసివేయబడుతుంది.

(Electrically Erasable and Programmable Read Only Memory)

EEPROM (ఎలెక్ట్రాసిబుల్ ఎర్రబుల్ మరియు ప్రోగ్రామబుల్ రీడ్ ఓన్లీ మెమరీ)

EEPROM is programmed and erased electrically. It can be erased and reprogrammed about ten thousand times. Both erasing and programming take about 4 to 10 ms (millisecond). In EEPROM, any location can be selectively erased and programmed. EEPROMs can be erased one byte at a time, rather than erasing the entire chip. Hence, the process of reprogramming is flexible but slow.

EEPROM ప్రోగ్రాం మరియు విద్యుత్పరంగా తొలగించబడుతుంది. ఇది పదివేల సార్లు తొలగించి, పునఃప్రారంభించబడుతుంది. రెండు వేయడం మరియు ప్రోగ్రామింగ్ 4 నుండి 10 ms (మిల్లీసెకను) పడుతుంది. EEPROM లో, ఏ స్థానానికైనా ఎన్నుకోవచ్చు మరియు ప్రోగ్రామ్ చేయబడుతుంది. EEPROM లు మొత్తం చిప్ను తొలగించడం కంటే ఒక సమయంలో ఒక బైట్ను తొలగించగలవు. కాబట్టి, reprogramming ప్రక్రియ అనువైన కానీ నెమ్మదిగా ఉంటుంది .

Advantages of ROM (ROM యొక్క ప్రయోజనాలు)

The advantages of ROM are as follows – ROM **యొక్క ప్రయోజనాలు క్రింది విధంగా ఉన్నాయి**

- Non-volatile in nature(ప్రకృతిలో అస్థిరత)
- Cannot be accidentally changed
- అనుకోకుండా మార్చబడలేదు
- Cheaper than RAMs
- RAMs కంటే చౌక
- Easy to test
- సులువు పరీక్షించడానికి
- More reliable than RAMs
- RAMs కంటే ఎక్కువ నమ్మదగిన
- Static and do not require refreshing
- స్టాటిక్ మరియు రిఫ్రెష్ అవసరం లేదు
- Contents are always known and can be verified
- విషయాలు ఎల్లప్పుడూ తెలిసిన మరియు ధృవీకరించబడవచ్చు

Motherboard (మదర్ బోర్డు)

The motherboard serves as a single platform to connect all of the parts of a computer together. It connects the CPU, memory, hard drives, optical drives, video card, sound card, and other ports and expansion cards directly or via cables. It can be considered as the backbone of a computer.

మదర్‌బోర్డు కలిసి కంప్యూటర్ యొక్క అన్ని భాగాలను కలిపే ఒకే వేదికగా పనిచేస్తుంది. ఇది CPU, మెమరీ, హార్డ్ డ్రైవ్లు, ఆప్టికల్ డ్రైవ్లు, వీడియో కార్డ్, సౌండ్ కార్డ్ మరియు ఇతర పోర్ట్స్ మరియు విస్తరణ కార్డులను ప్రత్యక్షంగా లేదా తంతులు ద్వారా కలుపుతుంది. ఇది కంప్యూటర్ యొక్క వెన్నెముకగా పరిగణించబడుతుంది.

Features of Motherboard
మదర్ బోర్డు యొక్క లక్షణాలు

A motherboard comes with following features –
ఒక మదర్ బోర్డు క్రింది లక్షణాలతో వస్తుంది -

- Motherboard varies greatly in supporting various types of components.
- వివిధ రకాలైన భాగాలను మద్దతుగా **మదర్ బోర్డు** బాగా మారుతుంది
- Motherboard supports a single type of CPU and few types of memories.
- **మదర్ బోర్డు** సింగిల్ రకం CPU మరియు కొన్ని రకాల జ్ఞాపకాలను మద్దతు ఇస్తుంది.
- Video cards, hard disks, sound cards have to be compatible with the motherboard to function
- properly.
- వీడియో కార్డులు, హార్డ్ డిస్కు, సౌండ్ కార్డులు సరిగా పనిచేయడానికి **మదర్ బోర్డు** అనుకూలంగా ఉండాలి.
- Motherboards, cases, and power supplies must be compatible to work properly together.
- **మదర్ బోర్డు**, కేసులు, మరియు విద్యుత్ సరఫరా సరిగా కలిసి పనిచేయడానికి అనుగుణంగా ఉండాలి.
- Popular Manufacturers

  ప్రసిద్ధ తయారీదారులు

  Following are the popular manufacturers of the motherboard. Intel ASUS

  మదర్ బోర్డు యొక్క ప్రముఖ తయారీదారులు అనుసరిస్తున్నారు. ఇంటెల్
ASUS

  AOpen, ABIT,

  Biostar,

  Gigabyte, MSI

Description of Motherboard
మదర్ బోర్డు వివరణ

The motherboard is mounted inside the case and is securely attached via small screws through pre-drilled holes. Motherboard contains ports to connect all of the internal components. It provides a single socket for CPU, whereas for memory, normally one or more slots are available. Motherboards provide ports to attach the floppy drive, hard drive, and optical drives via ribbon cables. Motherboard carries fans and a special port designed for power supply.

కేసు లోపల **మదర్ బోర్డు** మౌంట్ చేయబడింది మరియు ముందటి డ్రిల్లింగ్ రంధ్రాల ద్వారా చిన్న మరలు ద్వారా సురక్షితంగా జోడించబడుతుంది. **మదర్ బోర్డు** అన్ని అంతర్గత భాగాలను కలిపే పోర్టులను కలిగి ఉంటుంది. ఇది CPU కోసం ఒకే సాకెట్ను అందిస్తుంది, అయితే మెమరీ కోసం, సాధారణంగా ఒకటి లేదా ఎక్కువ స్లాట్లు అందుబాటులో ఉన్నాయి. రిబ్బన్ తంతులు ద్వారా ఫ్లాపీ డ్రైవ్, హార్డు డ్రైవు మరియు ఆప్టికల్ డ్రైవ్లను అటాచ్ చెయ్యడానికి **మదర్ బోర్డు** పోర్టులను అందిస్తాయి. మదర్ బోర్డు అభిమానులను మరియు విద్యుత్ సరఫరా కోసం రూపొందించిన ఒక ప్రత్యేక పోర్ట్ను కలిగి ఉంటుంది.

There is a peripheral card slot in front of the motherboard using which video cards, sound cards, and other expansion cards can be connected to the motherboard.

వీడియో కార్డులు, ధ్వని కార్డులు మరియు ఇతర విస్తరణ కార్డులు **మదర్ బోర్డు** అనుసంధానం చేయగల **మదర్ బోర్డు** ముందు పరిధీయ కార్డు స్లాట్ ఉంది.

On the left side, motherboards carry a number of ports to connect the monitor, printer, mouse, keyboard, speaker, and network cables. Motherboards also provide USB ports, which allow compatible devices to be connected in plug-in/plug-out fashion. For example, pen drive, digital cameras, etc.

ఎడమ వైపున, మదర్బోర్డులు మానిటర్, ప్రింటర్, మౌస్, కీబోర్డు, స్పీకర్ మరియు నెట్వర్క్ కేబుల్స్ను అనుసంధానించడానికి అనేక పోర్టులను కలిగి ఉంటాయి. మదర్బోర్డులు ప్లగ్-ఇన్ / ప్లగ్-అవుట్ పద్ధతిలో అనుకూల పరికరాలను అనుసంధానించే USB పోర్టులను కూడా అందిస్తాయి. ఉదాహరణకు, పెన్ డ్రైవ్, డిజిటల్ కెమెరాలు, మొదలైనవి

Memory Units (మెమరీ యూనిట్లు)

Memory unit is the amount of data that can be stored in the storage unit. This storage capacity is expressed in terms of Bytes.

మెమరీ యూనిట్ నిల్వ యూనిట్లో నిల్వ చేయగల డేటా మొత్తం. ఈ నిల్వ సామర్థ్యం బైట్ల పరంగా వ్యక్తీకరించబడింది.

The following table explains the main memory storage units −

క్రింది పట్టిక ప్రధాన మెమరీ నిల్వ యూనిట్లను వివరిస్తుంది −

Bit (Binary Digit)

A binary digit is logical 0 and 1 representing a passive or an active state of a component in an electric circuit.

బిట్ (బైనరీ డిజిట్)

ఒక బైనరీ అంకె తార్కిక 0 మరియు 1 ఒక విద్యుత్ సర్క్యూట్లో ఒక భాగం యొక్క నిష్క్రియాత్మక లేదా చురుకైన స్థితిని సూచిస్తుంది.

Nibble

A group of 4 bits is called nibble.

బిట్ల సమూహాన్ని nibble అంటారు.

Byte

A group of 8 bits is called byte. A byte is the smallest unit, which can represent a data item or a character.బె

8 బిట్స్ సమూహం బైట్ అంటారు. ఒక బైట్ అనేది ఒక చిన్న వస్తువు, ఇది ఒక డేటా అంశం లేదా పాత్రను సూచిస్తుంది.

Word (పదం)

A computer word, like a byte, is a group of fixed number of bits processed as a unit, which varies from computer to computer but is fixed for each computer.

The length of a computer word is called word-size or word length. It may be as small as 8 bits or may be as long as 96 bits. A computer stores the information in the form of computer words.

The following table lists some higher storage units –

బైట్ లాంటి కంప్యూటర్ వర్డ్, యూనిట్గా ప్రాసెస్ చేయబడిన బిట్స్ యొక్క స్థిర సంఖ్య యొక్క సమూహం, ఇది కంప్యూటర్ నుండి కంప్యూటర్కు మారుతూ ఉంటుంది కానీ ప్రతి కంప్యూటర్కు స్థిరంగా ఉంటుంది. ఒక కంప్యూటర్ పదం యొక్క పొడవు పద-పరిమాణం లేదా పదం పొడవు అని పిలుస్తారు. ఇది 8 బిట్స్ అంత చిన్నదిగా ఉండవచ్చు లేదా 96 బిట్స్ వరకు ఉండవచ్చు. ఒక కంప్యూటర్ కంప్యూటర్ పదాలు రూపంలో సమాచారాన్ని నిల్వ చేస్తుంది. క్రింది పట్టిక కొన్ని అధిక నిల్వ యూనిట్లు జాబితా -

Kilobvte (KB)
కిలోబైట్ (KB)

1 KB = 1024 Bytes

Megabyte (MB)

మెగాబైట్(MB)

1MB = 1024 KB

GigaByte (GB)

1 GB = 1024 MB

TeraByte (TB)

1 TB = 1024 GB

PetaByte (PB)

1 PB = 1024 TB

Ports పోర్ట్స్

A port is a physical docking point using which an external device can be connected to the computer. It can also be programmatic docking point through which information flows from a program to the computer or over the Internet.

ఒక పోర్ట్ అనేది బాహ్య పరికరం కంప్యూటర్కు కనెక్ట్ చేయగల భౌతిక డాకింగ్ పాయింట్. ఇది కార్యక్రమంలో నుండి కంప్యూటర్కు లేదా ఇంటర్నెట్లో ప్రవహిస్తున్న సమాచార ప్రోగ్రామింగ్ డాకింగ్ పాయింట్గా కూడా ఉంటుంది.

Characteristics of Ports
పోర్ట్స్ యొక్క లక్షణాలు

A port has the following characteristics –
ఒక పోర్ట్ క్రింది లక్షణాలను కలిగి ఉంది –

- External devices are connected to a computer using cables and ports.
- బాహ్య పరికరాలు కేబుల్స్ మరియు పోర్ట్స్ ఉపయోగించి కంప్యూటర్కు అనుసంధానించబడ్డాయి .
- Ports are slots on the motherboard into which a cable of external device is plugged in.
- పోర్ట్స్ మదర్బోర్డుపై స్లాట్లుగా ఉంటుంది, వీటిలో బాహ్య పరికరం యొక్క కేబుల్ ప్లగ్ చేయబడుతుంది.
- Examples of external devices attached via ports are the mouse, keyboard, monitor, microphone, speakers, etc.
- పోర్ట్స్ ద్వారా జతచేయబడిన బాహ్య పరికరాల ఉదాహరణలు మౌస్, కీబోర్డ్, మానిటర్, మైక్రోఫోన్, స్పీకర్లు మొదలైనవి .

Let us now discuss a few important types of ports –
ఇప్పుడు కొన్ని ముఖ్యమైన పోర్టుల రకాల గురించి చర్చించండి -

Serial Port
సీరియల్

పోర్ట్

- Used for external modems and older computer mouse
  బాహ్య మోడెమ్లు మరియు పాత కంప్యూటర్ మౌస్ కోసం ఉపయోగిస్తారు
- Two versions: 9 pin, 25 pin model
  రెండు వెర్షన్లు: 9 పిన్, 25 పిన్ మోడల్ డేటా
- Data travels at 115 kilobits per second
  సెకనుకు 115 కిలోబిట్లు వద్ద ప్రయాణిస్తుంది

Parallel Port (సమాంతర పోర్ట్)

- Used for scanners and printers(స్కానర్లు మరియు ప్రింటర్ల కోసం వాడతారు)
- Also called printer port(ప్రింటర్ పోర్ట్స్ కూడా పిలుస్తారు)
- 25 pin model(• 25 పిన్ మోడల్)
- IEEE 1284-compliant Centronics port
- IEEE 1284-కంప్లైంట్ సెంట్రోనిక్స్ పోర్ట్

PS/2 Port (PS / 2 పోర్ట్)

- Used for old computer keyboard and mouse
- పాత కంప్యూటర్ కీబోర్డ్ మరియు మౌస్ కోసం ఉపయోగిస్తారు
- Also called mouse port
- మౌస్ పోర్ట్ అని కూడా పిలుస్తారు
- Most of the old computers provide two PS/2 port, each for the mouse and keyboard
- పాత కంప్యూటర్లు చాలావరకు రెండు PS / 2 పోర్ట్లను, మౌస్ మరియు కీబోర్డులకు ప్రతినిస్తాయి
- IEEE 1284-compliant Centronics port
  IEEE 1284-కంప్లైంట్ సెంట్రోనిక్స్ పోర్ట్

Universal Serial Bus (or USB) Port
యూనివర్సల్ సీరియల్ బస్ (లేదా USB) పోర్ట్

- It can connect all kinds of external USB devices such as external hard disk, printer, scanner,

mouse, keyboard, etc.

- బాహ్య హార్డ్ డిస్క్, ప్రింటర్, స్కానర్, మౌస్, కీబోర్డు, మొదలైన అన్ని రకాల బాహ్య USB పరికరాలను ఇది కనెక్ట్ చేయవచ్చు.
- It was introduced in 1997.
- ఇది 1997 లో ప్రవేశపెట్టబడింది.
- Most of the computers provide two USB ports as minimum
- చాలావరకూ కంప్యూటర్లు కనీసంగా రెండు USB పోర్టులను అందిస్తాయి
- Data travels at 12 megabits per seconds.
- సెకనుకు 12 megabits వద్ద డేటా ప్రయాణిస్తుంది .
- USB compliant devices can get power from a USB port.
- USB కంప్లైంట్ పరికరములు ఒక USB పోర్ట్ నుండి శక్తిని పొందగలవు .

VGAPort
(VGAపోర్ట్)

Connects monitor to a computer's video card.
మానిటర్ను కంప్యూటర్ యొక్క వీడియో కార్డ్కు కలుపుతుంది .

- It has 15 holes. (ఇది 15 రంధ్రాలు.)
- Similar to the serial port connector. However, serial port connector has pins, VGA port has holes.
  సీరియల్ పోర్ట్ కనెక్టర్ లాగానే. అయితే, సీరియల్ పోర్ట్ కనెక్టర్ పిన్స్ ఉంది, VGA పోర్ట్ రంధ్రాలు ఉన్నాయి .

Power Connector (పవర్ కనెక్టర్)

- Three-pronged plug.(మూడు-భాగం ప్లగ్.)
- Connects to the computer's power cable that plugs into a power bar or wall socket.
  శక్తి బార్ లేదా గోడ సాకెట్లో ప్లగ్ చేసే కంప్యూటర్ యొక్క పవర్ కేబుల్కు కనెక్ట్ చేస్తుంది .

Firewire Port (ఫైర్వైర్ పోర్ట్)

- Transfers large amount of data at very fast speed.
- చాలా వేగంగా వేగంతో డేటాను పెద్ద మొత్తంలో బదిలీ చేస్తుంది
- Connects camcorders and video equipment to the computer.
- కంప్యూటర్కు క్యామ్కార్డర్లు మరియు వీడియో పరికరాలను కలుపుతుంది.
- Data travels at 400 to 800 megabits per seconds.
- సెకనుకు 400 నుంచి 800 megabits వద్ద డేటా ప్రయాణిస్తుంది.
- Invented by Apple. (ఆపిల్ చేత కనుగొనబడింది.)
- It has three variants: 4-Pin FireWire 400 connector, 6-Pin FireWire 400 connector, and 9-Pin FireWire 800 connector.
- ఇది మూడు రకాలు: 4-పిన్ ఫైర్వైర్ 400 కనెక్టర్, 6-పిన్ ఫైర్వైర్ 400 కనెక్టర్, మరియు 9-పిన్ ఫైర్వైర్ 800 కనెక్టర్.

Modem Port (మోడెం పోర్ట్)

- Connects a PC's modem to the telephone network.

- టెలిఫోన్ నెట్వర్క్కు PC యొక్క మోడెమును అనుసంధానిస్తుంది.

Ethernet Port (ఈథర్నెట్ పోర్ట్)

Connects to a network and high speed Internet.
నెట్వర్క్ మరియు హై స్పీడ్ ఇంటర్నెట్కు కలుపుతుంది.

- Connects the network cable to a computer.
- నెట్వర్క్ కేబుల్ను ఒక కంప్యూటర్కు కలుపుతుంది.
- This port resides on an Ethernet Card.
- ఈ పోర్ట్ ఒక ఈథర్నెట్ కార్డుపై నివసిస్తుంది.

• నెట్వర్క్ బ్యాండ్విడ్త్ మీద ఆధారపడి సెకనుకు 10 megabits per 1000 megabits కు డేటా ప్రయాణిస్తుంది.

Game Port

- Connect a joystick to a PC (PC కు జాయ్స్టిక్ ను కనెక్ట్ చేయండి)
- Now replaced by USB(ఇప్పుడు USB ద్వారా భర్తీ చేయబడింది)

Digital Video Interface, DVI(port డిజిటల్ వీడియో ఇంటర్ఫేస్, DVI పోర్ట్)

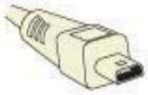
- Connects Flat panel LCD monitor to the computer's high-end video graphic cards.
- ఫ్లాట్ ప్యానెల్ LCD మానిటర్ను కంప్యూటర్ హై ఎండ్ వీడియో గ్రాఫిక్ కార్డులకు కలుపుతుంది.
- Very popular among video card manufacturers.
- వీడియో కార్డు తయారీదారులలో బాగా ప్రాచుర్యం పొందింది.

Sockets

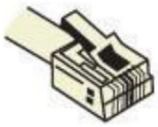
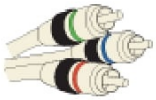
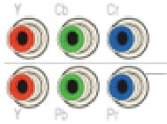
- Sockets connect the microphone and speakers to the sound card of the computer.

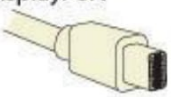
Cable	Port	How it's used
USB 	USB 	Transmits data at various speeds. USB 1.0 @ up to 12MB/second USB 2.0 @ up to 480MB/second USB 3.0 @ up to 5GB/second USB cables are backward compatible, but a 3.0 cable is required to get 3.0 speeds.
USB Type A 	USB Type A 	Transmits data and delivers power (USB 1.0 does not deliver power). Commonly seen on devices with permanently attached cables. Example: A keyboard to a PC.

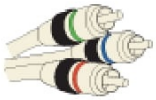
USB Type-B 	USB Type-B 	Transmits data and delivers power to peripherals. Example: A printer to a PC
USB Mini A 	USB Mini A 	Transmits data and delivers power to smaller devices. Mini-A has been superseded and is no longer being used for new devices. Example: A digital camera to a printer

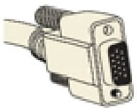
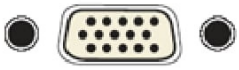
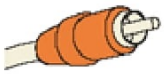
USB Mini B 	USB Mini B 	Transmits data and delivers power to smaller devices. Example: A digital camcorder to a PC
Micro-A USB 	Micro-A USB 	Transmits data and delivers power to portable devices. Similar width to mini USB but approximately half as thick. Example: A smartphone to a PC
USB Micro B 	USB Micro B 	Transmits data and delivers power to portable devices. Similar width to mini USB but approximately half as thick. Example: A PDA to a PC
eSATA 	eSATA 	Transmits high-speed data. A branch of the Serial ATA interface. Faster than FireWire and USB 1.0 and 2.0. Example: An external hard drive to a PC

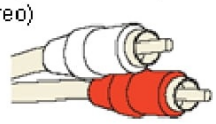
FireWire  ▪ 4-pin ▪ 6-pin	FireWire  ▪ 4-pin ▪ 6-pin	Transmits high-speed data. The six-pin version delivers power; the four-pin does not. FireWire is also called i.LINK and IEEE1394. Faster than USB 1.0 and 2.0. Example: A digital camcorder to a PC
RJ45 Ethernet 	RJ45 Ethernet 	Transmits high-speed data on local area networks (LANs), including Internet and intranet networks. Example: A PC to a router

RJ11 	RJ11 	Transmits faxes and data on local area networks via phone line. Much slower than Ethernet. Example: A PC to a fax machine.
Component video 	Component video  ▪ standard-definition ▪ high-definition	Transmits and protects copyrighted digital video and audio at speeds up to 4.9GB/second, with a refresh rate fast enough for 1080p video. Example: A DVD player to an HDTV.
HDMI (High-Definition Multimedia Interface) 	HDMI 	Transmits and protects copyrighted digital video and audio at speeds up to 10.2GB/second, with a refresh rate fast enough for 1080p and 3D video. However, HDMI 1.3 will display 3D content in 1080i and 1.4 will display 3D in full 1080p. Example: A 3D Blu-ray player to a 3D-capable HDTV.

DisplayPort 	DisplayPort 	Transmits and protects copyrighted digital audio and video with bi-directional communication. Example: A PC to an HD monitor
Mini DisplayPort 	Mini DisplayPort 	Transmits and protects copyrighted digital audio and video with bi-directional communication for smaller devices. Example: A laptop to an HD monitor.

DVI (Digital Visual Interface)  DVI-D (digital) DVI-I (Integrated)	DVI  DVI-D (digital) DVI-I (Integrated)	DVI-D transmits digital video without audio. DVI-I transmits digital and analog video without audio. Example: An HD tuner to an HDTV
Component video 	Component video  ▪ standard-definition ▪ high-definition	Transmits video and comes in standard definition and high definition (HD). Higher quality than S-video and composite. Example: A DVD player to an HDTV
S-Video 	S-Video 	Transmits video as two separate signals: lumen (luminance) and chroma (color). Higher quality than composite but cannot deliver HD video. Example: A video game console to a TV
Yellow RCA (Composite Video) 	Yellow RCA (Composite video) 	Transmits Analog video. Cannot be used for HD or digital video. Example: A DVD player to a TV

VGA (Video Graphics Array) 	VGA 	Transmits Analog video from a PC to a monitor or TV. Example: A laptop PC to a monitor
Coaxial digital audio 	Coaxial 	Transmits digital audio. Example: Stereo speakers to a receiver
Toslink optical digital 	Optical 	Transmits digital audio. Example: A video game console to a receiver

5.1 Channel Outputs (analog) 	5.1 Channel Inputs (analog) 	Transmits up to six specific audio channels (such as left, right, center, left surround, etc.) from your DVD player to an external device. Example: A DVD player to a receiver
Composite/Stereo (RCA stereo) 	Composite/Stereo (RCA stereo) 	Transmits left and right channel audio. Example: Stereo speakers to a receiver
RCA mono 	RCA mono 	Transmits analog audio. Example: A subwoofer to a home theater system

MICROPROCESSOR

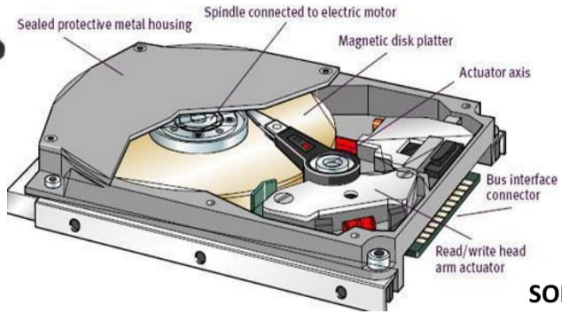
A microprocessor is a computer processor which incorporates the functions of a computer's central processing unit on a single integrated circuit, or at most a few integrated circuits

ఒక మైక్రోప్రాసెసర్ అనేది ఒక కంప్యూటర్ ప్రాసెసర్, ఇది కంప్యూటర్ యొక్క సెంట్రల్ ప్రాసెసింగ్ యూనిట్ యొక్క విధులను ఒకే ఇంటిగ్రేటెడ్ సర్క్యూట్లో కలిగి ఉంటుంది, లేదా కొన్ని ఇంటిగ్రేటెడ్ సర్క్యూట్లలో

HARD DISK DRIVE (హార్డ్ డిస్క్ డ్రైవ్)

A hard disk drive, hard disk, hard drive or fixed disk is a data storage device that uses magnetic storage to store and retrieve digital information using one or more rigid rapidly rotating disks coated with magnetic material.

హార్డ్ డిస్క్ డ్రైవ్, హార్డ్ డిస్క్, హార్డు డ్రైవు లేదా ఫిక్స్డ్ డిస్క్ అనేది ఒక డేటా నిల్వ పరికరం, ఇది అయస్కాంత పదార్థంతో కప్పబడిన ఒకటి లేదా అంతకంటే ఎక్కువ దృఢమైన వేగంగా తిరిగే డిస్కును ఉపయోగించి డిజిటల్ సమాచారాన్ని నిల్వ చేయడానికి మరియు తిరిగి పొందడానికి అయస్కాంత నిల్వను ఉపయోగిస్తుంది.



COMPUTER SOFTWARE

కంప్యూటర్ సాఫ్ట్ వేర్

There are two main types of software: systems software and application software. Systems software includes the programs that are dedicated to managing the computer itself, such as the operating system,file management utilities, and disk operating system(or DOS).

సాఫ్ట్వేర్ యొక్క రెండు ప్రధాన రకాలు: సిస్టమ్స్ సాఫ్ట్వేర్ మరియు అప్లికేషన్ సాఫ్ట్వేర్. సిస్టమ్స్ సాఫ్ట్ వేర్ ఆపరేటింగ్ సిస్టమ్, ఫైల్ మేనేజ్మెంట్ యుటిలిటీస్ మరియు డిస్క్ ఆపరేటింగ్ సిస్టం (లేదా డాస్) వంటి కంప్యూటర్ను నిర్వహించడానికి అంకితమైన ప్రోగ్రామ్లను కలిగి ఉంటుంది.

Multimeter (మల్టిమీటర్)

A multimeter or a multitester, also known as a VOM (volt-ohm-milliammeter), is an electronic measuring instrument that combines several measurement functions in one unit. A typicalmultimeter can measure

voltage, current, and resistance. Analogmultimeters use a microammeter with a moving pointer to display readings.

VOM (ఓల్ట్-ఓహ్మ్-మిల్లియంమీటర్) అని కూడా పిలువబడే ఒక మల్టిమీటర్ లేదా బహుళస్థాయి, ఒక యూనిట్లో అనేక కొలత చర్యలను కలిగి ఉండే ఒక ఎలక్ట్రానిక్ కొలిచే పరికరం. ఒక విలక్షణ మల్టిమీటర్ వోల్టేజ్, ప్రస్తుత, మరియు ప్రతిఘటనను కొలవగలదు. Analogmultimeters రీడింగులను ప్రదర్శించడానికి కదిలే పాయింటర్తో మైక్రోమీటర్ను ఉపయోగిస్తారు.

A digital multimeter (DMM) is a test tool used to measure two or more electrical values—principally voltage (volts), current (amps) and resistance (ohms). It is a standard diagnostic tool for technicians in the electrical/electronic industries.

ఒక డిజిటల్ మల్టిమీటర్ (DMM) అనేది రెండు లేదా అంతకంటే ఎక్కువ విద్యుత్ విలువలు-ప్రధానంగా వోల్టేజ్ (వోల్ట్లు), ప్రస్తుత (ఆంప్స్) మరియు నిరోధకత (ఓంమ్స్) ను కొలిచే ఒక పరీక్ష సాధనం. ఇది ఎలక్ట్రికల్ / ఎలక్ట్రానిక్ పరిశ్రమలలో సాంకేతిక నిపుణుల కోసం ఒక ప్రామాణిక డయాగ్నస్టిక్ సాధనం.

SOFTWARE INSTALLATION
సాఫ్ట్ వేర్ ఇన్స్టాలేషన్

Planning the Installation (సంస్థాపనను ప్లాన్ చేస్తోంది)

- As with any OS installation, we must first plan the installation process. When you run the Windows 7 Setup program, you must provide information about how to install and configure the operating system. Thorough planning can make your installation of Windows 7 more efficient by helping you to avoid potential problems during installation. An understanding of the configuration options will also help to ensure that you have properly configured your system.

  ఏ OS సంస్థాపన మాదిరిగా, మనము మొదట సంస్థాపనా విధానాన్ని ప్లాన్ చేయాలి. మీరు Windows 7 సెటప్ ప్రోగ్రాంను అమలు చేస్తున్నప్పుడు, మీరు ఆపరేటింగ్ సిస్టమ్ను ఎలా ఇన్స్టాల్ చేయాలి మరియు కాన్ఫిగర్ చేయాలో గురించి సమాచారాన్ని అందించాలి. సంస్థాపనా సమయములో సంభావ్య సమస్యలను నివారించుటకు మీకు సహాయం చేయటం ద్వారా మీ ప్రణాళికను Windows 7 మరింత సమర్థవంతంగా చేయగలదు. ఆకృతీకరణ ఐచ్చికముల యొక్క అవగాహన మీరు మీ సిస్టమ్ను సరిగా ఆకృతీకరించినట్లు నిర్ధారించుకోవటానికి సహాయపడుతుంది .

Here are some of the most important things you should take into consideration when planning for your Windows 7 installation:

మీ Windows 7 ఇన్స్టలేషన్ కోసం ప్లాన్ చేస్తున్నప్పుడు మీరు పరిగణించవలసిన ముఖ్యమైన కొన్ని విషయాలు ఇక్కడ ఉన్నాయి:

- Check System Requirements
- సిస్టమ్ అవసరాలు తనిఖీ
- Check Hardware and Software Compatibility
- హార్డ్వేర్ మరియు సాఫ్ట్వేర్ అనుకూలత తనిఖీ
- Determine Disk Partitioning Options
- డిస్కు విభజనీకరణ ఐచ్ఛికాలను నిర్ణయించుట
- Complete a Pre-Installation Checklist
- ముందస్తు-సంస్థాపన చెక్లిస్టును పూర్తి చేయండి

Microsoft states the minimum recommended specs for Windows 7:

మైక్రోసాఫ్ట్ విండోస్ 7 కోసం కనిష్ట సిఫార్సు చేసిన స్పెసిఫికేషన్స్:

- 1 GHz 32-bit or 64-bit processor
- 1 GHz 32-bit లేదా 64-బిట్ ప్రాసెసర్
- 1 GB of system memory
- 1 GB వ్యవస్థ మెమరీ
- 16 GB of available disk space
- అందుబాటులో 16 GB డిస్క్ స్థలం
- Support for DirectX 9 graphics with 128 MB memory (to enable the Aero theme)
- irectX 9 గ్రాఫిక్స్ 128 MB మెమొరీతో (ఎయిరో థీమ్ను ఎనేబుల్ చెయ్యడానికి)

- DVD-R/W Drive DVD-R / W డ్రైవ్
- Internet access (to activate and get updates)
- ఇంటర్నెట్ యాక్సెస్ (సక్రియం మరియు నవీకరణలను పొందడానికి)

32-bit or 64-bit Version?

You need to decide whether to install the 32-bit or 64-bit version of Windows 7. The Windows 7 installation disc package includes both 32-bit and 64-bit versions of Windows 7. Basically, the 64-bit version of Windows handles large amounts of random access memory (RAM) more effectively than a 32-bit system. So if you plan on using Windows 7 on a computer with more than 3 GB or RAM, I would strongly suggest to use the 64-bit version. Most programs designed for the 32-bit version of Windows will work on the 64-bit version of Windows, and if they don't, you can always use Windows XP.

మీరు Windows 7 యొక్క 32-బిట్ లేదా 64-బిట్ వెర్షన్ను ఇన్స్టాల్ చేయాలో లేదో నిర్ణయించుకోవాలి. Windows 7 ఇన్స్టాలేషన్ డిస్క్ ప్యాకేజీ Windows 7 యొక్క 32-బిట్ మరియు 64-బిట్ వెర్షన్లను కలిగి ఉంటుంది. సాధారణంగా, 64-బిట్ వెర్షన్ విండోస్ హ్యాండిల్స్ 32-bit సిస్టమ్ కంటే ఎక్కువ సమర్థవంతమైన రాండమ్ యాక్సెస్ మెమొరీ (RAM). కాబట్టి మీరు Windows 7 ను 3 GB లేదా RAM కంటే ఎక్కువ ఉన్న కంప్యూటర్లో ప్లాన్ చేస్తే, నేను 64-బిట్ వెర్షన్ను ఉపయోగించాలని గట్టిగా సూచించాను. Windows యొక్క 32-బిట్ వెర్షన్ కోసం రూపొందించిన అనేక ప్రోగ్రామ్లు Windows యొక్క 64- బిట్ వర్షన్లో పని చేస్తాయి, మరియు అలా చేయకపోతే, మీరు ఎల్లప్పుడూ Windows XP ను ఉపయోగించవచ్చు .

Note: Either way, you cannot use an existing 32-bit version of a previous OS to perform an in-place upgrade to a 64-bit version of Windows 7, and you'll need to format and install a fresh copy. Also, you cannot use an existing 64-bit version of a previous OS to perform an in-place upgrade to a 32-bit version of Windows 7.

గమనిక: ఏ విధంగా అయినా, మీరు Windows 7 యొక్క 64-బిట్ వెర్షన్కు ఇన్-ప్లేస్ అప్గ్రేడ్ కోసం మునుపటి OS యొక్క ఇప్పటికే ఉన్న 32-బిట్ వెర్షన్ను ఉపయోగించలేరు మరియు మీరు తాజా కాపీని ఆకృతీకరించాలి మరియు ఇన్స్టాల్ చేయాలి. ఇంకా, Windows 7 యొక్క 32-బిట్ సంస్కరణకు ఇన్-ప్లేస్ అప్గ్రేడ్ను నిర్వహించడానికి మీరు మునుపటి OS యొక్క ప్రస్తుత 64-బిట్ వెర్షన్ను ఉపయోగించలేరు.

Computer, I would strongly recommend that you format it and install a fresh copy of the OS.

కంప్యూటర్, మీరు దీన్ని ఫార్మాట్ చేసి, OS యొక్క తాజా కాపీని ఇన్స్టాల్ చేయాలని నేను గట్టిగా సిఫార్సు చేస్తాను.

ARPANET – Advanced Research Projects Agency Network

ARPANET - అధునాతన రీసెర్చ్ ప్రాజెక్ట్స్ ఏజెన్సీ నెట్ వర్క్

ARPANET – Advanced Research Projects Agency Network – the granddad of Internet was a network established by the US Department of Defense (DOD). The work for establishing the network started in the early 1960s and DOD sponsored major research work, which resulted in development on initial

protocols, languages and frameworks for network communication.

ARPANET - అధునాతన రీసెర్చ్ ప్రాజెక్ట్స్ ఏజన్సీ నెట్ వర్క్ - ఇంటర్నెట్ యొక్క granddad US డిపార్ట్మెంట్ ఆఫ్ డిఫెన్స్ (DOD) చేత స్థాపించబడిన నెట్వర్క్. 1960 ల ప్రారంభంలో మరియు DOD ప్రయోగాత్మక ప్రధాన పరిశోధన కార్యక్రమంలో నెట్వర్క్ను స్థాపించటానికి పని ప్రారంభమైంది, ఇది ప్రాధమిక ప్రోటోకాల్, భాషలు మరియు నెట్వర్క్ కమ్యూనికేషన్ కోసం చట్రాలు

It had four nodes at University of California at Los Angeles (UCLA), Stanford Research Institute (SRI), University of California at Santa Barbara (UCSB) and University of Utah. On October 29, 1969, the first message was exchanged between UCLA and SRI. E-mail was created by Roy Tomlinson in 1972 at Bolt Beranek and Newman, Inc. (BBN) after UCLA was connected to BBN.

ఇది యూనివర్శిటీ ఆఫ్ కాలిఫోర్నియాలో లాస్ ఏంజిల్స్ (UCLA), స్టాన్ఫోర్డ్ రీసెర్చ్ ఇన్స్టిట్యూట్ (SRI), శాన్డన్ బార్బరాలో ఉన్న యునివర్సిటీ ఆఫ్ కాలిఫోర్నియా (UCSB) మరియు ఉటా విశ్వవిద్యాలయం వద్ద నాలుగు నోడ్స్ ఉన్నాయి. అక్టోబరు 29, 1969 న, మొదటి సందేశం UCLA మరియు SRI ల మధ్య మార్పిడి చేయబడింది. 1972 లో రాయ్ టాంలిన్సన్ బోల్ట్ బెరానెక్ మరియు న్యూమాన్, ఇంక్. (BBN) వద్ద UCLA BBN కు అనుసంధానించబడిన తరువాత ఈ-మెయిల్ సృష్టించబడింది.

Internet

ARPANET expanded to connect DOD with those universities of the US that were carrying out defense-related research. It covered most of the major universities across the country. The concept of networking got a boost when University College of London (UK) and Royal Radar Network (Norway) connected to the ARPANET and a network of networks was formed.

అంతర్జాలం ARPANET, US లోని ఆ విశ్వవిద్యాలయాలతో రక్షణ-సంబంధిత పరిశోధనకు సంబంధించిన DOD ను అనుసంధానించడానికి విస్తరించింది. ఇది దేశంలోని అనేక ప్రధాన విశ్వవిద్యాలయాలను కవర్ చేసింది. యూనివర్సిటీ కాలేజ్ ఆఫ్ లండన్ (UK) మరియు రాయల్ రాడార్ నెట్ వర్క్ (నార్వే) ARPANET మరియు నెట్వర్క్ల నెట్వర్క్లతో అనుసంధానించబడినప్పుడు నెట్వర్కింగ్ యొక్క భావన ఊపందుకుంది.

The term Internet was coined by Vinton Cerf, Yogen Dalal and Carl Sunshine of Stanford University to describe this network of networks. Together they also developed protocols to facilitate information exchange over the Internet. Transmission Control Protocol (TCP) still forms the backbone of networking

నెట్ వర్క్ అనే పదాన్ని వినటన్ సెర్ఫ్, యోగేన్ దలాల్ మరియు స్టాన్ఫోర్డ్ యూనివర్సిటీ యొక్క కార్ల్ సన్షైన్ అనే పదాన్ని ఇంటర్నెట్ను వాడటం జరిగింది. ఇంటర్నెట్లో సమాచార మార్పిడిని సులభతరం చేసేందుకు వారు ప్రోటోకాల్లను అభివృద్ధి చేశారు. ట్రాన్స్మిషన్ కంట్రోల్ ప్రోటోకాల్ (TCP) ఇప్పటికీ నెట్వర్కింగ్ యొక్క వెన్నెముకను రూపొందిస్తుంది.

Telenet

Telenet was the first commercial adaptation of ARPANET introduced in 1974. With this the concept of Internet Service Provider (ISP) was also introduced. The main function of an ISP is to provide uninterrupted Internet connection to its customers at affordable rates.

1974 లో పరిచయం అయిన ARPANET యొక్క మొదటి వాణిజ్య ప్రకటన టెలినేట్. ఇంటర్నెట్ సర్వీస్ ప్రొవైడర్ (ISP) అనే భావన కూడా ప్రవేశపెట్టబడింది. సరసమైన ధరలలో దాని వినియోగదారులకు నిరంతరాయమైన ఇంటర్నెట్ కనెక్షన్ అందించటం ఒక ISP యొక్క ప్రధాన విధి .

World Wide Web (WWW) (వరల్డ్ వైడ్ వెబ్ (WWW)

With commercialization of internet, more and more networks were developed in different part of the world. Each network used different protocols for communicating over the network. This prevented different networks from connecting together seamlessly. In the 1980s, Tim Berners-Lee led a group of Computer scientists at CERN, Switzerland, to create a seamless network of varied networks, called the World Wide Web (WWW).

ఇంటర్నెట్ యొక్క వాణిజ్యీకరణతో, ప్రపంచంలోని వివిధ భాగాలలో మరింత ఎక్కువ నెట్వర్క్లు అభివృద్ధి చేయబడ్డాయి. నెట్వర్క్లో కమ్యూనికేట్ చేయడానికి ప్రతి నెట్వర్క్ వివిధ ప్రోటోకాల్లను ఉపయోగించింది. ఇది సజావుగా కలిసి కనెక్ట్ చేయకుండా వివిధ నెట్వర్క్లను నిరోధించింది. 1980 వ దశకంలో, వరల్డ్ వైడ్ వెబ్ (WWW) అని పిలువబడే వైవిధ్యమైన నెట్వర్క్ల యొక్క అతుకులులేని నెట్వర్క్ని సృష్టించడానికి, టిమ్ బెర్నెర్స్-లీ స్విట్జర్లాండ్లోని CERN కంప్యూటర్ శాస్త్రవేత్తల సమూహాన్ని నడిపించింది.

World Wide Web is a complex web of websites and web pages connected together through hypertexts. Hypertext is a word or group of words linking to another web page of the same or different website. When the hypertext is clicked, another web page opens.

వరల్డ్ వైడ్ వెబ్ అనేది వెబ్సైట్లు మరియు హైపర్టెక్స్ట్ ద్వారా కలిపి వెబ్ పేజీల యొక్క క్లిష్టమైన వెబ్. హైపర్టెక్స్ట్ అనేది అదే పదం లేదా విభిన్న వెబ్ సైట్ యొక్క మరొక వెబ్ పేజీకి లింక్ చేసే పదాల పదం లేదా సమూహం. హైపెర్ టెక్స్ట్ క్లిక్ చేసినప్పుడు, మరొక వెబ్ పేజీ తెరుచుకుంటుంది.

The evolution from ARPANET to WWW was possible due to many new achievements by researchers and computer scientists all over the world. Here are some of those developments

ARPANET నుండి WWW కు పరిణామం ప్రపంచవ్యాప్తంగా పరిశోధకులు మరియు కంప్యూటర్ శాస్త్రవేత్తలచే అనేక కొత్త విజయాలు సాధించగలిగే అవకాశం ఉంది. ఆ అభివృద్ధిలో కొన్ని ఉన్నాయి

Year	Milestone
1957	Advanced Research Project Agency formed by US US ద్వారా ఏర్పడిన అధునాతన రీసెర్చ్ ప్రాజెక్ట్ ఏజెన్సీ
1969	ARPANET became functional ARPANETఫంక్షనల్గామారింది
1970	ARPANET connected to BBNs ARPANET BBN లకు కనెక్ట్ చేయబడింది
1972	Roy Tomlinson develops network messaging or E-mail. Symbol @ comes to mean "at" రాయ్ టాంలిన్సన్ నెట్వర్క్ సందేశాలు లేదా ఇ-మెయిల్ను అభివృద్ధి చేస్తాడు. చిహ్నం @ "వద్ద"

1973	APRANET connected to Royal Radar Network of Norway APRANET నార్వే రాయల్ రాడార్ నెట్వర్క్కు కనెక్ట్ చేయబడింది
1974	Term Internet coined First commercial use of ARPANET, Telenet, is approved పదం ఇంటర్నెట్ సృష్టించబడింది ARPANET యొక్క మొదటి వాణిజ్య ఉపయోగం, Telenet, ఆమోదించబడింది
1982	TCP/IP introduced as standard protocol on ARPANET TCP / IP ARPANET పై ప్రామాణిక ప్రోటోకాల్గా పరిచయం చేయబడింది
1983	Domain Name System introduced డొమైన్ నేమ్ సిస్టం పరిచయం చేయబడింది

1986	National Science Foundation brings connectivity to more people with its NSFNET program నేషనల్ సైన్స్ ఫౌండేషన్ దాని NSFNET కార్యక్రమంతో ఎక్కువమందికి కనెక్టివిటీని తెస్తుంది
1990	ARPANET decommissioned First web browser Nexus developed HTML developed
2002-2004	Web 2.0 is born

Before we dive into details of networking, let us discuss some common terms associated with data communication.

Channel

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

మేము నెట్ వర్కింగ్ యొక్క వివరాలు లోకి ప్రవేశించే ముందు, డేటా కమ్యూనికేషన్తో అనుబంధించబడిన కొన్ని సాధారణ పదాలను చర్చించనివ్వండి.ఛానల్సమాచార మార్పిడికి సంబంధించిన కేబుల్స్ వంటి భౌతిక మాధ్యమం ఛానల్ అని పిలుస్తారు. ప్రసార ఛానల్ అనలాగ్ లేదా డిజిటల్ కావచ్చు. పేరు సూచించినట్లుగా, అనలాగ్ సంకేతాలను ఉపయోగించి అనలాగ్ చానెల్స్ డేటాను డిజిటల్ సిగ్నల్స్ ఉపయోగించి డేటా ప్రసారం చేస్తున్నప్పుడు ప్రసారం చేస్తాయి.

waves.

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

జనాదరణ పొందిన నెట్వర్క్ పరిభాషలో, డేటా పంపబడిన లేదా అందుకున్న డేటాను డేటా చానల్ అని పిలుస్తారు. ఈ డేటా ఛానల్ రాగి తంతి తంతులు వంటి ప్రసార మాధ్యమం కావచ్చు లేదా రేడియో తరంగాలు వంటి ప్రసార మాధ్యమం కావచ్చు.

DataTransferRate
డేటా బదిలీ రేట్

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

డేటా బదిలీ రేటు డేటా బదిలీ రేటు అంటారు, యూనిట్ సమయం ప్రకారం కొలుస్తారు ప్రసారం ఛానెల్, పైగా డేటా బదిలీ లేదా అందుకున్నప్పుడు. సెకనుకు బిట్స్ (బి పి ఎస్) కొలమానం చిన్నది. 1 bps అనగా 1 బిట్ (0 లేదా 1) డేటా 1 సెకనులో బదిలీ చేయబడుతుంది.

Here are some commonly used data transfer rates –
ఇక్కడ కొన్ని సాధారణంగా ఉపయోగించే డేటా బదిలీ రేట్లు

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

Bandwidth
బ్యాండ్విడ్త్

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

నెట్వర్క్ ద్వారా మద్దతు ఇవ్వగల డేటా బదిలీ రేట్లు దాని బ్యాండ్విడ్త్ అని పిలుస్తారు. ఇది సెకనుకు బిట్స్ కొలుస్తారు (bps). ఆధునిక రోజు నెట్వర్కు బ్యాండ్విడ్తును Kbps, Mbps మరియు Gbps లో అందిస్తాయి. నెట్వర్క్ యొక్క బ్యాండ్విడ్తును ప్రభావితం చేసే కొన్ని అంశాలు

- Network devices used
- ఉపయోగించిన నెట్వర్క్ పరికరాలు
- Protocols used
- ఉపయోగించే ప్రోటోకాల్లు
- Number of users connected
- వినియోగదారులు కనెక్ట్ సంఖ్య
- Network overheads like collision, errors, etc.
- ఘర్షణ, లోపాలు మొదలైన వాటి వంటి నెట్వర్క్ ఓవర్ హెడ్స్

Throughput

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

డేటాను నెట్వర్క్ ద్వారా బదిలీ చేయగల వాస్తవ వేగం. వాస్తవ డేటాను బదిలీ చేయడంతో పాటు, నెట్వర్క్ బ్యాండ్విడ్త్ దోష సందేశాలు, రసీదు ఫ్రేములు,

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

నిర్గమాంశంగా బ్యాండ్విడ్త్ కంటే నెట్వర్క్ వేగం, సామర్థ్యం మరియు సామర్థ్యం వినియోగం యొక్క ఉత్తమ కొలత.

What is a Computer Network
కంప్యూటర్ నెట్వర్క్ అంటే ఏమిటి

A computer network is a group of computers or computer like devices connected together to share the network resources like files, printers, network services etc. A typical computer network consists of users working in workstations (also called as clients, or desktops), running client Operating Systems like Windows 7 or Windows 8/8.1 and store their files inside a central network server.

ఒక కంప్యూటర్ నెట్వర్క్ అనేది కంప్యూటర్లు లేదా కంప్యూటర్లు వంటి సమూహాలు, ఫైల్లు, ప్రింటర్లు, నెట్వర్క్ సేవలు వంటి నెట్వర్క్ వనరులను పంచుకోవడానికి ఒకదానితో ఒకటి కనెక్ట్ చేయబడి ఉంటుంది. ఒక సాధారణ కంప్యూటర్ నెట్వర్క్ వర్క్స్టేషన్ల (క్లయింట్లుగా పిలుస్తారు, లేదా డెస్క్టాప్లు) లో పని చేసే వినియోగదారులను కలిగి ఉంటుంది, Windows 7 లేదా Windows 8 / 8.1 వంటి ఆపరేటింగ్ సిస్టమ్స్ మరియు ఒక కేంద్ర నెట్వర్క్ సర్వర్ లోపల వారి ఫైల్స్ నిల్వ.

Computer networks are required for network communication and network resource sharing (printers, scanners, storage spaces etc). To build and connect computer networks, we need computers (Clients and Servers) and special network infrastructure devices.
నెట్వర్క్ కమ్యూనికేషన్లు మరియు నెట్వర్క్ వనరుల భాగస్వామ్యం (ప్రింటర్లు, స్కానర్లు, నిల్వ స్థలాలను మొదలైనవి) కోసం కంప్యూటర్ నెట్వర్క్లు అవసరం. కంప్యూటర్ నెట్వర్క్లను నిర్మించడానికి మరియు కనెక్ట్ చేయడానికి, మాకు కంప్యూటర్లు (క్లయింట్లు మరియు సర్వర్లు) మరియు ప్రత్యేక నెట్వర్క్ ఇన్ఫ్రాస్ట్రక్చర్ పరికరాలు అవసరం .

Computer networks are built using network infrastructure devices. Click the following link to see some important network infrastructure devices.
కంప్యూటర్ నెట్వర్క్లు నెట్వర్క్ ఇన్ఫ్రాస్ట్రక్చర్ పరికరాలను ఉపయోగించి నిర్మించబడ్డాయి. కొన్ని ముఖ్యమైన నెట్వర్క్ అవస్థాపన పరికరాలను చూడటానికి కింది లింక్ని క్లిక్ చేయండి.

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

కంప్యూటర్ నెట్వర్క్లు వనరులను మరియు కమ్యూనికేషన్లో పంచుకోవడానికి నెట్వర్క్లో వినియోగదారులకు సహాయపడతాయి. ఇ-మెయిల్లు, ఆన్లైన్ వార్తాపత్రికలు, బ్లాగ్లు, చాట్ మరియు ఇంటర్నెట్ అందించే ఇతర సేవలు లేకుండా మీరు ఇప్పుడు ప్రపంచాన్ని

ఊహించగలరా?

The following are the important uses and benefits of a computer network.
కంప్యూటర్ నెట్వర్క్ యొక్క ముఖ్యమైన ప్రయోజనాలు మరియు ప్రయోజనాలు క్రిందివి.

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

ఫైల్ పేరింగ్: నెట్వర్క్ల నెట్వర్కింగ్ డేటా ఫైళ్లను పంచుకోవడానికి నెట్వర్క్ వాడుకదారులకు సహాయపడుతుంది.

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

హార్డ్వేర్ భాగస్వామ్య: వినియోగదారులు కంప్యూటర్ నెట్వర్కు లేకుండా ప్రింటర్లు, స్కానర్లు, CD-ROM డ్రైవులు, హార్డు డ్రైవులు వంటి పరికరాలనుపంచుకోవచ్చు.

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

అప్లికేషన్ భాగస్వామ్యం: అప్లికేషన్స్ నెట్వర్కో పంచుకోవచ్చు, మరియు ఇది క్లయింట్ / సర్వర్ అప్లికేషన్లను అమలు చేయడానికి అనుమతిస్తుంది

User communication: Networks allow users to communicate using e-mail, newsgroups, and video conferencing etc.
వాడుకరి కమ్యూనికేషన్ : యూజర్లు ఇ-మెయిల్, న్యూస్గ్రూప్లు మరియు వీడియో కాన్ఫరెన్సింగ్ మొదలైన వాటిని ఉపయోగించి కమ్యూనికేట్ చేయడానికి వినియోగదారులను అనుమతిస్తాయి .

Network gaming: A lot of network games are available, which allow multi-users to play from different locations.
నెట్వర్క్ గేమింగ్: చాలా మంది నెట్వర్క్ ఆటలు అందుబాటులో ఉన్నాయి, ఇది బహుళ-వినియోగదారులను వేర్వేరు ప్రదేశాల నుండి ఆడటానికి అనుమతిస్తుంది.

Voice over IP (VoIP): Voice over Internet Protocol (IP) is a revolutionary change in telecommunication which allows to send telephone calls (voice data) using standard Internet Protocol (IP) rather than by traditional PSTN.
వాయిస్ ఓవర్ IP (VoIP): వాయిస్ ఓవర్ ఇంటర్నెట్ ప్రోటోకాల్ (IP) టెలీకమ్యూనికేషన్స్లో ఒక విప్లవాత్మక మార్పు, ఇది సాంప్రదాయ PSTN ద్వారా కాకుండా ప్రామాణిక ఇంటర్నెట్ ప్రోటోకాల్ (IP) ను ఉపయోగించి టెలిఫోన్ కాల్లను (వాయిస్ డేటా) పంపడానికి అనుమతిస్తుంది .

Client Operating Systems (Workstation Operating Systems) and Network Operating Systems - NOS (Server Operating Systems)

క్లయింట్ ఆపరేటింగ్ సిస్టమ్స్ (వర్క్స్టేషన్ ఆపరేటింగ్ సిస్టమ్స్) మరియు నెట్వర్క్ ఆపరేటింగ్ సిస్టమ్స్ - NOS (సర్వర్ ఆపరేటింగ్ సిస్టమ్స్)

You have to understand two key technical terms to move further, "Client" and "Server".
మీరు "కీబోర్డు" మరియు "సర్వర్" లను కదిలించటానికి రెండు కీ సాంకేతిక పదాలను అర్థం చేసుకోవాలి .

What is a Client Computer? You can think a client as a computer in your network, where a network user is performing some network activity. For Example: Downloading a file from a File Server, Browsing Intranet/Internet etc. The network user normally uses a client computer to perform his day to day work.

క్లయింట్ కంప్యూటర్ అంటే ఏమిటి? మీ నెట్వర్క్లో ఒక క్లయింట్ వలె ఒక క్లయింట్ను మీరు ఆలోచించవచ్చు, ఇక్కడ నెట్వర్క్ వినియోగదారుడు కొన్ని నెట్వర్క్ కార్యాచరణను నిర్వహిస్తున్నారు. ఉదాహరణకు: ఒక ఫైల్ సర్వర్, బ్రౌజింగ్ ఇంట్రానెట్ / ఇంటర్నెట్ నుండి ఒక ఫైల్ను డౌన్లోడ్ చేయడం. నెట్వర్క్ వినియోగదారు సాధారణంగా రోజువారీ పనిని నిర్వహించడానికి క్లయింట్ కంప్యూటర్ను ఉపయోగిస్తుంది.

What is a Server Computer? The client computer establishes a connection to a Server computer and accesses the services installed on the Server Computer. A Server is not meant for a network user to browse in internet or do spreadsheet work. A Server computer is installed with appropriate Operating System and related Software to serve the network clients with one or more services, continuously without a break.
సర్వర్ కంప్యూటర్ అంటే ఏమిటి? క్లయింట్ కంప్యూటర్ సర్వర్ కంప్యూటర్కు కనెక్షన్ను ఏర్పాటు చేస్తుంది మరియు సర్వర్ కంప్యూటర్లో ఇన్స్టాల్ చేయబడిన సేవలను ప్రాప్తి చేస్తుంది. ఇంటర్నెట్లో బ్రౌజ్ చేయడానికి లేదా స్ప్రెడ్షీట్ పని చేయడానికి నెట్వర్క్ వినియోగదారు కోసం ఒక సర్వర్ ఉద్దేశించబడింది కాదు. ఒక సర్వర్ కంప్యూటర్ తగిన ఆపరేటింగ్ సిస్టమ్తో మరియు సంబంధిత సాఫ్ట్వేర్తో నెట్వర్క్ క్లయింట్లను ఒకటి లేదా మరిన్ని సేవలను అందించడానికి, విరామం లేకుండా నిరంతరంగా ఇన్స్టాల్ చేయబడుతుంది .

An Operating System (also known as "OS") is the most important set of software programs which are loaded initially into any computer-like device by a bootstrap program. Operating System controls almost all the resources in a computer, including networks, data storage, user & user password database, peripheral devices etc.

ఒక ఆపరేటింగ్ సిస్టం ("OS" అని కూడా పిలుస్తారు) అనేది సాఫ్ట్వేర్ ప్రోగ్రామ్ల యొక్క అతి ముఖ్యమైన సమితి, ఇది బూట్స్ట్రాప్ ప్రోగ్రామ్ ద్వారా ఏదైనా కంప్యూటర్ లాంటి పరికరంలో మొదట లోడ్ చేయబడుతుంది. ఆపరేటింగ్ సిస్టమ్ నెట్వర్క్లలో, డేటా నిల్వ, యూజర్ & యూజర్ పాస్వర్డ్ను డేటాబేస్, పరిధీయ పరికరాలు మొదలైనవి సహా కంప్యూటర్లో దాదాపు అన్ని వనరులను నియంత్రిస్తుంది.

Operating System Software products are so complex software products. Operating System Software products are compiled from millions of lines of source code. Operating system products we have currently are created by the hard work of thousands of engineers for decades, internally in a company (Example: Windows) or by dedicated global volunteer communities (Example: GNU/Linux, BSD Unix).

ఆపరేటింగ్ సిస్టమ్ సాఫ్ట్వేర్ ఉత్పత్తులు చాలా క్లిష్టమైన సాఫ్ట్వేర్ ఉత్పత్తులు. ఆపరేటింగ్ సిస్టం సాఫ్ట్వేర్ ఉత్పత్తులు సోర్స్ కోడ్ యొక్క లక్షల లైన్ల నుండి సంకలనం చేయబడ్డాయి. ఆపరేటింగ్ సిస్టం ఉత్పత్తులు ప్రస్తుతం మేము దశాబ్దాలుగా వేలసంఖ్యల ఇంజనీర్ల కృషి ద్వారా, అంతర్గతంగా ఒక కంపెనీలో (ఉదాహరణ: Windows) లేదా అంకితమైన గ్లోబల్ వాలంటీర్ కమ్యూనిటీలు (ఉదాహరణ: GNU / Linux, BSD Unix) ద్వారా సృష్టించబడతాయి.

Network Operating Systems - NOS (Server Operating Systems)

A Network Server computer offers its services to a group of Network Client devices. A Server computer typically has more computing resources like Processors & Processing Power, more Physical Memory (RAM), more Storage Space etc., compared to client computers. The Server computer machine runs on Server Operating System, also called as Network Operating System (NOS), which normally has more features and processing capabilities compared with the client computer's Operating System. The server

నెట్వర్క్ ఆపరేటింగ్ సిస్టమ్స్ - NOS (సర్వర్ ఆపరేటింగ్ సిస్టమ్స్)

ఒక నెట్వర్క్ సర్వర్ కంప్యూటర్ నెట్వర్క్ క్లయింట్ పరికరాల సమూహానికి తన సేవలను అందిస్తుంది. క్లయింట్ కంప్యూటర్లతో పోల్చినప్పుడు, ఒక సర్వర్ కంప్యూటర్లో సాధారణంగా ప్రోసెసర్ల & ప్రోసెసింగ్ పవర్, మరింత భౌతిక మెమరీ (RAM), మరింత నిల్వ స్పేస్ మొదలైన కంప్యూటింగ్ వనరులు ఉన్నాయి. సర్వర్ కంప్యూటర్ యంత్రం సర్వర్ ఆపరేటింగ్ సిస్టం పై నడుస్తుంది, ఇది నెట్వర్క్ ఆపరేటింగ్ సిస్టం (NOS) అని కూడా పిలుస్తారు, ఇది సాధారణంగా క్లయింట్ కంప్యూటర్ యొక్క ఆపరేటింగ్ సిస్టంతో పోలిస్తే మరిన్ని లక్షణాలు మరియు ప్రాసెసింగ్ సామర్థ్యాలను కలిగి ఉంటుంది. సర్వర్

May be installed with special software, to function as a Server Role. The special software allows a Server Computer to function a particular server role, like a File Server, Web Server, Mail Server, Directory Server etc.

ఒక ప్రత్యేకమైన సాఫ్టువేరుతో, ఒక సర్వర్ రోల్ గా పనిచేయవచ్చు. సర్వర్ సాఫ్ట్వేర్, సర్వర్ సర్వర్, వెబ్ సర్వర్, మెయిల్ సర్వర్, డైరెక్టరీ సర్వర్ మొదలైనవి వంటి ప్రత్యేక సర్వర్ పాత్రను ప్రత్యేక సాఫ్ట్వేర్ను అనుమతిస్తుంది.

- Windows NT (obsolete)
- Windows 2000 (obsolete)
- Windows 2003 (Legacy)
- Windows 2008 / Windows 2008 R2 (Legacy)
- Windows 2012 / Windows 2012 R2 (Current)
- Unix (Oracle Solaris, IBM AIX, HP UX, FreeBSD, NetBSD, OpenBSD, SCO Unix etc)
- GNU/Linux (RedHat Enterprise Linux, Debian Linux, SUSE Enterprise, Ubuntu Server, CentOS Server, Mandriva, Fedora etc.

GNU / Linux (RedHat Enterprise Linux, Debian Linux, SUSE Enterprise, ఉబుంటు సర్వర్, CentOS సర్వర్, మాండ్రివా, ఫెడోరా మొదలైనవి.

Client Operating Systems (Workstation Operating Systems, or Desktop Operating Systems)

క్లయింట్ ఆపరేటింగ్ సిస్టమ్స్ (వర్క్‌స్టేషన్ ఆపరేటింగ్ సిస్టమ్స్, లేదా డెస్క్‌టాప్ ఆపరేటింగ్ సిస్టమ్స్)

Most popular Client Workstation Operating Systems are listed below.

- Windows 95/98/ME Vista (obsolete)
- Windows NT Workstation / Windows 2000 Professional (obsolete)
- Windows XP (Legacy)
- Windows 7 (Legacy)
- Windows 8 / Windows 8.1 (Current)
- RedHat Enterprise Linux Desktop
- SuSE Desktop
- Ubuntu Desktop
- LinuxMint

Common Network Application Software

సాధారణ నెట్‌వర్క్ అప్లికేషన్ సాఫ్ట్‌వేర్

Web Browser: A web browser is a network application which enables the users to access the internet. Web browser interprets HTML (HyperText Mark-up language) files sent from a Web Server and displays the content in its screen. Web Browser is the most widely used network application.

వెబ్ బ్రౌజర్: ఒక వెబ్ బ్రౌజర్ ఇంటర్నెట్ అప్లికేషన్ను యాక్సెస్ చేయడానికి వినియోగదారులను అనుమతిస్తుంది. వెబ్ బ్రౌజర్ HTML (హైపర్‌టెక్స్ట్ మార్క్-అప్ లాంగ్వేజ్) వెబ్ సర్వర్ నుండి పంపిన ఫైళ్ళను మరియు దాని స్క్రీన్లో కంటెంట్ని ప్రదర్శిస్తుంది. వెబ్ బ్రౌజర్ అనేది విస్తృతంగా ఉపయోగించే నెట్‌వర్క్ అప్లికేషన్.

Most widely used Web Browser products are

ఎక్కువగా ఉపయోగించే వెబ్ బ్రౌజర్ ఉత్పత్తులు

- Mozilla Firefox
- Microsoft Internet Explorer
- Google Chrome
- Opera
- Apple Safari

E-mail Applications: E-mail (Electronic Mail) Applications are used for composing and sending e-mails within the same network or to outside the network.

ఇ-మెయిల్ అప్లికేషన్స్: ఇ-మెయిల్ (ఎలక్ట్రానిక్ మెయిల్) అనువర్తనాలు ఒకే నెట్‌వర్క్ లోపల లేదా నెట్ వర్క్ వెలుపల ఇ-మెయిల్లను కంపోజ్ చేయడం మరియు పంపడం కోసం ఉపయోగించబడతాయి.

Most widely used E-mail (Electronic Mail) Applications products are

అత్యంత విస్తృతంగా ఉపయోగించే ఇ-మెయిల్ (ఎలక్ట్రానిక్ మెయిల్) అప్లికేషన్స్ ఉత్పత్తులు

- Mozilla Thunderbird
- Microsoft Outlook
- Evolution

Instant Messaging Chat Applications: Instant Messaging Chat Applications are used these days for corporate communication and for general chat.
ఇన్స్టాంట్ మెసేజింగ్ చాట్ అప్లికేషన్స్: తక్షణ సందేశ చాట్ అప్లికేషన్లు కార్పొరేట్ కమ్యూనికేషన్ మరియు సాధారణ చాట్ కోసం ఈ రోజులను ఉపయోగిస్తాయి .

Most widely used Instant Messaging Chat Applications products are

అత్యంత విస్తృతంగా ఉపయోగించిన తక్షణ సందేశ చాట్ అప్లికేషన్స్ ఉత్పత్తులు

Apache OpenMeetings
Microsoft Lync
Yahoo Messanger
Cisco WebEx

Collaboration Applications: Collaboration network applications are mainly used inside a company for a group of employees to work together for a common task. Collaboration network applications allow employees to transfer their files to a central storage repository and work together on it.

సహకార అనువర్తనాలు: కలయిక నెట్వర్క్ అప్లికేషన్లు ప్రధానంగా ఒక ఉద్యోగ బృందంలో కలిసి పనిచేయడానికి ఒక సంస్థలో ప్రధానంగా పనిచేస్తాయి. సహకార నెట్వర్క్ అనువర్తనాలు ఉద్యోగులను వారి నిల్వలను కేంద్ర నిల్వ రిపోజిటరీకి బదిలీ చేయడానికి మరియు దానిపై కలిసి పనిచేయడానికి అనుమతిస్తాయి.

Microsoft SharePoint
Oracle Beehive
Novell GroupWise

Types of Networks
నెట్వర్క్ రకాలు

Networks can be categorized depending on size, complexity, level of security, or geographical range. We will discuss some of the most popular topologies based on geographical spread.

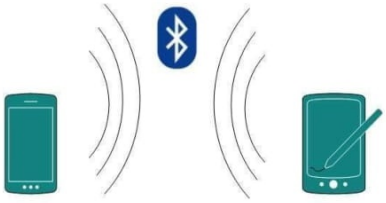
పరిమాణాల, సంక్లిష్టత, భద్రతా స్థాయి లేదా భౌగోళిక పరిధి ఆధారంగా నెట్వర్క్లను వర్గీకరించవచ్చు. మేము భౌగోళిక వ్యాప్తిపై ఆధారపడిన అత్యంత ప్రసిద్ధ స్థలవర్గాల గురించి చర్చించను.

Personal Area Network (PAN)
వ్యక్తిగత ప్రాంతం నెట్వర్క్ (పాస్)

PAN is the acronym for Personal Area Network. PAN is the interconnection between devices within the

range of a person's private space, typically within a range of 10 metres. If you have transferred images or songs from your laptop to mobile or from mobile to your friend's mobile using Bluetooth, you have set up and used a personal area network.

పాన్ వ్యక్తిగత ఏరియా నెట్వర్క్ కోసం సంక్షిప్త రూపం. PAN అనేది ఒక వ్యక్తి యొక్క వ్యక్తిగత స్థల పరిధిలోని పరికరాల మధ్య ఇంటర్కనెక్షన్, ఇది సాధారణంగా 10 మీటర్ల పరిధిలో ఉంటుంది. మీ లాప్టాప్ నుండి మొబైల్ లేదా మొబైల్ నుండి బ్లూటూత్ను ఉపయోగించి మీ స్నేహితుని మొబైల్కు మీరు చిత్రాలను లేదా పాటలను బదిలీ చేసినట్లయితే, మీరు సెటప్ చేసి వ్యక్తిగత ప్రదేశ నెట్వర్క్ను ఉపయోగించారు.

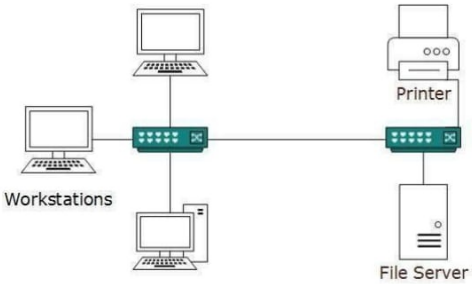


A person can connect her laptop, smart phone, personal digital assistant and portable printer in a network at home. This network could be fully Wi-Fi or a combination of wired and wireless.

ఇంటిలో ఒక నెట్వర్క్లో తన ల్యాప్టాప్, స్మార్ట్ ఫోన్, వ్యక్తిగత డిజిటల్ అసిస్టెంట్ మరియు పోర్టబుల్ ప్రింటర్ను ఒక వ్యక్తి కనెక్ట్ చేయవచ్చు. ఈ నెట్వర్క్ పూర్తిగా Wi-Fi లేదా వైర్డు మరియు వైర్లెస్ కలయిక కావచ్చు .

Local Area Network (LAN)

లోకల్ ఏరియా నెట్వర్క్ (LAN)



LAN or Local Area Network is a wired network spread over a single site like an office, building or manufacturing unit. LAN is set up to when team members need to share software and hardware resources with each other but not with the outside world. Typical software resources include official documents, user manuals, employee handbook, etc.

Hardware resources that can be easily shared over the network include printer, fax machines, modems, memory space, etc. This decreases infrastructure costs for the organization drastically.

LAN లేదా లోకల్ ఏరియా నెట్వర్క్ అనేది కార్యాలయం, భవనం లేదా ఉత్పాదక విభాగం వంటి ఒకే సైట్లో విస్తరించిన వైర్డు నెట్వర్క్. LAN సభ్యులు బృందం సభ్యులు మరియు హార్డ్వేర్ వనరులను పరస్పరం భాగస్వామ్యం చేయవలసి ఉంటుంది, కానీ వెలుపలి ప్రపంచంలో కాదు. సాధారణ సాఫ్ట్వేర్ వనరులు అధికారిక పత్రాలు, వినియోగదారు మాన్యువల్లు, ఉద్యోగి హ్యాండ్బుక్, మొదలైనవి. హార్డ్వేర్ వనరులను సులభంగా భాగస్వామ్యం చేయవచ్చు నెట్వర్క్లో ప్రింటర్, ఫాక్స్ మెషీన్స్, మోడెములు, మెమొరీ స్పేస్ మొదలైనవి ఉన్నాయి. ఇది సంస్థకు మౌలిక సదుపాయాల ఖర్చులను తగ్గిస్తుంది.

Metropolitan Area Network (MAN)

A LAN may be set up using wired or wireless connections. A LAN that is completely wireless is called Wireless LAN or WLAN.

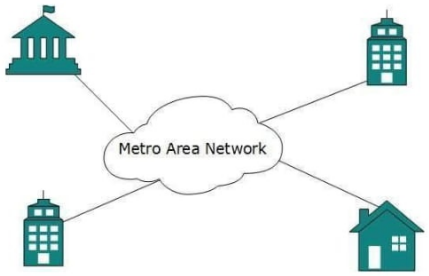
వైర్డు లేదా వైర్లెస్ కనెక్షన్లను ఉపయోగించి LAN ని ఏర్పాటు చేయవచ్చు. పూర్తిగా వైర్లెస్ అని పిలువబడే ఒక LAN వైర్లెస్ LAN లేదా WLAN అంటారు.

The Metropolitan Area Network (MAN) generally expands throughout a city such as cable TV network. It can be in the form of Ethernet, Token-ring, ATM, or Fiber Distributed Data Interface (FDDI).

మెట్రోపాలిటన్ ఏరియా నెట్వర్క్ (MAN) సాధారణంగా కేబుల్ TV నెట్వర్క్ వంటి నగరం అంతటా విస్తరిస్తుంది. ఇది ఈథర్నెట్, టోకెన్-రింగ్, ATM లేదా ఫైబర్ డిస్ట్రిబ్యూటెడ్ డేటా ఇంటర్ఫేస్ (FDDI)

Metro Ethernet is a service which is provided by ISPs. This service enables its users to expand their Local Area Networks. For example, MAN can help an organization to connect all of its offices in a city.

మెట్రో ఈథర్నెట్ అనేది ISP లచే అందించబడిన ఒక సేవ. ఈ సేవ దాని వినియోగదారులకు వారి స్థానిక ఏరియా నెట్వర్క్లను విస్తరించడానికి అనుమతిస్తుంది. ఉదాహరణకు, ఒక సంస్థ తన కార్యాలయాలను నగరంలో కనెక్ట్ చేయడానికి ఒక సంస్థకు సహాయపడుతుంది.



Backbone of MAN is high-capacity and high-speed fiber optics. MAN works in between Local Area Network and Wide Area Network. MAN provides uplink for LANs to WANs or internet.

MAN యొక్క వెన్నెముక అధిక సామర్థ్యం మరియు వేగవంతమైన ఫైబర్ ఆప్టిక్స్. స్థానిక ఏరియా నెట్వర్క్ మరియు వైడ్ ఏరియా నెట్వర్క్ మధ్య MAN పనిచేస్తుంది. WAN లు లేదా ఇంటర్నెట్కు LAN ల కోసం అప్లింక్ని MAN అందిస్తుంది.

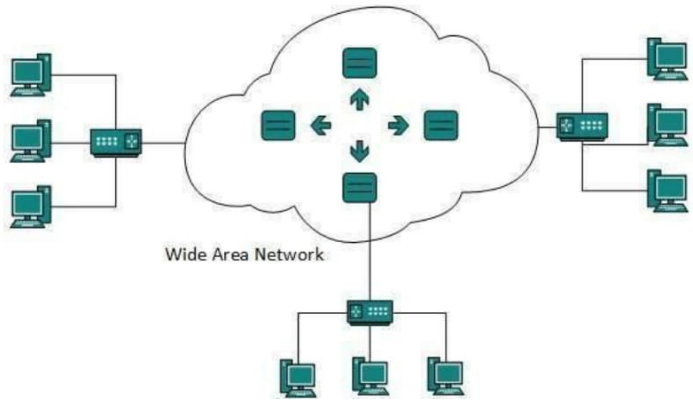
Wide Area Network (WAN)

వైడ్ ఏరియా నెట్వర్క్ (WAN)

As the name suggests,the Wide Area Network (WAN) covers a wide area which may span across provinces and even a whole country. Generally, telecommunication networks are Wide Area Network. These networks provide connectivity to MANs and LANs. Since they are equipped with very high speed backbone, WANs use very expensive network equipment.

పేరు సూచించినట్లుగా, వైడ్ ఏరియా నెట్వర్క్ (డబ్ల్యుఎన్) విస్తృతమైన ప్రదేశంను కలిగి ఉంటుంది, ఇది ప్రావిన్సుల అంతటా మరియు మొత్తం దేశం అంతటా విస్తరించవచ్చు. సాధారణంగా, టెలికమ్యూనికేషన్ నెట్వర్క్లు వైడ్ ఏరియా నెట్వర్క్. ఈ నెట్వర్క్లు MANS మరియు LAN లకు కనెక్టివిటీని అందిస్తాయి. వారు చాలా అధిక వేగం వెన్నెముక కలిగి ఉన్నందున, WAN లు చాలా ఖరీదైన నెట్వర్క్

పరికరాలను ఉపయోగిస్తాయి



WAN may use advanced technologies such as Asynchronous Transfer Mode (ATM), Frame Relay, and Synchronous Optical Network (SONET). WAN may be managed by multiple administrations.

అసిక్రోనస్ బదిలీ మోడ్ (ATM), ఫ్రేమ్ రిలే మరియు సిన్క్రోనస్ ఆప్టికల్ నెట్వర్క్ (SONET) వంటి అధునాతన సాంకేతికతలను WAN వాడవచ్చు. WAN బహుళ నిర్వహణల ద్వారా నిర్వహించబడుతుంది.

Differences between Local Area Networks (LANs) and Wide Area Network (WAN)

స్థానిక ఏరియా నెట్వర్క్ల (LANs) మరియు వైడ్ ఏరియా నెట్వర్క్ (WAN) మధ్య విబేధాలు

A Local Area Network (LAN) is a private computer network that connects computers in small physical areas. Example: A small office, A Single building, multiple buildings inside a campus etc. Wide Area Networks (WAN) is type of computer network to connect offices which are located in different geographical locations. Wide Area Network (WAN) depends mainly on Internet Service Providers (ISPs) for connection solutions.

ఒక స్థానిక ఏరియా నెట్వర్క్ (LAN) అనేది చిన్న కంప్యూటర్లలో కంప్యూటర్లను అనుసంధానించే ప్రైవేట్ కంప్యూటర్ నెట్వర్క్. ఉదాహరణకు: ఒక చిన్న కార్యాలయం, ఒక సింగిల్ బిల్డింగ్, క్యాంపస్ లోపల పలు భవనాలు. వైడ్ ఏరియా నెట్వర్క్లు (WAN) వివిధ రకాలైన కార్యాలయాలను కలిపే కంప్యూటర్ నెట్వర్క్ రకం భౌగోళిక స్థానాలు. వైడ్ ఏరియా నెట్వర్క్ (WAN) కనెక్షన్ పరిష్కారాల కోసం ఇంటర్నెట్ సర్వీస్ ప్రొవైడర్లు (ISP లు) ప్రధానంగా ఆధారపడి ఉంటుంది.

Local Area Network (LAN) has higher bandwidth rates. Current Local Area Networks (LANs) runs on bandwidths of 100 Mbps, 1 Gbps or 10 Gbps. Wide Area Networks (WAN) has lower bandwidth rates compared with Local Area Network (LAN). Current Wide Area Networks runs on bandwidths of 4 Mbps, 8 Mbps, 20 Mbps, 50 Mbps or 100 Mbps.

స్థానిక ఏరియా నెట్వర్క్ (LAN) అధిక బ్యాండ్విడ్త్ రేట్లను కలిగి ఉంది. ప్రస్తుత స్థానిక ఏరియా నెట్వర్క్లు (LAN లు) 100 Mbps, 1 Gbps లేదా 10 Gbps యొక్క బ్యాండ్విడ్త్లలో నడుస్తుంది. వైడ్ ఏరియా నెట్వర్క్స్ (WAN) లోకల్ ఏరియా నెట్వర్క్ (LAN) తో పోలిస్తే తక్కువ బ్యాండ్విడ్త్ రేట్లు ఉన్నాయి. ప్రస్తుత వైడ్ ఏరియా నెట్వర్క్లు 4 Mbps, 8 Mbps, 20 Mbps, 50 Mbps లేదా 100 Mbps యొక్క బ్యాండ్

విడ్త్స్ పై నడుస్తుంది

Local Area Network (LAN) bandwidth rates are almost constant. Local Area Network (LAN) bandwidth rates are dependent on characteristics of the LAN technology in use (Normally FastEthernet or Gigabit Ethernet). Since most of Wide Area Networks (WAN) connectivity solutions are dependent on Internet Service Providers (ISPs), budget related constraints affect the quality of WAN.

స్థానిక ఏరియా నెట్వర్క్ (LAN) బ్యాండ్విడ్త్ రేట్లు దాదాపు స్థిరంగా ఉన్నాయి. స్థానిక ఏరియా నెట్వర్క్ (LAN) బ్యాండ్విడ్త్ రేట్లు ఉపయోగంలో LAN టెక్నాలజీ లక్షణాలు (సాధారణంగా ఫాస్ట్ఈథర్నెట్ లేదా గిగాబిట్ ఈథర్నెట్) ఆధారపడి ఉంటాయి. వైడ్ ఏరియా నెట్వర్క్లు (WAN) అనుసంధాన పరిష్కారాలు ఇంటర్నెట్ సేవా ప్రొవైడర్స్ (ISP లు) పై ఆధారపడి ఉంటాయి కాబట్టి, బడ్జెట్ సంబంధిత అడ్డంకులు WAN యొక్క నాణ్యతను ప్రభావితం చేస్తాయి.

Most of the current Local Area Networks (LANs) use Ethernet as the LAN Standard (FastEthernet 100 Mbps, or Gigabit Ethernet 1/10 Gbps). WAN uses technologies like VPN (Virtual Private Network) over Internet, MPLS, FrameRelay, or Leased Lines as WAN connectivity solutions.

ప్రస్తుత లోకల్ ఏరియా నెట్వర్క్స్ (LAN లు) చాలావరకు ఈథర్నెట్ను LAN స్టాండర్డ్ (ఫాస్ట్ఈథర్నెట్ 100 Mbps లేదా గిగాబిట్ ఈథర్నెట్ 1/10 Gbps) గా ఉపయోగిస్తుంది. WAN ఇంటర్నెట్, MPLS, FrameRelay, లేదా లీనియర్ లైన్స్ వంటి WAN కనెక్టివిటీ పరిష్కారాలు వంటి VPN (వర్చువల్ ప్రైవేట్ నెట్వర్క్) వంటి సాంకేతికతలను ఉపయోగిస్తుంది.

Since Local Area Networks (LANs) are private networks, managed by dedicated local network administrators, Local Area Networks (LANs) are more reliable and secure than Wide Area Networks (WANs). Since Wide Area Networks (WANs) involve 3rd party service providers, WAN networks are less reliable and secure.

స్థానిక ఏరియా నెట్వర్క్స్ (LAN లు) ప్రైవేట్ నెట్వర్కు కావడం వలన ప్రత్యేక స్థానిక నెట్వర్క్ నిర్వాహకులు నిర్వహించబడుతున్నారు, స్థానిక ఏరియా నెట్వర్క్స్ (LAN లు) వైడ్ ఏరియా నెట్వర్క్స్ (WAN లు) కంటే మరింత విశ్వసనీయమైన మరియు సురక్షితమైనవి. వైడ్ ఏరియా నెట్వర్కు (WAN లు) 3 వ పార్టీ సర్వీసు ప్రొవైడర్లను కలిగి ఉన్నందున, WAN నెట్వర్కు తక్కువ నమ్మకమైన మరియు సురక్షితమైనవి

Initial set-up costs for Local Area Networks (LANs) are low as the devices required to set up the networks are cheap. Initial set-up costs for Wide Area Networks (WANs) are high, because of the devices (Routers, Firewalls etc), cables and manpower required.

నెట్వర్కు సెటప్ చేయడానికి అవసరమైన పరికరాలకు తక్కువ ప్రాంతీయ నెట్వర్కు (LAN లు) ప్రారంభ సెట్-అప్ ఖర్చులు తక్కువగా ఉన్నాయి. పరికరాల (రూటర్లు, ఫైర్వాల్స్ తదితరాలు), తంతులు మరియు మానవీయ అవసరాలను బట్టి వైడ్ ఏరియా నెట్వర్క్స్ (WANs) ప్రారంభ సెట్-అప్ ఖర్చులు ఎక్కువగా ఉంటాయి.

Local Area Networks (LANs) running costs are less Wide Area Networks (WANs) running costs are high. Wide Area Networks (WANs) normally have recurring monthly cost as Service Provider access fees.

స్థానిక ఏరియా నెట్వర్కు (LANs) నడుస్తున్న వ్యయాలు తక్కువ వైడ్ ఏరియా నెట్వర్కు (WAN లు) నడుస్తున్న వ్యయాలు ఎక్కువగా ఉంటాయి. వైడ్ ఏరియా నెట్వర్కు (WAN లు) సాధారణంగా నెలవారీ ధరలను సేవా ప్రొవైడర్ యాక్సెస్ ఫీజుగా పునరావృతమవుతాయి

Wide Area Networks (WANs) are more congested than Local Area Networks (LANs).

వైడ్ ఏరియా నెట్వర్కు (WAN లు) స్థానిక ఏరియా నెట్వర్క్స్ (LANs) కంటే మరింత వేగంగా ఉన్నాయి.

Most important Categories of Computer Networks are Local Area Networks (LAN) and Wide Area Networks (WAN). LAN and WAN are the most widely used terms to describe about Computer Networks. However, another Categories of Computer Networks are also rarely used to describe about Computer Networks. Following are the two other categories, which are used to describe about Computer Networks.

కంప్యూటర్ నెట్వర్క్ల యొక్క అతి ముఖ్యమైన వర్గాలు స్థానిక ఏరియా నెట్వర్క్స్ (LAN) మరియు వైడ్ ఏరియా నెట్వర్క్స్ (WAN). LAN మరియు WAN కంప్యూటర్ నెట్వర్క్స్ గురించి వివరించడానికి అత్యంత విస్తృతంగా ఉపయోగించే పదాలు. అయినప్పటికీ, కంప్యూటర్ నెట్వర్క్స్ యొక్క మరొక వర్గాలు అరుదుగా కంప్యూటర్ నెట్వర్క్స్ గురించి వివరించడానికి ఉపయోగిస్తారు. కంప్యూటర్ నెట్వర్క్ల గురించి వివరించడానికి ఉపయోగించబడే రెండు ఇతర వర్గాలు ఉన్నాయి.

1) Campus Area Networks (CAN) 2) Metropolitan Area Network (MAN).

1) క్యాంపస్ ఏరియా నెట్వర్క్స్ (CAN) 2) మెట్రోపాలిటన్ ఏరియా నెట్వర్క్ (MAN).

You can consider Campus Area Networks (CAN) and Metropolitan Area Network (MAN) as the larger versions of Local Area Networks (LAN).

మీరు క్యాంపస్ ఏరియా నెట్వర్క్స్ (CAN) మరియు మెట్రోపాలిటన్ ఏరియా నెట్వర్క్ (MAN) లను స్థానిక ఏరియా నెట్వర్క్స్ (LAN) యొక్క పెద్ద వెర్షన్లుగా పరిగణించవచ్చు.

Campus Area Networks (CAN)

క్యాంపస్ ఏరియా నెట్వర్క్స్ (CAN)

Campus Area Networks (CAN) is a computer network consisting of multiple Local Area Networks (LANs), which is connected together in a huge Campus. For example; inside a huge University, a huge Business Park or a huge Hospital, spanned over multiple buildings, spread over 100s of Acres of land area.

క్యాంపస్ ఏరియా నెట్వర్క్స్ (CAN) అనేది ఒక పెద్ద కంప్యూటర్ క్యాంపస్లో అనుసంధానించబడిన బహుళ లోకల్ ఏరియా నెట్వర్క్లు (LANs) కలిగి ఉన్న ఒక కంప్యూటర్ నెట్వర్క్. ఉదాహరణకి; పెద్ద యూనివర్సిటీలో, ఒక భారీ వ్యాపారం పార్క్ లేదా భారీ ఆసుపత్రి, అనేక భవనాలపై విస్తరించి, 100 ఎకరాల భూమి ప్రాంతంలో విస్తరించింది

Metropolitan Area Network (MAN)

మెట్రోపాలిటన్ ఏరియా నెట్వర్క్ (MAN)

Metropolitan Area Network (MAN) is larger than Campus Area Networks (CAN) when considering the area covered, but, smaller than a Wide Area Networks (WAN). Metropolitan Area Network (MAN) interconnects a number of Local Area Networks (LANs) using a high-bandwidth backbone links inside a city.

మెట్రోపాలిటన్ ఏరియా నెట్వర్క్ (MAN) క్యాంపస్ ఏరియా నెట్వర్క్స్ (CAN) కంటే పెద్దదిగా ఉంటుంది, ఇది వైశాల్యంలో విస్తరించివున్నది, కానీ వైడ్ ఏరియా నెట్వర్క్స్ (WAN) కంటే చిన్నది. మెట్రోపాలిటన్ ఏరియా నెట్వర్క్ (MAN) ఒక నగరంలో అధిక-బ్యాండ్విడ్త్ వెన్నెముక లింకులను ఉపయోగించి పలు స్థానిక ఏరియా నెట్వర్క్స్ (LANs) అనుసంధానిస్తుంది

Computer networks can be logically classified as 1) Peer-to-Peer networks and 2) Client-Server networks

కంప్యూటర్ నెట్వర్క్లు తార్కికంగా వర్గీకరించబడతాయి 1) పీర్ టు పీర్ నెట్వర్క్లు మరియు 2) క్లయింట్-సర్వర్ నెట్వర్క్లు

Peer-to-Peer networks

పీర్-టు-పీర్ నెట్వర్క్లు

A Peer-to-Peer network has no dedicated Servers. Here in Peer-to-Peer network, a number of workstations (or clients) are connected together for the purpose of sharing devices, information or data. All the workstations are considered as equal. Any one computer can act as client or server at any instance. This network is ideal for small networks where there is no need for dedicated servers, like home networks, small business networks, or retail shops. The Microsoft term for Peer-to-Peer network is “Workgroup”.

భాగస్వామ్య పరికరాలు, సమాచారం లేదా డేటా యొక్క ఉద్దేశ్యంతో కలిసి కనెక్ట్ చేయబడతాయి. అన్ని వర్క్స్టేషన్లు సమానంగా పరిగణిస్తారు. ఏదైనా కంప్యూటర్ ఏదైనా క్లయింట్ లేదా సర్వర్ వలె పని చేస్తుంది. హోమ్ నెట్వర్క్లు, చిన్న వ్యాపార నెట్వర్క్లు లేదా రిటైల్ దుకాణాలు వంటి అంకితమైన సర్వర్లకు అవసరంలేని ఈ నెట్వర్క్ చిన్న నెట్వర్క్లకు అనువైనది. పీర్-టు-పీర్ నెట్వర్క్ కోసం Microsoft టర్మ్ "వర్క్ గ్రూప్"

There is no limitation for the number of computers in a peer-to-peer network. But Peer-to-Peer implementations are meant for small networks. Typically a Workgroup contain less than 10 workstations.

పీర్-టూ-పీర్ నెట్వర్క్లో కంప్యూటర్ల సంఖ్యకు ఎటువంటి పరిమితి లేదు. కానీ పీర్-టూ-పీర్ అమలులు చిన్న నెట్వర్క్లకు ఉద్దేశించబడ్డాయి. సాధారణంగా ఒక వర్క్ గ్రూప్లో 10 వర్క్స్టేషన్ల కంటే తక్కువ ఉంటుంది

Normal Workstation Operating Systems are Windows 95/98 (obsolete), Windows ME (obsolete), NT Workstation (obsolete), Windows 2000 professional (obsolete), Windows XP, Vista, Windows 7, Windows 8/8.1, Ubuntu Desktop, RHEL Desktop etc.

Windows వర్క్స్టేషన్ ఆపరేటింగ్ సిస్టమ్స్ విండోస్ 95/98 (వాడుకలో), Windows ME (వాడుకలో), NT వర్క్స్టేషన్ (వాడుకలో), విండోస్ 2000 ప్రొఫెషనల్ (వాడుకలో లేని), విండోస్ XP, విస్టా, విండోస్ 7, విండోస్ 8 / 8.1, ఉబుంటు డెస్క్టాప్, RHEL డెస్క్టాప్

Client-Server Networks

క్లయింట్-సర్వర్ నెట్వర్క్స్

Peer-to-Peer computer networks are good for small business organizations. For example: A small pharmacy outlet, An automobile service center, A small clinic etc. The main disadvantage of Peer-to-Peer networks are listed below.

పీర్-టు-పీర్ కంప్యూటర్ నెట్వర్క్లు చిన్న వ్యాపార సంస్థలకు మంచివి. ఉదాహరణకు: ఒక చిన్న ఫార్మసీ అవుట్లెట్, ఒక ఆటోమొబైల్ సర్వీస్ సెంటర్, ఒక చిన్న క్లినిక్ మొదలైనవి. Peer-to- పీర్ నెట్వర్క్ల ప్రధాన ప్రతికూలత క్రింద ఇవ్వబడ్డాయి.

Everything is kept distributed in different computers.

అంతా విభిన్న కంప్యూటర్లలో పంపిణీ చేయబడుతుంది.

User generated files are stored in individual computers. Data backup is extremely difficult.

యూజర్ ఉత్పత్తి ఫైళ్లు వ్యక్తిగత కంప్యూటర్లలో నిల్వ చేయబడతాయి. డేటా బ్యాకప్ చాలా కష్టం.

Each computer has its own user database. There is no centralized user & user privilege management. Users need to remember their user ids and passwords in every computer. Managing network users is extremely difficult.

ప్రతి కంప్యూటర్కు దాని స్వంత యూజర్ డేటాబేస్ ఉంది. కేంద్రీకృతమైన యూజర్ & వినియోగదారు అధికార నిర్వహణ ఏదీ లేదు. యూజర్లు ప్రతి కంప్యూటర్లో వారి యూజర్ ఐడిలు మరియు పాస్వర్డ్లను గుర్తుంచుకోవాలి. నెట్వర్క్ వినియోగదారులు నిర్వహించడం చాలా కష్టం.

As the organization's network grows, they must gradually upgrade their Peer-to-Peer network to Client-Server based network.
సంస్థ యొక్క నెట్వర్క్ పెరుగుతుంది కాబట్టి, వారు క్రమంగా వారి పీర్-టు-పీర్ నెట్వర్క్ను క్లయింట్-సర్వర్ ఆధారిత నెట్వర్క్కి అప్గ్రేడ్ చేయాలి.

The Client/Server computer network model is made-up of Client compters and Server compters. Now we need to understand the terms Client and Server.
క్లయింట్ / సర్వర్ కంప్యూటర్ నెట్వర్క్ మోడల్ క్లయింట్ compters మరియు సర్వర్ compters తయారు చేస్తారు. ఇప్పుడు మేము క్లయింట్ మరియు సర్వర్ నిబంధనలను అర్థం చేసుకోవాలి.

What is a Client? A computer which is seeking any resource from another computer is a Client Computer. You can think a client as a computer in your network, where a network user is performing some network activity. For Example: Downloading a file from a File Server, Browsing Intranet/Internet etc. The network user normally uses a client computer to perform his day to day work.

క్లయింట్ అంటే ఏమిటి? మరొక కంప్యూటర్ నుండి వనరు కోరుకునే కంప్యూటర్ ఒక క్లయింట్ కంప్యూటర్. మీ నెట్వర్క్లో ఒక క్లయింట్ వలె ఒక క్లయింట్ను మీరు ఆలోచించవచ్చు, ఇక్కడ నెట్వర్క్ వినియోగదారుడు కొన్ని నెట్వర్క్ కార్యాచరణను నిర్వహిస్తున్నారు. ఉదాహరణకు: ఒక ఫైల్ సర్వర్, బ్రౌజింగ్ ఇంట్రానెట్ / ఇంటర్నెట్ నుండి ఒక ఫైల్ను డౌన్లోడ్ చేయడం. నెట్వర్క్ వినియోగదారు సాధారణంగా రోజువారీ పనిని నిర్వహించడానికి క్లయింట్ కంప్యూటర్ను ఉపయోగిస్తుంది

What is a Server? If a computer has a resource which is served to another computer, it is a Server computer. The client establishes a connection to a Server and accesses the services installed on the Server. A Server is not meant for a network user to browse in internet or do spreadsheet work. A Server computer is installed with appropriate Operating System and related Software to serve the network clients with one or more services, continuously without a break.
ఒక సర్వర్ అంటే ఏమిటి? ఒక కంప్యూటర్కు మరొక కంప్యూటర్కు అందించబడిన వనరు ఉంటే, ఇది సర్వర్ కంప్యూటర్. క్లయింట్ సర్వర్కు కనెక్షన్ను ఏర్పాటు చేస్తుంది మరియు సర్వర్లో ఇన్స్టాల్ చేసిన సేవలను ప్రాప్యత చేస్తుంది. ఇంటర్నెట్లో బ్రౌజ్ చేయడానికి లేదా స్ప్రెడ్షీట్ పని చేయడానికి నెట్వర్క్ వినియోగదారు కోసం ఒక సర్వర్ ఉద్దేశించబడింది కాదు. ఒక సర్వర్ కంప్యూటర్ తగిన ఆపరేటింగ్ సిస్టమ్తో మరియు సంబంధిత సాఫ్ట్వేర్తో నెట్వర్క్ క్లయింట్లను ఒకటి లేదా మరిన్ని సేవలను అందించడానికి, విరామం లేకుండా నిరంతరంగా ఇన్స్టాల్ చేయబడుతుంది.

In a Client-Server network, high-end servers, installed with the Network Operating System (Server Operating System) and the related software, serve the clients continuously on a network, by providing them with specific services upon request.

క్లయింట్-సర్వర్ నెట్వర్క్లో, నెట్వర్క్ ఆపరేటింగ్ సిస్టమ్ (సర్వర్ ఆపరేటింగ్ సిస్టమ్) మరియు సంబంధిత సాఫ్ట్వేర్తో ఇన్స్టాల్ చేయబడిన ఉన్నత-స్థాయి సర్వర్లు, అభ్యర్థనపై నిర్దిష్ట సేవలను అందించడం ద్వారా నెట్వర్క్లను నిరంతరంగా సేవలు అందిస్తాయి.

Well known Server Operating System Products are Windows 2012 / Windows 2012 R2, Unix (Oracle Solaris, IBM AIX, HP UX, FreeBSD, NetBSD, OpenBSD, SCO Unix etc), GNU/Linux (RedHat Enterprise Linux, Debian Linux, SUSE Enterprise, Ubuntu Server, CentOS Server, Mandriva, Fedora etc.

GNU / Linux (RedHat Enterprise Linux, డెబియన్ లినక్స్, SUSE ఎంటర్ప్రైజెస్, డెవలప్మెంట్ సిస్టమ్స్), విండోస్ 2012 / విండోస్ 2012 R2, యూనిక్స్ (ఒరాకిల్ సోలారిస్, IBM AIX, HP UX, FreeBSD, NetBSD, OpenBSD, SCO Unix మొదలైనవి) ఉబుంటు సర్వర్, సెంట్రస్ సర్వర్, మాండ్రివా, ఫెడోరా మొదలైనవి

Client-Server networks require dedicated servers. Server hardware is more costlier than normal Desktop computers. Client-Server networks cost more than peer-to-peer networks. Network Operating System (Server Operating System) are also costlier than Desktop Operating Systems.

క్లయింట్-సర్వర్ నెట్వర్కు ప్రత్యేక సర్వర్లకు అవసరం. సాధారణ డెస్క్టాప్ కంప్యూటర్ల కంటే సర్వర్ హార్డ్వేర్ ఎక్కువ ఖరీదు. క్లయింట్-సర్వర్ నెట్వర్కు పీర్-టు-పీర్ నెట్వర్క్ల కంటే ఎక్కువ ఖర్చు చేస్తాయి. డెస్క్టాప్ ఆపరేటింగ్ సిస్టమ్స్ కంటే నెట్వర్క్ ఆపరేటింగ్ సిస్టమ్ (సర్వర్ ఆపరేటింగ్ సిస్టమ్) కూడా ఖరీదు .

Different types of Servers used in networks are listed below.

నెట్వర్క్లలో ఉపయోగించిన వివిధ రకాల సర్వర్లు క్రింద ఇవ్వబడ్డాయి .

File Server: File servers are used to store the user documents and files centrally. An ideal file server should have a large amount of memory and storage space, fast hard-disks, multiple processors, fast network adapters, redundant power supplies etc.

ఫైల్ సర్వర్: ఫైల్ సర్వర్లు యూజర్ పత్రాలు మరియు ఫైళ్లను కేంద్రంగా నిల్వ చేయడానికి ఉపయోగించబడతాయి. ఒక ఆదర్శ ఫైల్ సర్వరు పెద్ద మొత్తంలో మెమొరీ మరియు నిల్వ స్థలాన్ని కలిగి ఉండాలి, ఫాస్ట్ హార్డ్ డిస్కు, బహుళ ప్రాసెసర్లు, ఫాస్ట్ నెట్వర్క్ ఎడాప్టర్లు, అనవసరమైన విద్యుత్ సరఫరా

A File server runs FTP (File Transfer Protocol) in Windows, Linux or Unix Networks, or SMBP (Server Message Block Protocol) in Windows Networks. Well known FTP software products are Micrsoft IIS, vsftpd, Apache FTP Server etc.

విండోస్ నెట్వర్క్ విండోస్, లైనక్స్ లేదా యూనిక్స్ నెట్వర్క్స్, లేదా SMBP (సర్వర్ మెసేజ్ బ్లాక్ ప్రోటోకాల్) లో ఫైల్ ఫైల్ సర్వర్ FTP (ఫైల్ ట్రాన్స్ఫర్ ప్రోటోకాల్) ను నడుపుతుంది. బాగా తెలిసిన FTP సాఫ్ట్వేర్ ఉత్పత్తులు మైక్రోసాఫ్ట్ IIS, vsftpd, Apache FTP సర్వర్ మొదలైనవి.

The main advantage of keeping network user files and electronic documents centrally in a file server is that the network user files and documents can be managed (backup'd) easily. Think about managing network user files and electronic documents kept distributed inside user workstations in a network consists of thousands of computers! Nearly impossible.

నెట్వర్క్ యూజర్ ఫైల్స్ మరియు ఎలక్ట్రానిక్ పత్రాలను ఒక ఫైల్ సర్వర్లో ఉంచడం యొక్క ప్రధాన ప్రయోజనం ఏమిటంటే, నెట్వర్క్ యూజర్ ఫైల్లు మరియు పత్రాలను సులభంగా నిర్వహించవచ్చు (బ్యాకప్). నెట్వర్కు యూజర్ ఫైళ్లను మేనేజింగ్ మరియు ఒక నెట్వర్క్లో వినియోగదారు వర్క్స్టేషన్ల లోపల పంపిణీ చేయబడిన ఎలక్ట్రానిక్ పత్రాలను నిర్వహించడం గురించి ఆలోచించండి వేలాది

కంప్యూటర్లు! దాదాపు అసాధ్యం.

Print Server: Print Server, which redirects print jobs from client computers to specific printers.
ప్రింట్ సర్వర్: ప్రింట్ సర్వర్, క్లయింట్ కంప్యూటర్ల నుండి నిర్దిష్ట ప్రింటర్లకు ముద్రణ జాబ్లను దారి మళ్లించే.

Mail Server: Mail Servers are used to transmit emails using email protocols. Most widely used email transmission protocol is SMTP (Simple Mail Transfer Protocol). Mail Servers exchange emails between different domains.

మెయిల్ సర్వర్: మెయిల్ సర్వర్లు ఇమెయిల్ ప్రోటోకాల్లను ఉపయోగించి ఇమెయిల్లను ప్రసారం చేయడానికి ఉపయోగించబడతాయి. అత్యంత విస్తృతంగా ఉపయోగించే ఇమెయిల్ ప్రసార ప్రోటోకాల్ SMTP (సింపుల్ మెయిల్ ట్రాన్స్ఫర్ ప్రోటోకాల్). మెయిల్ సర్వర్లు వివిధ డొమైన్ల మధ్య ఇమెయిల్లను మార్పిడి చేస్తాయి.

Most widely used Mail Server software products are Microsoft Exchange Server, SENDMAIL (now proofpoint), qmail, Postfix etc.
మైక్రోసాఫ్ట్ ఎక్స్ఛేంజ్ సర్వర్, SENDMAIL (ఇప్పుడు ప్రూఫ్ పాయింట్), qmail, పోస్ట్ఫిక్స్ మొదలగునవి.

Application Server: Common computer applications or programs which are required by different network users can be run in a central server, which enables multiple network users to access common network applications from the network. Typically Application Servers run business logic. Which means, every business is different and the Application Server is the Server Software which controls the business process. Some examples for Application Server Software are SAP BASIS, WebLogic, WebSphere etc.
అప్లికేషన్ సర్వర్: వేర్వేరు నెట్వర్క్ వినియోగదారుల ద్వారా అవసరమయ్యే సాధారణ కంప్యూటర్ అప్లికేషన్లు లేదా కార్యక్రమాలు సెంట్రల్ సర్వర్లో అమలు చేయబడతాయి, ఇది నెట్వర్క్ నుండి సాధారణ నెట్వర్క్ అనువర్తనాలను ప్రాప్తి చేయడానికి పలు నెట్వర్క్ వినియోగదారులను అనుమతిస్తుంది. సాధారణంగా అప్లికేషన్ సర్వర్లు వ్యాపార లాజిక్ను అమలు చేస్తాయి. దీని అర్థం, ప్రతి వ్యాపారం భిన్నంగా ఉంటుంది మరియు అప్లికేషన్ సర్వర్ వ్యాపార ప్రక్రియను నియంత్రించే సర్వర్ సాఫ్ట్వేర్. అప్లికేషన్ సర్వర్ సాఫ్ట్వేర్ కోసం కొన్ని ఉదాహరణలు SAP

Database Server: Database Server allows authorized network clients to create, view, modify and/or delete an organization's data, stored in a common database.
డేటాబేస్ సర్వర్: డేటాబేస్ సర్వర్ అధీకృత నెట్వర్క్ ఖాతాదారులకు ఒక సాధారణ డేటాబేస్లో నిల్వచేసిన ఒక సంస్థ యొక్క డేటాను సృష్టించడానికి, వీక్షించడానికి, సవరించడానికి మరియు / లేదా తొలగించడానికి అనుమతిస్తుంది .

Examples of Database Management Systems are Oracle 10g/11g, Microsoft SQL Server 2000/2005/2008/2012, PostgreSQL,IBM DB2, MySQL, Sybase, Informix etc.
డేటాబేస్ మేనేజ్మెంట్ సిస్టమ్స్ ఉదాహరణలు ఒరాకిల్ 10g / 11g, మైక్రోసాఫ్ట్ SQL సర్వర్ 2000/2005/2008/2012, PostgreSQL, IBM DB2, MySQL, Sybase, ఇన్ఫార్మిక్స్ మొదలైనవి .

Directory Servers: Directory Servers allows the central administration and management of network users and network resources. Directory Servers provide the basic functions of network security, Authentication, Authorization and Accounting.

డైరెక్టరీ సర్వర్లు: డైరెక్టరీ సర్వర్లు సెంట్రల్ అడ్మినిస్ట్రేషన్ మరియు నెట్వర్క్ యూజర్లు మరియు నెట్వర్క్ వనరుల నిర్వహణను

అనుమతిస్తుంది. డైరెక్టరీ సర్వర్లు నెట్వర్క్ భద్రత, ప్రామాణీకరణ, ఆథరైజేషన్ మరియు అకౌంటింగ్ యొక్క ప్రాథమిక విధులను అందిస్తాయి.

Examples of Directory Servers are Microsoft Active Directory, NetIQ eDirectory, Fedora Directory Server, OpenLDAP etc.

డైరెక్టరీ సర్వర్లు యొక్క ఉదాహరణలు Microsoft Active Directory, NetIQ eDirectory, Fedora డైరెక్టరీ సర్వర్, OpenLDAP మొదలైనవి.

Centralized and Distributed Computer Network Model

సెంట్రలైజ్డ్ మరియు డిస్ట్రిబ్యూటెడ్ కంప్యూటర్ నెట్వర్క్ మోడల్

Another logical classification of computer networks is Centralized and Distributed Computer Network Model.

కంప్యూటర్ నెట్వర్క్ల యొక్క మరొక తార్కిక వర్గీకరణ సెంట్రలైజ్డ్ మరియు డిస్ట్రిబ్యూటెడ్ కంప్యూటర్ నెట్వర్క్ మోడల్.

In Centralized computer network model, the network resources are placed and managed from a main location. Centralized network model allows administrators to manage the resources centrally (typically in Head Office). The network servers and other critical network resources are located in a central location in a secure and dedicated server room.

కేంద్రీకృత కంప్యూటర్ నెట్వర్క్ నమూనాలో, నెట్వర్క్ వనరులు ఒక ప్రధాన స్థానం నుండి ఉంచుతారు మరియు నిర్వహించబడతాయి.

సెంట్రలైజ్డ్ నెట్వర్క్ మోడల్ నిర్వాహకులు వనరులను కేంద్రంగా (ప్రధానంగా హెడ్ ఆఫీసులో) నిర్వహించడానికి అనుమతిస్తుంది.

నెట్వర్క్ సర్వర్లు మరియు ఇతర క్లిష్టమైన నెట్వర్క్ వనరులు సురక్షిత మరియు అంకితమైన సర్వర్ గదిలో కేంద్ర స్థానం లో ఉన్నాయి.

Centralized network model provides following advantages to Network and System Administrators. Centralized network model provides Network and System Administrators better access to network Devices

కేంద్రీకృత నెట్వర్క్ నమూనా నెట్వర్క్ మరియు సిస్టమ్ అడ్మినిస్ట్రేటర్లకు క్రింది ప్రయోజనాలను అందిస్తుంది. సెంట్రైస్డ్ నెట్వర్క్ మోడల్ నెట్వర్క్ మరియు సిస్టమ్ అడ్మినిస్ట్రేటర్లను నెట్వర్క్కు మంచి ప్రాప్తిని అందిస్తుంది పరికరాల.

In Centralized network model, Network Resources can be managed more easily Centralized network model provides better Network Security.

సెంట్రైజ్డ్ నెట్వర్క్ మోడల్లో, నెట్వర్క్ రిసోర్సెస్ను మరింత సులభంగా నిర్వహించవచ్చు.

The main disadvantage is more work load of Network and System Administrators and increased risk of communication failure due to a catastrophe in the central location.

ప్రధాన ప్రతికూలత నెట్వర్క్ మరియు సిస్టమ్ అడ్మినిస్ట్రేటర్స్ యొక్క ఎక్కువ పని లోడ్ మరియు కేంద్ర స్థానంలో ఒక విపత్తు కారణంగా కమ్యూనికేషన్ వైఫల్యం పెరగడం

In Distributed network model, the network resources are placed and managed from different geographical locations. Designated network and system administrators manage the network resources in different locations. These days most of the Enterprise network models are distributed.

పంపిణీ చేయబడిన నెట్వర్క్ నమూనాలో, నెట్వర్క్ వనరులు వేర్వేరు భౌగోళిక ప్రాంతాల్లో ఉంచబడతాయి మరియు నిర్వహించబడతాయి. నియమించబడిన నెట్వర్క్ మరియు సిస్టమ్ నిర్వాహకులు వివిధ ప్రాంతాలలో నెట్వర్క్ వనరులను నిర్వహించండి. ఈ రోజుల్లో అత్యధిక Enterprise నెట్వర్క్ నమూనాలు పంపిణీ చేయబడతాయి.

Internetworks, Internet, Intranet and Extranet

ఇంటర్ నెట్వర్క్స్, ఇంటర్నెట్, ఇంట్రానెట్ మరియు ఎక్స్ట్రానెట్ Internetworks

Before discussing about the terms internet, intranet and extranet, we need to discuss the term Internetwork.

ఇంటర్నెట్, ఇంట్రానెట్ మరియు ఎక్స్ట్రానెట్ పదాలు గురించి చర్చించడానికి ముందు, మేము ఈ పదాన్ని చర్చించవలసి ఉంటుంది ఇంటర్.

An internetwork can be defined as two or more computer networks (typically Local Area Networks LAN) which are connected together, usinng Network Routers.

ఒక ఇంటర్నెట్వర్క్ను రెండు లేదా అంతకంటే ఎక్కువ కంప్యూటర్ నెట్వర్క్లు (సాధారణంగా స్థానిక ఏరియా నెట్వర్క్స్ LAN) గా నిర్వచించవచ్చు, ఇది నెట్వర్క్ రూటర్లు ఉపయోగిస్తుంది.

Each network in an Internetwork has its own Network Address, which is different from other networks inside the Internetwork. Network Address is used to identify the networks inside an Internetwork.

ఇంటర్ నెట్వర్లో ఉన్న ప్రతి నెట్వర్క్ ఇంటర్ నెట్ వర్క్ లోపల ఇతర నెట్వర్క్ల నుండి భిన్నమైన దాని సొంత నెట్వర్క్ చిరునామాను కలిగి ఉంటుంది. ఇంటర్ నెట్ వర్క్ లోపల నెట్వర్క్లను గుర్తించడానికి నెట్వర్క్ చిరునామా ఉపయోగించబడుతుంది

Internetwork allows different users at different geographical locations of an organization to share data, resources and to communicate. Modern businesses cannot even function without Internetwork. Internet, Intranet and Extranet are different types of internetwork.

సంస్థ యొక్క విభిన్న భౌగోళిక ప్రాంతాల్లో డేటా, వనరులు మరియు కమ్యూనికేట్ చేయడానికి పంచుకోవడానికి ఇంటర్ నెట్ వర్క్ అనుమతిస్తుంది. ఆధునిక వ్యాపారాలు ఇంటర్ వర్క్ లేకుండా పనిచేయవు. ఇంటర్నెట్, ఇంట్రానెట్ మరియు ఎక్స్ట్రానెట్ అనేవి ఇంటర్ నెట్ వర్క్ యొక్క వివిధ రకాలు.

Internet, Intranet and Extranet

ఇంటర్నెట్, నెట్ మరియుఎక్స్ట్రానెట్

Internet: Internet is a worldwide, publicly accessible computer network of interconnected computer networks (internetwork) that transmit data using the standard Internet Protocol (IP). Internet is the world's largest Internet work .

అంతర్జాలం: ఇంటర్నెట్ అనేది ఇంటర్నెట్ ఇంటర్నెట్ ఎక్స్ ప్రోటోకాల్ (ఐపి) ను ఉపయోగించి డేటాను ప్రసారం చేసే ఇంటర్కనెక్టడ్ కంప్యూటర్ నెట్వర్క్ల (ఇంటర్ నెట్వర్క్) యొక్క ప్రపంచవ్యాప్త, బహిరంగంగా అందుబాటులో ఉన్న కంప్యూటర్ నెట్వర్క్. ఇంటర్నెట్ ప్రపంచంలోనే అతిపెద్ద ఇంటర్నెట్వర్క్.

The terms World Wide Web (WWW) and Internet are not the same. The Internet is a collection of interconnected computer networks, linked by copper wires, fiber-optic cables, wireless connections, etc. World Wide Web (WWW) is a collection of interconnected documents and other resources, linked by hyperlinks and URLs. The World Wide Web is one of the services accessible via the Internet, along with various others including email, file sharing, remote administration, video streaming, online gaming etc.

నిబంధనలు వరల్డ్ వైడ్ వెబ్ (WWW) మరియు ఇంటర్నెట్ అదే కాదు. ఇంటర్నెట్ అనేది ఇంటర్కనెక్టడ్ కంప్యూటర్ నెట్వర్క్ల సముదాయం, ఇది రాగి వైర్లు, ఫైబర్-ఆప్టిక్ తంతులు, వైర్లెస్ కనెక్షన్లు మొదలైనవాటికి సంబంధించినది. వరల్డ్ వైడ్ వెబ్ (WWW) అనుసంధానమైన పత్రాలు మరియు ఇతర వనరుల సంకలనం, హైపర్ లింక్లు మరియు URL లతో ముడిపడి ఉంది. వరల్డ్ వైడ్ వెబ్

ఇంటర్నెట్ ద్వారా అందుబాటులో ఉన్న సేవలలో ఒకటి, ఇమెయిల్, ఫైల్ షేరింగ్, రిమోట్ అడ్మినిస్ట్రేషన్, వీడియో స్ట్రీమింగ్, ఆన్లైన్ గేమింగ్ మొదలైనవి.

Intranet: An intranet is a private network that is contained within an enterprise. It may consist of many interlinked local area networks and use any Wide Area Network (WAN) technologies for network connectivity. The main purpose of an intranet is to share company information and computing resources among employees. Intranet is a private Internetwork, which is usually created and maintained by a private organization. The content available inside Intranet are intended only for the members of that organization (usually employees of a company).

ఇంట్రానెట్: ఇంట్రానెట్ ఒక సంస్థలో ఉన్న ఒక ప్రైవేట్ నెట్వర్క్. ఇది అనేక అంతర్లీనంగా ఉన్న స్థానిక ప్రాంత నెట్వర్క్లను కలిగి ఉంటుంది మరియు నెట్వర్క్ కనెక్టివిటీ కోసం ఏ వైడ్ ఏరియా నెట్వర్క్ (WAN) సాంకేతిక పరిజ్ఞానాలను ఉపయోగిస్తుంది. ఇంట్రానెట్ యొక్క ప్రధాన ప్రయోజనం కంపెనీ సమాచారం మరియు ఉద్యోగుల మధ్య వనరులను గణించడం. ఇంట్రానెట్ అనేది ఒక ప్రైవేట్ ఇంటర్ నెట్వర్క్, ఇది సాధారణంగా ఒక ప్రైవేట్ సంస్థ ద్వారా సృష్టించబడుతుంది మరియు నిర్వహించబడుతుంది. ఇంట్రానెట్ లోపల అందుబాటులో ఉన్న కంటెంట్ ఆ సంస్థ యొక్క సభ్యులకు మాత్రమే ఉద్దేశించబడింది (సాధారణంగా కంపెనీ యొక్క ఉద్యోగులు).

Extranet: An extranet can be viewed as part of a company's intranet that is extended to users outside the company like suppliers, vendors, partners, customers, or other business associates.

ఎక్స్ట్రానెట్: ఒక ఎక్స్ట్రానెట్ను సంస్థ యొక్క ఇంట్రానెట్లో భాగంగా వీక్షించవచ్చు, ఇది సరఫరాదారులు, విక్రేతలు, భాగస్వాములు, వినియోగదారులు లేదా ఇతర వ్యాపార భాగస్వాములు వంటి సంస్థకు వెలుపల వినియోగదారులకు విస్తరించబడుతుంది.

Extranet is required for normall day-to-day business activities. For example, Placing order to registered vendors, Billing & Invoices, Payments, Joint Ventures, Product Brochures for Partners, Discounted price lists for partners etc.

రోజువారీ వ్యాపార కార్యకలాపాలకు ఎక్స్ట్రానెట్ అవసరం. ఉదాహరణకు, రిజిస్టర్డ్ విక్రేతలకు, బిల్లింగ్ & ఇన్వాయిస్లు, చెల్లింపులు, జాయింట్ వెంచర్స్, పార్టనర్లకు ఉత్పత్తి బ్రోచర్లు, భాగస్వాముల కోసం రాయితీ ధరల జాబితాలు మొదలైనవాటిని ఉంచడం.

What is a Network Protocol

నెట్వర్క్ ప్రోటోకాల్ అంటే ఏమిటి

A network protocol can be viewed as a common network communication standard, which is used to define a method of exchanging data over a computer network. Network protocols define rules and conventions for communication between different devices, participating in a computer network.

ఒక నెట్వర్క్ ప్రోటోకాల్ను ఒక సాధారణ నెట్వర్క్ కమ్యూనికేషన్ ప్రమాణంగా చూడవచ్చు, ఇది కంప్యూటర్ నెట్వర్క్లో డేటాను మార్పిడి చేసే పద్ధతిని నిర్వచించడానికి ఉపయోగిస్తారు. నెట్వర్క్ ప్రోటోకాల్లు కంప్యూటర్ పరికరంలో పాల్గొనే వివిధ పరికరాల మధ్య కమ్యూనికేషన్ కోసం నియమాలు మరియు సమావేశాలను నిర్వచిస్తాయి.

Almost all protocols used in the Internet are common standards defined by RFC (Request for Comments).

ఇంటర్నెట్లో ఉపయోగించే దాదాపు అన్ని ప్రోటోకాల్స్ RFC (విమర్శల కోసం అభ్యర్థన) ద్వారా నిర్వచించబడిన సాధారణ ప్రమాణాలు.

Examples of standard network protocols are TCP (Transmission Control Protocol), UDP (User Datagram

Protocol), IP (Internet Protocol), ARP (Address Resolution Protocol), HTTP (Hypertext Transfer Protocol), FTP (File Transfer Protocol), TFTP (Trivial File Transfer Protocol), SMTP (Simple Mail Transfer Protocol), SSH (Secure Shell), Telnet etc.

ప్రామాణిక నెట్వర్క్ ప్రోటోకాల్ యొక్క ఉదాహరణలు TCP (ట్రాన్స్మిషన్ కంట్రోల్ ప్రోటోకాల్), UDP (వినియోగదారు డేటాగ్రామ్ ప్రోటోకాల్), IP (ఇంటర్నెట్ ప్రోటోకాల్), ARP (అడ్రస్ రిజల్యూషన్ ప్రోటోకాల్), HTTP (హైపర్టెక్స్ట్ ట్రాన్స్ఫర్ ప్రోటోకాల్), FTP (ఫైల్ ట్రాన్స్ఫర్ ప్రోటోకాల్), TFTP (ట్రివియల్ ఫైల్ ట్రాన్స్ఫర్ ప్రోటోకాల్), SMTP (సింపుల్ మెయిల్ ట్రాన్స్ఫర్ ప్రోటోకాల్), SSH (సెక్యూర్ షెల్), టెల్నెట్.

Devices participating in network communication should know about the common network protocol and communicate according to the way, defined by the network protocol. In other words, standard network protocol software must be running on both devices participating in network communication.

నెట్వర్క్ కమ్యూనికేషన్లో పాల్గొనే పరికరాలను సాధారణ నెట్వర్క్ ప్రోటోకాల్ గురించి తెలుసుకోవాలి మరియు నెట్వర్క్ ప్రోటోకాల్ ద్వారా నిర్వచించబడిన విధంగా, కమ్యూనికేట్ చేయాలి. మరో మాటలో చెప్పాలంటే, నెట్వర్క్ కమ్యూనికేషన్లో పాల్గొనే రెండు పరికరాల్లో ప్రామాణిక నెట్వర్క్ ప్రోటోకాల్ సాఫ్ట్వేర్ను తప్పనిసరిగా అమలు చేయాలి.

To explain it more clearly, if you are using your browser to browse web pages from a web server (example, www.omnisecu.com), you are using a protocol called HTTP (Hypertext Transfer Protocol). Your computer must request web pages from web server using HTTP and the web server must response back to your computer using HTTP.

వెబ్ బ్రౌజర్ నుండి (ఉదాహరణకు, www.omnisecu.com) వెబ్ పేజీలను బ్రౌజ్ చేయడానికి మీరు మీ బ్రౌజరును ఉపయోగిస్తుంటే మరింత స్పష్టంగా వివరించడానికి, మీరు HTTP (హైపర్టెక్స్ట్ ట్రాన్స్ఫర్ ప్రోటోకాల్) అనే ప్రోటోకాల్ను ఉపయోగిస్తున్నారు. HTTP మరియు వెబ్ సర్వర్ ఉపయోగించి వెబ్ సర్వర్ నుండి వెబ్ పేజీలు HTTP ను ఉపయోగించి మీ కంప్యూటర్కు ప్రతిస్పందనగా తప్పనిసరిగా మీ కంప్యూటర్ను అభ్యర్థించాలి.

How HTTP (Hypertext Transfer Protocol) should work is defined as a common standard, RFC (Request for Comments) 2616. Anyone can follow the common standard and create their own Browser or Web server.

ఎలా HTTP (హైపర్టెక్స్ట్ ట్రాన్స్ఫర్ ప్రోటోకాల్) ఒక సాధారణ ప్రమాణంగా నిర్వచించబడాలి, RFC (వ్యాఖ్యలు కోసం అభ్యర్థన) 2616. ఎవరైనా సాధారణ ప్రమాణాన్ని అనుసరించవచ్చు మరియు వారి సొంత బ్రౌజర్ లేదా వెబ్ సర్వర్ని సృష్టించవచ్చు .

Difference between Proprietary and Standard Protocols

యాజమాన్య మరియు ప్రామాణిక ప్రోటోకాల్స్ మధ్య వ్యత్యాసం

Two terms are often used in networking industry, when describing network protocols.

నెట్వర్కు ప్రోటోకాల్లను వివరించేటప్పుడు రెండు పదాలు తరచూ నెట్వర్కింగ్ పరిశ్రమలో ఉపయోగించబడతాయి.

1) Proprietary Protocol 2) Standard Protocol

Proprietary protocols are usually developed by a single company for the devices (or Operating System) which they manufacture. AppleTalk is a proprietary protocol developed by Apple Inc. Appletalk protocol may work well in network environments consisting only Apple devices. But other vendors may not

support Appletalk protocol. Proprietary protocols will not scale well in network environments consisting of multi-vendor equipments.

యాజమాన్య ప్రోటోకాల్లు సాధారణంగా పరికరాల (లేదా ఆపరేటింగ్ సిస్టం) కోసం ఒకే సంస్థ ద్వారా అభివృద్ధి చేస్తాయి. ఆపిల్టాక్ ఆపిల్ ఇంక్ ద్వారా అభివృద్ధి చేయబడిన యాజమాన్య ప్రోటోకాల్. ఆపిల్టాల్క్ ప్రోటోకాల్ ఆపిల్ పరికరాలతో కూడిన నెట్వర్క్ పరిసరాలలో బాగా పనిచేస్తుంది. కానీ ఇతర విక్రేతలు Appletalk ప్రోటోకాల్కు మద్దతు ఇవ్వలేవు. బహుళ-విక్రేత పరికరాలను కలిగి ఉండే నెట్వర్క్ పరిసరాలలో యాజమాన్య ప్రోటోకాల్లు బాగా స్కేల్ చేయవు.

Standard protocols are agreed and accepted by whole industry. Standard protocols are not vendor specific. Standard protocols are often developed by collaborative effort of experts from different organizations.
ప్రామాణిక ప్రోటోకాల్లను మొత్తం పరిశ్రమ అంగీకరించింది మరియు అంగీకరించింది. ప్రామాణిక ప్రోటోకాల్స్ విక్రేత నిర్దిష్ట కాదు. వివిధ సంస్థల నిపుణుల సహకార కృషి ద్వారా ప్రామాణిక ప్రోటోకాల్లను తరచుగా అభివృద్ధి చేస్తారు.
Examples of standard protocols are IP, TCP, UDP etc. RFC (Request for Comments) is an IETF platform to develop Standard Protocols.
ప్రామాణిక ప్రోటోకాల్స్ యొక్క ఉదాహరణలు IP, TCP, UDP మొదలైనవి. RFC (వ్యాఖ్యల కొరకు అభ్యర్థన) అనేది ప్రామాణిక ప్రోటోకాల్లను అభివృద్ధి చేయడానికి ఒక IETF వేదిక.

To understand the concept of standard protocols more clearly, take a real world example of shaving blade. A shaving blade has a globally agreed and accepted shape, so that it can fit well in a razor manufactured by different vendors.

ప్రామాణిక ప్రోటోకాల్స్ యొక్క భావనను మరింత స్పష్టంగా అర్థం చేసుకోవడానికి, బ్లేడును కత్తిరించే వాస్తవ ప్రపంచ ఉదాహరణను తీసుకోండి. ఒక షేవింగ్ బ్లేడ్ ప్రపంచవ్యాప్త అంగీకరించింది మరియు ఆమోదించబడిన ఆకారం కలిగి ఉంది, దీని వలన వేరే అమ్మకందారులచే తయారు చేయబడిన రేజర్లో ఇది బాగా సరిపోతుంది.

What are RFCs (Request for Comments)
RFCs (వ్యాఖ్యలు కోసం అభ్యర్థన) ఏమిటి

A RFC (Request for Comments) is a pure technical document published by the Internet Engineering Task Force (IETF). Request for Comments (RFCs) are mainly used to develop a "standard" network protocol, a function of a network protocol or any feature which is related with network communication.
ఒక RFC (వ్యాఖ్యల కొరకు అభ్యర్థన) అనేది ఇంటర్నెట్ ఇంజనీరింగ్ టాస్క్ ఫోర్స్ (IETF) చేత ప్రచురించబడిన స్వచ్ఛమైన సాంకేతిక పత్రం. వ్యాఖ్యలు కోసం అభ్యర్థన (RFC లు) ప్రధానంగా ఒక "ప్రామాణిక" నెట్వర్క్ ప్రోటోకాల్, నెట్వర్క్ ప్రోటోకాల్ యొక్క ఒక ఫంక్షన్ లేదా నెట్వర్క్ కమ్యూనికేషన్తో సంబంధం ఉన్న ఏదైనా లక్షణాన్ని అభివృద్ధి చేయడానికి ఉపయోగిస్తారు.

Some RFCs are informational and others are published Internet standards. The final version of the RFC becomes the standard and is published with a number. No further comments or changes are permitted for the final version. Changes are permitted only via subsequent RFCs that supersede the previous RFCs.

కొన్ని RFC లు సమాచారం మరియు ఇతరులు ఇంటర్నెట్ ప్రమాణాలు ప్రచురించబడుతున్నాయి. RFC యొక్క చివరి వెర్షన్ ప్రమాణంగా మారుతుంది మరియు ఇది ఒక సంఖ్యతో ప్రచురించబడుతుంది. చివరి సంస్కరణకు తదుపరి వ్యాఖ్యలు లేదా మార్పులు అనుమతించబడవు. మునుపటి RFC లను అధిగమించిన తదుపరి RFC ల ద్వారా మాత్రమే మార్పులు అనుమతించబడతాయి .

At the early stages of network communication, each vendor had their own proprietary network communication protocols. Different network protocols for the same purpose were a serious problem in heterogeneous network environments, consisting of devices and Operating Systems from different vendors.

నెట్వర్క్ కమ్యూనికేషన్ యొక్క ప్రారంభ దశల్లో, ప్రతి విక్రేత వారి సొంత యాజమాన్య నెట్వర్క్ కమ్యూనికేషన్ ప్రోటోకాల్స్ను కలిగి ఉన్నారు. అదే ప్రయోజనం కోసం వేర్వేరు నెట్వర్క్ ప్రోటోకాల్లు వైవిధ్యమైన నెట్వర్క్ వాతావరణాలలో తీవ్రమైన సమస్యగా ఉన్నాయి, వేర్వేరు వ్యాపారుల నుండి పరికరాలను మరియు ఆపరేటింగ్ సిస్టమ్లను కలిగి ఉంటుంది .

"Standard" network protocols are not considered as proprietary. Any vendor can develop application software or drivers based on defined RFC standard. Hence RFC provides a strong base for cross platform network communication.

"ప్రామాణిక" నెట్వర్క్ ప్రోటోకాల్లు యాజమాన్యంగా పరిగణించబడవు. ఏదైనా విక్రేత అనువర్తన సాఫ్ట్వేర్ లేదా నిర్దిష్ట RFC ప్రామాణిక ఆధారంగా డ్రైవర్లను అభివృద్ధి చేయవచ్చు. అందువల్ల క్రాస్ ప్లాట్ఫాట్ కమ్యూనికేషన్ కోసం RFC బలమైన ఆధారాన్ని అందిస్తుంది.

All the standard network protocols (like, HTTP, FTP, SMTP, TCP, UDP, IP etc) are defined as RFCs. Individuals may join the IETF working groups to help draft and develop networking standards or network protocols

అన్ని ప్రామాణిక నెట్వర్క్ ప్రోటోకాల్లు (HTTP, FTP, SMTP, TCP, UDP, IP మొదలైనవి) RFC లుగా నిర్వచించబడ్డాయి. వ్యక్తులు IETF వర్కింగ్ గ్రూపులలో ముసాయిదా సహాయం మరియు నెట్వర్కింగ్ ప్రమాణాలు లేదా నెట్వర్క్ ప్రోటోకాల్లను అభివృద్ధి చేయటానికి ఉండవచ్చు

Organizations which control Internet, Network Protocols and Standards

ఇంటర్నెట్, నెట్వర్క్ ప్రోటోకాల్స్ మరియు స్టాండర్డ్స్ ను నియంత్రించే సంస్థలు

Institute of Electrical and Electronics Engineers (IEEE)

ఇన్స్టిట్యూట్ ఆఫ్ ఎలక్ట్రికల్ అండ్ ఎలక్ట్రానిక్స్ ఇంజనీర్స్ (IEEE)

The Institute of Electrical and Electronics Engineers (IEEE, pronounced as "eye-triple-e") is an organization which was formed in 1963 in USA. The Institute of Electrical and Electronics Engineers (IEEE) is the world's largest association for Electrical and Electronics Engineers. Institute of Electrical and Electronics Engineers (IEEE) was formed by the merger of two other technical organizations, American Institute of Electrical Engineers and Institute of Radio Engineers in 1st January, 1963. Today, IEEE has about 500,000 members, from different countries in the world.

ఇన్స్టిట్యూట్ ఆఫ్ ఎలక్ట్రికల్ అండ్ ఎలక్ట్రానిక్స్ ఇంజనీర్స్ (IEEE, "కంటి-ట్రిపుల్-ఇ" గా ఉచ్ఛరిస్తారు) a అమెరికాలో 1963 లో స్థాపించబడిన సంస్థ. ఇన్స్టిట్యూట్ ఆఫ్ ఎలక్ట్రికల్ అండ్ ఎలక్ట్రానిక్స్ ఇంజనీర్స్ (IEEE) ఎలక్ట్రికల్ అండ్ ఎలక్ట్రానిక్స్ ఇంజనీర్స్ కోసం ప్రపంచంలోని అతిపెద్ద సంస్థ. ఇన్స్టిట్యూట్ ఆఫ్ ఎలక్ట్రికల్ అండ్ ఎలక్ట్రానిక్స్ ఇంజనీర్స్ (IEEE) రెండు ఇతర సాంకేతిక సంస్థల, అమెరికన్ ఇన్స్టిట్యూట్ ఆఫ్ ఎలెక్ట్రికల్ ఇంజనీర్స్ మరియు ఇన్స్టిట్యూట్ ఆఫ్ రేడియో ఇంజనీర్స కలయికతో జనవరి 1, 1963 లో ఏర్పడింది. నేడు, IEEE ప్రపంచంలోని వివిధ దేశాల నుండి 500,000 మంది సభ్యులను కలిగి ఉంది.

The Institute of Electrical and Electronics Engineers (IEEE) develop and maintain standards in every technology field related with electricity. The Institute of Electrical and Electronics Engineers (IEEE) develop and maintain Local Area Network (LAN) networking standards including Ethernet (IEEE 802.3 family standards) and Wireless LAN (IEEE 802.11 family standards).

ఇన్స్టిట్యూట్ ఆఫ్ ఎలక్ట్రికల్ అండ్ ఎలక్ట్రానిక్స్ ఇంజనీర్స్ (IEEE) విద్యుత్తో సంబంధించి ప్రతి టెక్నాలజీ రంగంలో ప్రమాణాలను అభివృద్ధి చేసి, నిర్వహించాలి. ఇన్స్టిట్యూట్ ఆఫ్ ఎలక్ట్రికల్ అండ్ ఎలక్ట్రానిక్స్ ఇంజనీర్స్ (IEEE) ఈథర్నెట్ (IEEE 802.3 ఫ్యామిలీ స్టాండర్డ్స్) మరియు వైర్లెస్ LAN (IEEE 802.11 ఫ్యామిలీ స్టాండర్డ్స్) లతో సహా స్థానిక ఏరియా నెట్వర్క్ (LAN) నెట్వర్కింగ్ ప్రమాణాలను అభివృద్ధి చేసి నిర్వహించవచ్చు.

Internet Corporation for Assigned Names and Numbers (ICANN) & Internet Assigned Numbers Authority (IANA)

ఇంటర్నెట్ కార్పోరేషన్ ఫర్ అసైన్డ్ నేమ్స్ అండ్ నంబర్స్ (ICANN) & ఇంటర్నెట్ అసైన్డ్ నంబర్స్ అథారిటీ (IANA)

The Internet Corporation for Assigned Names and Numbers (ICANN, pronounced "eye can") is an international non-profit corporation which is in charge of Internet Protocol (IP) address allocation (IPv4 and IPv6), Domain Names allocation (examples, omnisecu.com, msn.com, google.com) Global public Domain Name System management, DNS Root Server maintenance, Port Number allocation etc.

ఇంటర్నెట్ ప్రోటోకాల్ (IP) అడ్రస్ కేటాయింపు (IPv4 మరియు IPv6), డొమైన్ పేర్లు కేటాయింపు (ఉదాహరణలు, omnisecu.) అనేది అంతర్జాతీయ లాభాపేక్ష రహిత సంస్థ, ఇది అసైన్డ్ నేమ్స్ అండ్ నంబర్స్ (ICANN, "కన్ను చెయ్యవచ్చు" com, msn.com, google.com) గ్లోబల్ పబ్లిక్ డొమెయిన్ నేమ్ సిస్టం మేనేజ్మెంట్, DNS రూట్ సర్వర్ నిర్వహణ, పోర్ట్ నంబర్ కేటాయింపు మొదలైనవి

Previously Internet Assigned Numbers Authority (IANA) was in control of above functions. Now above functions are under ICANN.

గతంలో ఇంటర్నెట్ అసైన్డ్ నంబర్స్ అథారిటీ (IANA) పైన విధులు నియంత్రణలో ఉంది. ఇప్పుడు పైన ఉన్న పనులు ICANN కింద ఉన్నాయి.

Internet Architecture Board (IAB)

ఇంటర్నెట్ ఆర్కిటెక్చర్ బోర్డు (IAB)

Internet Architecture Board (IAB, pronounced "i-a-b") defines the architecture for the Internet. The Internet Architecture Board (IAB) purpose is to provide oversight of the architecture for the protocols and other procedures used by the Internet.

ఇంటర్నేషనల్ ఆర్కిటెక్చర్ బోర్డ్ (IAB, ఉచ్చారణ "i-a-b") అంతర్జాలం యొక్క నిర్మాణాన్ని నిర్వచిస్తుంది. అంతర్జాలం యొక్క ప్రోటోకాల్స్ మరియు ఇతర విధానాల కోసం నిర్మాణాన్ని పర్యవేక్షించడం ఇంటర్నెట్ ఆర్కిటెక్చర్ బోర్డు (IAB) ఉద్దేశ్యం.

Internet Society (ISOC)

ఇంటర్నెట్ సొసైటీ (ISOC)

The Internet Society (ISOC) is mainly involved in policy, governance, technology, education & training

and development of internet.

ఇంటర్నెట్ సొసైటీ (ISOC) ప్రధానంగా పాలసీ, పాలన, సాంకేతికత, విద్య మరియు శిక్షణ మరియు ఇంటర్నెట్ అభివృద్ధికి సంబంధించినది .

Following is a quote of from Internet Society (ISOC) website.

క్రింది ఇంటర్నెట్ సొసైటీ (ISOC) వెబ్సైట్ నుండి ఒక కోట్ ఉంది.

"The Internet Society is here to ensure that the Internet continues to develop as an open platform; one that serves the economic, social, and educational needs of individuals throughout the world."

"ఇంటర్నెట్ అనేది ఓపెన్ ప్లాట్ఫారమ్గా అభివృద్ధి చెందుతున్నదని నిర్ధారించడానికి ఇక్కడ ఇంటర్నెట్ సొసైటీ ఉంది, ప్రపంచవ్యాప్తంగా వ్యక్తుల యొక్క ఆర్థిక, సామాజిక మరియు విద్యా అవసరాలను తీరుస్తుంది."

Internet Research Task Force (IRTF) & Internet Engineering Task Force (IETF)

ఇంటర్నెట్ రీసెర్చ్ టాస్క్ ఫోర్స్ (IRTF) & ఇంటర్నెట్ ఇంజనీరింగ్ టాస్క్ ఫోర్స్ (IETF)

The Internet Research Task Force (IRTF, pronounced as "i-r-t-f") is a technology research organization which is working on focused long-term research on technical topics related to standard Internet protocols, applications, architecture and technology.

ఇంటర్నెట్ రీసెర్చ్ టాస్క్ ఫోర్స్ (IRTF, "i-r-t-f" గా ఉచ్ఛరిస్తారు) అనేది ఒక సాంకేతిక పరిశోధనా సంస్థ, ఇది ప్రామాణిక ఇంటర్నెట్ ప్రోటోకాల్, అప్లికేషన్లు, ఆర్కిటెక్చర్ మరియు టెక్నాలజీకి సంబంధించిన సాంకేతిక అంశాలపై దృష్టి సారించిన దీర్ఘ-కాల పరిశోధనలపై పని చేస్తుంది.

Internet Engineering Task Force (IETF, pronounced as "i-e-t-f") is another organization working to develop the short-term issues of network engineering protocols and standards.

ఇంటర్నెట్ ఇంజనీరింగ్ టాస్క్ ఫోర్స్ (IETF, "i-e-t-f" అని ఉచ్ఛరిస్తారు) నెట్వర్క్ ఇంజనీరింగ్ ప్రోటోకాల్స్ మరియు ప్రమాణాల యొక్క స్వల్పకాలిక సమస్యలను అభివృద్ధి చేసే మరొక సంస్థ .

Internet Engineering Task Force (IETF) develop the maintain high quality relevant technical standards, mainly network protocols. The network protocol standards are developed under a platform, called as Request for Comments (RFCs).

ఇంటర్నెట్ ఇంజనీరింగ్ టాస్క్ ఫోర్స్ (IETF) నిర్వహించడానికి అధిక నాణ్యతా సంబంధిత సాంకేతిక ప్రమాణాలను, ప్రధానంగా నెట్వర్క్ ప్రోటోకాల్స్ను అభివృద్ధి చేస్తుంది. నెట్వర్క్ ప్రోటోకాల్ ప్రమాణాలు ప్లాట్ఫారమ్ కింద అభివృద్ధి చేయబడ్డాయి, వీటిని అభ్యర్థన కోసం అభ్యర్థన (RFC లు)

A Request for Comments (RFC) is a technical publication of the Internet Engineering Task Force (IETF) and the Internet Society. Request for Comments (RFCs) are mainly used to develop a network protocol, a function of a network protocol or any feature which is related with network communication. All the standard network protocols (like, HTTP, FTP, SMTP, TCP, UDP, IP etc) are defined as RFSs. Individuals may join the IETF working groups to help draft and develop networking standards or network protocols.

ఒక అభ్యర్థన కోసం అభ్యర్థన (RFC) అనేది ఇంటర్నెట్ ఇంజనీరింగ్ టాస్క్ ఫోర్స్ యొక్క సాంకేతిక ప్రచురణ (IETF) మరియు ఇంటర్నెట్

సొసైటీ. వ్యాఖ్యలు కోసం అభ్యర్థన (RFC లు) ప్రధానంగా నెట్వర్క్ ప్రోటోకాల్, నెట్వర్క్ ప్రోటోకాల్ యొక్క ఒక ఫంక్షన్ లేదా నెట్వర్క్ కమ్యూనికేషన్తో సంబంధం ఉన్న ఏదైనా లక్షణాన్ని అభివృద్ధి చేయడానికి ఉపయోగిస్తారు. అన్ని ప్రామాణిక నెట్వర్క్ ప్రోటోకాల్లు (HTTP, FTP, SMTP, TCP, UDP, IP మొదలైనవి) RFS లుగా నిర్వచించబడ్డాయి. వ్యక్తులు IETF వర్కింగ్ గ్రూపులలో ముసాయిదా సహాయం మరియు నెట్వర్కింగ్ ప్రమాణాలు లేదా నెట్వర్క్ ప్రోటోకాల్లను అభివృద్ధి చేయటానికి ఉండవచ్చు.

World Wide Web Consortium (W3C)

వరల్డ్ వైడ్ వెబ్ కన్సార్టియం (W3C)

World Wide Web Consortium (W3C) is global organization working to define technologies related with World Wide Web like HTML, scripting languages, protocols for Web servers etc.

వరల్డ్ వైడ్ వెబ్ కన్సార్టియం (W3C) అనేది వరల్డ్ వైడ్ వెబ్ HTML, స్క్రిప్టింగ్ లాంగ్వేజ్, వెబ్ సర్వర్ల కోసం ప్రోటోకాల్స్ వంటి సాంకేతికతలను నిర్వచించడానికి పని చేస్తుంది.

Network Topologies
నెట్వర్క్ టోపోలాజీలు

The way in which devices are interconnected to form a network is called network topology. Some of the factors that affect choice of topology for a network are –

నెట్వర్కును ఏర్పరుచుటకు పరికరములు అనుసంధానించబడిన విధంగా నెట్వర్క్ టోపోలాజీ అంటారు. నెట్వర్క్ కోసం టోపాలజీ ఎంపిక ప్రభావితం కొన్ని కారకాలు

- **Cost** – Installation cost is a very important factor in overall cost of setting up an infrastructure. So cable lengths, distance between nodes, location of servers, etc. have to be considered when designing a network.

  • మౌలిక సదుపాయాన్ని ఏర్పాటు చేయడానికి మొత్తం ఖర్చులో ఖర్చు-సంస్థాపన వ్యయం చాలా ముఖ్యమైన అంశం. కాబట్టి కేబుల్ పొడవులు, నోడ్ల మధ్య దూరం, సర్వర్ల స్థానం, మొదలైనవి ఒక నెట్వర్క్ను రూపొందిస్తున్నప్పుడు పరిగణించాలి.

- **Flexibility** – Topology of a network should be flexible enough to allow reconfiguration of office set up, addition of new nodes and relocation of existing nodes.
  ఫ్లెక్సిబులిటీ - ఒక నెట్వర్క్ యొక్క టోపాలజీ కార్యాలయపు పునఃనిర్మాణాన్ని, కొత్త నోడ్లను అదనంగా మరియు ఇప్పటికే ఉన్న నోడ్ల పునఃస్థాపనకు అనుమతించడానికి తగినంత సౌకర్యవంతమైన ఉండాలి.

- **Reliability** – Network should be designed in such a way that it has minimum down time. Failure of one node or a segment of cabling should not render the whole network useless.
- **విశ్వసనీయత** - నెట్వర్క్ కనీస సమయం తక్కువగా ఉన్న విధంగా రూపొందించాలి. ఒక నోడ్ యొక్క వైఫల్యం లేదా కేబులింగ్ విభాగంలో మొత్తం నెట్వర్క్ పనికిరానిది కాదు.

- **Scalability** – Network topology should be scalable, i.e. it can accommodate load of new devices

and nodes without perceptible drop in performance.

స్కేలబిలిటీ - నెట్వర్క్ టోపోలాజి అనేది స్కేలబుల్గా ఉండాలి, అంటే ఇది పనితీరులో గ్రహణశీల డ్రాప్ లేకుండా కొత్త పరికరాలను మరియు నోడ్లను లోడ్ చేయగలదు .

- **Ease of installation** – Network should be easy to install in terms of hardware, software and technical personnel requirements.

  సంస్థాపన యొక్క సౌలభ్యం - హార్డ్వేర్, సాఫ్ట్వేర్ మరియు సాంకేతిక సిబ్బంది అవసరాలను తీర్చడం కోసం నెట్వర్క్ను సులభంగా ఇన్స్టాల్ చేసుకోవచ్చు .

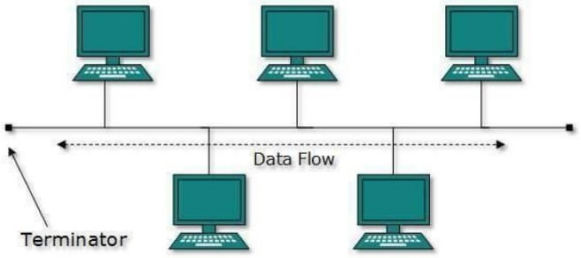
- **Ease of maintenance** – Troubleshooting and maintenance of network should be easy.

నిర్వహణ యొక్క సౌలభ్యం - ట్రబుల్ షూటింగ్ మరియు నిర్వహణ నెట్వర్క్ సులభంగా ఉండాలి .

Bus Topology
బస్ టోపోలాజి

Data network with bus topology has a **linear transmission cable**, usually **coaxial**, to which many **network devices** and **workstations** are attached along the length. **Server** is at one end of the bus. When a workstation has to send data, it transmits **packets** with **destination address** in its header along the bus.

బస్ టోపోలాజీతో ఉన్న డేటా నెట్వర్క్ సాధారణంగా సరళ ప్రసార కేబుల్ను కలిగి ఉంటుంది, సాధారణంగా ఇది చాలా పొడవుతో పాటు అనేక నెట్వర్క్ పరికరాలు మరియు వర్క్స్టేషన్లు జోడించబడతాయి. బస్ యొక్క చివరిలో సర్వర్ ఉంది. ఒక వర్క్స్టేషన్ డేటాను పంపించాల్సినప్పుడు, అది బస్లో ఉన్న దాని ముఖ్య భాగంలో గమ్య చిరునామాతో ప్యాకెట్లను ప్రసారం చేస్తుంది.



The data travels in both the directions along the bus. When the destination terminal sees the data, it copies it to the local disk.

డేటా బస్సు వెంట రెండు దిశలలో ప్రయాణిస్తుంది. గమ్యం టెర్మినల్ డేటాను చూసినప్పుడు, అది స్థానిక డిస్కుకు కాపీ చేస్తుంది.

Advantages of Bus Topology బస్ టోపోలాజి యొక్క ప్రయోజనాలు

These are the advantages of using bus topology –

ఈ బస్ టోపోలాజిని ఉపయోగించడం యొక్క ప్రయోజనాలు -

- Easy to install and maintain (సులువు ఇన్స్టాల్ మరియు నిర్వహించడానికి)
- Can be extended easily(సులభంగా విస్తరించవచ్చు)
- Very reliable because of single transmission line

(సింగిల్ ట్రాన్స్మిషన్ లైన్ కారణంగా చాలా నమ్మకమైనది)

- Disadvantages of Bus Topology
- బస్ టోపోలాజి యొక్క ప్రతికూలతలు

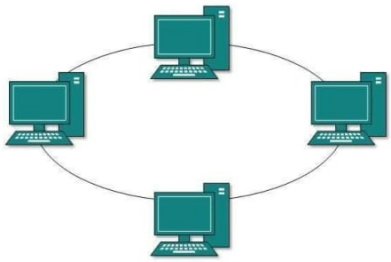
These are some disadvantages of using bus topology –
ఇవి బస్ టోపోలాజీని ఉపయోగించుకోవడానికి కొన్ని ప్రతికూలతలు

- Troubleshooting is difficult as there is no single point of control
- నియంత్రణా నియంత్రణ ఏదీ లేనందున ట్రబుల్ షూటింగ్ కష్టం
- One faulty node can bring the whole network down
  నియంత్రణా నియంత్రణ ఏదీ లేనందున ట్రబుల్ షూటింగ్ కష్టం
- Dumb terminals cannot be connected to the bus
- యంత్రణా నియంత్రణ ఏదీ లేనందున ట్రబుల్ షూటింగ్ కష్టం

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.
రింగ్ టోపోలాజీలో ప్రతి టెర్మినల్ సరిగ్గా రెండు నోడ్లకు అనుసంధానించబడి, నెట్వర్క్ ఒక వృత్తాకార ఆకారంను ఇస్తుంది. డేటా

ముందుగా నిర్ణయించిన దిశలో మాత్రమే ప్రయాణిస్తుంది



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 raverses 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.
ఒక టెర్మినల్ డేటాను పంపించాల్సినప్పుడు, అది దానిని పొరుగున ఉన్న నోడ్కు బదిలీ చేస్తుంది, అది దానిని తదుపరిదానికి బదిలీ చేస్తుంది. తదుపరి బదిలీ డేటా విస్తరించడానికి ముందు. ఈ విధంగా, నెట్వర్క్ నెట్వర్క్ను రజ్జు చేసి, గమ్య నోడ్కు చేరుకుంటుంది, ఇది నెట్వర్క్ నుండి తొలగిస్తుంది. డేటా పంపినవారికి చేరుకున్నట్లయితే, అది డేటాను తొలగిస్తుంది మరియు తరువాత దానిని పంపుతుంది.

Advantages of Ring Topology
రింగ్ టోపాలజీ యొక్క ప్రయోజనాలు

These are the advantages of using ring topology –
ఈరింగ్టోపోలాజిని ఉపయోగించడం యొక్క ప్రయోజనాలు

- Small cable segments are needed to connect two nodes
- రెండు నోడ్లను కనెక్ట్ చేయడానికి చిన్న కేబుల్ విభాగాలు అవసరమవుతాయి
- Ideal for optical fibres as data travels in only one direction
  డేటా ఒక దిశలో ప్రయాణిస్తుంది వంటి ఆప్టికల్ ఫైబర్స్ కోసం ఆదర్శ

- Very high transmission speeds possible
  చాలా ఎక్కువ ప్రసార వేగం సాధ్యం

Disadvantages of Ring Topology
రింగ్ టోపాలజీ యొక్క ప్రతికూలతలు

These are some the disadvantages of using ring topology –
ఈ రింగ్ టోపోలాజిని ఉపయోగించే కొన్ని ప్రతికూలతలు

- Failure of single node brings down the whole network
  ఒకే నోడ్ యొక్క వైఫల్యం మొత్తం నెట్వర్క్ను తెస్తుంది
- Troubleshooting is difficult as many nodes may have to be inspected before faulty one is identified

అనేక నోడ్స్ తప్పుగా గుర్తించబడటానికి ముందు తనిఖీ చేయవలసి వచ్చినప్పుడు ట్రబుల్ షూటింగ్ కష్టం

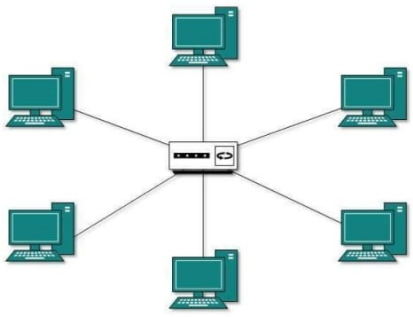
- Difficult to remove one or more nodes while keeping the rest of the network intact

చెక్కుచెదరకుండా ఉన్న మిగిలిన నెట్వర్క్ను ఉంచుతూ ఒకటి లేదా అంతకంటే ఎక్కువ నోడ్లను తొలగించటం కష్టం

Star Topology
స్టార్ టోపోలాజీ

In star topology, server is connected to each node individually. Server is also called the central node. Any exchange of data between two nodes must take place through the server. It is the most popular topology for information and voice networks as central node can process data received from source node before sending it to the destination node.

స్టార్ టోపోలాజీలో, సర్వర్ ప్రతి నోడ్కు వ్యక్తిగతంగా అనుసంధానించబడి ఉంటుంది. సర్వర్ కూడా కేంద్ర నోడ్ అని పిలుస్తారు. రెండు నోడ్ల మధ్య ఉన్న ఏ డేటా మార్పిడి అయినా సర్వర్ ద్వారా జరగాలి. సెంట్రల్ నోడ్, గమ్య నోడ్కు పంపే ముందే మూలం నోడ్ నుంచి డేటాను ప్రాసెస్ చేయగలదు, ఇది సమాచారం మరియు వాయిస్ నెట్వర్క్లకు అత్యంత ప్రసిద్ధ టోపోలాజి.



Advantages of Star Topology
స్టార్ టోపాలజీ యొక్క ప్రయోజనాలు

These are the advantages of using star topology
ఇవి స్టార్ టోపోలాజిని వాడుకునే ప్రయోజనాలు

- Failure of one node does not affect the network
- నోడ్ యొక్క వైఫల్యం నెట్వర్క్ను ప్రభావితం చేయదు

- Troubleshooting is easy as faulty node can be detected from central node immediately
- కేంద్ర నోడ్ నుండి తప్పుగా నోడ్ గుర్తించబడటంతో ట్రబుల్షూటింగ్ సులభం
- Simple access protocols required as one of the communicating nodes is always the central node
- భాషించే నోడ్లలో ఒకదానికి అవసరమైన సాధారణ యాక్సెస్ ప్రోటోకాల్లు ఎల్లప్పుడూ కేంద్ర నోడ్

Disadvantages of Star Topology

స్టార్ టోపోలాజి యొక్క ప్రతికూలతలు

These are the disadvantages of using star topology –

ఇవి స్టార్ టోపోలాజిని ఉపయోగించే ప్రతికూలతలు

- Long cables may be required to connect each node to the server

సర్వర్కు ప్రతి నోడ్ను కనెక్ట్ చేయడానికి లాంగ్ కేబుల్స్ అవసరం కావచ్చు

- Failure of central node brings down the whole network

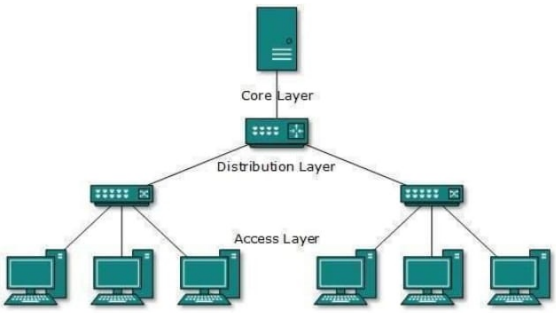
కేంద్ర నోడ్ యొక్క వైఫల్యం మొత్తం నెట్వర్క్ను తెస్తుంది

Tree Topology

ట్రీ టోపాలజీ

Tree topology has a group of star networks connected to a linear bus backbone cable. It incorporates features of both star and bus topologies. Tree topology is also called hierarchical topology

ట్రీ టోపోలాజీలో ఒక సరళ బస్ వెన్నెముక కేబుల్తో అనుసంధానమైన స్టార్ నెట్వర్క్ల సమూహం ఉంది. ఇది స్టార్ మరియు బస్ టోపోలాజీల యొక్క లక్షణాలను కలిగి ఉంటుంది. ట్రీ టోపోలాజిని కూడా హెరారికల్ టోపోలాజీ అని కూడా పిలుస్తారు.



Advantages of Tree Topology

ట్రీ టోపాలజీ యొక్క ప్రయోజనాలు

These are some of the advantages of using tree topology –

ఇవి చెట్టు టోపోలాజిని ఉపయోగించే కొన్ని ప్రయోజనాలు

- Existing network can be easily expanded
- ఇప్పటికే ఉన్న నెట్వర్క్ సులభంగా విస్తరించబడుతుంది
- Point-to-point wiring for individual segments means easier installation and maintenance
- వ్యక్తిగత విభాగాల కోసం పాయింట్-టు-పాయింట్ వైరింగ్ సులభంగా సంస్థాపన మరియు నిర్వహణ అంటే

- Well suited for temporary networks
- తాత్కాలిక నెట్వర్క్లకు బాగా సరిపోతుంది

Disadvantages of Tree Topology

చెట్టు టోపాలజీ యొక్క ప్రతికూలతలు

These are some of the disadvantages of using tree topology

ఇవి చెట్టు టోపోలాజిని ఉపయోగించే ప్రతికూలమైనవి

–Technical expertise required to configure and wire tree topology

ఆకృతీకరించుటకు మరియు వైర్ చెట్టు టోపోలాజికి సాంకేతిక నైపుణ్యం అవసరం

- Failure of backbone cable brings down entire network
- వెన్నెముక కేబుల్ వైఫల్యం మొత్తం నెట్వర్క్ను తెస్తుంది
- Insecure network
- అసురక్షిత నెట్వర్క్
- Maintenance difficult for large networks
- పెద్ద నెట్వర్క్ల కోసం నిర్వహణ కష్టం

Types of network devices

నెట్వర్క్ పరికరాల రకాలు

Network devices are the devices used for organizing a network, connecting to a network, routing the packets, strengthening the signals, communicating with others, surfing the web, sharing files on the network and many more uses.

నెట్వర్క్ పరికరాలను నెట్వర్క్ను నిర్వహించడానికి, నెట్వర్క్కి కనెక్ట్ చేయడం, ప్యాకెట్లను రూటింగ్ చేయడం, సంకేతాలను పటిష్టం చేయడం, ఇతరులతో కమ్యూనికేట్ చేయడం, వెబ్ సర్ఫింగ్, నెట్వర్క్లో ఫైల్లను భాగస్వామ్యం చేయడం మరియు అనేక ఇతర ఉపయోగాలు వంటివి.

To build a home network or connect to other network you will need to have some common networking devices like internal or external modem, wireless router, cables, connectors and clipping tools.

హోమ్ నెట్వర్క్ను నిర్మించటానికి లేదా ఇతర నెట్వర్క్కు కనెక్ట్ చెయ్యడానికి మీరు అంతర్గత లేదా బాహ్య మోడెమ్, వైర్లెస్ రౌటర్, కేబుల్స్, కనెక్టర్ లు మరియు క్లిప్పింగ్ టూల్స్ వంటి సాధారణ నెట్వర్క్ పరికరాలను కలిగి ఉండాలి.

These networking devices are explained in brief in this chapter.

Types of network devices

నెట్వర్క్ పరికరాల రకాలు

- Modem
- Hub
- Switch
- NIC
- Repeater
- Bridge

- Router
- Gateway

Modem

Definition

Modem is a device that converts digital signal to analog signal as a modulator and analog signal to digital signal as a demodulator.

మోడెమ్ డిజిటల్ సిగ్నల్ను అనలాగ్ సిగ్నల్ను మాడ్యులేటర్గా మరియు అనలాగ్ సిగ్నల్గా డిజిటల్గా మారుస్తుంది డెమొడ్యూలేటర్గా సంకేతం

In simple language modem is a device that is used to connect with internet. Technically it is a device which enables digital data transmission to be transmitted over telecommunication lines. A Telco company uses entirely different data transmission technology from the technology that a PC uses for data transmission. A modem understands both technologies. It converts the technology that a PC uses in the technology which a Telco company understand. It enables communication between PC (Known as DTE) and Telco company's office (Known as DCE).

సాధారణ భాష మోడెమ్లో ఇంటర్నెట్తో కనెక్ట్ అయ్యే ఒక పరికరం. సాంకేతికంగా అది టెలికమ్యూనికేషన్ మార్గాల ద్వారా ప్రసారం చేయటానికి డిజిటల్ సమాచార బదిలీని కల్పించే పరికరం. ఒక టెలికాం సంస్థ డేటా బదిలీ కోసం ఒక PC ఉపయోగించే టెక్నాలజీ నుండి పూర్తిగా వేర్వేరు సమాచార ప్రసార సాంకేతిక పరిజ్ఞానాన్ని ఉపయోగిస్తుంది. మోడెమ్ రెండు టెక్నాలజీలను అర్థం చేసుకుంటుంది. ఇది టెకాకో కంపెనీని అర్థం చేసుకునే టెక్నాలజీలో PC ని ఉపయోగించే సాంకేతికతను ఇది మారుస్తుంది. ఇది PC (DTE అని పిలుస్తారు) మరియు Telco సంస్థ కార్యాలయం (DCE గా పిలువబడుతుంది) మధ్య కమ్యూనికేషన్ను అనుమతిస్తుంది.

Description
వివరణ

- Enable computers to communicate over telephone lines.
- టెలిఫోన్ లైన్లతో కమ్యూనికేట్ చేయడానికి కంప్యూటర్లను ప్రారంభించండి .
- Speed of modem is measured in bits per second and varies depending upon the type of modem.
- మోడెమ్ యొక్క వేగం సెకనుకు బిట్స్ లో కొలుస్తారు మరియు మోడెమ్ యొక్క రకాన్ని బట్టి మారుతుంది.
- Higher the speed, the faster you can send and receive data over the network.
- అధిక వేగం, వేగంగా మీరు నెట్వర్క్ డేటాను పంపవచ్చు మరియు స్వీకరించవచ్చు.
- Used to connect computer to the internet.
- ఇంటర్నెట్కు కంప్యూటర్ను కనెక్ట్ చేయడానికి ఉపయోగించబడుతుంది .

Working(వర్కింగ్)

- Consider a communication between two computers A and B.

A మరియు B. రెండు కంప్యూటర్ల మధ్య ఒక కమ్యూనికేషన్ను పరిగణించండి .

- Computer A transmits the digital signals to its modem in the form of binary 0's and 1's.

కంప్యూటర్ A బైనరీ 0 మరియు 1 యొక్క రూపంలో డిజిటల్ సంకేతాలను దాని మోడెమ్కు బదిలీ చేస్తుంది .

- Modem of computer A converts these digital signals it into analog signals and sends over the

telephone line. This process is called as modulator.

కంప్యూటర్ యొక్క మోడెమ్ ఈ డిజిటల్ సంకేతాలను అనలాగ్ సిగ్నల్స్గా మారుస్తుంది మరియు టెలిఫోన్ లైన్పై పంపుతుంది . ఈ ప్రక్రియను మాడ్యులేటర్గా పిలుస్తారు.

- While at the other end, modem of computer B receives the analog signals and converts back into digital signals. This process is called as demodulator.
- మరోవైపు, కంప్యూటర్ B యొక్క మోడెమ్ అనలాగ్ సిగ్నల్స్ అందుకుంటుంది మరియు డిజిటల్ సిగ్నల్స్గా మారుతుంది. ఈ ప్రక్రియను demodulator గా పిలుస్తారు
- Converted digital signals by the modem are sent to the computer B for processing.
  మోడెమ్ ద్వారా డిజిటల్ సిగ్నల్స్ మార్చబడినవి ప్రాసెసింగ్ కోసం కంప్యూటర్ B కు పంపబడతాయి.
- In similar way computer B can communicate with computer A.

అదేవిధంగా కంప్యూటర్ B కంప్యూటర్ కంప్యూటర్తో కమ్యూనికేట్ చేయవచ్చు .

Types based on transmission media

అదేవిధంగా కంప్యూటర్ B కంప్యూటర్ కంప్యూటర్తో కమ్యూనికేట్ చేయవచ్చు

Asvnchronous Modem

ఎన్క్రోనస్ మోడెమ్

Asynchronous modem uses start and stop bit for

ఎసిన్క్రోనస్ మోడెమ్ ప్రారంభం మరియు బిట్ ఆపడానికి ఉపయోగిస్తుంది

Svnchronization instead of clock.

బదులుగా గడియారం యొక్క సమకాలీకరణ.

Contents or data in each frame is placed between

start and stop bit.

ప్రతీ ఫ్రేములోని విషయములు లేదా డేటా ప్రారంభానికి మరియు ఆపే బిట్ మధ్య ఉంచుతారు .

- Data is grouped in very short blocks to prevent slipping of data, so usually character data is transmitted.
- డేటా డేటాను జారకుండా నివారించడానికి చాలా చిన్న బ్లాక్లో సమూహం చేయబడుతుంది, కాబట్టి సాధారణంగా పాత్ర డేటా బదిలీ చేయబడుతుంది.
- Transmission is simple and inexpensive.
- ట్రాన్స్మిషన్ సులభం మరియు చవకైనది .
- Used in pc to pc communication
- pc కమ్యూనికేషన్కు pc లో వాడతారు

Synchronous Modem

సిన్క్రోనస్ మోడెమ్

- Asynchronous modem uses clock on transmitter and receiver devices for synchronization.

అసిన్క్రోనస్ మోడెమ్ సమకాలీకరణ కోసం ట్రాన్స్మిటర్ మరియు రిసీవర్ పరికరాల్లో గడియారాన్ని ఉపయోగిస్తుంది .

- Before transmitting data both devices will synchronize the clock with each other.

డేటాను ప్రసారం చేయడానికి ముందు రెండు పరికరాలను గడియారం ఒకదానితో ఒకటి సమకాలీకరిస్తుంది

- Data is grouped in blocks and can transmit wide variety of data types in a frame.

డేటా బ్లాక్స్ లో సమూహం మరియు ఒక ఫ్రేమ్ లో వివిధ రకాల డేటా రకాల ప్రసారం చేయవచ్చు

- Transmission speed is faster than asynchronous modems.

అసిక్రోనస్ మోడెముల కన్నా వేగంగా ట్రాన్స్మిషన్ వేగం .

- Used in dedicated leased line and high speed broad bands.

ప్రత్యేకమైన కిరాయి లైన్ మరియు హై స్పీడ్ బ్రాడ్ బ్యాండ్లలో వాడతారు

Basic types

- External Modem
- Internal Modem
- Wireless Modem
- PC Card Modem

HUB

Definition

Hub is a connecting device in which various types of cables are connected to centralize network traffic through a single connecting point.

హబ్ అనేది అనుసంధానించే పరికరము, ఇందులో వివిధ రకాలైన కేబుళ్ళు ఒకే అనుసంధాన కేంద్రం ద్వారా నెట్వర్క్ ట్రాఫిక్ను కేంద్రీకరించటానికి అనుసంధానించబడి ఉంటాయి.

HUB is used to connect multiple computers in a single workgroup LAN network. Typically HUBs are available with 4,8,12,24,48 ports. Based on port type, there are two types of HUB:-

ఒకే పని సమూహ LAN నెట్వర్క్లో పలు కంప్యూటర్లను కనెక్ట్ చేయడానికి HUB ఉపయోగించబడుతుంది. సాధారణంగా HUB లు 4,8,12,24,48 పోర్ట్స్తో అందుబాటులో ఉన్నాయి. పోర్ట్ రకం ఆధారంగా, రెండు రకాలు HUB ఉన్నాయి

Ethernet HUB :- In this type of HUB all ports have RJ-45 connectors.
ఈథర్నెట్ హబ్: - హబ్ యొక్క ఈ రకమైన అన్ని పోర్టులకు RJ-45 కనెక్టర్ లు ఉన్నాయి

Combo HUB :- In this type of HUB ports have several different types of connectors such RJ-45, BNC, and AUI.

కాంబో హబ్: - HUB పోర్ట్స్ యొక్క ఈ రకమైన రకాలు RJ-45, BNC మరియు AUI వంటి వివిధ రకాలైన కనెక్టర్లను కలిగి ఉంటాయి.

HUBs generally have LED (light-emitting diode) indicator lights on each port to indicate the status of link, collisions, and other information.

HUB లు సాధారణంగా ప్రతి పోర్ట్లో LED (కాంతి ఉద్గార డయోడ్) సూచిక లైట్లు లింకు, గుద్దుకోవటం మరియు ఇతర సమాచారం యొక్క స్థితిని సూచిస్తాయి.

To understand the functionality of hub let's take an example from real life.
హబ్ యొక్క పనితీరును అర్థం చేసుకోవటానికి నిజ జీవితంలో ఒక ఉదాహరణ తీసుకుందాం.

There are four friends who share everything. One of them finds a photo of Amitabh Bachchan. To share this with friends, he will make three photo copies from Xerox machine and give one copy to each friend. He doesn't need a copy of photo for himself as he has the original one.

ప్రతిదీ భాగస్వామ్యం చేసే నాలుగు స్నేహితులు ఉన్నారు. వారిలో ఒకరు అమితాబ్ బచ్చన్ ఫోటోను కనుగొంటాడు. స్నేహితులతో ఈ పంచుకోవడానికి, అతను జిరాక్స్ యంత్రం నుండి మూడు ఫోటో కాపీలను తయారు చేస్తాడు మరియు ప్రతి ఒక్కరికి ఒక కాపీని ఇస్తాడు. అతను అసలు ఒక కలిగి తన కోసం ఫోటో యొక్క ఒక కాపీని అవసరం లేదు.

Now change the characters in this example. Replace friends with HUB's port, photo with data signal and Xerox machine with HUB.

ఇప్పుడు ఈ ఉదాహరణలోని అక్షరాలను మార్చండి. HUB పోర్టుతో, డేటా సిగ్నల్ మరియు జిరాక్స్ తో జిరాక్స్ మెషిన్ తో ఫోటోలను భర్తీ చేయండి

There is a HUB which has four ports. Ports share everything. One port received data signal from its connected device. It will make three copies of data signal from HUB and give one copy to each port. Receiver port doesn't need a copy of data signal for itself as it has it the original version.

నాలుగు పోర్టులను కలిగిన హబ్ ఉంది. పోర్ట్స్ ప్రతిదీ పంచుకుంటుంది. ఒక పోర్ట్ దాని కనెక్ట్ అయిన పరికరం నుండి డేటా సిగ్నల్ను అందుకుంది. ఇది HUB నుండి డేటా సిగ్నల్ యొక్క మూడు కాపీలను తయారు చేస్తుంది మరియు ప్రతి పోర్ట్కు ఒక కాపీని ఇస్తుంది. స్వీకర్త పోర్ట్కు దాని అసలు డేటా ఉన్నందున దాని కోసం డేటా సిగ్నల్ యొక్క నకలు అవసరం లేదు.

This is what exactly a HUB do. When a hub receives signal on its port, it repeats the signal and forwards that signal from all ports except the port on which the signal arrived.

సరిగ్గా HUB చేయండి. ఒక కేంద్రం దాని పోర్ట్ పై సిగ్నల్ను స్వీకరించినప్పుడు, ఇది సిగ్నల్ను తిరిగి పంపుతుంది మరియు సిగ్నల్ వచ్చే పోర్ట్ కాకుండా అన్ని పోర్టుల నుండి సంకేతంగా ఉంటుంది.

There are two types of HUB
రెండు రకాలు HUB ఉన్నాయి

Description

- Hub with multiple ports are used to connect topologies, segments of LAN and to monitor network traffic.
- బహుళ పోర్టులతో కూడిన కేంద్రం LAN ల యొక్క టోపోలాజిలను, విభాగాలను మరియు నెట్వర్క్ ట్రాఫిక్ను పర్యవేక్షించడానికి ఉపయోగించబడుతుంది.
- It manages and controls the send and received data to and from the computers.

- కంప్యూటరుకు మరియు పంపే మరియు అందుకున్న డేటాని ఇది నిర్వహిస్తుంది మరియు నియంత్రిస్తుంది
- Hub works on the physical layer of OSI or TCP/IP model.
- హబ్ OSI లేదా TCP / IP మోడల్ యొక్క భౌతిక పొరపై పనిచేస్తుంది .
- To avoid collision of data CSMA/CD protocol is used and protocol varies depending upon the vendor.
- డేటా CSMA / CD ప్రోటోకాల్ గుద్దుకోవటం నివారించేందుకు మరియు ప్రోటోకాల్ విక్రేత మీద ఆధారపడి ఉంటుంది .

Types Active

hub

It also forwards the data signal from all ports except the port on which signal arrived. But before forwarding, it improves quality of data signal by amplifying it. Due to this added features active HUB is also known as repeaters.

సక్రియ కేంద్రం ఇది సిగ్నల్ వచ్చే పోర్ట్ కాకుండా అన్ని పోర్టుల నుండి డేటా సిగ్నల్కు ముందుకు వస్తుంది. కానీ ముందు ఫార్వార్డింగ్, అది విస్తరించడం ద్వారా డేటా సిగ్నల్ నాణ్యతను మెరుగుపరుస్తుంది. క్రియాశీల HUB అనునది ఈ అదనపు లక్షణాల వలన కూడా పునరావృతములు అంటారు.

- Can store, amplify, split and retransmit the received signals.
- పొందగలిగిన సిగ్నల్స్ నిల్వ, విస్తరించు, స్ప్లిట్ మరియు పునఃప్రసారం చేయవచ్చు
- Requires additional electronic circuit for performing different functions.
- వివిధ ఫంక్షన్లను నిర్వహించడానికి అదనపు ఎలక్ట్రానిక్ సర్క్యూట్ అవసరమవుతుంది .
- It does work of repeater to amplify the signal, so it is also called as repeater.
- ఇది సిగ్నల్ను విస్తృతం చేయడానికి రిపీటర్ యొక్క పని చేస్తుంది, కనుక ఇది రిపీటర్గా కూడా పిలువబడుతుంది .

Passive hub (నిష్క్రియ కేంద్రం)

It forwards the data signal from all ports except the port on which signal arrived. It doesn't interfere in data signal.

ఇది సిగ్నల్ వచ్చే పోర్ట్ కాకుండా అన్ని పోర్టుల నుండి డేటా సిగ్నల్కు ముందుకు వస్తుంది. ఇది డేటా సిగ్నల్లో జోక్యం చేసుకోదు.

Intelligent hub

ఇంటెలిజెంట్ హబ్

- Performs functions of both active and passive hub.
- క్రియాశీల మరియు నిష్క్రియాత్మక కేంద్రంగా పనిచేసే విధులు నిర్వహిస్తుంది .
- Quickly routes the signals between the ports of hub.
- హబ్ యొక్క పోర్ట్స మధ్య సిగ్నల్స్ త్వరితంగా ప్రయాణిస్తుంది .
- Also performs different functions of router and bridge.
- రౌటర్ మరియు వంతెన యొక్క వివిధ విధులు నిర్వహిస్తుంది .
- So it is called as intelligent hub.
- కాబట్టి దీనిని తెలివైన కేంద్రంగా పిలుస్తారు .

Switch

Just like Hub and Bridge, switch is also used to connect multiple computers together in a LAN segment.

హబ్ మరియు వంతెన లాగానే, LAN విభాగంతో పాటు పలు కంప్యూటర్లను కలిపి స్విచ్ కూడా ఉపయోగించబడుతుంది.Switches available with 4,8,12,24,48,64 ports. Each switch port has a separate collision domain. Switch works at layer two in OSI Layer model. At layer two data signals are formatted in frames.

4,8,12,24,48,64 పోర్లతో అందుబాటులో ఉంది. ప్రతి స్విచ్ పోర్ట్కు ప్రత్యేకమైన ఖండన డొమైన్ ఉంది. OSI లేయర్ నమూనాలో పొర రెండు వద్ద పని చేస్తుంది. లేయర్ వద్ద రెండు డేటా సిగ్నల్స్ ఫ్రేములు ఫార్మాట్.

When a switch receives frame, it checks FCS (Frame checksum sequence) field in it. Switch process the frame only if it is valid. All invalided frames are automatically dropped. All valid frames are processed and forwarded to their destination MAC address.

ఒక స్విచ్ ఫ్రేమ్ను అందుకున్నప్పుడు, అది FCS (ఫ్రేమ్ చెక్సమ్ సీక్వెన్స్) ఫీల్డ్ను తనిఖీ చేస్తుంది. ఇది చెల్లుబాటు అయితే మాత్రమే ఫ్రేమ్ను ప్రాసెస్ చేయండి. అన్ని ఎంబైల్డ్ ఫ్రేములు ఆటోమేటిక్గా పడిపోయాయి. అన్ని చెల్లుబాటు అయ్యే ఫ్రేములు ప్రాసెస్ మరియు వారి గమ్యం MAC చిరునామాకు ఫార్వార్డ్ చేయబడతాయి.

Switch makes their switching decisions in hardware by using application specific integrated circuits (ASICs). Unlike generic processor such as we have in our PC, ASICs are specialized processors built only to perform very few particular tasks. In cisco switch ASICs has single task, switch frames blazingly fast. For example an entry level catalyst 2960 switch has frame rate of 2.7 million frames per second. Higher end switches have higher FPS rate such as Catalyst 6500 has a rate of 400 million FPS rate.

స్విచ్ వారి స్విచ్చింగ్ నిర్ణయాలు హార్డ్వేర్లో అప్లికేషన్ నిర్దిష్ట ఇంటిగ్రేటెడ్ సర్క్యూట్లను (ASICs) ఉపయోగించడం ద్వారా చేస్తుంది. మా PC లో ఉన్న మాదిరిగా సాధారణ ప్రాసెసర్ వలె కాకుండా, ASICs ప్రత్యేకమైన కొన్ని ప్రత్యేక పనులను మాత్రమే నిర్వహించడానికి ప్రత్యేకంగా పనిచేస్తాయి. సిస్కో స్విచ్ ASIC లలో ఒకే పని ఉంది, స్విచ్ ఫ్రేములు బ్లూస్గా ఉంటాయి. ఉదాహరణకు ఎంట్రీ లెవల్ ఉత్ప్రేరకం 2960 స్విచ్ సెకనుకు 2.7 మిలియన్ ఫ్రేముల ఫ్రేం రేటును కలిగి ఉంది. హయ్యర్ ఎండ్ స్విచ్లు ఉత్పన్నమయ్యే FPS రేటును ఉత్ప్రేరకం 6500 రేటుతో 400 మిలియన్ FPS రేట్ కలిగి ఉంటుంది.

Switches support three methods of switching.
స్విచ్లు మూడు పద్ధతులు మారతాయి.

1. Store and Forward
2. Cut and Through
3. Fragment Free

Store and Forward
స్టోర్ మరియు ఫార్వర్డ్

This is the basic mode of switching. In this mode Switch buffers entire frame into the memory and run FCS (Frame Check Sequence) to ensure that frame is valid and not corrupted. A frame less than 64bytes

and higher than 1518bytes is invalid. Only valid frames are processed and all invalid frames are automatically dropped. Among these three methods, this method has highest latency. Latency is the time taken by device in passing frame from it.

ఇది ప్రాథమిక మార్పు మోడ్. ఈ మోడ్లో ఫ్రేమ్ మొత్తం ఫ్రేమ్ను మెమరీలోనికి మార్చండి మరియు ఆ ఫ్రేమ్ చెల్లుబాటు అయ్యేది మరియు అవినీతికి హామీ ఇవ్వకుండా FCS (ఫ్రేమ్ చెక్ సీక్వెన్స్) అమలు చేస్తుంది. 64 బైట్లు కంటే తక్కువ ఫ్రేమ్ మరియు 1518 బైట్లు కంటే ఎక్కువ చెల్లదు. చెల్లుబాటు అయ్యే ఫ్రేములు మాత్రమే ప్రాసెస్ చేయబడతాయి మరియు అన్ని చెల్లని ఫ్రేములు స్వయంచాలకంగా తొలగించబడతాయి. ఈ మూడు పద్ధతుల్లో, ఈ పద్ధతి అత్యధిక జాప్యం ఉంది. తాత్కాలిక హక్కు దాని నుండి ఫ్రేమ్ని దాటిన పరికరం ద్వారా తీసుకున్న సమయం .

Cut and Through
కట్ మరియు త్రూ

Cut and Through method has lowest latency. In this method Switch only read first six bytes from frame after the preamble. These six bytes are the destination address of frame. This is the fastest method of switching. This method also process invalid frames. Only advantage of this method is speed.
కట్ మరియు త్రూ పద్ధతిలో అత్యల్ప జాప్యం ఉంది. ఈ పద్ధతిలో స్విచ్ ఉపోద్ఘాతం తర్వాత మొదటి ఆరు బైట్లు చదువుతుంది. ఈ ఆరు బైట్లు ఫ్రేమ్ యొక్క గమ్యస్థాన చిరునామా. ఈ మార్పిడి వేగవంతమైన పద్ధతి. ఈ పద్ధతి చెల్లని ఫ్రేమ్లను కూడా ప్రాసెస్ చేస్తుంది. ఈ పద్ధతి యొక్క ప్రయోజనం వేగం మాత్రమే.

Fragment Free

This is a hybrid version of Store and Forward method and Cut and Through method. It takes goodies from both methods and makes a perfect method for switching. It checks first 64 bytes of frame for error. It processes only those frames that have first 64bytes valid. Any frame less than 64 bytes is known as runt. Runt is an invalid frame type. This method filters runt while maintaining the speed.

ఇది స్టోర్ మరియు ఫార్వార్డ్ పద్ధతి మరియు కట్ మరియు త్రూ పద్ధతి యొక్క హైబ్రిడ్ వెర్షన్. ఇది రెండు పద్ధతుల నుండి గూడీస్ పడుతుంది మరియు మార్పిడి కోసం ఒక పరిపూర్ణ పద్ధతి చేస్తుంది. లోపం కోసం ఫ్రేమ్ యొక్క మొదటి 64 బైట్లు ఇది తనిఖీ చేస్తుంది. ఇది మొదటి 64bytes చెల్లుబాటు అయ్యే మాత్రమే ఫ్రేములు ప్రాసెస్. 64 బైట్ల కంటే తక్కువగా ఉన్న ఫ్రేము రాంట్ అంటారు. రాంట్ చెల్లని ఫ్రేమ్ రకం. ఈ పద్ధతి వేగాన్ని కొనసాగించే సమయంలో వ్రేలాడుతూ ఉంటుంది.

NIC

In the list of networking devices, NIC stands on first place. Without this device, networking cannot be done. This is also known as network adapter card, Ethernet Card and LAN card. NIC allows our PC to communicate with other PCs. Basically it converts data transmission technology. A PC uses parallel data transmission technology to transmit data between its internal parts while the media that connects this PC with other PCs uses serial data transmission technology. A NIC converts parallel data stream into serial data stream and vice versa serial data stream is get converted in parallel data stream.
నెట్వర్కింగ్ పరికరాల జాబితాలో, NIC మొదటి స్థానంలో ఉంది. ఈ పరికరం లేకుండా, నెట్వర్కింగ్ చేయడం సాధ్యం కాదు. ఇది నెట్వర్క్

అడాప్టర్ కార్డు, ఈథర్నెట్ కార్డ్ మరియు LAN కార్డ్ అని కూడా పిలువబడుతుంది. NIC మా PC ఇతర PC లతో కమ్యూనికేట్ చేయడానికి అనుమతిస్తుంది. ప్రాథమికంగా అది డేటా ట్రాన్స్మిషన్ టెక్నాలజీని మారుస్తుంది. ఒక PC దాని అంతర్గత భాగాల మధ్య సమాచారాన్ని ప్రసారం చేయడానికి సమాంతర సమాచార ప్రసార సాంకేతిక పరిజ్ఞానాన్ని ఉపయోగిస్తుంది, ఇతర PC లతో ఈ PC ని అనుసంధానిస్తున్న మీడియా సీరియల్ డేటా ట్రాన్స్మిషన్ టెక్నాలజీని ఉపయోగిస్తుంది. ఒక NIC సీరియల్ డేటా స్ట్రీమ్లో సమాంతర డేటా ప్రవాహాన్ని మారుస్తుంది మరియు వైస్ వెర్సా సీరియల్ డేటా స్ట్రీమ్ సమాంతర డేటా స్ట్రీమ్లో మార్చబడుతుంది.

Usually all modern PCs have integrated NICs in motherboard. NICs are also available separately. For desktop or server system they are available in adapter format which can be plugged into the available slots of motherboard. For laptop or other small size devices they available in PCMCIA (Personal Computer Memory Card International Association) card format which can be inserted in PCMCIA slots.

సాధారణంగా అన్ని ఆధునిక PC లు మదర్బోర్డులో NIC లను చేర్చుకున్నాయి. NIC లు కూడా విడిగా అందుబాటులో ఉన్నాయి. డెస్క్టాప్ లేదా సర్వర్ సిస్టమ్ కోసం అవి అడాప్టర్ ఫార్మాట్ లో అందుబాటులో ఉన్నాయి, ఇవి మదర్బోర్డు యొక్క అందుబాటులో ఉన్న స్లాట్లలో ప్లగ్ చేయబడతాయి. ల్యాప్టాప్ లేదా ఇతర చిన్న పరిమాణం పరికరాల కోసం వారు PCMCIA (వ్యక్తిగత కంప్యూటర్ మెమరీ కార్డ్ ఇంటర్నేషనల్ అసోసియేషన్) కార్డు ఫార్మాట్లో PCMCIA స్లాట్లలో చేర్చవచ్చు.

Types of NICs

There are two types of NICs

Media Specific :- Different types of NICs are required to connect with different types of media. For example we cannot connect wired media with wireless NIC card. Just like this, we cannot connect coaxial cable with Ethernet LAN card. We have to use the LAN card that is particularly built for the media type which we have.

మీడియా నిర్దిష్ట:- వివిధ రకాలైన మీడియాతో కనెక్ట్ అవ్వడానికి వివిధ రకాల NIC లు అవసరం. ఉదాహరణకు వైర్లెస్ NIC కార్డుతో వైర్డు మాధ్యమాన్ని కనెక్ట్ చేయలేము. ఇదిలా ఉంటే, మేము ఈథర్నెట్ LAN కార్డుతో ఏకాక్షక కేబుల్ను కనెక్ట్ చేయలేము. మేము కలిగి ఉన్న మాధ్యమ రకం కోసం నిర్మించిన LAN కార్డును ఉపయోగించాలి.

Network Design Specific :- A specific network design needs a specific LAN card. For example FDDI, Token Ring and Ethernet have their own distinctive type of NICs card. They cannot use other's NIC card.

నెట్వర్క్ డిజైన్ ప్రత్యేకమైన: - నిర్దిష్ట నెట్వర్క్ రూపకల్పనకు ఒక నిర్దిష్ట LAN కార్డు అవసరం. ఉదాహరణకు FDDI, టోకెన్ రింగ్ మరియు ఈథర్నెట్ వారి స్వంత విలక్షణమైన NICs కార్డును కలిగి ఉంటాయి. వారు ఇతర NIC కార్డును ఉపయోగించలేరు.

Repeater

Definition

Repeater is a electronic device that reshapes and amplifies the signal received from one LAN segment to another.

రిపీటర్ అనేది ఒక ఎలక్ట్రానిక్ పరికరం, ఇది ఒక LAN సెగ్మెంట్ నుండి అందుకున్న సిగ్నల్ను మెరుగుపరుస్తుంది మరియు మెరుగుపరుస్తుంది.

Description

- Mostly used to boost the signals in the network.

- చాలా ఎక్కువగా నెట్వర్క్ సిగ్నల్స్ పెంచడానికి ఉపయోగిస్తారు
- Operates at physical layer in the OSI layer model.
- OSI లేయర్ నమూనాలో భౌతిక పొరలో పని చేస్తుంది
- Best suited for long distances network and bus topology.
- దూర ప్రాంతాల నెట్వర్క్ మరియు బస్ టోపోలాజీకి ఉత్తమమైనది
- Main advantage is that they remove unwanted noise from the incoming signals.
- ప్రధాన ప్రయోజనం వారు ఇన్కమింగ్ సిగ్నల్స్ నుండి అవాంఛిత శబ్దం తొలగించడానికి ఉంది .
- Requires separate power supply for functioning.
- పని కోసం ప్రత్యేక విద్యుత్ సరఫరా అవసరం .
- Repeater component parts varies from where they are used like in digital communication, wireless communication, fiber-optic system, cellular system etc.
- రీపీటర్ భాగాల భాగాలు డిజిటల్ కమ్యూనికేషన్, వైర్లెస్ కమ్యూనికేషన్, ఫైబర్-ఆప్టిక్ సిస్టం, సెల్యులార్ సిస్టం వంటి వాటిలో వాడతారు .

Bridge Definition

Bridge is a networking device that connects two or more LAN's together.

వంతెన అనేది రెండు లేదా అంతకంటే ఎక్కువ LAN లను కలిపే ఒక నెట్వర్కింగ్ పరికరం

Description

- Bridge is used when number of LANs starts increasing, the network traffic begins on overwhelming to available bandwidth.
- LAN ల సంఖ్య పెరుగుతున్నప్పుడు వంతెనను ఉపయోగించడం జరుగుతుంది, నెట్వర్క్ ట్రాఫిక్ అందుబాటులో ఉన్న బ్యాండ్విడ్త్ కు అధిక స్థాయిలో ప్రారంభమవుతుంది.
- Reduces the network traffic of LAN by dividing it into segments.
- ల్యాండ్ యొక్క నెట్వర్క్ ట్రాఫిక్ను విభాగాలలోకి విభజించడం ద్వారా తగ్గించడం .
- Operates at data link layer of OSI model.
- OSI మోడల్ యొక్క డేటా లింక్ పొరలో పని చేస్తుంది.
- Can transfer data between two different protocols like Ethernet (802.3) and token bus (802.4).

ఈథర్నెట్ (802.3) మరియు టోకెన్ బస్సు (802.4) వంటి రెండు వేర్వేరు ప్రోటోకాల్స్ మధ్య డేటా బదిలీ చేయగలదు .

- Checks the MAC address of the frame and decides to forward the frame or to discard the frame.
- ఫ్రేమ్ యొక్క MAC చిరునామాను తనిఖీ చేస్తుంది మరియు ఫ్రేమ్ను ముందుకు తీసుకెళ్లడానికి లేదా ఫ్రేమ్ని తొలగించడానికి నిర్ణయిస్తుంది.

Types

Transparent bridge

పారదర్శక వంతెన

- Source and destination devices are unaware of the bridge in between them, so called as transparent bridge.
- మూల మరియు గమ్య పరికరాలు వాటి మధ్యలో వంతెన గురించి తెలియదు, అలా పారదర్శక వంతెనగా పిలువబడతాయి .
- Accepts all incoming frames to the bridge.

- తెనలోకి వచ్చే అన్ని ఫ్రేమ్లను అంగీకరిస్తుంది
  - If the frame is unknown forward the frame to all LANs.
- ఫ్రేమ్ అన్ని LAN లకు ఫ్రేమ్కు ముందుగా తెలియకపోతే .
  - If the frame is from the same LAN discard the frame from bridge.
  - ఫ్రేమ్ అదే LAN నుండి ఫ్రేమ్ వంతెన నుండి ఫ్రేమ్ ని విసర్జించినట్లయితే.
  - If the incoming frame is from different LAN accept it and forward it to particular LAN.

ఇన్కమింగ్ ఫ్రేమ్ వేరొక LAN నుండి అది అంగీకరించితే మరియు దానిని ప్రత్యేక LAN కు పంపించండి .

Source route bridge

మూల మార్గం వంతెన

- Used on token ring networks.

టోకెన్ రింగ్ నెట్వర్క్లో ఉపయోగించబడుతుంది .

- Bridge derives the entire path of the frame embedded in the header of the frame and decides how to forward the frame through out the network till it reaches its destination.
  ఫ్రేమ్ యొక్క శీర్షికలో పొందుపర్చిన ఫ్రేమ్ యొక్క మొత్తం మార్గం వంతెన నుండి వంతెన పొందింది మరియు దాని గమ్యాన్ని చేరుకోవడానికి వరకు నెట్వర్క్ను తొలగించడం ద్వారా ఫ్రేమ్ను ఎలా ముందుకు తీసుకువెళుతుందో నిర్ణయిస్తుంది .

Translational bridge

అనువాద వంతెన

- Used when LANs have dissimilar protocols or speeds.

LANs అసమాన ప్రోటోకాల్లు లేదా వేగాలు ఉన్నప్పుడు ఉపయోగించబడుతుంది .

- Like Ethernet and token ring or Ethernet and FDDI.

ఈథర్నెట్ మరియు టోకెన్ రింగ్ లేదా ఈథర్నెట్ మరియు FDDI వంటివి .

Router

రూటర్ Definition

Router is internetwork connecting device that determines most efficient path for sending a data packet To any given network.

రౌటర్ అనేది ఇంటర్ నెట్ కనెక్ట్ చేస్తున్న పరికరం, అది ఒక డేటా పాకెట్ను పంపుటకు అత్యంత సమర్థవంతమైన మార్గమును నిర్ణయిస్తుందిఇచ్చిన ఏదైనా నెట్వర్క్.

Description(వివరణ)

- Used to connect two or more similar or dissimilar topological LANs or WLANs
- రెండు లేదా అంతకంటే ఎక్కువ సమానమైన లేదా అసమాన టోపోలాజికల్ LAN లు లేదా WLAN లను కనెక్ట్ చేయడానికి ఉపయోగిస్తారు
- Shares available bandwidth with multiple computers in a network.
- నెట్వర్క్లో బహుళ కంప్యూటర్లతో అందుబాటులో ఉన్న బ్యాండ్విడ్త్ పేర్లు.
- Provides a better protection as a hardware firewall against hacking.
- హ్యాకింగ్ వ్యతిరేకంగా హార్డ్వేర్ ఫైర్వాల్ ఒక మంచి రక్షణ అందిస్తుంది.
- Routers are intelligent enough to determine shortest and fastest path from source to destination in a network using algorithms.

- మార్గాలు అల్గోరిథంలను ఉపయోగించి నెట్వర్క్ మూలం నుండి చిన్నదైన మరియు వేగవంతమైన మార్గాన్ని నిర్దేశించడానికి తగినంత మేధో సందేశములు.
- Operates at network layer of OSI model.
- OSI మోడల్ యొక్క నెట్వర్క్ పొరలో పనిచేస్తోంది.
- Wireless routers are now widely used in home and offices as they allow a user to connect easily without installing any cables.
- వైర్లెస్ రౌటర్లు యిప్పుడు హోమ్ మరియు కార్యాలయాలలో విస్తృతంగా వాడబడుతున్నాయి, ఎటువంటి కేబుల్స్ను ఇన్స్టాల్ చేయకుండా ఒక వినియోగదారు సులువుగా కనెక్ట్ అవ్వడానికి వీలు కల్పిస్తుంది.

Types based on defining paths

మార్గాలను నిర్వచించడం ఆధారంగా రకాలు

Static router

స్టాటిక్ రౌటర్

- System administrator defines the shortest path in the network by executing commands.
- వ్యవస్థ నిర్వాహకుడు ఆదేశాలను అమలు చేయడం ద్వారా నెట్వర్క్లో అతిచిన్న మార్గంను నిర్వచిస్తాడు.
- Have some limitations and not that much effective than dynamic router.
- డైనమిక్ రౌటర్ కంటే చాలా తక్కువ పరిమితులను కలిగి ఉండకూడదు.

Dvnamic router

డైనమిక్ రౌటర్

- Router itself determines the shortest path between the computers in the network.

రౌటర్ కూడా నెట్వర్క్లోని కంప్యూటర్ల మధ్య అతిచిన్న మార్గంను నిర్ణయిస్తుంది .

- System administrator doesn't need to interact with router that saves time and cost.

సిస్టమ్ అడ్మినిస్ట్రేటర్ సమయం మరియు ఖర్చుని ఆదా చేసే రౌటర్తో పరస్పరం వ్యవహరించాల్సిన అవసరం లేదు .

- This types of routers are used in greater extend compare to static router.

ఈ రౌటర్ల రకాలు విస్తృతంగా విస్తరించడానికి స్టాటిక్ రౌటర్తో పోల్చబడతాయి .

Basic types

- Wired routers
- Wireless routers
- GatewayDefinition

Gateway is a network point that act as entry point to other network and translates one data format to another.

నిర్వచనం గేట్వే అనేది ఇతర నెట్వర్క్లకు ఎంట్రీ పాయింట్గా పనిచేసే ఒక నెట్వర్క్ పాయింట్ మరియు ఒక డేటా ఫార్మాట్ను అనువదిస్తుంది.

మరో

Description

Following are some common functions of the gateway :

వివరణ గేట్వే యొక్క కొన్ని సాధారణ విధులు క్రిందివి:

- Protocol translation : translates protocol format into required protocol format of the network,

such as X.25 to TCP/IP.

- ప్రోటోకాల్ అనువాదం: నెట్వర్క్ యొక్క అవసరమైన ప్రోటోకాల్ ఫార్మాట్లోకి ప్రోటోకాల్ ఆకృతిని అనువదిస్తుంది, X.25 వంటి TCP / IP కు.
- Network address translation: translates your public IP address to the private IP addresses on your network
- నెట్వర్క్ అడ్రస్ ట్రాన్స్లేషన్: మీ పబ్లిక్ IP చిరునామాని మీ నెట్వర్క్లోని ప్రైవేట్ IP చిరునామాలకు అనువదిస్తుంది
- DHCP service : automatically assigns IP address to a computer from a defined range of addresses for a given network.
- DHCP సేవ: ఇచ్చిన నెట్వర్కు కొరకు నిర్వచించిన శ్రేణి చిరునామాల నుండి కంప్యూటర్కు స్వయంచాలకంగా IP చిరునామాను అప్పగించును.
- **Monitoring and regulating each packet entering and leaving the network.**
- ప్రతి ప్యాకెట్ను పర్యవేక్షించడం మరియు క్రమబద్ధీకరిస్తుంది.

Uses(ఉపయోగాలు)

To route the traffic from one network to another.

ట్రాఫిక్ను ఒక నెట్వర్క్ నుండి మరొకదానికి తరలించడానికి

To connect LAN to WAN or VPN (Virtual Private Network).

- LAN ని WAN లేదా VPN (వర్చువల్ ప్రైవేట్ నెట్వర్క్) కి కనెక్ట్ చేయండి.
- Acts as a proxy server and firewall server to protect from virus, malware and harmful attacks.
- వైరస్, మాల్వేర్ మరియు హానికరమైన దాడుల నుండి రక్షించడానికి ప్రాక్సీ సర్వర్ మరియు ఫైర్వాల్ సర్వర్ వలె పనిచేస్తుంది.
- To keep history of accessed website, bandwidth usage, timing of each user of the network in a database.
- యాక్సెస్ చేసిన వెబ్సైట్ యొక్క చరిత్ర, బ్యాండ్విడ్త్ వినియోగం, నెట్వర్క్ యొక్క ప్రతి వినియోగదారు యొక్క సమయ డేటాబేస్లో ఉంచడానికి

What is NIC (Network Interface Card)

NIC ఏమిటి (నెట్వర్క్ ఇంటర్ఫేస్ కార్డ్)

A NIC (Network Interface Card) provides the hardware interface between a computer and a network. These days, almost all new computer motherboards have in-built NIC (Network Interface Card).

ఒక NIC (నెట్వర్క్ ఇంటర్ఫేస్ కార్డ్) కంప్యూటర్ మరియు నెట్వర్క్ మధ్య హార్డ్వేర్ ఇంటర్ఫేస్ను అందిస్తుంది. ఈ రోజుల్లో, దాదాపు అన్ని కొత్త కంప్యూటర్ మదర్బోర్డులు అంతర్నిర్మిత NIC (నెట్వర్క్ ఇంటర్ఫేస్ కార్డ్) కలిగి ఉన్నాయి.

Some NIC (Network Interface Card) cards are meant for wired networks while others are for wireless network. Most widely used wired LAN Technology is Ethernet. Ethernet based NIC (Network Interface Card) cards are available in every local electronic hardware

Shops. Normal speed rating of Ethernet based wired NIC (Network Interface Card) available these days are 10/100/1000 Mbps (Mega bits per second).

కొన్ని NIC (నెట్వర్క్ ఇంటర్ఫేస్ కార్డ్) కార్డులు వైర్డు నెట్వర్క్ల కొరకు ఉద్దేశించబడ్డాయి, మరికొందరు వైర్లెస్ నెట్వర్కు కొరకు. విస్తృతంగా ఉపయోగించే వైర్డు LAN టెక్నాలజీ ఈథర్నెట్. ఈథర్నెట్ ఆధారిత NIC (నెట్వర్క్ ఇంటర్ఫేస్ కార్డ్) కార్డులు ప్రతి స్థానిక ఎలక్ట్రానిక్ హార్డ్వేర్లో అందుబాటులో ఉన్నాయి.

దుకాణాలు. అందుబాటులో ఉన్న ఈథర్నెట్ ఆధారిత వైర్డు NIC (నెట్వర్క్ ఇంటర్ఫేస్ కార్డ్) యొక్క సాధారణ వేగం రేటింగ్ ఈ రోజుల్లో 10/100/1000 Mbps (సెకనుకు మెగా బిట్స్).

Every computer participating in network must have at least one NIC. Computers can have more than one NIC card also, if required.Every NIC (Network Interface Card) has a 48-bit globally unique identifier called as MAC Address (Media Access Control Address) burned into its ROM chip. This MAC address is used to deliver Ethernet Frames (packets) to a computer.

నెట్వర్క్లో పాల్గొనే ప్రతి కంప్యూటర్లో కనీసం ఒక NIC ఉండాలి. అవసరమైతే కంప్యూటర్లు ఒకటి కంటే ఎక్కువ NIC కార్డులను కలిగివుంటాయి. ప్రతి NIC (నెట్వర్క్ ఇంటర్ఫేస్ కార్డ్) దాని ROM చిప్పలో బూడిదైన MAC చిరునామా (మీడియా యాక్సెస్ కంట్రోల్ అడ్రస్) గా పిలువబడే 48-బిట్ గ్లోబల్లీ ఏకైక ఐడెంటిపైయర్ను కలిగి ఉంది. ఈ MAC అడ్రస్ ఈథర్నెట్ ఫ్రేమ్స్ (ప్యాకెట్లను) ఒక కంప్యూటర్కు అందించటానికి ఉపయోగించబడుతుంది

The NIC driver software passes the data between the Operating System and the NIC. Latest Operating Systems include different NIC driver software for almost all major NIC vendors. If your NIC card is not detected or not working, you must find a suitable NIC driver software from the NIC vendor's website and install it on the computer.

NIC డ్రైవర్ సాఫ్ట్వేర్ ఆపరేటింగ్ సిస్టమ్ మరియు NIC మధ్య డేటాను పంపుతుంది. దాదాపు అన్ని ప్రధాన NIC అమ్మకందారులకు వివిధ ఆపరేటింగ్ సిస్టమ్లు వివిధ NIC డ్రైవర్ సాఫ్ట్వేర్ ఉన్నాయి. మీ NIC కార్డు గుర్తించబడకపోయినా లేదా పనిచేయకపోయినా, మీరు NIC విక్రేత వెబ్సైట్ నుండి తగిన NIC డ్రైవర్ సాఫ్ట్ వేర్ ను కనుగొని కంప్యూటర్లో దాన్ని ఇన్స్టాల్ చేయాలి.

Network Cable Types

నెట్వర్క్ కేబుల్ రకాలు

Cables are commonly used to carry communication signals within Local Area Networks (LAN). There are three common types of cable media that can be used to connect devices to a network and they are coaxial cable, twisted-pair cable, and fiber-optic cable.

కేబుల్లు సాధారణంగా స్థానిక ఏరియా నెట్వర్క్ల (LAN) లో కమ్యూనికేషన్ సంకేతాలను తీసుకువెళ్లడానికి ఉపయోగిస్తారు. పరికరాలను ఒక నెట్వర్క్కు కనెక్ట్ చేయడానికి ఉపయోగించే మూడు సాధారణ రకాల కేబుల్ మాధ్యమాలు ఉన్నాయి మరియు ఇవి కోక్సియల్ కేబుల్, ట్విస్టెడ్-జత కేబుల్ మరియు ఫైబర్-ఆప్టిక్ కేబుల్.

Coaxial cable

ఏకాక్షక కేబుల్

Coaxial cable looks similar to the cable used to carry TV signal. A solid-core copper wire runs down the middle of the cable. Around that solid-core copper wire is a layer of insulation, and covering that

insulation is braided wire and metal foil, which shields against electromagnetic interference. A final layer of insulation covers the braided wire.

ఏకాక్షక కేబుల్ టీవీ సిగ్నల్ ను ఉపయోగించటానికి ఉపయోగించే కేబుల్ మాదిరిగానే ఉంటుంది. ఒక ఘన-కోర్ కాపర్ వైర్ కేబుల్ మధ్యలో నడుస్తుంది. ఆ ఘన-కోర్ రాగి తీగ చుట్టూ ఇన్సులేషన్ యొక్క పొర, మరియు ఇన్సులేషన్ అల్లిన వైర్ మరియు లోహపు రేకు, ఇది విద్యుదయస్కాంత జోక్యానికి వ్యతిరేకంగా కవచాలను కలిగి ఉంటుంది. ఇన్సులేషన్ తుది పొర అల్లిన వైర్ను కప్పి ఉంచింది.

There are two types of coaxial cabling: thinnet and thicknet. Thinnet is a flexible coaxial cable about ¼ inch thick. Thinnet is used for short-distance. Thinnet connects directly to a workstation's network adapter card using a British Naval Connector (BNC). The maximum length of thinnet is 185 meters. Thicknet coaxial is thicker cable than thinnet. Thicknet cable is about ½ inch thick and can support data transfer over longer distances than thinnet. Thicknet has a maximum cable length of 500 meters and usually is used as a backbone to connect several smaller thinnet-based networks.

రెండు రకాల ఏకాక్షక కేబులింగ్: thinnet మరియు thicknet. Thinnet ¼ అంగుళాల మందపాటి గురించి ఒక సౌకర్యవంతమైన ఏకాక్షక కేబుల్. Thinnet స్వల్ప దూరం కోసం ఉపయోగిస్తారు. Thinnet ఒక బ్రిటీష్ నావల్ కనెక్టర్ (BNC) ను ఉపయోగించి ఒక వర్క్స్టేషన్ యొక్క నెట్వర్క్ ఎడాప్టర్ కార్డుకు నేరుగా అనుసంధానిస్తుంది. గరిష్ట పొడవు 185 మీటర్లు. Thicknet ఏకాక్షక thinnet కంటే మందంగా కేబుల్. Thicknet కేబుల్ గురించి ½ అంగుళాల మందంగా మరియు thinnet కంటే ఎక్కువ దూరాలకు డేటా బదిలీ మద్దతు. Thicknet గరిష్ట కేబుల్ పొడవును 500 మీటర్లు కలిగి ఉంటుంది మరియు చాలా చిన్న thinnet- ఆధారిత నెట్ వర్క్ లను అనుసంధానించుటకు సాధారణంగా ఒక వెన్నెముకగా ఉపయోగించబడుతుంది .

The bandwidth for coaxial cable is 10 Mbps (Mega bits per second)
కోక్సియల్ కేబుల్ కోసం బ్యాండ్విడ్త్ 10 Mbps (సెకనుకు మెగా బిట్స్.

Type of Cable used to wire Local Area Networks (LAN) these days is Twisted Pair cable. It is extremely difficult to find a live business network using coaxial cable.

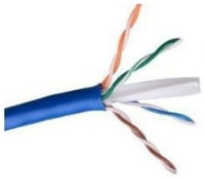
స్థానిక ఏరియా నెట్వర్క్స్ (LAN) ను వాడేందుకు ఉపయోగించే కేబుల్ రకం ఈ రోజుల్లో ట్విస్టెడ్ పెయిర్ కేబుల్ ఉంది. కోక్సియల్ కేబుల్ ఉపయోగించి ప్రత్యక్ష వ్యాపార నెట్వర్క్ను కనుగొనడం చాలా కష్టం.

Twisted Pair Cable
ట్విస్టెడ్ పెయిర్ కేబుల్

Twisted-pair cable is the most common type of cabling you can see in today's Local Area Networks (LAN) networks. A pair of wires forms a circuit that can transmit data. The pairs are twisted to provide protection against crosstalk. Crosstalk is the undesired signal noise generated by the Electro-Magnetic fields of the adjacent wires.

Twisted-pair కేబుల్ మీరు నేటి స్థానిక ఏరియా నెట్వర్క్స్ (LAN) నెట్వర్క్లలో చూడవచ్చు కేబుల్ అత్యంత సాధారణ రకం. ఒక జత వైర్లు డేటాను ప్రసారం చేసే ఒక సర్క్యూట్ను ఏర్పరుస్తాయి. జతల crosstalk వ్యతిరేకంగా రక్షణ అందించడానికి వక్రీకృత ఉంటాయి. క్రాస్టాక్ ప్రక్కనే ఉన్న తీగల ఎలెక్ట్రో మాగ్నెటిక్ క్షేత్రాల ద్వారా ఉత్పన్నమైన సిగ్నల్ శబ్దం.

When a wire is carrying a current, the current creates a magnetic field around the wire. This field can interfere with signals on nearby wires. To eliminate this, pairs of wires carry



signals in opposite directions, so that the two magnetic fields also occur in opposite directions and cancel each other out. This process is known as cancellation.

ఒక వైర్ ప్రస్తుత మోసుకెళ్ళే సమయంలో, ప్రస్తుత వైర్ చుట్టూ అయస్కాంత క్షేత్రాన్ని సృష్టిస్తుంది. ఈ ఫీల్డ్ సమీపంలోని వైర్లపై సిగ్నల్స్తో జోక్యం చేసుకోవచ్చు. ఈ తొలగించడానికి, తీగలు జతల తీసుకు వ్యతిరేక దిశలలో సంకేతాలు, అందువలన రెండు అయస్కాంత క్షేత్రాలు కూడా సంభవిస్తాయి వ్యతిరేక దిశలు మరియు ప్రతి ఇతర రద్దు. ఈ ప్రక్రియను రద్దు చేయడం అని పిలుస్తారు.

Two Types of Twisted Pairs are Shielded Twisted Pair (STP) and Unshielded Twisted Pair (UTP).

ట్విస్టెడ్ పెయిర్ల రెండు రకాలు ట్విస్టెడ్ పెయిర్ (STP) మరియు అన్షీల్డ్ ట్విస్టెడ్ పెయిర్ (UTP) షీల్డ్ చేయబడ్డాయి.

Unshielded twisted-pair (UTP) cable is the most common networking media. Unshielded twisted-pair (UTP) consists of four pairs of thin, copper wires covered in color-coded plastic insulation that are twisted together. The wire pairs are then covered with a plastic outer jacket. UTP cables are of small diameter and it doesn't need grounding. Since there is no shielding for UTP cabling, it relies only on the cancellation to avoid noise.

అన్షీల్డ్ వక్రీకృత-జత (UTP) కేబుల్ అత్యంత సాధారణ నెట్వర్కింగ్ మీడియా. అన్షీల్డ్ వక్రీకృత-జత (UTP) కలయికతో కూడిన ప్లాస్టిక్ ఇన్సులేషన్లో కవర్ చేయబడిన నాలుగు జతల సన్నని, రాగి తీగలు ఉన్నాయి. వైర్ జతల అప్పుడు ఒక ప్లాస్టిక్ బయటి జాకెట్ తో కప్పబడి ఉంటాయి. UTP కేబుల్స్ చిన్న వ్యాసంతో ఉన్నాయి మరియు అది నిలుపుదల అవసరం లేదు. UTP కేబులింగ్ కోసం షీల్డింగ్ ఉండనందున, శబ్దం నివారించడానికి మాత్రమే రద్దు చేయబడుతుంది.

Colors used for Twisted Pair wires are Orange, Orange-White, Blue, Blue-White, Green, Green-White, Brown and Brown-White. Following image shows a dissected Unshielded Twisted Pair cable.

ఆరెంజ్, ఆరెంజ్-వైట్, బ్లూ, బ్లూ-వైట్, గ్రీన్, గ్రీన్-వైట్, బ్రౌన్ మరియు బ్రౌన్-వైట్, ట్విస్టెడ్ పెయిర్ వైర్లు కోసం ఉపయోగించే రంగులు. కింది చిత్రం ఒక dissected అన్షీల్డ్ ట్విస్టెడ్ పెయిర్ కేబుల్ చూపిస్తుంది.

The connector used on a UTP cable is called as RJ-45 (Registered Jack 45) connector. Below picture shows an RJ45 jack, attached to UTP cable. Eight color-coded wires inside Twisted-Pair cable is attached to eight pins in a RJ45 jack as shown below. Each wire in the Twisted Pair cable is crimped into 8 pins in the RJ45 jack.

UTP కేబుల్లో ఉపయోగించే కనెక్టర్ని RJ-45 (రిజిస్టర్డ్ జాక్ 45) కనెక్టర్గా పిలుస్తారు. క్రింద చిత్రం ఒక RJ45 జాక్ చూపిస్తుంది, UTP కేబుల్ జత. క్రింద చూపిన విధంగా ట్విస్టెడ్-పెయిర్ కేబుల్ లోపల ఎనిమిది రంగు-కోడెడ్ వైర్లు RJ45 జాక్లో ఎనిమిది పిన్స్తో జతచేయబడ్డాయి. ట్విస్టెడ్ పెయిర్ కేబుల్లోని ప్రతి వైర్ RJ45 జాక్లో 8 పిన్స్గా విభజించబడింది.

One end of the Unshielded Twisted Pair cable with RJ45 jacks attached is plugged in to computer's

Ethernet NIC card port and other end end is plugged to the wall mount plate with female RJ45 port (receptacle), as shown below.

RJ45 జాక్స్ తో అన్వీల్డ్ ట్విస్టెడ్ పెయిర్ కేబుల్ యొక్క ఒక ముగింపు కంప్యూటర్ యొక్క ఈథర్నెట్ NIC కార్డు పోర్ట్కు ప్లగ్ చేయబడుతుంది మరియు ఇతర ముగింపు ముగింపు పురుషుడు RJ45 పోర్ట్ (రిసెప్టకిల్) తో గోడ మౌంట్ ప్లేట్కు ప్లగ్ చేయబడుతుంది, క్రింద చూపిన విధంగా.

From the wall mount RJ45 female receptacle, Unshielded Twisted Pair cable is wired to the Local Area Network (LAN) switches.

గోడ మౌంట్ నుండి RJ45 మహిళా రిసెప్టాల్, అన్షైల్డ్ ట్విస్టెడ్ పెయిర్ కేబుల్ స్థానిక ఏరియా నెట్వర్క్ (LAN) స్విచ్లకు వైర్డుతుంది.

UTP cabling has different categories. Each category of UTP cabling was designed for a specific type of communication or transfer rate. The most popular categories in use today is 5e and 6, which can reach transfer rates of over 1000 Mbps (1 Gbps).

PTU . కేబులింగ్ వివిధ కేతగిరీలు కలిగి ఉంది PTUకేబులింగ్ యొక్క ప్రతి వర్గం నిర్దిష్ట రకం కమ్యూనికేషన్ లేదా బదిలీ రేటు కోసం రూపొందించబడింది e5 నేడు ఉపయోగించిన అత్యంత ప్రజాదరణ పొందిన కేతగిరీలు .మరియు (spbG 1) spbM 1000 ,6బదిలీ రేట్లు చేరతాయి.

Unshielded Twisted Pair cables support a maximum distance of 100 Meters (from NIC Card to Switch Port), without signal distortion.

అన్వీల్డ్ ట్విస్టెడ్ పెయిర్ కేబుల్స్ సిగ్నల్ వక్రీకరణ లేకుండా, 100 మీటర్ల (NIC కార్డ్ నుండి స్విచ్ పోర్ట్ వరకు) గరిష్ట దూరానికి మద్దతు ఇస్తుంది.

The following table shows different UTP categories and corresponding transfer rate.

క్రింది పట్టిక వివిధ UTP కేతగిరీలు మరియు సంబంధిత బదిలీ రేటును చూపుతుంది.

UTP Category	Purpose	Transfer Rate
Category 1	Voice Only	
Category 2	Data	4 Mbps
Category 3	Data	10 Mbps
Category 4	Data	16 Mbps
Category 5	Data	100 Mbps
Category 5e	Data	1 Gbps
Category 6	Data	1/10 Gbps

How to Crimp Ri45
Rj45 ఎలా క్రిమ్ప్ చేయడం

RJ-45 connectors are normally used in telephone and network cables. Occasionally they are used for serial network connections. When the RJ-45 connectors first came into use, they were primarily used for telephones. The great advances in technology created a need for another size connector and the RJ-45 was adapted to fit. Today there are 2 different RJ-45 connector sizes available, 1 for Cat 5 cable and 1 for Cat 6 cable. The user has to make sure they have the one suited to their job. The easiest way to tell them apart is to compare them side by side. The Cat 6 connector is larger than the Cat 5 connector. Below are instructions for crimping RJ-45 connectors to a cable.

RJ-45 కనెక్టర్లను సాధారణంగా టెలిఫోన్ మరియు నెట్వర్క్ కేబుల్స్లో ఉపయోగిస్తారు. అప్పుడప్పుడు వారు సీరియల్ నెట్వర్క్ కనెక్షన్లకు ఉపయోగిస్తారు. RJ-45 కనెక్షన్లు మొట్టమొదట ఉపయోగంలోకి వచ్చినప్పుడు, వారు ప్రధానంగా టెలిఫోన్ల కోసం ఉపయోగిస్తారు. సాంకేతిక పరిజ్ఞానం యొక్క గొప్ప పురోగతులు మరొక పరిమాణ కనెక్టర్ కోసం అవసరమయ్యాయి మరియు RJ-45 సరిపోయేలా రూపొందించబడింది. నేడు 2 విభిన్న RJ-45 కనెక్టర్ పరిమాణాలు అందుబాటులో ఉన్నాయి, క్యాట్ 5 కేబుల్ కోసం 1 మరియు క్యాట్ 6 కేబుల్ కోసం 1. వినియోగదారు వారి ఉద్యోగానికి అనుగుణంగా ఉందని నిర్ధారించుకోవాలి. వాటిని వేరుగా చెప్పడానికి సులభమైన మార్గం వాటిని పక్కపక్కనే పోల్చడం. కాట్ 6 కనెక్టర్ కన్నా 5 కనెక్టర్ కన్నా పెద్దది. క్రింద కేబుల్కు RJ-45 కనెక్టర్లను crimping కోసం సూచనలు ఉన్నాయి.

STEPS

Purchase your cable and your RJ-45 connectors. Most ethernet cable is sold on spools of varying lengths, so you might have to measure and cut the amount you need when you get home.

మీ కేబుల్ మరియు మీ RJ-45 కనెక్టర్లను కొనుగోలు చేయండి. చాలా ఈథర్నెట్ కేబుల్ వివిధ పొడవులు యొక్క spools విక్రయిస్తుంది, కాబట్టి మీరు ఇంటికి వచ్చినప్పుడు మీరు అవసరం మొత్తం కొలిచేందుకు మరియు కట్ ఉంటుంది.

Strip 1 to 2 inches (2.5 to 5.1 cm) of the outer skin at the end of the cable wire by making a shallow cut in the skin with a utility knife. Run the knife around the cable, and the jacket should slide off easily. There will be 4 pairs of twisted wires exposed, each of them a different color or color combination.

యుటిలిటీ కత్తితో చర్మంలో నిస్సార కట్ చేయడం ద్వారా కేబుల్ వైర్ చివరలో బాహ్య చర్మం యొక్క 1 నుండి 2 అంగుళాలు (2.5 నుండి 5.1 సెం.మీ. కేబుల్ చుట్టూ కత్తి అమలు, మరియు జాకెట్ సులభంగా ఆఫ్ స్లయిడ్ ఉండాలి. బహిర్గతం వక్రీకృత తీగలు 4 జతల ఉంటుంది, వాటిలో ప్రతి వేరే రంగు లేదా రంగు కలయిక.

- Orange-white striped and solid orange
- ఆరెంజ్-వైట్ చారల మరియు ఘన నారింజ
- Green-white striped and solid green
- ఆకుపచ్చ-తెలుపు చారల మరియు ఘన ఆకుపచ్చ
- Blue-white striped and solid blue
- నీలం-తెలుపు చారల మరియు ఘన నీలం
- Brown-white striped and solid brown
- బ్రౌన్-వైట్ చారలు మరియు గోధుమ గోధుమ

Fold each pair of wires backwards to expose the core of the cable . Cut off the core and discard
కేబుల్ యొక్క కోర్ని బహిర్గతం చేసేందుకు ప్రతి జత తీగలు వెనుకకు రెట్లు. కోర్ కత్తిరించండి మరియు విస్మరించండి

Straighten the twisted wires using 2 pair of tweezers. Grasp a wire beneath a bend with 1 pair of tweezers, and use the other pair to gently straighten the bend. The straighter your wires, the easier your job will be.

జంట పట్టకార్లను ఉపయోగించడం ద్వారా వక్రీకృత తీగలు నిఠారుగా చేయండి. 1 జత ట్వీజెర్లతో ఒక వంపు కింద ఒక తీగను గ్రహించండి, మరియు మిగిలిన జతలను శాంతముగా నిటారుగా నిలువుగా నిలబెట్టండి. Straighter మీ తీగలు, సులభంగా మీ ఉద్యోగం ఉంటుంది

Arrange the untwisted wires in a row, placing them into the position, running from right to left, in which they will go into the RJ-45 connector:
వరుసగా అవాంఛిత తీగలు అమర్చండి, కుడివైపు నుండి ఎడమ వైపు నుండి నడుపుతూ, వాటిని స్థానానికి తీసుకొని, దీనిలో వారు RJ-45 కనెక్టర్లోకి ప్రవేశిస్తారు.

- Orange with a white stripe
- Orange
- Green with a white stripe
- Blue
- Blue with a white strip
- Green
- Brown with a white stripe
- Brown

Trim the untwisted wires to a suitable length by holding the RJ-45 connector next to the wires. The insulation on the cable should be just inside the bottom of the RJ-45 connector. The wires should be trimmed so that they line up evenly with the top of the RJ-45 connector.

వైర్లకు పక్కన ఉన్న RJ-45 కనెక్టర్ని పట్టుకుని తగిన పొడవుకు అంటించని వైర్లు త్రిప్పండి. కేబుల్ పై ఇన్సులేషన్ RJ-45 కనెక్టర్ లోపల కేవలం లోపల ఉండాలి. తీగలు సరిగ్గా RJ-45 కనెక్టర్ తో సమానంగా వరుసలో ఉండాలి.

- Trim the wires in small increments, checking frequently to ensure a correct fit. It's better to cut the untwisted wires a few times than have to go back and start all over again because you trimmed off too much.

చిన్న ఇంక్రిమెంట్లలో తీగలు ట్రిమ్, సరైన సరిపోతుందని నిర్ధారించడానికి తరచుగా తనిఖీ. మీరు చాలా దూరంగా ఆఫ్ trimmed ఎందుకంటే తిరిగి వెళ్లి మళ్లీ ప్రారంభించడానికి కలిగి కంటే untwisted వైర్లు కట్ ఉత్తమం.

Insert the wires into the RJ-45 connector, making sure that they stay aligned and each color goes into its appropriate channel. Make sure that each wire goes all the way to the top of the RJ-45 connector. If you don't make these checks, you will find that your newly crimped RJ-45 connector is useless.

RJ-45 కనెక్టర్లోకి వైర్లను చొప్పించండి, అవి సమలేఖనం చేయబడతాయని మరియు ప్రతి రంగు దాని తగిన ఛానెల్లోకి వెళ్లిపోతుందని నిర్ధారించుకోండి. ప్రతి వైర్ RJ-45 కనెక్టర్ పైన అన్ని మార్గం వెళుతుంది నిర్ధారించుకోండి. మీరు ఈ తనిఖీలను చేయకపోతే, మీ కొత్తగా చంపిన RJ-45 కనెక్టర్ నిరుపయోగం అవుతుంది.

Use the crimping tool to crimp the RJ-45 connector to the cable by pressing the jacket and cable into the connector so that the wedge at the bottom of the connector is pressed into the jacket. Recrimp the cable once more to ensure proper connection.

కనెక్టర్ లోకి జాకెట్ మరియు కేబుల్ నొక్కడం ద్వారా కేబుల్ కు RJ-45 కనెక్టర్ ముడుతకు crimping సాధనం ఉపయోగించండి కాబట్టి కనెక్షన్ దిగువన చీలిక జాకెట్ లోకి నొక్కిన. సరైన కనెక్షన్ను నిర్ధారించడానికి కేబుల్ను మరలా మరల మరల ఉంచండి.

Use a cable tester to assure that your cable is working properly when both ends are crimped.

Optical Fiber Cabling
ఆప్టికల్ ఫైబర్ కాబలింగ్

Optical Fiber cables use optical fibers that carry digital data signals in the form of modulated pulses of light. An optical fiber consists of an extremely thin cylinder of glass, called the core, surrounded by a concentric layer of glass, known as the cladding. There are two fibers per cable—one to transmit and one to receive. The core also can be an optical-quality clear plastic, and the cladding can be made up of gel that reflects signals back into the fiber to reduce signal loss.

ఆప్టికల్ ఫైబర్ కేబుల్స్ ఆప్టికల్ ఫైబర్లను డిజిటల్ డేటా సంకేతాలను కాంతి యొక్క మాడ్యులేట్ పప్పుల రూపంలో కలిగి ఉంటాయి. ఒక ఆప్టికల్ ఫైబర్ గ్లాస్ యొక్క చాలా సన్నని సిలిండర్ను కలిగి ఉంటుంది, ఇది కోర్ గా పిలువబడుతుంది, ఇది గాఢత యొక్క గాడమైన పొరతో కప్పబడి ఉంటుంది. కేబుల్ ఒకటికి రెండు ఫైబర్లు ప్రసారం చేయబడతాయి మరియు ఒకటి అందుకోవచ్చు. కోర్ కూడా ఒక ఆప్టికల్ నాణ్యత స్పష్టమైన ప్లాస్టిక్ ఉంటుంది, మరియు క్లాడింగ్ సిగ్నల్ నష్టం తగ్గించడానికి ఫైబర్ తిరిగి సంకేతాలు ప్రతిబింబిస్తుంది జెల్ తయారు చేయవచ్చు.

There are two types of fiber optic cable: Single Mode Fibre (SMF) and Multi Mode Fibre (MMF).

రెండు రకాల ఫైబర్ ఆప్టిక్ కేబుల్ ఉన్నాయి: సింగిల్ మోడ్ ఫైబర్ (SMF) మరియు మల్టీ మోడ్ ఫైబర్ (MMF)

1. Single Mode Fibre (SMF) uses a single ray of light to carry transmission over long distances.
   సింగిల్ మోడ్ ఫైబర్ (ఎస్ఎమ్ఎఫ్) చాలా దూరాలకు ప్రసారం చేయడానికి కాంతి యొక్క ఒకే రేను ఉపయోగిస్తుంది .

2. Multi Mode Fibre (MMF) uses multiple rays of light simultaneously with each ray of light running at a different reflection angle to carry the transmission over short distances.
   బహుళ మోడ్ ఫైబర్ (MMF) కాంతి యొక్క ప్రతి కిరణంతో కాంతి యొక్క బహుళ కిరణాలను ఏకకాలంలో ఉపయోగిస్తుంది .

There are two major Unshielded Twisted Pair Cable wiring standards used widely in networking industry. Telecommunications Industry Association (TIA)/Electronic Industries Alliance (EIA) developed the TIA/EIA 568A & TIA/EIA 568B standards for Unshielded Twisted Pair wiring.

నెట్వర్కింగ్ పరిశ్రమలో విస్తృతంగా ఉపయోగించిన రెండు పెద్ద అన్షీల్డ్ ట్విస్టెడ్ పెయిర్ కేబుల్ వైరింగ్ ప్రమాణాలు ఉన్నాయి. టెలీకమ్యూనికేషన్స్ ఇండస్ట్రీ అసోసియేషన్ (TIA) / ఎలక్ట్రానిక్ ఇండస్ట్రీస్ అలయన్స్ (EIA) TIA / EIA 568A & TIA / EIA 568B

ప్రమాణాలను అన్వైల్డ్ ట్విస్టెడ్ పెయిర్ వైరింగ్ కొరకు అభివృద్ధి చేసింది.

TIA/EIA 568A and TIA/EIA-568B standards determine the order of the wires placed in the RJ45 connector.

TIA / EIA 568A మరియు TIA / EIA-568B ప్రమాణాలు RJ45 కనెక్టర్లో ఉంచిన వైర్ల క్రమాన్ని నిర్ధారిస్తాయి.

Functionally, there is no difference between TIA/EIA 568A and TIA/EIA-568B standards. Only the difference is that the position of Green and Orange wires are switched.

క్రియాత్మకంగా, TIA / EIA 568A మరియు TIA / EIA-568B ప్రమాణాల మధ్య వ్యత్యాసం లేదు. తేడా మాత్రమే గ్రీన్ మరియు ఆరెంజ్ తీగలు స్థానం స్విచ్ అని ఉంది.

You can follow any standard. If a specific standard is mentioned in the network installation project documents, follow that.

మీరు ఏ ప్రమాణాన్ని అనుసరించవచ్చు. ఒక నిర్దిష్ట ప్రమాణం నెట్వర్క్ సంస్థాపన ప్రణాళిక పత్రాలలో ప్రస్తావించబడినట్లయితే, దాన్ని అనుసరించండి.

If you terminate the RJ45 jacks at both ends of a patch cable with same standard (either TIA/EIA 568A on both sides or TIA/EIA 568B on both sides), you will get a Straight-through cable. If you terminate RJ45 jacks at both ends with different TIA/EIA 568 standards (one side TIA/EIA 568A and other side TIA/EIA 568B) you will get a Crossover cable.

మీరు ఒకే పాచ్ (రెండు వైపులా TIA / EIA 568A లేదా రెండు వైపులా TIA / EIA 568B గాని) తో ఒక పాచ్ కేబుల్ రెండు చివరలను RJ45 జాక్స్ రద్దు ఉంటే, మీరు ఒక స్ట్రెయిట్-ద్వారా కేబుల్ పొందుతారు. మీరు వివిధ TIA / EIA 568 ప్రమాణాలు (ఒక వైపు TIA / EIA 568A మరియు ఇతర వైపు TIA / EIA 568B) తో రెండు చివరలను RJ45 జాక్స్ రద్దు ఉంటే మీరు ఒక క్రాస్ఓవర్ కేబుల్ పొందుతారు.

Straight-Through Cables

CAT 5 UTP cabling usually uses only four wires when sending and receiving information on the network. The four wires, which are used, are wires 1, 2, 3, and 6. When you configure the wire for the same pin at either end of the cable, this is known as a straight-through cable.

CAT 5 UTP కేబులింగ్ సాధారణంగా నెట్వర్క్ సమాచారం పంపడం మరియు స్వీకరించినప్పుడు కేవలం నాలుగు తీగలు మాత్రమే ఉపయోగిస్తుంది. ఉపయోగించిన నాలుగు వైర్లు, తీగలు 1, 2, 3 మరియు 6. కేబుల్ యొక్క చివరిలో ఇదే పిన్ కోసం మీరు వైర్ను కాన్ఫిగర్ చేసినప్పుడు, ఇది నేరుగా-ద్వారా కేబుల్గా పిలువబడుతుంది.

We can see that the wires 1 and 2 are used to transmit the data from the computer and 3 and 6 are used to receive data on the computer. The transmit wire on the computer matches with the receive wire on the switch. For the transmission of data to take place, the transmit pins on the computer should match

వైర్లెస్ 1 మరియు 2 కంప్యూటర్ నుండి డేటాను ప్రసారం చేయడానికి మరియు 3 మరియు 6 కంప్యూటర్లో డేటాను స్వీకరించడానికి ఉపయోగించబడుతున్నాయని మేము చూడగలం. కంప్యూటర్లో ప్రసారం వైర్ స్విచ్లో స్వీకరించే వైర్తో సరిపోతుంది. డేటా ప్రసారం కోసం ప్రసారం కోసం, కంప్యూటర్లో ప్రసారం పిన్స్ మ్యాచ్ ఉండాలి

With the receive pins on the switch and the transmit pins on the switch should match to receive pins on the computer. Here we can see that the pins 1, 2, 3 and 6 on the computer matches with pins 1, 2, 3 and 6 on the switch. Hence we use the term Straight-through.

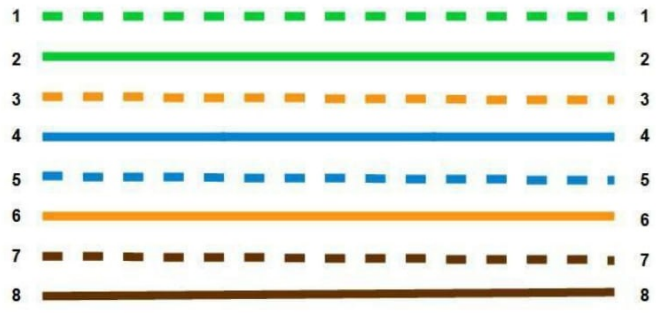
స్విచ్లో స్వీకరించే పిన్స్ మరియు స్విచ్ ప్రసారం పిన్స్ కంప్యూటర్లో పిన్స్ అందుకోవడానికి సరిపోలాలి. ఇక్కడ మనము కంప్యూటర్ మ్యాచ్లలో పిన్స్ 1, 2, 3 మరియు 6 స్విచ్లలో పిన్స్ 1, 2, 3 మరియు 6 తో చూస్తాము. అందువల్ల మనం స్ట్రైట్-ఎట్ అనే పదాన్ని వాడతాము.

Following image shows the wire/pin positions of a Straight-through Unshielded Twisted Pair cable, using TIA/EIA 568A standard.

TIA / EIA 568A స్టాండర్డ్ ఉపయోగించి స్ట్రెయిట్-బై అన్షీల్డ్ ట్విస్టెడ్ పెయిర్ కేబుల్ యొక్క వైర్ / పిన్ స్థానాలను క్రింది చిత్రం చూపిస్తుంది.

Note that the white striped wires are used to connect positive pins and solid color wires are used to connect negetive pins.

తెలుపు చారల వైర్లు సానుకూల పిన్స్ మరియు ఘన రంగు తీగలు కనెక్ట్ చేయడానికి వాడతారు.



Cross-Over Cables

క్రాస్ ఓవర్ కేబుల్స్

If we want to connect two computers together with a straight-through cable, we can see that, the transmit pins will be connected to transmit pins and receive pins will be connected to receive pins. We will not be able to directly connect two computers or two switches together using straight through cables.

మేము రెండు కంప్యూటర్లను సరళమైన తంతితో కలిపి అనుసంధానించాలనుకుంటే, ప్రసరణ పిన్స్ పిన్స్ను ప్రసారం చేయడానికి

మరియు పిన్నులను పిన్స్ అందుకోడానికి అనుసంధానం చేయటానికి కనెక్ట్ చేయబడతాయి. నేరుగా రెండు కేబుళ్లను లేదా రెండు స్విచ్లను నేరుగా తంతులు ద్వారా నేరుగా కనెక్ట్ చేయలేము.

To connect two computers together without using a switch (or two switches directly), we need a crossover cable by switching wires 1 and 2 with wires 3 and 6 at one end of the cable. If we shift the pins, we can make sure that the transmit pins on Computer A will match with the receive pins on Computer B and the transmit pins on Computer B will match with the receive pins on Computer A.

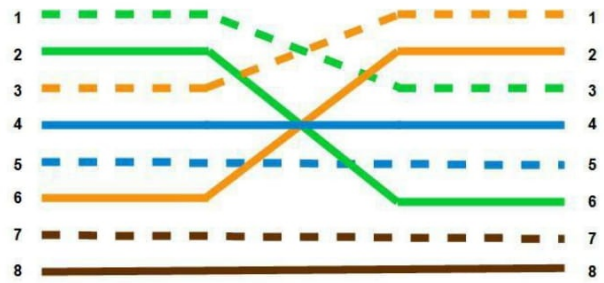
ఒక స్విచ్ (లేదా రెండు స్విచ్లు నేరుగా) ఉపయోగించకుండా కలిసి రెండు కంప్యూటర్లను కనెక్ట్ చేయడానికి, కేబుల్ యొక్క ఒక చివరన వైర్లు 3 మరియు 6 తో తీగలు 1 మరియు 2 ను మార్చడం ద్వారా క్రాస్ఓవర్ కేబుల్ అవసరం. మేము పిన్స్ను మార్చినట్లయితే, కంప్యూటర్ A పై ప్రసారం పిన్నులు కంప్యూటర్ B లో స్వీకరించే పిన్స్ మరియు కంప్యూటర్ B పై ప్రసార పిన్స్తో సరిపోలడం కంప్యూటర్ కంప్యూటర్లో అందిన పిన్స్

Following image shows the wire/pin positions Cross-over Unshielded Twisted Pair cable, using TIA/EIA 568A/568B standards.

TIA / EIA 568A / 568B ప్రమాణాలను ఉపయోగించి వైర్ / పిన్ స్థానాలు క్రాస్-ఓవర్ అన్షీల్డ్ ట్విస్టెడ్ పెయిర్ కేబుల్ను చూపిస్తుంది.

Note that the white striped wires are used to connect positive pins and solid color wires are used to connect negetive pins.

తెలుపు చారల వైర్లు సానుకూల పిన్స్ మరియు ఘన రంగు తీగలు కనెక్ట్ చేయడానికి వాడతారు.



The following table illustrates the different types of twisted pair cable which must be used to connect different network infrastructure devices.

విభిన్న నెట్వర్క్ ఇన్ఫ్రాస్ట్రక్చర్ పరికరాలను అనుసంధానించడానికి తప్పక వివిధ రకాల వక్రీకృత జంట కేబుల్ను క్రింది పట్టిక ఉదహరించింది.

	Hub	Switch	Router	Workstation
Hub	Cross-over	Cross-over	Straight	Straight
Switch	Cross-over	Cross-over	Straight	Straight
Router	Straight	Straight	Cross-over	Cross-over
Workstation	Straight	Straight	Cross-over	Cross-over

Straight-through and Crossover terms are not much relevant for new Switch models. New Cisco Switches are packed with a feature known as Automatic Medium-Dependent Interface crossover (Auto-MDIX). Auto-MDIX watches for a wrong cable connection and automatically changes the pins to make the link work. Meaning that, you can use either Straight-through or Crossover to connect any type of device for Auto-MDIX enabled new switch models.

స్ట్రెట్-మరియు క్రాస్ఓవర్ నిబంధనలు నూతన స్విచ్ మోడళ్లకు చాలా సందర్భోచితంగా ఉండవు. కొత్త సిస్కో స్విచ్లు ఆటోమేటిక్ మీడియమ్-డిపెండెంట్ ఇంటర్ఫేస్ క్రాస్ఓవర్ (స్వీయ MDIX) అని పిలిచే ఒక ఫీచర్తో ప్యాక్ చేయబడతాయి. స్వీయ MDIX తప్పు కేబుల్ కనెక్షన్ కోసం గడియారాలు మరియు స్వయంచాలకంగా లింక్ పనిని చేయడానికి పిన్నులను మారుస్తుంది. అర్థం, మీరు స్వీయ MDIX ప్రారంభించిన కొత్త స్విచ్ మోడళ్లకు ఏ రకమైన పరికరాన్ని అయినా కనెక్ట్ చేయడానికి స్ట్రెయిట్-ద్వారా లేదా క్రాస్ఓవర్ని ఉపయోగించవచ్చు

Warning: The concept of Automatic Medium-Dependent Interface crossover (Auto-MDIX) is not applicable for CCNA or Network+ exams. Straight-through and Crossover terms are relevant for CCNA or Network+ exams. **If you pick the wrong cable, you may lose your marks.**

హెచ్చరిక: ఆటోమేటిక్ మీడియమ్-డిపెండెంట్ ఇంటర్ఫేస్ క్రాస్ఓవర్ (స్వీయ MDIX) భావన CCNA లేదా నెట్వర్క్ + పరీక్షలకు వర్తించదు. స్ట్రాంట్-అండ్ క్రాస్ఓవర్ నిబంధనలు CCNA లేదా నెట్వర్క్ + పరీక్షలకు సంబంధించినవి. మీరు తప్పు కేబుల్ ఎంచుకుంటే, మీరు మీ మార్కులు కోల్పోవచ్చు

Difference between Baseband and Broadband

బేస్బ్యాండ్ మరియు బ్రాడ్ బ్యాండ్ మధ్య వ్యత్యాసం

In Baseband, data is sent as digital signals through the media as a single channel that uses the entire bandwidth of the media. Baseband communication is bi-directional, which means that the same channel can be used to send and receive signals. In Baseband, frequency-division multiplexing is not possible. (Multiplexing (short muxing) is a process where multiple analog message signals or digital data streams are combined into one signal over a shared medium.)

బేస్బ్యాండ్లో, మీడియా మొత్తం డిజిటల్ బ్యానర్విడ్త్ను ఉపయోగించే ఒక సింగిల్ ఛానల్గా డిజిటల్ సిగ్నల్స్గా పంపబడుతుంది. బేస్బ్యాండ్ కమ్యూనికేషన్ ద్వి-డైరెక్షనల్, అంటే అదే ఛానల్ సంకేతాలను పంపడానికి మరియు స్వీకరించడానికి ఉపయోగించబడుతుంది. బేస్బ్యాండ్లో, ఫ్రీక్వెన్సీ-డివిజన్ మల్టీప్లెక్స్ సాధ్యం కాదు. (మల్టీప్లెక్స్ (చిన్న మిక్సింగ్) అనేవి బహుళ అనలాగ్ సందేశ సంకేతాలు లేదా డిజిటల్ డేటా ప్రవాహాలు భాగస్వామ్య మాధ్యమం మీద ఒక సిగ్నల్గా మిళితం చేయబడిన ఒక ప్రక్రియ.

Broadband sends information in the form of an analog signal. Each transmission is assigned to a portion of the bandwidth, hence multiple transmissions are possible at the same time. Broadband communication is unidirectional, so in order to send and receive, two pathways are needed. This can be accomplished either by assigning a frequency for sending and assigning a frequency for receiving along the same cable or by using two cables, one for sending and one for receiving. In broadband frequency-division multiplexing is possible.

బ్రాడ్బ్యాండ్ ఒక అనలాగ్ సిగ్నల్ రూపంలో సమాచారం పంపుతుంది. ప్రతి ట్రాన్స్మిషన్ బ్యాండ్విడ్త్ యొక్క ఒక భాగానికి కేటాయించబడుతుంది, అందువల్ల అదే సమయంలో బహుళ ప్రసారాలు సాధ్యమవుతాయి. బ్రాడ్బ్యాండ్ కమ్యూనికేషన్ ఏకదిశాత్మకమైనది, కాబట్టి పంపేందుకు మరియు స్వీకరించడానికి, రెండు మార్గాలు అవసరమవుతాయి. ఒకే కేబుల్ వద్ద లేదా రెండు తంతులు ఉపయోగించడం, ఒకటి పంపడం కోసం మరియు స్వీకరించడానికి ఒకటి ఉపయోగించడం కోసం ఒక పౌనఃపున్యం పంపడం మరియు కేటాయించడం కోసం ఒక ఫ్రీక్వెన్సీని కేటాయించడం ద్వారా ఇది సాధించవచ్చు. బ్రాడ్బ్యాండ్ ఫ్రీక్వెన్సీ-డివిజన్ మల్టీప్లెక్స్లో సాధ్యమే.

Network Access Methods,

నెట్వర్క్ యాక్సెస్ మెథడ్స్

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

CSMA / CD (క్యారియర్ సెన్స్ మల్టిపుల్ యాక్సెస్ / కొలిసిస్ డిటెక్షన్

In CSMA/CD (Carrier Sense Multiple Access/Collision Detection) Access Method, every host has equal access to the wire and can place data on the wire when the wire is free from traffic. When a host want to place data on the wire, it will “sense” the wire to find whether there is a signal already on the wire. If CSMA / CD లో (క్యారియర్ సెన్స్ మల్టిపుల్ యాక్సెస్ / కొలిసిస్ డిటెక్షన్) యాక్సెస్ మెథడ్, ప్రతి హోస్ట్ వైర్కు సమానమైన ప్రాప్యతను కలిగి ఉంటుంది మరియు వైర్ ట్రాఫిక్ నుండి ఉచితంగా ఉన్నప్పుడు వైర్పై డేటాను ఉంచవచ్చు. ఒక అతిథేయ వైర్ మీద డేటాను ఉంచాలని కోరుకుంటే, వైర్లో ఇప్పటికే ఒక సిగ్నల్ ఉందో లేదో తెలుసుకోవడానికి వైర్ "భావన" చేస్తుంది.

there is traffic already in the medium, the host will wait and if there is no traffic, it will place the data in the medium. But, if two systems place data on the medium at the same instance, they will collide with each other, destroying the data. If the data is destroyed during transmission, the data will need to be retransmitted. After collision, each host will wait for a small interval of time and again the data will be retransmitted, to avoid collision again.

మాధ్యమంలో ఇప్పటికే ట్రాఫిక్ ఉంది, హోస్ట్ వేచి ఉంటుంది మరియు ట్రాఫిక్ లేకపోతే, అది మాధ్యమంలో డేటా ఉంచుతుంది. అయితే, ఇదే సందర్భంలో రెండు వ్యవస్థలు మాధ్యమంలో డేటాను ఉంచినట్లయితే, అవి ఒకదానితో ఒకటి పరస్పరం పరస్పరం కొట్టుకొని, డేటాను నాశనం చేస్తాయి. ప్రసార సమయంలో డేటా నాశనం చేయబడితే, డేటా పునఃప్రారంభం కావాలి. ఘర్షణ తర్వాత, ప్రతి అతిథేయ సమయం ఒక చిన్న విరామం కోసం వేచి ఉండి, మళ్లీ డేటా పునఃపరిశీలించబడుతుంది, మళ్ళీ ప్రమాదాన్ని నివారించడానికి.

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

CSMA / CA (క్యారియర్ సెన్స్ మల్టిపుల్ యాక్సెస్ **/** తాకిడి తప్పించుకోవటం**)**

In CSMA/CA, before a host sends real data on the wire it will “sense” the wire to check if the wire is free. If the wire is free, it will send a piece of “dummy” data on the wire to see whether it collides with any other data. If it does not collide, the host will assume that the real data also will not collide.

ఒక హోస్ట్ వైర్లో వాస్తవ డేటాను పంపించే ముందు CSMA / CA లో, వైర్ ఉచితం కావాలో తనిఖీ చేయడానికి వైర్ "భావన" చేస్తుంది. వైర్ ఉచితం అయితే, ఇది వేరే డేటాతో గుద్దుతుందో లేదో చూడటానికి వైర్పై "నకిలీ" డేటాను పంపుతుంది. అది కొట్టుకోకపోతే, వాస్తవిక సమాచారం కూడా కొట్టుకుపోవని హోస్ట్ ఊహించుకుంటుంది.

Token Passing
టోకెన్ పాసింగ్

In CSMA/CD and CSMA/CA the chances of collisions are there. As the number of hosts in the network increases, the chances of collisions also will become more. In token passing, when a host want to transmit data, it should hold the token, which is an empty packet. The token is circling the network in a very high speed. If any workstation wants to send data, it should wait for the token. When the token has reached the workstation, the workstation can take the token from the network, fill it with data, mark the token as being used and place the token back to the network.

CSMA / CD మరియు CSMA / CA లో ప్రమాదాలలో aa అవకాశాలు ఉన్నాయి. నెట్వర్క్లో హోస్ట్ల సంఖ్య పెరుగుతూ ఉండగా, ప్రమాదాల అవకాశాలు కూడా ఎక్కువ అవుతుంది. టోకెన్ తరలింపులో, అతిధేయ డేటాను బదిలీ చేయాలనుకున్నప్పుడు, అది ఖాళీ పాకెట్ అయిన టోకెన్ను కలిగి ఉండాలి. టోకెన్ చాలా అధిక వేగంతో నెట్వర్క్ను చుట్టుముడుతుంది. ఏదైనా వర్క్స్టేషన్ డేటాను పంపించాలనుకుంటే, అది టోకెన్ కోసం వేచి ఉండాలి. టోకెన్ వర్క్స్టేషన్కు చేరుకున్నప్పుడు, వర్క్స్టేషన్ నెట్వర్క్ నుండి టోకెన్ను తీసుకొని దానిని డేటాతో నింపుతుంది, టోకెన్ను గుర్తించేదిగా గుర్తించి టోకెన్ను తిరిగి నెట్వర్క్కి.

LAN Technologies Ethernet
LAN టెక్నాలజీస్ ఈథర్నెట్

Ethernet, Fast Ethernet and Gigabit Ethernet are the LAN technologies most commonly used today. Ethernet Version 1 was developed by Xerox Corporation during the early 1970s. Later in 1982 Xerox, Intel and DEC (Digital Equipment Corporation) together released Ethernet Version 2. Since then, Ethernet is the most popular LAN technology used in networking.

ఈథర్నెట్, ఫాస్ట్ ఈథర్నెట్ మరియు గిగాబిట్ ఈథర్నెట్ లాంగ్ టెక్నాలజీలు సాధారణంగా ఉపయోగించేవి. 1970 ల ప్రారంభంలో జిరాక్స్ కార్పొరేషన్ ఈథర్నెట్ వెర్షన్ 1 ను అభివృద్ధి చేసింది. తరువాత 1982 లో జిరాక్స్, ఇంటెల్ మరియు DEC (డిజిటల్ ఎక్విప్మెంట్ కార్పొరేషన్) కలిసి ఈథర్నెట్ సంస్కరణ 2 విడుదల చేసింది. అప్పటి నుండి, ఈథర్నెట్ నెట్వర్కింగ్లో ఉపయోగించిన అత్యంత ప్రజాదరణ LAN సాంకేతికత.

The network topology on which all the latest Ethernet technologies built is Star Topology.

అన్ని ఆధునిక ఈథర్నెట్ టెక్నాలజీలను నిర్మించిన నెట్వర్క్ టోపోలాజి స్టార్ టోపోలాజీ.Advantages of Ethernet are

- Low cost components
  తక్కువ ఖర్చు భాగాలు
- Easy to install
  సులువు ఇన్స్టాల్
- Easy to troubleshoot
  సమస్యా పరిష్కారం సులభం

All the devices (Servers, Workstations, Printers, Scanners etc) connected in an Ethernet network share a common transmission medium. Ethernet uses Carrier Sense Multiple Access/Collision Detection (CSMA/CD) for determining when a computer is free to transmit data on to the access medium. Using Carrier Sense Multiple Access/Collision Detection (CSMA/CD), all computers monitor the transmission

medium and wait until the medium is free before transmitting. If two computers try to transmit at the same time, a collision occurs. The computers then stop, wait for a random time interval, and attempt to transmit again.

అన్ని పరికరములు (సర్వర్లు, వర్క్స్టేషన్లు, ప్రింటర్లు, స్కానర్లు మొదలైనవి) ఈథర్నెట్ నెట్వర్కులో అనుసంధానించబడిన ఒక సాధారణ ప్రసార మాధ్యమం. ఈథర్నెట్ క్యారియర్ సెన్స్ మల్టిస్ యాక్సెస్ / కొలిసిస్ డిటెక్షన్ (CSMA / CD) ను ఒక కంప్యూటర్ యాక్సెస్ మాధ్యమంలో డేటాను బదిలీ చేయగలదా అని నిర్ణయించుకొనుటకు ఉపయోగిస్తుంది. క్యారియర్ సెన్స్ బహుళ యాక్సెస్ / కొలిసిస్ డిటెక్షన్ (CSMA / CD) ఉపయోగించి, అన్ని కంప్యూటర్లు ప్రసార మాధ్యమాన్ని పర్యవేక్షిస్తాయి మరియు ప్రసారం చేయడానికి ముందు మాధ్యమం ఉచితం వరకు వేచి ఉండండి. రెండు కంప్యూటర్లు అదే సమయంలో ప్రసారం చేయటానికి ప్రయత్నిస్తే, ఘర్షణ జరుగుతుంది. కంప్యూటర్లు ఆపివేస్తే, యాదృచ్ఛిక సమయం విరామం కోసం వేచి ఉండండి మరియు మళ్ళీ ప్రసారం చేయటానికి ప్రయత్నిస్తాయి.

Collisions were common in Ethernet network (when used in a shared media) and network infrastructure devices like Ethernet Hubs usually have a small light on their front panel, that blink when collisions happen in your network.

ఈథర్నెట్ నెట్వర్క్ (ఈడ్ని మీడియాలో ఉపయోగించినప్పుడు) మరియు ఈథర్నెట్ హబ్స్ వంటి నెట్వర్క్ మౌలిక సదుపాయాల పరికరాలు సాధారణంగా వారి ముందు ప్యానెల్లో ఒక చిన్న కాంతిని కలిగి ఉంటాయి,

These days, all the business networks are installed and connected using Ethernet Switches instead of Ethernet Hubs. There is no collision when devices are connected using Ethernet Switches.

ఈ రోజుల్లో, అన్ని వ్యాపార నెట్వర్కు ఈథర్నెట్ హబ్కు బదులుగా ఈథర్నెట్ స్విచ్లు ఉపయోగించి మరియు కనెక్ట్ చేయబడతాయి. ఈథర్నెట్ స్విచ్లు ఉపయోగించి పరికరాలను కనెక్ట్ చేసినప్పుడు ఎటువంటి ఘర్షణ లేదు.

Original Ethernet operate at a speed of 10 Mbps (Mega bits per second). Ethernet is capable of using a variety of media. Another faster version of Ethernet, which is even faster than Fast Ethernet, is Gigabit Ethernet. Gigabit Ethernet provides a data transmission speed of 1,000Mbps. Gigabit Ethernet was first designed and developed as a high-speed backbone medium for large LANs. But almost all latest LANs are Gigabit Ethernet capable and Category 5eand Category 6 UTP cable can be used as the Gigabit Ethernet medium.

ఒరిజినల్ ఈథర్నెట్ 10 Mbps (సెకనుకు మెగా బిట్స్) వేగంతో పనిచేస్తాయి. ఈథర్నెట్ వివిధ రకాల మీడియాలను ఉపయోగించుకోగలదు. ఫాస్ట్ ఈథర్నెట్ కన్నా వేగవంతమైన ఈథర్నెట్ యొక్క వేగవంతమైన సంస్కరణ, గిగాబిట్ ఈథర్నెట్. గిగాబిట్ ఈథర్నెట్ 1000Mbps యొక్క సమాచార ప్రసారం వేగాన్ని అందిస్తుంది. గిగాబిట్ ఈథర్నెట్ మొట్టమొదటిగా పెద్ద లాంగ్స్ కోసం అధిక-వేగవంతమైన వెన్నెముక మాధ్యమంగా రూపొందించబడింది మరియు అభివృద్ధి చేయబడింది. కానీ దాదాపు అన్ని తాజా LAN లు గిగాబిట్ ఈథర్నెట్ సామర్థ్యం మరియు కేటగిరి 5 మరియు వర్గం 6 UTP కేబుల్ను గిగాబిట్ ఈథర్నెట్ మాధ్యమంగా ఉపయోగించవచ్చు.

Ethernet networks typically operate at baseband speeds of either 100Mbps (Fast Ethernet), 1000Mbps (Gigabit Ethernet).

ఈథర్నెట్ నెట్వర్కు సాధారణంగా 100Mbps (ఫాస్ట్ ఈథర్నెట్), 1000Mbps (గిగాబిట్ ఈథర్నెట్) యొక్క బేస్బ్యాండ్ వేగంతో పనిచేస్తాయి.

Fast Ethernet (100 Mbps) or Gigabit Ethernet (1000 Mbps) cannot operate on network infrastructure devices like Ethernet Hubs, Ethernet Switches and network cards designed for a 10Mbps Ethernet network. Many latest network infrastructure devices like Ethernet Switches and Ethernet network cards are capable to operate at speed of 10 Mbps or 100 Mbps or 1000 Mbps. (10/100/100).

ఫాస్ట్ ఈథర్నెట్ (100 Mbps) లేదా గిగాబిట్ ఈథర్నెట్ (1000 Mbps) ఈథర్నెట్ హబ్స్, ఈథర్నెట్ స్విచ్లు మరియు 10Mbps ఈథర్నెట్ నెట్వర్క్ కోసం రూపొందించిన నెట్వర్క్ కార్డుల వంటి నెట్వర్క్ మౌలిక సదుపాయాల పరికరాలపై పనిచేయదు. ఈథర్నెట్ స్విచ్లు మరియు ఈథర్నెట్ నెట్వర్క్ కార్డుల వంటి అనేక తాజా నెట్వర్క్ అవస్థాపన పరికరాలు 10 Mbps లేదా 100 Mbps లేదా 1000 Mbps వేగంతో పనిచేస్తాయి. (10/100/100)

Even a faster version of Gigabit Ethernet, 10 Gigabit Ethernet is now available. 10 Gigabit Ethernet works well with both fiber optic and copper media.
గిగాబిట్ ఈథర్నెట్ యొక్క వేగవంతమైన సంస్కరణ, ఇప్పుడు 10 గిగాబిట్ ఈథర్నెట్ అందుబాటులో ఉంది. 10 గిగాబిట్ ఈథర్నెట్ రెండు ఫైబర్ ఆప్టిక్ మరియు కాపర్ మీడియాలతో బాగా పనిచేస్తుంది

What is Ethernet Media Standards. How to identify bandwidth and cable type from media standard
ఈథర్నెట్ మీడియా స్టాండర్డ్స్ అంటే మీడియా స్టాండర్డ్ నుండి బ్యాండ్విడ్త్ మరియు కేబుల్ రకాలను ఎలా గుర్తించాలి

Ethernet, Fast Ethernet and Gigabit Ethernet, are identified by three-part names, which is also known as Media Standard. An example of Media Standard is 10BASE-T. The first part of the Media Standard specifies the transmission speed (10, in this case specifies 10 Mbps)

ఈథర్నెట్, ఫాస్ట్ ఈథర్నెట్ మరియు గిగాబిట్ ఈథర్నెట్లు మూడు భాగాల పేర్లతో గుర్తించబడతాయి, వీటిని మీడియా స్టాండర్డ్ అని కూడా పిలుస్తారు. మీడియా స్టాండర్డ్ యొక్క ఉదాహరణ 10BASE-T. మీడియా స్టాండర్డ్ యొక్క మొదటి భాగం ట్రాన్స్మిషన్ వేగం పేర్కొంటుంది (10, ఈ సందర్భంలో 10 Mbps నిర్దేశిస్తుంది).

The second part of the name "BASE" specifies that the Ethernet signal is a Baseband signal.
BASE" పేరులోని రెండవ భాగం ఈథర్నెట్ సిగ్నల్ ఒక బేస్బ్యాండ్ సిగ్నల్ అని పేర్కొంటుంది.
The final part of the Ethernet Media Standard specifies the kind of cable used. Here "T" specifies twisted-pair cable. The following table shows the common Ethernet Media Standards.

ఈథర్నెట్ మీడియా స్టాండర్డ్ యొక్క ఆఖరి భాగం ఉపయోగించిన కేబుల్ రకం నిర్దేశిస్తుంది. ఇక్కడ "T" వక్రీకృత-జత కేబుల్ నిర్దేశిస్తుంది. కింది పట్టిక సాధారణ ఈథర్నెట్ మీడియా స్టాండర్డ్స్ చూపిస్తుంది.

Media Standard	Cable Type	Bandwidth Capacity	Maximum Length
10Base2	Coax	10 Mbps	185m
10Base5	Coax	10 Mbps	500m
10BaseT	UTP (CAT 3 or higher)	10 Mbps	100m
100BaseTX	UTP (CAT 5 or higher)	100 Mbps	100m
10BaseFL	Fibre Optic	10 Mbps	2Km
100BaseFX	Fibre Optic	100 Mbps	HD 400m/FD 2km
1000BaseT	UTP (CAT 5e or higher)	1 Gbps (1000 Mbps)	100m
1000BaseSX	Fibre Optic	1 Gbps (1000 Mbps)	MMF 550m
1000BaseLX	Fibre Optic	1 Gbps (1000 Mbps)	MMF 500m/SMF 10km
1000BaseCX	Fibre Optic	1 Gbps (1000 Mbps	100m
10GbaseSR	Fibre Optic	10 Gbps	300m
10GbaseLR	Fibre Optic	10 Gbps	SMF 10km

Note: X represents a higher grade of connection, and 100BaseTX is twisted-pair cable cabling that can use either UTP or STP at 100 Mbps. With fibre-optic cable such as 100BaseFX, the speed is quicker than standard 10BaseF. The “L” stands for “Long” in long wave length lasers and "S" stands for Short Wave Length.

గమనిక: X అధిక స్థాయి కనెక్షన్ని సూచిస్తుంది, మరియు 100BaseTX 100 Mbps వద్ద UTP లేదా STP ను ఉపయోగించగల ట్విస్టెడ్-జత కేబుల్ క్యాబ్లింగ్. 100BaseFX వంటి ఫైబర్-ఆప్టిక్ కేబుల్తో, వేగం 10BaseF కంటే వేగంగా ఉంటుంది. "L" అనేది దీర్ఘకాల వేవ్ పొడవు లేజర్లలో "లాంగ్" మరియు "S" అనేది చిన్న వేవ్ పొడవుకు.

What is FDDI, Advantages of FDDI
FDDI ఏమిటి, FDDI యొక్క ప్రయోజనాలు

Fiber Distributed Data Interface (FDDI) is an expensive LAN technology that employs a pair of fibre-optic rings. One is primary ring and the second ring is used to replace the primary ring in the case of a network failure. Fiber Distributed Data Interface (FDDI) uses fiber-optic cable and is wired in a ring topology and Fiber Distributed Data Interface (FDDI) uses token passing as its media-access method and can operate at high speeds.

ఫైబర్ డిస్ట్రిబ్యూటెడ్ డేటా ఇంటర్ఫేస్ (FDDI) ఫైబర్-ఆప్టిక్ వలయాలను జతచేసే ఒక ఖరీదైన LAN సాంకేతికత. ఒక ప్రాథమిక రింగ్ మరియు రెండవ రింగ్ ఒక నెట్వర్క్ వైఫల్యం సందర్భంలో ప్రాథమిక రింగ్ స్థానంలో ఉంది. ఫైబర్ డిస్ట్రిబ్యూటెడ్ డేటా ఇంటర్ఫేస్ (FDDI) ఫైబర్-ఆప్టిక్ కేబుల్ను ఉపయోగిస్తుంది మరియు రింగ్ టోపోలాజిలో వైర్డుతుంది మరియు ఫైబర్ డిస్ట్రిబ్యూటెడ్ డేటా ఇంటర్ఫేస్ (FDDI) దాని మీడియా-యాక్సెస్ పద్ధతిగా టోకెన్ పాస్ని ఉపయోగిస్తుంది మరియు అధిక వేగంతో పనిచేయవచ్చు.

The Fiber Distributed Data Interface (FDDI) provides high-speed network backbones that can be used to connect and extend LANs.
ఫైబర్ డిస్ట్రిబ్యూటెడ్ డాటా ఇంటర్ఫేస్ (FDDI) హై-స్పీడ్ నెట్వర్క్ వెన్నెముకలను అనుసంధానిస్తుంది మరియు విస్తరించడానికి LAN లను అందిస్తుంది.

Like token ring, FDDI also has error-detection and correction capabilities. In a normally operating Fiber Distributed Data Interface (FDDI) ring, the token passes by each network device fast. If the token is not seen within the maximum amount of time that it takes to circulate the largest ring, it indicates a network problem.

టోకెన్ రింగ్ మాదిరిగా, FDDI లోపం-గుర్తింపు మరియు దిద్దుబాటు సామర్థ్యాలు కూడా ఉన్నాయి. సాధారణంగా ఆపరేటింగ్ ఫైబర్ డిస్ట్రిబ్యూటెడ్ డాటా ఇంటర్ఫేస్ (FDDI) రింగ్ లో, టోకెన్ ప్రతి నెట్వర్క్ పరికరం శీఘ్రంగా వెళుతుంది. టోకెన్ అతిపెద్ద రింగ్ ప్రసారం చేయడానికి గరిష్ట సమయం లోపల చూడకపోతే, ఇది నెట్వర్క్ సమస్యను సూచిస్తుంది.

Fiber-optic cable such as the cable used with Fiber Distributed Data Interface (FDDI) can support very large volumes of data over large distances.
ఫైబర్-ఆప్టిక్ కేబుల్, ఫైబర్ డిస్ట్రిబ్యూటెడ్ డేటా ఇంటర్ఫేస్ (FDDI) తో ఉపయోగించే కేబుల్ వంటి పెద్ద దూరాలకు సంబంధించిన డేటా.
Fiber Distributed Data Interface (FDDI) is an expensive technology to set up because the network devices require a special network card and also fiber-optic cabling is required, which is expensive than twisted-pair cable. Because most Fiber Distributed Data Interface (FDDI) installations use a redundant second ring, more cabling is required.

ఫైబర్ డిస్ట్రిబ్యూటెడ్ డేటా ఇంటర్ఫేస్ (FDDI) అనేది ఒక ఖరీదైన సాంకేతికత, ఎందుకంటే నెట్వర్క్ పరికరాలకు ప్రత్యేక నెట్వర్క్ కార్డు అవసరం మరియు ఫైబర్-ఆప్టిక్ కేబులింగ్ అవసరమవుతుంది, ఇది వక్రీకృత-జంట కేబుల్ కంటే ఖరీదైనది. ఎందుకంటే చాలా ఫైబర్ పంపిణీ డేటా ఇంటర్ఫేస్ (FDDI) సంస్థాపనలు అనవసరమైన రెండవ రింగ్ను ఉపయోగిస్తాయి, మరింత కేబులింగ్ అవసరం.

IEEE 802 Standard

IEEE 802 ప్రామాణిక

The IEEE 802 Standards comprises a family of networking standards that cover the physical layer specifications of technologies. The following tables show the most popular IEEE 802 Standards.

IEEE 802 స్టాండర్డ్స్ సాంకేతిక పరిజ్ఞానం యొక్క భౌతిక లేయర్ లక్షణాలు కవర్ చేసే నెట్వర్కింగ్ ప్రమాణాల యొక్క కుటుంబం. కింది పట్టికలలో అత్యంత ప్రజాదరణ పొందిన IEEE 802 స్టాండర్డ్స్ చూపించు.

Standard	Description
802.1	Internetworking
802.2	Logical link control
802.3	Ethernet
802.4	Token bus
802.5	Token ring
802.6	Metropolitan area network (MAN)
802.7	Broadband technology
802.8	Fiber-optic technology
802.9	Voice and data integration
802.10	Network security
802.11	Wireless networking
802.12	Demand priority networking

Standard	Description
802.3	Ethernet CSMA /CD (10 Mbps)
802.3u	Fast Ethernet (100 Mbps)
802.3z	Gigabit Ethernet over fiber-optic cabling or coaxial cabling
802.3ab	Gigabit Ethernet over twisted-pair cabling
802.3ae	10-Gigabit Ethernet

Computer Network Models

ఈథర్నెట్ స్టాండర్డ్స్

Networking engineering is a complicated task, which involves software, firmware, chip level engineering, hardware, and electric pulses. To ease network engineering, the whole networking concept is divided into multiple layers. Each layer is involved in some particular task and is independent of all other layers. But as a whole, almost all networking tasks depend on all of these layers. Layers share data between them and they depend on each other only to take input and send output.

నెట్వర్కింగ్ ఇంజనీరింగ్ అనేది క్లిష్టమైన పని, ఇది సాఫ్ట్ వేర్, ఫర్మ్వేర్, చిప్ లెవెల్ ఇంజనీరింగ్, హార్డ్వేర్ మరియు విద్యుత్ పప్పులను కలిగి ఉంటుంది. నెట్వర్క్ ఇంజనీరింగ్ను తగ్గించడానికి, మొత్తం నెట్వర్కింగ్ భావన బహుళ పొరలుగా విభజించబడింది. ప్రతి పొర కొన్ని నిర్దిష్ట పనిలో పాలుపంచుకుంటుంది మరియు అన్ని ఇతర పొరల నుండి స్వతంత్రంగా ఉంటుంది. కానీ మొత్తంగా, దాదాపుగా అన్ని నెట్వర్కింగ్ పనులు ఈ పొరల మీద ఆధారపడి ఉంటాయి. పొరలు వాటి మధ్య డేటాను పంచుకుంటాయి మరియు అవి ఇన్పుట్ తీసుకోవడం మరియు అవుట్పుట్ను పంపడానికి మాత్రమే ఒకదానిపై ఆధారపడి ఉంటాయి.

Network Protocols are a set of rules governing exchange of information in an easy, reliable and secure way. Before we discuss the most common protocols used to transmit and receive data over a network, we need to understand how a network is logically organized or designed. The most popular model used to establish open communication between two systems is the **Open Systems Interface (OSI) model** proposed by ISO

నెట్వర్క్ ప్రోటోకాల్లు ఒక సులభమైన, విశ్వసనీయ మరియు సురక్షితమైన మార్గంలో సమాచారాన్ని మార్పిడి చేసే నియమాల సమితి. ఒక నెట్వర్క్లో డేటాను ప్రసారం చేయడానికి మరియు స్వీకరించడానికి ఉపయోగించే అత్యంత సాధారణ ప్రోటోకాల్లను చర్చించడానికి

ముందు, మేము ఒక నెట్వర్క్ తార్కికంగా వ్యవస్థాపించబడిన లేదా రూపకల్పన చేయబడినట్లుగా అర్థం చేసుకోవాలి. రెండు వ్యవస్థల మధ్య బహిరంగ సంభాషణను స్థాపించడానికి ఉపయోగించిన అత్యంత ప్రజాదరణ పొందిన నమూనా ISO ద్వారా ప్రతిపాదించబడిన ఓపెన్ సిస్టమ్స్ ఇంటర్ఫేస్ (OSI) మోడల్

OSI Model (OSI మోడల్)

OSI model is not a **network architecture** because it does not specify the exact services and protocols for each layer. It simply tells what each layer should do by defining its input and output data. It is up to network architects to implement the layers according to their needs and resources available.

OSI మోడల్ అనేది ఒక నెట్వర్క్ నిర్మాణం కాదు, ఎందుకంటే ఇది ప్రతి పొరకు ఖచ్చితమైన సేవలు మరియు ప్రోటోకాల్స్ను పేర్కొనలేదు. దాని ఇన్పుట్ మరియు అవుట్పుట్ డేటాను నిర్వచించడం ద్వారా ప్రతి పొర ఏమి చేయాలి అని ఇది కేవలం చెబుతుంది. వారి అవసరాలను మరియు వనరులను బట్టి పొరలను అమలు చేయడానికి నెట్వర్క్ వాస్తుశిల్పులు వరకు ఇది ఉంది

These are the seven layers of the OSI model –
ఈ OSI మోడల్ యొక్క ఏడు పొరలు

- **Physical layer** –It is the first layer that physically connects the two systems that need to communicate. It transmits data in bits and manages simplex or duplex transmission by modem. It also manages Network Interface Card's hardware interface to the network, like cabling, cable terminators, topography, voltage levels, etc.
  భౌతిక పొర -ఇది కమ్యూనికేట్ చేయడానికి అవసరమైన రెండు వ్యవస్థలను భౌతికంగా కలుపుతున్న మొదటి పొర. ఇది బిట్స్లో డేటాను బదిలీ చేస్తుంది మరియు మోడెమ్ ద్వారా సింప్లెక్స్ లేదా డ్యూప్లెక్స్ ప్రసారంను నిర్వహిస్తుంది. ఇది నెట్వర్క్ ఇంటర్ఫేస్ కార్డ్ యొక్క హార్డ్వేర్ ఇంటర్ఫేస్ను నెట్వర్క్కు, కేబ్లింగ్, కేబుల్ టెర్మినేటర్స్, స్థలాకృతి, వోల్టేజ్ స్థాయిలు, మొదలైన వాటికి కూడా నిర్వహిస్తుంది .
- **Data link layer** – It is the firmware layer of Network Interface Card. It assembles datagrams into frames and adds start and stop flags to each frame. It also resolves problems caused by damaged, lost or duplicate frames.
  డేటా లింక్ పొర - ఇది నెట్వర్క్ ఇంటర్ఫేస్ కార్డ్ యొక్క ఫర్మ్వేర్ పొర. ఇది ఫ్రేమ్లలో డేటాగ్రామ్లను ఏర్పరుస్తుంది మరియు ప్రతి ఫ్రేమ్కు ఫ్లాగ్లను ప్రారంభించి, ఆపివేస్తుంది. ఇది దెబ్బతిన్న, కోల్పోయిన లేదా నకిలీ ఫ్రేమ్ల ద్వారా వచ్చే సమస్యలను కూడా పరిష్కరిస్తుంది .

- **Network layer** – It is concerned with routing, switching and controlling flow of information between the workstations. It also breaks down transport layer datagrams into smaller datagrams.
  నెట్వర్క్ పొర - వర్క్స్టేషన్ల మధ్య సమాచారం యొక్క ప్రవాహాన్ని రూటింగ్, స్విచింగ్ మరియు నియంత్రించటంతో ఇది ఆందోళన కలిగిస్తుంది. ఇది రవాణా పొర డాటాగ్రామ్లను చిన్న datagrams లోకి విచ్ఛిన్నం చేస్తుంది.
- **Transport layer** – Till the session layer, file is in its own form. Transport layer breaks it down into data frames, provides error checking at network segment level and prevents a fast host from overrunning a slower one. Transport layer isolates the upper layers from network hardware.
- **రవాణా పొర** - సెషన్ లేయర్ వరకు, ఫైల్ దాని స్వంత రూపంలో ఉంటుంది. రవాణా పొర డేటా ఫ్రేమ్లలోకి విచ్ఛిన్నం చేస్తుంది, నెట్వర్క్ సెగ్మెంట్ స్థాయిలో లోపాలను తనిఖీ చేస్తుంది మరియు వేగవంతమైన హోస్ట్ను నెమ్మదిగా నెమ్మదిగా నిరోధిస్తుంది.

రవాణా పొర నెట్వర్క్ హార్డ్వేర్ నుండి ఎగువ పొరలను వేరు చేస్తుంది.

- **Session layer** − This layer is responsible for establishing a session between two workstations that want to exchange data.
- సెషన్ లేయర్ - ఈ పొర డేటాను మార్పిడి చేయదలిచిన రెండు వర్క్స్టేషన్ల మధ్య ఒక సెషన్ను స్థాపించడానికి బాధ్యత వహిస్తుంది
- **Presentation layer** − This layer is concerned with correct representation of data, i.e. syntax and semantics of information. It controls file level security and is also responsible for converting data to network standards.
- ప్రెజెంటేషన్ పొర - ఈ పొర డేటా సరైన ప్రాతినిధ్యంతో ఉంటుంది, అనగా సమాచారం యొక్క వాక్యనిర్మాణం మరియు సంకేతాలు. ఇది ఫైల్ స్థాయి భద్రతను నియంత్రిస్తుంది మరియు నెట్వర్క్ ప్రమాణాలకు డేటాను మార్చడానికి కూడా బాధ్యత వహిస్తుంది.
- **Application layer** − It is the topmost layer of the network that is responsible for sending application requests by the user to the lower levels. Typical applications include file transfer, E-mail, remote logon, data entry, etc.
- అప్లికేషన్ లేయర్ - ఇది వినియోగదారుల యొక్క దరఖాస్తు అభ్యర్థనలను తక్కువ స్థాయికి పంపే బాధ్యత నెట్వర్క్ యొక్క అతి పొరగా ఉంటుంది. సాధారణ అనువర్తనాల్లో ఫైల్ బదిలీ, ఇ-మెయిల్, రిమోట్ లాగాన్, డేటా ఎంట్రీ మొదలైనవి ఉంటాయి.

It is not necessary for every network to have all the layers. For example, network layer is not there in broadcast networks.
ప్రతి నెట్వర్క్ కోసం అన్ని పొరలు అవసరం లేదు. ఉదాహరణకు, ప్రసార నెట్వర్క్లలో నెట్వర్క్ లేయర్ లేదు.

When a system wants to share data with another workstation or send a request over the network, it is received by the application layer. Data then proceeds to lower layers after processing till it reaches the physical layer.
ఒక వ్యవస్థ వేరొక వర్క్స్టేషన్తో డాటాను పంచుకొనుటకు లేదా నెట్వర్క్పైన ఒక అభ్యర్థనను పంపించునప్పుడు, అది దరఖాస్తు లేయర్ చేత పొందబడుతుంది. అప్పుడు భౌతిక పొరను చేరేవరకు ప్రాసెసింగ్ తర్వాత పొరలు తక్కువగా ఉంటుంది.

At the physical layer, the data is actually transferred and received by the physical layer of the destination workstation. There, the data proceeds to upper layers after processing till it reaches application layer.
భౌతిక పొర వద్ద, డేటా నిజానికి గమ్యం వర్క్స్టేషన్ భౌతిక పొర బదిలీ మరియు అందుకున్న. అక్కడ, దరఖాస్తు పొరను చేరుకునే వరకు ప్రాసెస్ చేసిన తర్వాత ఎగువ పొరలకు డేటా కొనసాగుతుంది.

At the application layer, data or request is shared with the workstation. So each layer has opposite functions for source and destination workstations. For example, data link layer of the source workstation adds start and stop flags to the frames but the same layer of the destination workstation will remove the start and stop flags from the frames.
అప్లికేషన్ లేయర్ వద్ద, డేటా లేదా అభ్యర్థన వర్క్స్టేషన్తో భాగస్వామ్యం చేయబడుతుంది. కాబట్టి ప్రతి పొర మూలం మరియు గమ్యం వర్క్స్టేషన్ల కోసం వ్యతిరేకమైన విధులను కలిగి ఉంది. ఉదాహరణకు, సోర్స్ వర్క్స్టేషన్ యొక్క డాటా లింక్ పొర ఫ్రేమ్లకు ప్రారంభము మరియు ఫ్లాగ్లను ఆపివేస్తుంది కానీ గమ్యం వర్క్స్టేషన్ యొక్క అదే పొర ఫ్రేమ్ల నుండి ప్రారంభమును తీసివేసి

ప్లాగ్లను ఆపుతుంది.

Let us now see some of the protocols used by different layers to accomplish user requests.

వినియోగదారు అభ్యర్థనలను నెరవేర్చడానికి వివిధ లేయర్ల ద్వారా ఉపయోగించే కొన్ని ప్రోటోకాల్స్ను ఇప్పుడు చూద్దాము.

TCP/IP

TCP/IP stands for **Transmission Control Protocol/Internet Protocol**. TCP/IP is a set of layered protocols used for communication over the Internet. The communication model of this suite is client-server model. A computer that sends a request is the client and a computer to which the request is sent is the server.

TCP / IP అనేది ట్రాన్స్మిషన్ కంట్రోల్ ప్రోటోకాల్ / ఇంటర్నెట్ ప్రోటోకాల్. TCP / IP అనేది ఇంటర్నెట్లో కమ్యూనికేషన్ కోసం ఉపయోగించే లేయర్డ్ ప్రోటోకాల్స్. ఈ సూట్ యొక్క కమ్యూనికేషన్ మోడల్ క్లయింట్-సర్వర్ మోడల్. అభ్యర్థనను పంపుతున్న ఒక కంప్యూటర్ క్లయింట్ మరియు అభ్యర్థన పంపిన ఒక కంప్యూటర్ సర్వర్.

TCP/IP has four layers –

TCP / IP కు నాలుగు పొరలు ఉన్నాయి -

- **Application layer** – Application layer protocols like HTTP and FTP are used.
  అప్లికేషన్ లేయర్ - HTTP మరియు FTP వంటి అప్లికేషన్ లేయర్ ప్రోటోకాల్లు ఉపయోగించబడతాయి.
- **Transport layer** – Data is transmitted in form of datagrams using the Transmission Control Protocol (TCP). TCP is responsible for breaking up data at the client side and then reassembling it on the server side.
  రవాణా పొర - డేటా ట్రాన్స్మిషన్ కంట్రోల్ ప్రోటోకాల్ (TCP) ఉపయోగించి datagrams రూపంలో బదిలీ చేయబడుతుంది. క్లైంట్ వైపు డేటాను విడగొట్టటానికి TCP బాధ్యత వహిస్తుంది మరియు అది సర్వర్ వైపున పునఃప్రారంభించబడుతుంది .
- **Network layer** – Network layer connection is established using Internet Protocol (IP) at the network layer. Every machine connected to the Internet is assigned an address called IP address by the protocol to easily identify source and destination machines.
- నెట్వర్క్ పొర - నెట్వర్క్ పొరలో ఇంటర్నెట్ ప్రోటోకాల్ (IP) ఉపయోగించి నెట్వర్క్ లేయర్ కనెక్షన్ ఏర్పడుతుంది. ఇంటర్నెట్కు అనుసంధానించబడిన ప్రతి యంత్రం ప్రోటోకాల్ ద్వారా IP చిరునామా అని పిలవబడే చిరునామాను సులభంగా మూలం మరియు గమ్య యంత్రాలు గుర్తించడానికి కేటాయించబడుతుంది.
- **Data link layer** – Actual data transmission in bits occurs at the data link layer using the destination address provided by network layer.
  డేటా లింక్ పొర - బిట్స్ లో వాస్తవ డేటా బదిలీ నెట్వర్క్ లేయర్ అందించిన గమ్యం చిరునామాను ఉపయోగించి డేటా లింక్ లేయర్ వద్ద జరుగుతుంది .

TCP/IP is widely used in many communication networks other than the Internet.

TCP / IP విస్తృతంగా ఇంటర్నెట్ కాకుండా అనేక కమ్యూనికేషన్ నెట్వర్క్లలో ఉపయోగిస్తారు .

FTP

FTP stands for file transfer protocol As we have seen, the need for network came up primarily to facilitate sharing of files between researchers. And to this day, file transfer remains one of the most

used facilities. The protocol that handles these requests is **File Transfer Protocol** or **FTP**.

ఫైల్ బదిలీ ప్రోటోకాల్ కోసం FTP నిలుస్తుంది మేము చూసినట్లుగా, నెట్వర్క్ యొక్క అవసరం పరిశోధకుల మధ్య ఫైళ్ళను భాగస్వామ్యం చేయడాన్ని సులభతరం చేయడానికి ప్రధానంగా వచ్చింది. మరియు ఈ రోజు వరకు, ఫైల్ బదిలీ చాలా ఉపయోగించిన సౌకర్యాలు ఒకటి. ఈ అభ్యర్థనలను నిర్వహించే ప్రోటోకాల్ ఫైల్ ట్రాన్స్ఫర్ ప్రోటోకాల్ లేదా FTP .

Using FTP to transfer files is helpful in these ways –
ఫైళ్ళను బదిలీ చేయడానికి FTP ను ఉపయోగించి ఈ మార్గాల్లో సహాయపడుతుంది

- Easily transfers files between two different networks

రెండు వేర్వేరు నెట్వర్క్ల మధ్య సులభంగా ఫైళ్లను బదిలీ చేస్తుంది

- Can resume file transfer sessions even if connection is dropped, if protocol is configure appropriately

కనెక్షన్ పడిపోయినప్పటికీ ఫైల్ బదిలీ సెషన్లను పునఃప్రారంభించవచ్చు, ప్రోటోకాల్ సరిగ్గా కన్ఫిగర్ అయితే

Enables collaboration between geographically separated teams

భౌగోళికంగా విభజించబడిన జట్ల మధ్య సహకారాన్ని ప్రారంభిస్తుంది

PPP

Point to Point Protocol or PPP is a data link layer protocol that enables transmission of TCP/IP traffic over serial connection, like telephone line.

పాయింట్ టు పాయింట్ పాయింట్ ప్రోటోకాల్ లేదా PPP అనేది డేటా లింక్ లేయర్ ప్రోటోకాల్, ఇది టెలిఫోన్ లైన్ వంటి సీరియల్ కనెక్షన్ ద్వారా TCP / IP ట్రాఫిక్ యొక్క బదిలీని అనుమతిస్తుంది.

To do this, PPP defines these three things –

- A framing method to clearly define end of one frame and start of another, incorporating errors detection as well.
- ఒక ఫ్రేమింగ్ పద్ధతి ఒక ఫ్రేమ్ యొక్క ముగింపును మరియు మరొదానిని స్పష్టంగా నిర్వచించడానికి, లోపాలను గుర్తించే లోపాలను కలిగి ఉంటుంది.
- Link control protocol (LCP) for bringing communication lines up, authenticating and bringing them down when no longer needed.
  సమాచార నియంత్రణ రేఖలను తీసుకురావడానికి లింక్ నియంత్రణ ప్రోటోకాల్ (LCP), ధృవీకరించడం మరియు ఇకపై అవసరమైనప్పుడు వాటిని తీసుకురావడం .

Network control protocol (NCP) for each network layer protocol supported by other networks. Using PPP, home users can avail Internet connection over telephone lines.

నెట్వర్క్ నెట్వర్క్ ప్రోటోకాల్ (NCP) ప్రతి నెట్వర్క్ పొర ప్రోటోకాల్కు ఇతర నెట్వర్కు మద్దతు ఇస్తుంది. PPP ఉపయోగించి, హోమ్ వినియోగదారులు టెలిఫోన్ లైన్ల ద్వారా ఇంటర్నెట్ కనెక్షన్ పొందవచ్చు .

As you can see, the TCP/IP model, is a bit more abstract and fluid. This made it easier to implement and allowed it to become the dominant way that networking layers are categorized.

మీరు చూడగలిగినట్లుగా, TCP / IP నమూనా, ఒక బిట్ మరింత వియుక్త మరియు ద్రవం. ఇది అమలు చేయడం సులభతరం చేసింది నెట్ వర్కింగ్ పొరలు వర్గీకరణ చేయగల ఆధిపత్య మార్గం అయ్యేందుకు ఇది అనుమతించింది .

Interfaces

Interfaces are networking communication points for your computer. Each interface is associated with a physical or virtual networking device.

ఇంటర్ఫేస్లు మీ కంప్యూటర్ కోసం నెట్వర్కింగ్ కమ్యూనికేషన్ పాయింట్లు. ప్రతి ఇంటర్ఫేస్ భౌతిక లేదా వర్చ్యువల్ నెట్వర్కింగ్ పరికరముతో ముడిపడివుంది.

Typically, your server will have one configurable network interface for each Ethernet or wireless internet card you have.
సాధారణంగా, మీ సర్వర్ ప్రతి Ethernet లేదా వైర్లెస్ ఇంటర్నెట్ కార్డు కోసం ఒక కాన్ఫిగర్ నెట్వర్క్ ఇంటర్ఫేస్ను కలిగి ఉంటుంది.

In addition, it will define a virtual network interface called the "loopback" or localhost interface. This is used as an interface to connect applications and processes on a single computer to other applications and processes. You can see this referenced as the "lo" interface in many tools.
అదనంగా, అది "లూప్ బాక్" లేదా స్థానిక హోస్ట్ ఇంటర్ఫేస్ అని పిలువబడే ఒక వాస్తవ నెట్వర్క్ ఇంటర్ఫేస్ను నిర్వచిస్తుంది. ఇది అనువర్తనాలు మరియు ప్రక్రియలను ఒకే కంప్యూటర్లో ఇతర అనువర్తనాలు మరియు ప్రాసెస్లకు కనెక్ట్ చేయడానికి ఇంటర్ఫేస్గా ఉపయోగించబడుతుంది. మీరు అనేక టూల్స్ లో "తక్కువ" ఇంటర్ఫేస్ గా సూచించిన ఈ చూడగలరు.

Many times, administrators configure one interface to service traffic to the internet and another interface for a LAN or private network.
అనేక సార్లు, నిర్వాహకులు ఇంటర్నెట్కు సేవ ట్రాఫిక్ మరియు LAN లేదా ప్రైవేట్ నెట్వర్క్ కోసం మరొక ఇంటర్ఫేస్కు ఒక ఇంటర్ఫేస్ను కాన్ఫిగర్ చేస్తుంది.

In DigitalOcean, in datacenters with private networking enabled, your VPS will have two networking interfaces (in addition to the local interface). The "eth0" interface will be configured to handle traffic from the internet, while the "eth1" interface will operate to communicate with the private network.

DigitalOcean లో, ప్రైవేట్ నెట్వర్కింగ్ తో డేటాసెట్స్ లో, మీ VPS రెండు నెట్వర్కింగ్ ఇంటర్ఫేస్లు కలిగి ఉంటుంది (స్థానిక ఇంటర్ఫేస్కు అదనంగా). "Eth0" ఇంటర్ఫేస్ ఇంటర్నెట్ నుండి ట్రాఫిక్ను నిర్వహించడానికి కాన్ఫిగర్ చేయబడుతుంది, అయితే "eth1" ఇంటర్ఫేస్ ప్రైవేట్ నెట్వర్క్ కమ్యూనికేట్ చేయడానికి పనిచేస్తాయి.

Protocols

Networking works by piggybacking a number of different protocols on top of each other. In this way, one piece of data can be transmitted using multiple protocols encapsulated within one another.
నెట్వర్కింగ్ పరస్పరం పైన వేర్వేరు ప్రోటోకాల్లను piggybacking ద్వారా పనిచేస్తుంది. ఈ విధంగా, ఒకదానిలో ఒకదానికి ఒకటి కప్పబడి ఉన్న బహుళ ప్రోటోకాల్లను ఉపయోగించి డేటా యొక్క ఒక భాగం బదిలీ చేయబడుతుంది.

We will talk about some of the more common protocols that you may come across and attempt to explain the difference, as well as give context as to what part of the process they are involved with.
మీరు మరింత సాధారణ ప్రోటోకాల్ల గురించి మాట్లాడతారు, మీరు వ్యత్యాసం వివరించడానికి మరియు వ్యత్యాసం వివరించడానికి

ప్రయత్నిస్తారు, అంతేకాకుండా వారు ఏ పద్ధతితో సంబంధం కలిగి ఉంటారనే దాని గురించి సందర్భాన్ని ఇస్తారు.

We will start with protocols implemented on the lower networking layers and work our way up to protocols with higher abstraction.
మేము తక్కువ నెట్వర్కింగ్ పొరలలో అమలు చేయబడిన ప్రోటోకాల్స్తో మొదలు పెడతాము మరియు అధిక సంగ్రహణతో ప్రోటోకాల్లకు మా మార్గం వరకు పని చేస్తాము.

Media Access Control

Media access control is a communications protocol that is used to distinguish specific devices. Each device is supposed to get a unique MAC address during the manufacturing process that differentiates it from every other device on the internet.
మీడియా యాక్సెస్ కంట్రోల్ నిర్దిష్ట పరికరాలను గుర్తించడానికి ఉపయోగించే సమాచార ప్రోటోకాల్. ప్రతి పరికరం ఇంటర్నెట్లో ప్రతి ఇతర పరికరం నుండి వేరు చేసే ఉత్పాదక ప్రక్రియ సమయంలో ఒక ప్రత్యేక MAC చిరునామాను పొందవలసి ఉంటుంది.

Addressing hardware by the MAC address allows you to reference a device by a unique value even when the software on top may change the name for that specific device during operation.

MAC చిరునామా ద్వారా హార్డ్వేర్ను సంప్రదించడం ద్వారా పరికరాన్ని ప్రత్యేక ఉపకరణం కోసం నిర్దిష్ట పరికరం కోసం పేరును మార్చినప్పుడు కూడా ఒక ప్రత్యేక విలువతో పరికరాన్ని సూచించడానికి మిమ్మల్ని అనుమతిస్తుంది.

Media access control is one of the only protocols from the link layer that you are likely to interact with on a regular basis.
మీడియా ప్రాప్యత నియంత్రణ మీరు రోజు సంప్రదించడానికి అవకాశం ఉన్న లింక్ లేయర్ నుండి మాత్రమే ప్రోటోకాల్స్లో ఒకటి.

IP

The IP protocol is one of the fundamental protocols that allow the internet to work. IP addresses are unique on each network and they allow machines to address each other across a network. It is implemented on the internet layer in the IP/TCP model.

ఇంటర్నెట్ ప్రోటోకాల్ను అనుమతించే ప్రాథమిక ప్రోటోకాల్లో IP ప్రోటోకాల్ ఒకటి. IP చిరునామాలను ప్రతి నెట్వర్క్లో ప్రత్యేకంగా ఉంటాయి మరియు వారు నెట్వర్క్లను ఒక నెట్వర్క్లో ఒకదానిని ప్రసంగించడానికి అనుమతిస్తాయి. ఇది IP / TCP నమూనాలో ఇంటర్నెట్ పొరలో అమలు చేయబడుతుంది.

Networks can be linked together, but traffic must be routed when crossing network boundaries. This protocol assumes an unreliable network and multiple paths to the same destination that it can dynamically change between.
నెట్వర్క్లు కలిసి లింక్ చేయబడతాయి, అయితే నెట్వర్క్ సరిహద్దులను దాటినప్పుడు ట్రాఫిక్ను తప్పించాలి. ఈ ప్రోటోకాల్ ఒక నమ్మకమైన నెట్వర్క్ మరియు బహుళ మార్గాలను అదే గమ్యస్థానాన్ని ఊహిస్తుంది, ఇది డైనమిక్ మధ్య మారుతుంది.

There are a number of different implementations of the protocol. The most common implementation today is IPv4, although IPv6 is growing in popularity as an alternative due to the scarcity of IPv4 addresses available and improvements in the protocols capabilities.

ప్రోటోకాల్ యొక్క అనేక అమలులు ఉన్నాయి. ఈ IPv4 సర్వసాధారణమైన అమలు, అయినప్పటికీ IPv4 ప్రోటోకాల్ సామర్థ్యాలలో IPv4 చిరునామాల కొరత మరియు మెరుగుదలలు కారణంగా ప్రత్యామ్నాయంగా ప్రజాదరణను పెంచుతున్నాయి.

ICMP

ICMP stands for internet control message protocol. It is used to send messages between devices to indicate the availability or error conditions. These packets are used in a variety of network diagnostic tools, such as ping and traceroute.

ICMP అనేది ఇంటర్నెట్ నియంత్రణ సందేశ ప్రోటోకాల్. లభ్యత లేదా లోపం పరిస్థితులను సూచించడానికి పరికరాల మధ్య సందేశాలను పంపడానికి ఇది ఉపయోగించబడుతుంది. ఈ పాకెట్లు పింగ్ మరియు ట్రేస్‌ఆర్‌అవుట్ వంటి అనేక రకాల నెట్‌వర్క్ విశ్లేషణ ఉపకరణాల్లో ఉపయోగించబడతాయి.

Usually ICMP packets are transmitted when a packet of a different kind meets some kind of a problem. Basically, they are used as a feedback mechanism for network communications.

సాధారణంగా ఒక ప్యాకెట్ వేరొక రకమైన సమస్యను కొంత రకమైన సమస్యతో కలిసినప్పుడు ICMP ప్యాకెట్లను బదిలీ చేస్తారు. ప్రాథమికంగా, వారు నెట్‌వర్క్ కమ్యూనికేషన్ల కోసం అభిప్రాయ యంత్రాంగాన్ని ఉపయోగిస్తారు.

TCP

TCP stands for transmission control protocol. It is implemented in the transport layer of the IP/TCP model and is used to establish reliable connections.

ప్రసార నియంత్రణ ప్రోటోకాల్ కోసం TCP నిలుస్తుంది. ఇది IP / TCP మోడల్ యొక్క రవాణా పొరలో అమలు చేయబడుతుంది మరియు విశ్వసనీయ కనెక్షన్లను స్థాపించడానికి ఉపయోగించబడుతుంది.

TCP is one of the protocols that encapsulates data into packets. It then transfers these to the remote end of the connection using the methods available on the lower layers. On the other end, it can check for errors, request certain pieces to be resent, and reassemble the information into one logical piece to send to the application layer.

TCP అనేది ప్రోటోకాల్లలో ఒకటి, ఇది ప్యాకెట్లలోకి డేటాను కలుపుతుంది. ఇది తరువాత కింది పొరలలో అందుబాటులో ఉన్న పద్ధతులను ఉపయోగించి కనెక్షన్ యొక్క రిమోట్ ముగింపుకు బదిలీ చేస్తుంది. ఇంకొక చివరలో, ఇది లోపాలను తనిఖీ చేయవచ్చు, కొన్ని ముక్కలు కోరడానికి అభ్యర్థిస్తుంది, మరియు అప్లికేషన్ లాయర్కు పంపడానికి ఒక తార్కిక భాగానికి సమాచారాన్ని పునఃభాగస్వామ్యం చేస్తుంది.

The protocol builds up a connection prior to data transfer using a system called a three-way handshake. This is a way for the two ends of the communication to acknowledge the request and agree upon a method of ensuring data reliability.

ప్రోటోకాల్ మూడు-మార్గం హ్యాండ్షేక్ అనే వ్యవస్థను ఉపయోగించి డేటా బదిలీకి ముందు కనెక్షన్ను రూపొందించింది. ఇది అభ్యర్థనను గుర్తించడానికి మరియు డేటా విశ్వసనీయతను భరోసా చేసే పద్ధతిని అంగీకరించడానికి కమ్యూనికేషన్ యొక్క రెండు చివరల కోసం ఒక మార్గం.

After the data has been sent, the connection is torn down using a similar four-way handshake.

TCP is the protocol of choice for many of the most popular uses for the internet, including WWW, FTP, SSH, and email. It is safe to say that the internet we know today would not be here without TCP.

డేటా పంపబడిన తరువాత, కనెక్షన్ ఇదే నాలుగు-మార్గం హ్యాండ్షేక్తో ఉపయోగించి నలిగిపోతుంది. TCP అనేది WWW, FTP, SSH మరియు ఇమెయిల్తో సహా, ఇంటర్నెట్కు అత్యంత ప్రజాదరణ పొందిన అనేక ప్రయోజనాల ఎంపికకు ప్రోటోకాల్. నేడు మాకు తెలిసిన ఇంటర్నెట్ TCP లేకుండా ఇక్కడ ఉండదని చెప్పడం సురక్షితం.

UDP

UDP stands for user datagram protocol. It is a popular companion protocol to TCP and is also implemented in the transport layer.
UDP యూజర్ డేటాగ్రామ్ ప్రోటోకాల్ కోసం ఉంటుంది. ఇది TCP కి ఒక ప్రసిద్ధ కంపానియన్ ప్రోటోకాల్ మరియు రవాణా పొరలో అమలు చేయబడుతుంది.

The fundamental difference between UDP and TCP is that UDP offers unreliable data transfer. It does not verify that data has been received on the other end of the connection. This might sound like a bad thing, and for many purposes, it is. However, it is also extremely important for some functions.

UDP మరియు TCP మధ్య మౌలిక వ్యత్యాసం UDP నమ్మలేని డేటా బదిలీని అందిస్తుంది. ఇది కనెక్షన్ యొక్క మరొక చివరిలో డేటా స్వీకరించినట్లు ధృవీకరించలేదు. ఇది ఒక చెడ్డ అంశం లాగా అనిపిస్తుంది, మరియు అనేక ప్రయోజనాల కోసం ఇది. అయితే, కొన్ని

Because it is not required to wait for confirmation that the data was received and forced to resend data, UDP is much faster than TCP. It does not establish a connection with the remote host, it simply fires off the data to that host and doesn't care if it is accepted or not.

ఎందుకంటే డేటా అందుకున్నట్లు మరియు డేటాను తిరిగి పంపించాలని నిర్ధారణ కోసం వేచి ఉండవలసిన అవసరం లేదు, TCP కంటే UDP చాలా వేగంగా ఉంటుంది. ఇది రిమోట్ హోస్ట్తో ఒక కనెక్షన్ను ఏర్పాటు చేయదు, అది ఆ హోస్ట్కు డేటాను తొలగిస్తుంది మరియు అంగీకరించబడకపోతే లేదా పట్టించుకోదు.

Because it is a simple transaction, it is useful for simple communications like querying for network resources. It also doesn't maintain a state, which makes it great for transmitting data from one machine to many real-time clients. This makes it ideal for VOIP, games, and other applications that cannot afford delays.

ఇది సాధారణ లావాదేవి కాబట్టి, నెట్వర్క్ వనరులను ప్రశ్నించడం వంటి సాధారణ సమాచారాలకు ఇది ఉపయోగకరంగా ఉంటుంది. ఇది ఒక రాష్ట్రాన్ని నిర్వహించదు, ఇది ఒక యంత్రం నుండి డేటాను అనేక నిజ-సమయ క్లయింట్లకు ప్రసారం చేస్తుంది. ఇది VOIP, ఆటలు, మరియు ఆలస్యం పొందని ఇతర అనువర్తనాలకు ఇది ఉత్తమమైనది.

HTTP

HTTP stands for hypertext transfer protocol. It is a protocol defined in the application layer that forms the basis for communication on the web.

HTTP హైపర్టెక్స్ట్ ట్రాన్స్ఫర్ ప్రోటోకాల్ కోసం ఉంటుంది. ఇది వెబ్లో సమాచార ప్రసారంకు ఆధారమైన దరఖాస్తు పొరలో నిర్వచించిన ప్రోటోకాల్.

HTTP defines a number of functions that tell the remote system what you are requesting. For instance, GET, POST, and DELETE all interact with the requested data in a different way.
మీరు అభ్యర్థిస్తున్న రిమోట్ సిస్టమ్కు చెప్పే అనేక విధులు HTTP నిర్వచిస్తుంది. ఉదాహరణకు, GET, POST, మరియు తొలగించినవి అన్ని వేరొక విధంగా అభ్యర్థించిన డేటా సంకర్షణ.

FTP

FTP stands for file transfer protocol. It is also in the application layer and provides a way of transferring complete files from one host to another.
ఫైల్ బదిలీ ప్రోటోకాల్ కోసం FTP నిలుస్తుంది. ఇది అప్లికేషన్ పొరలో కూడా ఉంది మరియు ఒక హోస్ట్ నుండి మరొకదానికి పూర్తి ఫైళ్లను బదిలీ చేయడానికి ఒక మార్గాన్ని అందిస్తుంది.

It is inherently insecure, so it is not recommended for any externally facing network unless it is implemented as a public, download-only resource.
ఇది అంతర్గతంగా అసురక్షితమైనది, కనుక ఇది బహిరంగ, దిగుమతి-మాత్రమే వనరు వలె అమలు చేయకపోతే ఏదైనా బాహ్యంగా ఎదుర్కొంటున్న నెట్వర్క్ కోసం సిఫార్సు చేయబడదు.

DNS

DNS stands for domain name system. It is an application layer protocol used to provide a human-friendly naming mechanism for internet resources. It is what ties a domain name to an IP address and allows you to access sites by name in your browser.

DNS డొమైన్ పేరు వ్యవస్థ కోసం నిలుస్తుంది. ఇది ఇంటర్నెట్ వనరులకు మానవ-స్నేహపూర్వక నామకరణ విధానాన్ని అందించడానికి ఉపయోగించే ఒక అప్లికేషన్ పొర ప్రోటోకాల్. ఇది ఒక IP చిరునామాకు డొమైన్ పేరుని ఏమిటి మరియు మీరు మీ బ్రౌజర్లో పేరు ద్వారా సైట్లను ప్రాప్తి చేయడానికి అనుమతిస్తుంది .

SSH

SSH stands for secure shell. It is an encrypted protocol implemented in the application layer that can be used to communicate with a remote server in a secure way. Many additional technologies are built around this protocol because of its end-to-end encryption and ubiquity.
SSH సురక్షిత షెల్ కోసం ఉంటుంది. సురక్షితమైన మార్గంలో రిమోట్ సర్వర్తో కమ్యూనికేట్ చేయడానికి ఉపయోగించే అనువర్తన పొరలో ఇది అమలు చేయబడిన ఎన్క్రిప్టెడ్ ప్రోటోకాల్. అనేక అదనపు టెక్నాలజీలు ఈ ప్రోటోకాల్ చుట్టూ నిర్మించబడ్డాయి, ఎందుకంటే ఇది ఎండ్-టు-ఎండ్ ఎన్క్రిప్షన్ మరియు ఎక్కువిటీ.

There are many other protocols that we haven't covered that are equally important. However, this should give you a good overview of some of the fundamental technologies that make the internet and networking possible
మేము సమానంగా ముఖ్యమైనవి అని కవర్ కాదు అనేక ఇతర ప్రోటోకాల్లు ఉన్నాయి. అయితే, ఇది మీకు ఇంటర్నెట్ మరియు

నెట్వర్కింగ్ సాధించే ప్రాథమిక సాంకేతిక పరిజ్ఞానాల యొక్క మంచి సమీక్షను అందిస్తుంది.

Network Protocols Definition

Is a set of rules and formats for sending and receiving data successfully over the network.
నెట్వర్క్లో విజయవంతంగా డేటా పంపడం మరియు అందుకోవడం కోసం నియమాలు మరియు ఆకృతుల సమితి.

Description

- TCP/IP is standard protocol used to communicate over the internet.
- TCP / IP ఇంటర్నెట్లో కమ్యూనికేట్ చేయడానికి ఉపయోగించే ప్రామాణిక ప్రోటోకాల్.
- Every protocol has advantages and some disadvantages.
- ప్రతి ప్రోటోకాల్ ప్రయోజనాలు మరియు కొన్ని అప్రయోజనాలు ఉన్నాయి.
- Protocols differs in their functioning at various levels.
- వివిధ స్థాయిలలో వారి పనితీరులో ప్రోటోకాల్లు భిన్నంగా ఉంటాయి.
- Some protocols are simpler, reliable and faster than others.
- కొన్ని ప్రోటోకాల్లు సరళమైనవి, నమ్మదగినవి మరియు ఇతరులకన్నా వేగంగా ఉంటాయి.
- Protocol are either implemented on software or hardware.
- ప్రోటోకాల్ సాఫ్ట్వేర్ లేదా హార్డ్వేర్లో అమలు చేయబడుతుంది.

Layer levels protocols
లేయర్ స్థాయిలు ప్రోటోకాల్లు

Application layer protocols:

English – detected

- DHCP (Dynamic Host Configuration Protocol)
- DHCP (డైనమిక్ హోస్ట్ కాన్ఫిగరేషన్ ప్రోటోకాల్)
- DNS (Domain Name System)
- FTP (File Transfer Protocol)
- HTTP (Hypertext Transfer Protocol)
- MIME (Multipurpose Internet Mail Extensions)
- POP and POP3 (Post Office Protocol(version 3))
- RTSP (Real Time Streaming Protocol)
- SHTTP (Secure Hypertext Transfer Protocol)
- SMTP (Simple Mail Transfer Protocol)
- SSH (Secure Shell Protocol)
- Telnet (Telnet Remote Protocol)
- TFTP (Trivial File transfer Protocol)

- TLS (Transport Layer Security Protocol)
- URL (Universe Resource Locator)

Transport layer protocols:
రవాణా పొర ప్రోటోకాల్లు :

- TCP (Transmission Control Protocol)
- UDP (User Datagram Protocol)
- Datagram Congestion Control Protocol (DCCP)
- Stream Control Transmission Protocol (SCTP)

Internet layer protocols:
ఇంటర్నెట్ లేయర్ ప్రోటోకాల్లు :

- IP (Internet Protocol(IPv4)
- IPv6 (Internet Protocol)
- ICMP (Internet Control Message Protocol)
- IGMP (Internet Group Management Protocol
- IPsec (IP Security)

Link layer protocols:
పొర ప్రోటోకాల్లను లింక్ చేయండి :

- ARP (Address Resolution Protocol)
- RARP (Reverse Address Resolution Protocol)
- SLIP (Serial Line IP)
- Ethernet

Mobile Communication Protocols

మొబైల్ కమ్యూనికేషన్ ప్రోటోకాల్స్

Any device that does not need to remain at one place to carry out its functions is a mobile device. So laptops, smartphones and personal digital assistants are some examples of mobile devices. Due to their portable nature, mobile devices connect to networks wirelessly. Mobile devices typically use radio waves to communicate with other devices and networks. Here we will discuss the protocols used to carry out mobile communication.

దాని కార్యకలాపాలు నిర్వహించడానికి ఒక ప్రదేశంలో ఉండవలసిన అవసరం లేని పరికరం మొబైల్ పరికరం. కాబట్టి లాప్టాప్లు, స్మార్ట్ఫోన్లు మరియు వ్యక్తిగత డిజిటల్ సహాయకులు మొబైల్ పరికరాలకు కొన్ని ఉదాహరణలు. వారి పోర్టబుల్ స్వభావం కారణంగా, మొబైల్ పరికరాలు తీగరహిత నెట్వర్క్కు కనెక్ట్ చేస్తాయి. మొబైల్ పరికరాలు సాధారణంగా ఇతర పరికరాలు మరియు నెట్వర్క్లతో కమ్యూనికేట్ చేయడానికి రేడియో తరంగాలను ఉపయోగిస్తాయి. ఇక్కడ మొబైల్ కమ్యూనికేషన్ను నిర్వహించడానికి ఉపయోగించే ప్రోటోకాల్లను మేము చర్చిస్తాము.

Mobile communication protocols use multiplexing to send information. Multiplexing is a method to combine multiple digital or analog signals into one signal over the data channel. This ensures optimum utilization of expensive resource and time. At the destination these signals are de-multiplexed to recover individual signals.

మొబైల్ కమ్యూనికేషన్ ప్రోటోకాల్స్ సమాచారాన్ని పంపేందుకు మల్టీప్లెక్స్ను ఉపయోగిస్తాయి. మల్టీప్లెక్స్ అనేది బహుళ డిజిటల్ లేదా అనలాగ్ సంకేతాలను డేటా ఛానల్లో ఒక సిగ్నల్గా మిళితం చేయడానికి ఒక పద్ధతి. ఇది ఖరీదైన వనరు మరియు సమయాన్ని సరైన వినియోగంతో నిర్ధారిస్తుంది. గమ్యం వద్ద ఈ సంకేతాలు వ్యక్తిగత సంకేతాలను తిరిగి పొందడానికి మల్టిప్లెక్స్డ్.

These are the types of multiplexing options available to communication channels –

ఇవి కమ్యూనికేషన్ చానెళ్లకు అందుబాటులో ఉన్న మల్టీప్లెక్స్ ఎంపికల రకాలు –

- **FDM (Frequency Division Multiplexing)** − Here each user is assigned a different frequency from the complete spectrum. All the frequencies can then simultaneously travel on the data channel.

  FDM (ఫ్రీక్వెన్సీ డివిజన్ మల్టిప్లెక్స్) - ఇక్కడ ప్రతి వినియోగదారుడు పూర్తి స్పెక్ట్రం నుండి వేర్వేరు ఫ్రీక్వెన్సీని కేటాయించారు. అన్ని పౌనఃపున్యాల తర్వాత ఏకకాలంలో డేటా ఛానల్లో ప్రయాణించవచ్చు.

- **TDM (Time Division Multiplexing)** − A single radio frequency is divided into multiple slots and each slot is assigned to a different user. So multiple users can be supported simultaneously.

  TDM (టైమ్ డివిజన్ మల్టీప్లెక్స్) - ఒక్క రేడియో పౌనఃపున్యం బహుళ స్లాట్లుగా విభజించబడింది మరియు ప్రతి స్లాట్ వేరే వినియోగదారుకు కేటాయించబడుతుంది. కాబట్టి బహుళ వినియోగదారులు ఏకకాలంలో మద్దతు ఇవ్వగలరు.

- **CDMA (Code Division Multiplexing)** − Here several users share the same frequency spectrum simultaneously. They are differentiated by assigning unique codes to them. The receiver has the unique key to identify the individual calls.

  CDMA (కోడ్ డివిజన్ మల్టిప్లెక్స్) - ఇక్కడ పలువురు వినియోగదారులు ఒకే పౌనఃపున్య స్పెక్ట్రమ్ను ఏకకాలంలో పంచుకుంటారు. వారికి ప్రత్యేకమైన సంకేతాలను కేటాయించడం ద్వారా అవి విభిన్నంగా ఉంటాయి. వ్యక్తిగత కాల్స్ గుర్తించడానికి రిసీవర్ ఏకైక కీ ఉంది.

GSM

GSM stands for Global System for Mobile communications. GSM is one of the most widely used digital wireless telephony system. It was developed in Europe in 1980s and is now international standard in Europe, Australia, Asia and Africa. Any GSM handset with a SIM (Subscriber Identity Module) card can be used in any country that uses this standard. Every SIM card has a unique identification number. It has memory to store applications and data like phone numbers, processor to carry out its functions and software to send and receive messages

జిఎస్ఎం గ్లోబల్ సిస్టం ఫర్ మొబైల్ కమ్యూనికేషన్స్. GSM అత్యంత విస్తృతంగా ఉపయోగించే డిజిటల్ వైర్లెస్ టెలిఫోనీ వ్యవస్థలో ఒకటి. ఇది 1980 లలో ఐరోపాలో అభివృద్ధి చేయబడింది మరియు ఇప్పుడు ఐరోపా, ఆస్ట్రేలియా, ఆసియా మరియు ఆఫ్రికాలలో అంతర్జాతీయ ప్రమాణంగా ఉంది. ఒక SIM (సబ్స్క్రయిబర్ ఐడెంటిటీ మాడ్యూల్) కార్డుతో ఉన్న ఏదైనా GSM హ్యాండ్సెట్ ఈ ప్రమాణాన్ని ఉపయోగించే ఏ దేశంలోను ఉపయోగించవచ్చు. ప్రతి SIM కార్డుకు ప్రత్యేక గుర్తింపు సంఖ్య ఉంది. ఫోన్ నంబర్లు, దాని విధులు మరియు సాఫ్ట్వేర్ సందేశాలను పంపడానికి మరియు స్వీకరించడానికి ప్రాసెసర్ వంటి అనువర్తనాలు మరియు డేటాను నిల్వ చేయడానికి మెమరీని కలిగి ఉంది

GSM technology uses TDMA (Time Division Multiple Access) to support up to eight calls simultaneously. It also uses encryption to make the data more secure.

GSM సాంకేతికత TDMA (టైమ్ డివిజన్ మల్టిపుల్ యాక్సెస్) ను ఏకకాలంలో ఎనిమిది కాల్స్ వరకు మద్దతు ఇస్తుంది. డేటాను మరింత సురక్షితంగా చేయడానికి ఇది గుప్తీకరణను కూడా ఉపయోగిస్తుంది.

The frequencies used by the international standard is 900 MHz to 1800 MHz However, GSM phones used in the US use 1900 MHz frequency and hence are not compatible with the international system.
అంతర్జాతీయ ప్రమాణం ఉపయోగించిన పౌనఃపున్యాల 900 MHz కు 1800 MHz అయితే, US లో 1900 MHz ఫ్రీక్వెన్సీలో ఉపయోగించే GSM ఫోన్లు మరియు అందువల్ల అంతర్జాతీయ వ్యవస్థకు అనుకూలంగా లేవు.

CDMA

CDMA stands for Code Division Multiple Access. It was first used by the British military during World War II. After the war its use spread to civilian areas due to high service quality. As each user gets the entire spectrum all the time, voice quality is very high. Also, it is automatically encrypted and hence provides high security against signal interception and eavesdropping.

కోడ్ డివిజన్ మల్టిపుల్ యాక్సెస్ కొరకు CDMA ఉంటుంది. ఇది మొదటి ప్రపంచ యుద్ధం సమయంలో బ్రిటిష్ సైన్యం ఉపయోగించింది II. యుద్ధానంతరం దాని ఉపయోగం అధిక సేవ నాణ్యత కారణంగా పౌర ప్రాంతాలకు విస్తరించింది. ప్రతి వినియోగదారు మొత్తం పొందుతాడు స్పెక్ట్రం అన్ని సమయం, వాయిస్ నాణ్యత చాలా ఎక్కువగా ఉంటుంది. అలాగే, ఇది ఆటోమేటిక్గా గుప్తీకరించబడుతుంది మరియు అందువల్ల సిగ్నల్ అంతరాయం మరియు వినడంతో అధిక భద్రత కల్పిస్తుంది.

WLL

WLL stands for Wireless in Local Loop. It is a wireless local telephone service that can be provided in homes or offices. The subscribers connect to their local exchange instead of the central exchange wirelessly. Using wireless link eliminates last mile or first mile construction of network connection, thereby reducing cost and set up time. As data is transferred over very short range, it is more secure than wired networks.

WLL స్థానిక లూప్లో వైర్లెస్ కోసం నిలుస్తుంది. ఇది గృహాలు లేదా కార్యాలయాల్లో అందించబడే వైర్లెస్ స్థానిక టెలిఫోన్ సేవ. సబ్స్క్రైబర్లు సెంట్రల్ ఎక్స్ఛేంజ్ తీగరహితంగా కాకుండా వారి స్థానిక మార్పిడికి కలుపుతారు. వైర్లెస్ లింక్ని ఉపయోగించి చివరి మైలు లేదా నెట్వర్క్

కనెక్షన్ యొక్క మొట్టమొదటి మైలు నిర్మాణాన్ని తొలగిస్తుంది, తద్వారా ధర తగ్గించడం మరియు సమయాన్ని సెటప్ చేయడం. డేటా చాలా చిన్న పరిధిలో బదిలీ అయినందున, ఇది వైర్డు నెట్వర్క్ల కంటే మరింత సురక్షితం.

WLL system consists of user handsets and a base station. The base station is connected to the central exchange as well as an antenna. The antenna transmits to and receives calls from users through terrestrial microwave links. Each base station can support multiple handsets depending on its capacity.

WLL వ్యవస్థ వినియోగదారు హ్యాండ్సెట్లను మరియు బేస్ స్టేషన్ను కలిగి ఉంటుంది. బేస్ స్టేషన్ సెంట్రల్ ఎక్స్ఛేంజ్తో పాటు యాంటెన్నాకు అనుసంధానించబడి ఉంది. యాంటెన్నా టెరస్ట్రియల్ మైక్రోవేవ్ లింక్ల ద్వారా వినియోగదారుల నుండి కాల్లను అందుకుంటుంది మరియు అందుకుంటుంది. ప్రతి బేస్ స్టేషన్ దాని సామర్థ్యాన్ని బట్టి బహుళ హ్యాండ్సెట్లకు మద్దతు ఇస్తుంది.

GPRS

GPRS stands for General Packet Radio Services. It is a packet based wireless communication technology that charges users based on the volume of data they send rather than the time duration for which they are using the service. This is possible because GPRS sends data over the network in packets and its throughput depends on network traffic. As traffic increases, service quality may go down due to congestion, hence it is logical to charge the users as per data volume transmitted.

జనరల్ ప్యాకెట్ రేడియో సేవలకు GPRS ఉంటుంది. ఇది ప్యాకెట్ ఆధారిత వైర్లెస్ కమ్యూనికేషన్ టెక్నాలజీ, వారు సేవను ఉపయోగిస్తున్న సమయ వ్యవధి కంటే వారు పంపే డేటా వాల్యూమ్ ఆధారంగా వినియోగదారులకు రుసుము వసూలు చేస్తారు. GPRS అనునది నెట్వర్కుపైన పాకెట్లలో డాటాను పంపుచున్నందున అది సాధ్యపడుతుంది ఎందుకంటే దాని ట్రాపొట్ నెట్వర్క్ ట్రాఫిక్ పై ఆధారపడి ఉంటుంది. ట్రాఫిక్ పెరుగుతుంది కాబట్టి, రద్దీ కారణంగా సేవ నాణ్యత తగ్గిపోతుంది, దాంతో డేటా వాల్యూమ్ ప్రకారం వినియోగదారులకు ఛార్జ్ చేయడం తార్కికంగా ఉంటుంది.

GPRS is the mobile communication protocol used by second (2G) and third generation (3G) of mobile telephony. It pledges a speed of 56 kbps to 114 kbps, however the actual speed may vary depending on network load.

GPRS మొబైల్ టెలిఫోనీ రెండవ (2G) మరియు మూడవ తరం (3G) ఉపయోగించే మొబైల్ కమ్యూనికేషన్ ప్రోటోకాల్. ఇది 56 kbps వేగంతో 114 kbps కు హామీ ఇస్తుంది, అయినప్పటికీ అసలు వేగం నెట్వర్క్ లోడ్పై ఆధారపడి ఉంటుంది.

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

మోటరోలా 1983 లో మొట్టమొదటి వాణిజ్య మొబైల్ ఫోన్ పరిచయం అయినప్పటి నుండి, మొబైల్ టెక్నాలజీ చాలా దూరం వచ్చింది. ఇది టెక్నాలజీ, ప్రోటోకాల్స్, సర్వీసెస్ లేదా స్పీడ్ గా ఉండటం, మొబైల్ టెలిఫోనీలో మార్పులు మొబైల్ కమ్యూనికేషన్ యొక్క తరం గా

నమోదు చేయబడ్డాయి. ఇంతకుముందు తరాల నుండి వేరుచేసే ఈ తరాల ప్రాథమిక అంశాలను మేము ఇక్కడ చర్చిస్తాము.

1G Technology

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

1G వైర్లెస్ మొబైల్ కమ్యూనికేషన్ యొక్క మొదటి తరంను సూచిస్తుంది, ఇక్కడ అనలాగ్ సంకేతాలు డేటాను బదిలీ చేయడానికి ఉపయోగించబడ్డాయి. ఇది 1980 ల ప్రారంభంలో US లో పరిచయం చేయబడింది మరియు వాయిస్ కమ్యూనికేషన్ కోసం ప్రత్యేకంగా రూపొందించబడింది. 1G కమ్యూనికేషన్ యొక్క కొన్ని లక్షణాలు -

- Speeds up to 2.4 kbps
- 2.4 kbps వరకు వేగాన్ని పెంచుతుంది
- Poor voice quality
- పేద వాయిస్ నాణ్యత
- Large phones with limited battery life
- పరిమిత బ్యాటరీ జీవితకాలానికి • పెద్ద ఫోన్లు
- No data security
- డేటా భద్రత లేదు

2G Technology

2 జి టెక్నాలజీ

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

2G మొబైల్ టెలిఫోనీ రెండవ తరం సూచిస్తుంది, ఇది మొదటిసారిగా డిజిటల్ సిగ్నల్స్ను ఉపయోగించింది. ఇది ఫిన్లాండ్లో 1991 లో ప్రారంభించబడింది మరియు GSM సాంకేతికతను ఉపయోగించింది. 2G కమ్యూనికేషన్ యొక్క కొన్ని ప్రముఖ లక్షణాలు

- Data speeds up to 64 kbps
  64 kbps వరకు డేటా వేగాన్ని పెంచుతుంది
- Text and multimedia messaging possible
  టెక్స్ట్ మరియు మల్టీమీడియా సందేశం సాధ్యం
- Better quality than 1G
  1G కన్నా మెరుగైన నాణ్యత

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

GPRS సాంకేతికత ప్రవేశపెట్టినప్పుడు, ఇది వెబ్ బ్రౌజింగ్, ఇ-మెయిల్ సేవలు మరియు వేగవంతమైన అప్లోడ్ / డౌన్ లోడ్ వేగాలను ప్రారంభించింది. GPRS తో 2G కూడా 2.5G అని కూడా పిలుస్తారు, తరువాత మొబైల్ తరం యొక్క ఒక అడుగు తక్కువగా ఉంటుంది .

3G Technology

Third generation (3G) of mobile telephony began with the start of the new millennium and offered major advancement over previous generations. Some of the characteristics of this generation are –
మొబైల్ టెలిఫోనీ మూడవ తరం (3G) కొత్త సహస్రాబ్దం ప్రారంభంతో ప్రారంభమైంది మరియు మునుపటి తరాలపై భారీ అభివృద్ధిని అందించింది. ఈ తరానికి సంబంధించిన కొన్ని లక్షణాలు -

- Data speeds of 144 kbps to 2 Mbps
- 2 kbps కు 144 kbps డేటా వేగం
- High speed web browsing
- హై స్పీడ్ వెబ్ బ్రౌజింగ్
- Running web based applications like video conferencing, multimedia e-mails, etc
- వీడియో కాన్ఫరెన్సింగ్, మల్టీమీడియా ఇ-మెయిల్లు, మొదలైనవి వంటి వెబ్ ఆధారిత అనువర్తనాలను అమలు చేయడం
- Fast and easy transfer of audio and video files
- ఆడియో మరియు వీడియో ఫైళ్ళ ఫాస్ట్ మరియు సులభంగా బదిలీ
- 3D gaming
- 3D గేమింగ్

Every coin has two sides. Here are some downsides of 3G technology –
ప్రతి నాణెం రెండు వైపులా ఉంటుంది. ఇక్కడ 3G టెక్నాలజీ కొన్ని దుష్ప్రభావాలు ఉన్నాయి –

- Expensive mobile phones
  ఖరీదైన మొబైల్ ఫోన్లు
- High infrastructure costs like licensing fees and mobile towers
  హై ఫౌండేషన్ లైసెన్స్ ఫీజులు మరియు మొబైల్ టవర్లు వంటి ఖర్చులు
- Trained personnel required for infrastructure set up
  మౌలిక సౌకర్యాల ఏర్పాటుకు అవసరమైన శిక్షణ పొందిన సిబ్బంది

The intermediate generation, 3.5G grouped together dissimilar mobile telephony and data technologies and paved way for the next generation of mobile communication.
ఇంటర్మీడియట్ తరం, 3.5 జి మొబైల్ అసోసియేషన్, మొబైల్ టెక్నాలజీ మరియు డేటా టెక్నాలజీలను కలిపి, తదనంతర తరం మొబైల్ కమ్యూనికేషన్ కోసం నిర్మించబడింది.

4G Technology

Keeping up the trend of a new mobile generation every decade, fourth generation (4G) of mobile communication was introduced in 2011. Its major characteristics are –
ప్రతి దశాబ్దంలో కొత్త మొబైల్ తరం ధోరణిని కొనసాగించడం, నాలుగవ తరం (4G) మొబైల్ కమ్యూనికేషన్ 2011 లో ప్రవేశపెట్టబడింది. దీని ప్రధాన లక్షణాలు -

- Speeds of 100 Mbps to 1 Gbps
- Gbps కు 100 Mbps వేగం
- Mobile web access
- మొబైల్ వెబ్ యాక్సెస్

- High definition mobile TV
- హై డెఫినిషన్ మొబైల్ టీవీ
- Cloud computing
- క్లౌడ్ కంప్యూటింగ్
- IP telephony
- IP టెలిఫోనీ

Email Protocols

ఇమెయిల్ ప్రోటోకాల్లు

Email is one of the most popular uses of Internet world wide. As per a 2015 study, there are 2.6 billion email users worldwide who send some 205 billion email messages per day. With email accounting for so much traffic on the Internet, email protocols need to be very robust. Here we discuss some of the most popular email protocols used worldwide.

ఇంటర్నెట్ ప్రపంచ వ్యాప్తంగా అత్యంత ప్రజాదరణ పొందిన వాటిలో ఒకటి. ఒక 2015 అధ్యయనం ప్రకారం, రోజుకు 205 బిలియన్ ఇమెయిల్ సందేశాలను పంపే ప్రపంచవ్యాప్తంగా 2.6 బిలియన్ ఇమెయిల్ వినియోగదారులు ఉన్నారు. ఇంటర్నెట్లో చాలా ట్రాఫిక్ కోసం ఇమెయిల్ అకౌంటింగ్ తో, ఇమెయిల్ ప్రోటోకాల్స్ చాలా బలంగా ఉండాలి. ఇక్కడ ప్రపంచ వ్యాప్తంగా ఉపయోగించిన అత్యంత ప్రసిద్ధ ఇమెయిల్ ప్రోటోకాల్లను మేము చర్చించాము .

SMTP

SMTP stands for **Simple Mail Transfer Protocol**. It is connection oriented **application layer** protocol that is widely used to send and receive email messages. It was introduced in 1982 by **RFC 821** and last updated in 2008 by **RFC 5321**. The updated version is most widely used email protocol.

SMTP సాధారణ మెయిల్ ట్రాన్స్ఫర్ ప్రోటోకాల్ కోసం ఉంటుంది. ఇది ఇమెయిల్ సందేశాలను పంపడానికి మరియు అందుకోవడానికి విస్తృతంగా ఉపయోగించబడే కనెక్షన్ ఆధారిత అనువర్తన లేయర్ ప్రోటోకాల్. ఇది 1982 లో RFC 821 ద్వారా ప్రవేశపెట్టబడింది మరియు చివరికి 2008 లో RFC 5321 ద్వారా నవీకరించబడింది. నవీకరించిన సంస్కరణ విస్తృతంగా ఉపయోగించిన ఇమెయిల్ ప్రోటోకాల్ .

Mail servers and mail transfer agents use **SMTP** to both send and receive messages. However, user level applications use it only for sending messages. For retrieving they use IMAP or POP3 because they provide **mail box management**

మెయిల్ సర్వర్లు మరియు మెయిల్ బదిలీ ఏజెంట్లు SMTP ను రెండు సందేశాలను పంపేందుకు మరియు స్వీకరించడానికి ఉపయోగిస్తారు. అయితే, వినియోగదారు స్థాయి అనువర్తనాలు సందేశాలను పంపడానికి మాత్రమే దీనిని ఉపయోగిస్తాయి. తిరిగి పొందడానికి వారు IMAP లేదా POP3 ను ఉపయోగిస్తున్నారు ఎందుకంటే వారు మెయిల్ బాక్స్ నిర్వహణను అందిస్తారు

RFC or **Request for Comments** is a peer reviewed document jointly published by Internet Engineering Task Force and the Internet Society. It is written by researchers and computer scientists describing how the Internet should work and protocols and systems supporting them.

RFC లేదా అభ్యర్థనల కోసం అభ్యర్థన అనేది ఇంటర్నెట్ ఇంజనీరింగ్ టాస్క్ ఫోర్స్ మరియు ఇంటర్నెట్ సొసైటీ సంయుక్తంగా ప్రచురించబడిన ఒక పీర్ సమీక్ష పత్రం. ఇంటర్నెట్ పని మరియు ప్రోటోకాల్లు మరియు వ్యవస్థలు వాటిని ఎలా సమర్థించాలో వివరించే పరిశోధకులు మరియు కంప్యూటర్ శాస్త్రవేత్తలు దీనిని వ్రాశారు.

POP3

POP3 or **Post Office Protocol Version 3** is an **application layer** protocol used by email clients to retrieve email messages from mail servers over **TCP/IP** network. POP was designed to move the messages from server to local disk but version 3 has the option of leaving a copy on the server

POP3 లేదా పోస్ట్ ఆఫీస్ ప్రోటోకాల్ సంస్కరణ 3 అనేది TCP / IP నెట్‌వర్క్లో మెయిల్ సర్వర్ల నుండి ఇమెయిల్ సందేశాలను తిరిగి పొందడానికి ఇమెయిల్ క్లయింట్లచే ఉపయోగించే ఒక అప్లికేషన్ లేయర్ ప్రోటోకాల్. సర్వర్ నుండి స్థానిక డిస్క్కు సందేశాలను తరలించడానికి POP రూపకల్పన చేయబడింది, అయితే వెర్షన్ 3 సర్వర్లో ఒక కాపీని వదిలిపెట్టే అవకాశం ఉంది

POP3 is a very simple protocol to implement but that limits its usage. For example, POP3 supports only one mail server for each mailbox. It has now has been made obsolete by modern protocols like **IMAP**.

POP3 అనేది అమలు చేయడానికి చాలా సులభమైన ప్రోటోకాల్, కానీ అది దాని వినియోగాన్ని పరిమితం చేస్తుంది. ఉదాహరణకు, ప్రతి మెయిల్బాక్స్కు POP3 ఒక మెయిల్ సర్వర్ మాత్రమే మద్దతు ఇస్తుంది. IMAP వంటి ఆధునిక ప్రోటోకాల్స్ ఇప్పుడు వాడుకలో ఉంది.

IMAP

IMAP stands for **Internet Message Access Protocol**. IMAP was defined by **RFC 3501** to enable email clients to retrieve email messages from mail servers over a TCP/IP connection. IMAP is designed to retrieve messages from multiple mail servers and consolidate them all in the user's mailbox. A typical example is a corporate client handling multiple corporate accounts through a local mailbox located on her system.

IMAP అనేది ఇంటర్నెట్ మెసేజ్ యాక్సెస్ ప్రోటోకాల్. ఇమెయిల్ క్లయింట్లు TCP / IP కనెక్షన్ ద్వారా మెయిల్ సర్వర్ల నుండి ఇమెయిల్ సందేశాలను తిరిగి పొందడానికి ఎనేబుల్ చేయడానికి RFC 3501 ద్వారా IMAP నిర్వచించబడింది. IMAP బహుళ మెయిల్ సర్వర్ల నుండి సందేశాలను తిరిగి పొందడానికి మరియు యూజర్ యొక్క మెయిల్బాక్స్లో వాటిని అన్నింటినీ ఏకీకృతం చేయడానికి రూపొందించబడింది. ఆమె వ్యవస్థలో ఉన్న ఒక స్థానిక మెయిల్బాక్స్ ద్వారా పలు కార్పొరేట్ ఖాతాలను నిర్వహించే కార్పొరేట్ క్లయింట్ ఒక ఉదాహరణ .

All modern email clients and servers like Gmail, Outlook and Yahoo Mail support IMAP or POP3 protocol. These are some advantages that IMAP offers over POP3 –

అన్ని ఆధునిక ఇమెయిల్ క్లయింట్లు మరియు Gmail, Outlook మరియు Yahoo మెయిల్ మద్దతు IMAP లేదా POP3 ప్రోటోకాల్ వంటి సర్వర్లు. ఇవి IMP POP3 పై అందించే కొన్ని ప్రయోజనాలు –

- Faster response time than POP3
- POP3 కంటే వేగంగా ప్రతిస్పందన సమయం
- Multiple mail clients connected to a single mailbox simultaneously
- బహుళ మెయిల్ క్లయింట్లు ఒకే మెయిల్బాక్స్తో ఏకకాలంలో కనెక్ట్ చేయబడతాయి
- Keep track of message state like read, deleted, starred, replied, etc.
- చదివిన, తొలగించబడిన, నటించిన, ప్రత్యుత్తరం ఇచ్చిన, మొదలైనవి వంటి సందేశ స్థితిని ట్రాక్ చేయండి.
- Search for messages on the server
- సర్వర్లో సందేశాల కోసం శోధించండి

VoIP

VoIP is the acronym for **Voice over Internet Protocol**. It means telephone services over Internet. Traditionally Internet had been used for exchanging messages but due to advancement in technology, its service quality has increased manifold. It is now possible to deliver voice communication over IP networks by converting voce data into packets. VoIP is a set of protocols and systems developed to provide this service seamlessly.

వాయిస్ ఓవర్ ఇంటర్నెట్ ప్రోటోకాల్ కోసం VoIP అక్రోనిమ్. ఇది ఇంటర్నెట్లో టెలిఫోన్ సేవలను సూచిస్తుంది. సాంప్రదాయకంగా ఇంటర్నెట్ సందేశాలను మార్పిడి చేయడానికి ఉపయోగించబడింది, అయితే సాంకేతిక పరిజ్ఞానం అభివృద్ధి చెందడంతో, దాని యొక్క నాణ్యత నాణ్యత అనేక రెట్లు పెరిగింది. ప్యాకెట్లలో వోకే డేటాను మార్పిడి చేయడం ద్వారా IP నెట్వర్క్లో వాయిస్ కమ్యూనికేషన్ను అందించడం ఇప్పుడు సాధ్యపడుతుంది. VoIP ఈ సేవను సజావుగా అందించడానికి అభివృద్ధి చేయబడిన ప్రోటోకాల్లు మరియు వ్యవస్థల సమితి.

Here are some of the protocols used for VoIP −

- H.323
- Session Initiation Protocol (SIP)
- Session Description Protocol (SDP)
- Media Gateway Control Protocol (MGCP)
- Real-time Transport Protocol (RTP)
- Skype Protocol

We will discuss two of the most fundamental protocols – H.323 and SIP – here.

H.323

Is a VoIP standard for defining the components, protocols and procedures to provide real-time multimedia sessions including audio, video and data transmissions over packetswitched networks. Some of the services facilitated by H.323 include –

ప్యాకేజీలు పట్టిన నెట్వర్క్లపై ఆడియో, వీడియో మరియు డేటా ప్రసారాలతో సహా నిజ-సమయ మల్టీమీడియా సెషన్లను అందించడానికి భాగాలు, ప్రోటోకాల్లు మరియు విధానాలను నిర్వచించడానికి VoIP ప్రమాణం. H.323 చే ఇవ్వబడ్డ కొన్ని సేవలు -

- IP telephony
- Video telephony
- Simultaneous audio, video and data communications

SIP

SIP is an acronym for Session Initiation Protocol. SIP is a protocol to establish, modify and terminate multimedia sessions like IP telephony. All systems that need multimedia sessions are registered and provided SIP address, much like IP address. Using this address, caller can check callee's availability and invite it for a VoIP session accordingly.

SIP సెషన్ ఇనీషియేషన్ ప్రోటోకాల్ కోసం సంక్షిప్త రూపం. IP టెలిఫోనీ వంటి మల్టీమీడియా సెషన్లను ఏర్పాటు చేయడానికి, సవరించడానికి మరియు ముగించడానికి SIP ఒక ప్రోటోకాల్. మల్టీమీడియా సెషన్ల అవసరమైన అన్ని వ్యవస్థలు IP చిరునామా వలె SIP చిరునామాను నమోదు చేస్తాయి మరియు అందించబడతాయి. ఈ చిరునామాను ఉపయోగించి, కాలర్ క్యాలెల లభ్యతను తనిఖీ చేయవచ్చు మరియు దాని ప్రకారం ఒక VoIP సెషన్ కోసం దీన్ని ఆహ్వానించవచ్చు.

SIP facilitates multiparty multimedia sessions like video conferencing involving three or more people. In a short span of time SIP has become integral to VoIP and largely replaced H.323.

SIP మూడు లేదా అంతకంటే ఎక్కువ మంది వ్యక్తులతో వీడియో కాన్ఫరెన్సింగ్ వంటి బహుళ మల్టీమీడియా సెషన్లను అందిస్తుంది. స్వల్ప కాల వ్యవధిలో SIP VoIP కు సమగ్రమైనది మరియు ఎక్కువగా H.323 స్థానంలో ఉంది.

Wireless Technologies
వైర్లెస్ టెక్నాలజీస్

Wireless connection to internet is very common these days. Often an external modem is connected to the Internet and other devices connect to it wirelessly. This eliminated the need for last mile or first mile wiring. There are two ways of connecting to the Internet wirelessly – Wi-Fi and WiMAx.

Wireless connection to internet is very common these days. Often an external modem is connected to the Internet and other devices connect to it wirelessly. This eliminated the need for last mile or first mile wiring. There are two ways of connecting to the Internet wirelessly – Wi-Fi and WiMAx.

ఇంటర్నెట్కు వైర్లెస్ కనెక్షన్ ఈ రోజుల్లో సర్వసాధారణం. తరచుగా బాహ్య మోడెమ్ ఇంటర్నెట్కు అనుసంధానించబడి, ఇతర పరికరాలను తీగరహితంగా కలుపుతుంది. ఇది గత మైలు లేదా మొదటి మైలు వైరింగ్ అవసరాన్ని తీసివేసింది. Wi-Fi మరియు WiMAx - తీగరహిత ఇంటర్నెట్కు రెండు మార్గాలున్నాయి.ఇంటర్నెట్కు వైర్లెస్ కనెక్షన్ ఈ రోజుల్లో సర్వసాధారణం. తరచుగా బాహ్య మోడెమ్ ఇంటర్నెట్కు అనుసంధానించబడి, ఇతర పరికరాలను తీగరహితంగా కలుపుతుంది. ఇది గత మైలు లేదా మొదటి మైలు వైరింగ్ అవసరాన్ని తీసివేసింది. Wi-Fi మరియు WiMAx - తీగరహిత ఇంటర్నెట్కు రెండు మార్గాలున్నాయి.

Wi-Fi

Wi-Fi is the acronym for **wireless fidelity**. **Wi-Fi technology** is used to achieve connection to the Internet without a direct cable between device and Internet Service Provider. Wi-Fi enabled device and wireless router are required for setting up a Wi-Fi connection. These are some characteristics of wireless Internet connection –

Wi-Fi అనేది వైర్లెస్ విశ్వసనీయతకు సంక్షిప్త నామం. పరికరానికి మరియు ఇంటర్నెట్ సర్వీస్ ప్రొవైడర్కు మధ్య ప్రత్యక్ష కేబుల్ లేకుండా ఇంటర్నెట్కు కనెక్షన్ సాధించడానికి Wi-Fi సాంకేతికత ఉపయోగించబడుతుంది. Wi-Fi కనెక్షన్ను ఏర్పాటు చేయడానికి Wi-Fi

ప్రారంభించబడిన పరికరం మరియు వైర్లెస్ రౌటర్ అవసరం. ఈ వైర్లెస్ ఇంటర్నెట్ కనెక్షన్ యొక్క కొన్ని లక్షణాలు -

- Range of 100 yards
- Insecure connection
- Throughput of 10-12 Mbps

If a PC or laptop does not have Wi-Fi capacity, it can be added using a Wi-Fi card

The physical area of the network which provides Internet access through Wi-Fi is called **Wi-Fi hotspot**. **Hotspots** can be set up at home, office or any public space like airport, railway stations, etc. Hotspots themselves are connected to the network through wires.

Wi-Fi ద్వారా ఇంటర్నెట్ ప్రాప్యతను అందించే నెట్వర్క్ యొక్క భౌతిక ప్రాంతం Wi-Fi హాట్స్పాట్ అని పిలుస్తారు. హాట్స్పాట్లు హోమ్, కార్యాలయం లేదా విమానాశ్రయ, రైల్వే స్టేషన్లు వంటి ఇతర బహిరంగ ప్రదేశాలలో ఏర్పాటు చేయబడతాయి. హాట్స్పాట్స్ తాము వైర్ల ద్వారా నెట్వర్క్కు కనెక్ట్ చేయబడతాయి.

WiMax

To overcome the drawback of **Wi-Fi** connections, **WiMax (Worldwide Interoperability for Microwave Access)** was developed. WiMax is a collection of wireless communication standards based on **IEEE** WiMax provides multiple **physical layer** and **media access control** (MAC) options.

Wi-Fi కనెక్షన్ల లోపాలను అధిగమించడానికి WiMax (మైక్రోవేవ్ యాక్సెస్ కోసం ప్రపంచవ్యాప్త ఇంటర్ఆపరాబిలిటీ) అభివృద్ధి చేయబడింది. WiMax IEEE ఆధారంగా వైర్లెస్ కమ్యూనికేషన్ ప్రమాణాల సేకరణ WiMax పలు భౌతిక లేయర్ మరియు మీడియా యాక్సెస్ కంట్రోల్ (MAC) ఎంపికలను అందిస్తుంది.

WiMax Forum, established in 2001, is the principal body responsible to ensure conformity and interoperability among various commercial vendors. These are some of the characteristics of WiMax –

2001 లో స్థాపించబడిన WiMax ఫోరం, వివిధ వాణిజ్య విక్రేతల మధ్య అనుగుణ్యత మరియు అంతర్లీనతను నిర్ధారించే ప్రధాన సంస్థ. ఇవి WiMax యొక్క కొన్ని లక్షణాలు -

- Broadband wireless access
- Range of 6 miles
- Multilevel encryption available
- Throughput of 72 Mbps

The main components of a WiMax unit are –

- **WiMax Base Station** – It is a tower similar to mobile towers and connected to Internet through

high speed wired connection.

WiMax బేస్ స్టేషన్ - ఇది మొబైల్ టవర్లు మాదిరిగా ఒక టవర్ మరియు హై స్పీడ్ వైర్డు కనెక్షన్ ద్వారా ఇంటర్నెట్కు కనెక్ట్ చేయబడుతుంది .

- **WiMax Subscriber Unit (SU)** – It is a WiMax version of wireless modem. The only difference is that modem is connected to the Internet through cable connection whereas WiMax SU receives Internet connection wirelessly through microwaves.

  WiMax సబ్స్క్రయిబర్ యూనిట్ (SU) - ఇది వైర్లెస్ మోడెమ్ యొక్క WiMax వెర్షన్. ఒకే తేడా ఏమిటంటే, మోడెమ్ కేబుల్ కనెక్షన్ ద్వారా ఇంటర్నెట్కు అనుసంధానించబడి ఉంది, అయితే WiMax SU మైక్రోవేవ్ల ద్వారా ఇంటర్నెట్ కనెక్షన్ తీగరహితంగా అందుకుంటుంది .

Internet Protocol Version 4 (IPv4)

The Internet Protocol version 4 was designed to be allocated to approx. imately 4.3 billion addresses. At the beginning of Internet this was considered a much wider address space for which there was nothing to worry about.

ఇంటర్నెట్ ప్రోటోకాల్ వర్షన్ 4 సుమారు కేటాయించటానికి రూపొందించబడింది. 4.3 బిలియన్ చిరునామాలు. ఇంటర్నెట్ ప్రారంభంలో ఇది చాలా విస్తారమైన అడ్రస్ స్థలంగా భావించబడింది, దాని కోసం ఆందోళన ఏమీ లేదు.

The sudden growth in internet users and its wide spread use has exponentially increased the number of devices which needs real and unique IP to be able to communicate. Gradually, an IPS is required by almost every digital equipment which were made to ease human life, such as Mobile Phones, Cars and other electronic devices. The number of devices (other than computers/routers) expanded the demand for extra IP addresses, which were not considered earlier.

ఇంటర్నెట్ వినియోగదారులు మరియు దాని విస్తృత ఉపయోగంలో ఆకస్మిక పెరుగుదల విస్తృతంగా కమ్యూనికేట్ చెయ్యడానికి రియల్ మరియు ఏకైక IP అవసరం పరికరాలు సంఖ్య పెరిగింది. క్రమంగా, మొబైల్ ఫోన్లు, కార్లు మరియు ఇతర ఎలక్ట్రానిక్ పరికరాల వంటి మానవ జీవితాన్ని తగ్గించడానికి చేసిన దాదాపు ప్రతి డిజిటల్ పరికరాలు ఒక IPS అవసరం. పరికరాల సంఖ్య (కంప్యూటర్లు / రౌటర్ల కాకుండా) అదనపు ఐపి చిరునామాల కోసం డిమాండ్ను విస్తరించింది, వీటిని ముందుగా పరిగణించలేదు.

Allocation of IPv4 is globally managed by Internet Assigned Numbers Authority (IANA) under coordination with the Internet Corporation for Assigned Names and Numbers (ICANN). IANA works closely with Regional Internet Registries, which in turns are responsible for efficiently distributing IP addresses in their territories. There are five such RIRS. According to IANA reports, all the IPv4 address blocks have been allocated. To cope up with the situation, the following practices were being done:

IPv4 యొక్క కేటాయింపు ఇంటర్నెట్ అసైన్డ్ నంబర్స్ అథారిటీ (IANA), ఇంటర్నెట్ కార్పోరేషన్ ఫర్ అసైన్డ్ నేమ్స్ అండ్ నంబర్స్ (ICANN) తో సమన్వయంతో నిర్వహించబడుతుంది. ఐఎన్ఏ ప్రాంతీయ ఇంటర్నెట్ రిజిస్ట్రీస్తో కలిసి పనిచేస్తోంది, దాని ప్రాంతాలు ఐపి చిరునామాలను సమర్థవంతంగా పంపిణీ చేయడానికి బాధ్యత వహిస్తాయి. ఐదు వంటి RIRS ఉన్నాయి. IANA నివేదికల ప్రకారం, అన్ని IPv4 అడ్రస్ బ్లాక్స్ కేటాయించబడ్డాయి. పరిస్థితిని ఎదుర్కోవటానికి, కింది ఆచారాలు జరుగుతున్నాయి:

- **Private IPs:** Few blocks of IPs were declared for private use within a LAN so that the requirement for public IP addresses can be reduced.
  ప్రైవేట్ IP లు: IP ల యొక్క కొన్ని బ్లాకులు ఒక LAN లో ప్రైవేట్ ఉపయోగం కోసం ప్రకటించబడ్డాయి, కనుక పబ్లిక్ IP చిరునామాల అవసరాన్ని తగ్గించవచ్చు

- **NAT:** Network address translation is a mechanism by which multiple PCs/hosts with private IP addresses are enabled to access using one or few public IP addresses.
  NAT: నెట్వర్క్ అడ్రస్ ట్రాన్స్లేషన్ అనేది ఒక పబ్లిక్ IP చిరునామాలను ఉపయోగించి ప్రాప్తి చేయడానికి ప్రైవేట్ PC అడ్రెస్లతో బహుళ PC లు / హోస్ట్లను అనుమతించే ఒక యంత్రాంగాన్ని చెప్పవచ్చు.

- Unused Public IPs were reclaimed by RIRs.

What is TCP/IP?

TCP/IP is a set of protocols (Protocol Suit) that enable communication between computers. Protocols are rules or standards that govern communications. If two devices in a network need to communicate, they need to use a common protocol. This can be compared with how humans speak. A French person cannot communicate with a Vietnamese person since they speak different languages.

TCP / IP అనేది కంప్యూటర్ల మధ్య సంభాషణను ప్రారంభించే ప్రోటోకాల్స్ యొక్క సమితి (ప్రోటోకాల్ సూట్). ప్రోటోకాల్లు నియమాలు లేదా ప్రమాణాలు పాలించే సమాచారాలు. ఒక నెట్వర్క్లో రెండు పరికరాలను కమ్యూనికేట్ చేయాలంటే, వారు ఒక సాధారణ ప్రోటోకాల్ ఉపయోగించాలి. మానవులు మాట్లాడేటప్పుడు ఇది పోల్చవచ్చు. ఒక ఫ్రెంచ్ వ్యక్తి వియత్నమీస్ వ్యక్తితో మాట్లాడలేడు, వారు వివిధ భాషలను మాట్లాడతారు.

You can select from different network protocols to use in your network, but TCP/IP is the industry standard. Almost all Operating Systems now support TCP/IP. Internet is working on TCP/IP. TCP/IP is known as "the language of the Internet." If you want a computer to work on the Internet, you have to use TCP/IP.

మీరు మీ నెట్వర్క్లో వేరే నెట్వర్క్ ప్రోటోకాల్స్ నుండి ఎంచుకోవచ్చు, కానీ TCP / IP పరిశ్రమ ప్రమాణంగా ఉంటుంది. దాదాపు అన్ని ఆపరేటింగ్ సిస్టమ్స్ ఇప్పుడు TCP / IP కు మద్దతు ఇస్తుంది. ఇంటర్నెట్ TCP / IP లో పని చేస్తుంది. TCP / IP ను "ఇంటర్నెట్ భాష" అని పిలుస్తారు. మీరు కంప్యూటర్లో ఇంటర్నెట్ పని చేయాలనుకుంటే, మీరు TCP / IP ను ఉపయోగించాలి.

Features of TCP/IP

The industry was using TCP/IP around 35 years. It is a tested and proved protocol suit.

ఈ పరిశ్రమ TCP / IP ను సుమారు 35 ఏళ్ళకు వాడుతోంది. ఇది పరీక్షలు మరియు నిరూపితమైన ప్రోటోకాల్ దావా.

1) Multi-Vendor Support. TCP/IP is implemented by many hardware and software vendors. It is an industry standard and not limited to any specific vendor.
ఈ పరిశ్రమ TCP / IP ను సుమారు 35 ఏళ్ళకు వాడుతోంది. ఇది పరీక్షలు మరియు నిరూపితమైన ప్రోటోకాల్ దావా.

2)Interoperability. Today we can work in a heterogeneous network because of TCP/IP. A user who is sitting on a Windows box can download files from a Linux machine, because both Operating Systems support TCP/IP. TCP/IP eliminates the cross-platform boundaries.

సహాయ సహకారాలతో. ఈ రోజు మనం TCP / IP యొక్క వైవిధ్యమైన నెట్వర్క్లో పనిచేయవచ్చు. ఒక విండోస్ బాక్స్లో కూర్చొన్న యూజర్ లైనక్స్ యంత్రం నుండి ఫైళ్లను డౌన్లోడ్ చేసుకోవచ్చు, ఎందుకంటే ఆపరేటింగ్ సిస్టమ్స్ రెండూ TCP / IP కి మద్దతిస్తాయి. TCP / IP క్రాస్ ప్లాట్ఫాం సరిహద్దులను తొలగిస్తుంది.

3)Logical Addressing. Every network adapter has a globally unique and permanent physical address, which is known as MAC address (or hardware address). The physical address is burnt into the card while manufacturing. Low-lying hardware-conscious protocols on a LAN deliver data packets using the adapter's physical address. The network adapter of each computer listens to every transmission on the local network to determine whether a message is addressed to its own physical address.

లాజికల్ అడ్రెసింగ్. ప్రతి నెట్వర్క్ అడాప్టర్ ప్రపంచవ్యాప్తంగా ప్రత్యేకమైన మరియు శాశ్వత భౌతిక చిరునామాను కలిగి ఉంది, ఇది MAC చిరునామా (లేదా హార్డ్వేర్ చిరునామా) గా పిలువబడుతుంది. తయారీలో భౌతిక చిరునామా కార్డులో కాల్చివేయబడుతుంది. అడాప్టర్ యొక్క భౌతిక చిరునామాను ఉపయోగించి ఒక LAN లో ఉన్న అబద్ధం హార్డ్వేర్-జ్ఞాన ప్రోటోకాల్లు డేటా ప్యాకెట్లను బట్వాడా చేస్తాయి. ప్రతి కంప్యూటర్ యొక్క నెట్వర్క్ అడాప్టర్ స్థానిక నెట్వర్క్లోని ప్రతి బదిలీకి ఒక సందేశాన్ని తన సొంత భౌతిక చిరునామాకు పంపించాలో లేదో నిర్ణయించడానికి వినవచ్చు.

For a small LAN, this will work well. But when your computer is connected to a big network like internet, it may need to listen to millions of transmissions per second. This may cause your network connection to stop functioning.
ఒక చిన్న LAN కోసం, ఇది బాగా పని చేస్తుంది. కానీ మీ కంప్యూటర్ ఇంటర్నెట్ వంటి పెద్ద నెట్వర్క్కు కనెక్ట్ అయినప్పుడు, అది సెకనుకు మిలియన్ల ప్రసారాలకు వినవచ్చు. ఇది మీ నెట్వర్క్ కనెక్షన్ను ఆపడానికి కారణం కావచ్చు.

To avoid this, network administrators often segment (divide) big networks into smaller networks using devices such as routers to reduce network traffic, so that the unwanted data traffic from one network may not create problem in another network. A network can be again subdivided into smaller subnets so that a message can travel efficiently from its source to the destination. TCP/IP has a robust subnetting capability achieved using logical addressing. A logical address is an address configured through the network software. The logical addressing system used in TCP/IP protocol suit is known as IP address.

దీనిని నివారించడానికి, నెట్వర్క్ నిర్వాహకులు తరచూ చిన్న నెట్వర్క్లను చిన్న నెట్వర్క్లుగా నెట్వర్క్ ట్రాఫిక్ను తగ్గించేందుకు రౌటర్ల వంటి పరికరాలను ఉపయోగించి విభజించారు, తద్వారా ఒక నెట్వర్క్ నుండి అవాంఛిత డేటా ట్రాఫిక్ మరొక నెట్వర్క్లో సమస్యను సృష్టించలేకపోవచ్చు. ఒక నెట్వర్క్ మళ్ళీ చిన్న సబ్ నెట్ లలో ఉపవిభజన చేయబడుతుంది, తద్వారా సందేశాన్ని దాని మూలం నుండి గమ్యస్థానానికి సమర్థవంతంగా ప్రయాణించవచ్చు. TCP / IP లాజికల్ అడ్రసింగ్ ఉపయోగించి సాధించిన ఒక బలమైన సబ్నెట్టింగ్ సామర్థ్యం ఉంది. తార్కిక చిరునామా అనేది నెట్వర్క్ సాఫ్ట్వేర్ ద్వారా కాన్ఫిగర్ చేయబడిన చిరునామా. TCP / IP ప్రోటోకాల్ దావాలో

ఉపయోగించే లాజికల్ అడ్రసింగ్ సిస్టమ్ను IP చిరునామాగా పిలుస్తారు.

1)Routability. A router is a network infrastructure device which can read logical addressing information and direct data across the network to its destination.TCP/IP is a routable protocol, which means the TCP/IP data packets can be moved from one network segment to another.

Routability. ఒక రౌటర్ ఒక నెట్వర్క్ అవస్థాపన పరికరం, ఇది నెట్వర్క్ అంతటా తార్కిక చిరునామా సమాచారం మరియు ప్రత్యక్ష డేటాను చదివేటట్టు చేయవచ్చు. TCP / IP డేటా ప్యాకెట్లను ఒక నెట్వర్క్ సెగ్మెంట్ నుండి మరొకదానికి తరలించగలరని అర్థం చేసుకోగల ఒక పద్ధతి.

2)Name Resolution. IP addresses are designed for the computers and it is difficult for humans to remember many IP addresses. TCP/IP allows us to use human-friendly names, which are very easy to remember (Ex. www.omnisecu.com). Name Resolutions servers (DNS Servers) are used to resolve a human readable name (also known as Fully Qualified Domain Names (FQDN)) to an IP address and vice versa.

పేరు రిజల్యూషన్. IP చిరునామాలను కంప్యూటర్ల కోసం రూపొందించారు మరియు మానవులు అనేక IP చిరునామాలను గుర్తుంచుకోవడం కష్టం. TCP / IP మాకు మానవ-స్నేహపూర్వక పేర్లను ఉపయోగించడానికి అనుమతిస్తుంది, ఇది గుర్తుంచుకోవడానికి చాలా సులభం (Ex www.omnisecu.com). పేరును పరిష్కరిస్తుంది సర్వర్లు (DNS సర్వర్లు) ఒక మానవ రీడబుల్ పేరును (పూర్తిగా క్వాలిఫైడ్ డొమైన్ నేమ్స్ (FQDN) అని కూడా పిలుస్తారు) IP చిరునామాకు మరియు ఇదే విధంగా విరుద్ధంగా ఉంటుంది.

3)Error Control and Flow Control.The TCP/IP protocol has features that ensure the reliable delivery of data from source computer to the destination computer. TCP (Transmisssion Control Protocol) defines many of these error-checking, flow-control, and acknowledgement functions.

లోపం నియంత్రణ మరియు ఫ్లో కంట్రోల్. TCP / IP ప్రోటోకాల్కు మూలం కంప్యూటర్ నుండి డేటాను విశ్వసనీయ డెలివరీ లక్ష్య కంప్యూటర్కు నిర్ధారించే ఫీచర్లను కలిగి ఉంది. TCP (ట్రాన్స్మిస్సిషన్ కంట్రోల్ ప్రోటోకాల్) ఈ దోష-తనిఖీ, ప్రవాహ-నియంత్రణ, మరియు రసీదు ఫంక్షన్లను నిర్వచిస్తుంది.

4) Multiplexing/De-multiplexing. Multiplexing means accepting data from different applications and directing that data to different applications listening on different receiving computers. On the receiving side the data need to be directed to the correct application, for that data was meant for. This is called De-multiplexing. We can run many network applications on the same computer. By using logical channels called ports, TCP/IP provides means for delivering packets to the correct application. In TCP/IP, ports are identified by using TCP or UDP port numbers.

మల్టీప్లెక్సింగ్ / డి-బహుముఖీకరణం. మల్టీప్లెక్స్ అనేది వేర్వేరు అనువర్తనాల నుండి డేటాను స్వీకరిస్తుంది మరియు వేర్వేరు అనువర్తనాలకు వివిధ స్వీకరించే కంప్యూటర్లను వినడం ద్వారా డేటాను దర్శకత్వం చేస్తుంది. స్వీకరించిన వైపున, ఆ డేటా కోసం ఉద్దేశించిన సమాచారం కోసం సరైన దరఖాస్తుకు డేటాను పంపించాలి. దీనిని డి-మల్టీప్లెక్స్ అని పిలుస్తారు. మేము అదే కంప్యూటర్లో అనేక నెట్వర్క్ అనువర్తనాలను అమలు చేయగలము. తార్కిక ఉపయోగించడం ద్వారా

పోర్ట్స్ అని పిలువబడే ఛానెల్స్, TCP / IP సరైన అప్లికేషన్లకు ప్యాకెట్లను పంపిణీ చేయడానికి మార్గాలను అందిస్తుంది. TCP / IP లో, TCP లేదా UDP పోర్ట్ సంఖ్యలను ఉపయోగించడం ద్వారా పోర్ట్లు గుర్తించబడతాయి.

TCP/IP History

The predecessor of today's Internet was ARPAnet, created by the Advanced Research Projects Agency (ARPA) and launched in 1969 during "Cold War". The extreme distrust that existed between USA and USSR (Soviet Union) was almost on the verge of a nuclear war during that time. "Cold War" was the term used to describe the relationship between USA and USSR during period 1945 to 1990. ARPAnet was created in response to the potential threat of nuclear attack from the Soviet Union. One of ARPA's primary goals was to design a fault-tolerant network that would enable U.S. military leaders to stay in contact in case of nuclear war.

అధునాతన రీసెర్చ్ ప్రాజెక్ట్స్ ఏజెన్సీ (ARPA) చేత సృష్టించబడిన ARPAnet, నేటి ఇంటర్నెట్ యొక్క పూర్వీకుడు 1969 లో "కోల్డ్ వార్" సమయంలో ప్రారంభించబడింది. USA మరియు USSR (సోవియట్ యూనియన్) మధ్య ఉన్న అపనమ్మకం ఆ సమయంలో అణు యుద్ధం యొక్క అంచున ఉంది. "ప్రచ్ఛన్న యుద్ధం" అనేది 1945 నుండి 1990 వరకు USA మరియు USSR ల మధ్య సంబంధాన్ని వివరించడానికి ఉపయోగించబడింది. సోవియట్ యూనియన్ నుండి అణు దాడికి సంబంధించిన ప్రమాదానికి ప్రతిస్పందనగా ARPAnet సృష్టించబడింది. US సైనిక నాయకులు అణు యుద్ధం విషయంలో సంప్రదింపులో ఉండటానికి దోహదపడే ఒక తప్పు-తట్టుకునే నెట్వర్క్ను రూపొందించడానికి ARPA యొక్క ప్రధాన లక్ష్యాలలో ఒకటి.

The protocol used on the ARPAnet was called Network Control Protocol (NCP). As the ARPAnet grew, however, a new protocol was needed because NCP was not able to fulfil all the needs of a larger network.
ARPAnet లో ఉపయోగించిన ప్రోటోకాల్ను నెట్వర్క్ కంట్రోల్ ప్రోటోకాల్ (NCP) అని పిలుస్తారు. అయితే ARPAnet పెరగడంతో, ఒక కొత్త ప్రోటోకాల్ అవసరమైంది ఎందుకంటే NCP ఒక పెద్ద నెట్వర్క్ యొక్క అన్ని అవసరాలను నెరవేర్చలేకపోయింది.

In 1974 Vint Cerf and Bob Kahn, published a paper "A Protocol for Packet Network Interconnection." This paper describes the Transmission Control Protocol (TCP), which eventually replaced NCP.

1974 వింట్ సెర్ఫ్ మరియు బాబ్ కాహ్న్, ఒక పేపర్ "ప్యాకెట్ నెట్వర్క్ ఇంటర్కనెక్షన్" అనే ఒక పత్రాన్ని ప్రచురించారు. ఈ కాగితం ట్రాన్స్మిషన్ కంట్రోల్ ప్రోటోకాల్ (TCP) ను వివరిస్తుంది, చివరికి NCP స్థానంలో ఉంది.

By 1978, testing and further development of this language led to a new suite of protocols called Transmission Control Protocol/Internet Protocol (TCP/IP). In 1982, it was decided that TCP/IP would replace NCP as the standard language of the ARPAnet. RFC 801 describes how and why the transition from NCP to TCP was to take place. On January 1, 1983, ARPAnet switched over to TCP/IP, and the network continued to grow very fast.

1978 నాటికి, ఈ భాష పరీక్ష మరియు మరింత అభివృద్ధికి ట్రాన్స్మిషన్ కంట్రోల్ ప్రోటోకాల్ / ఇంటర్నెట్ ప్రోటోకాల్ (TCP / IP) అని పిలిచే కొత్త సూట్ ప్రోటోకాల్లకు దారితీసింది. 1982 లో, TCP / IP NCP ను ARPAnet యొక్క ప్రామాణిక భాషగా భర్తీ చేస్తుందని నిర్ణయించారు.

NCP నుండి TCP కు మార్పు ఎలా జరుగుతుందో మరియు ఎందుకు జరుగుతుందో RFC 801 వివరిస్తుంది. జనవరి 1, 1983 న, ARPAnet TCP / IP కు మారిపోయింది మరియు నెట్వర్క్ చాలా వేగంగా అభివృద్ధి చెందింది.

ARPAnet ceased to exist in 1990. The Internet has since grown from ARPAnet's roots, and TCP/IP has evolved to meet the changing requirements of the Internet.

ARPAnet 1990 లో ఉనికిలో నిలిచిపోయింది. ఇంటర్నెట్ నుండి ARPAnet యొక్క మూలాల నుండి పెరిగింది, మరియు TCP / IP ఇంటర్నెట్ యొక్క మారుతున్న అవసరాలకు అనుగుణంగా ఉద్భవించింది.

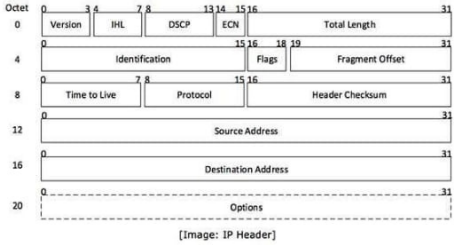
Internet Protocol is one of the major protocols in the TCP/IP protocols suite. This protocol works at the network layer of the OSI model and at the Internet layer of the TCP/IP model. Thus this protocol has the responsibility of identifying hosts based upon their logical addresses and to route data among them over the underlying network.

TCP / IP ప్రోటోకాల్స్ సూట్లోని ప్రధాన ప్రోటోకాల్లో ఇంటర్నెట్ ప్రోటోకాల్ ఒకటి . ఈ ప్రోటోకాల్ OSI మోడల్ యొక్క నెట్వర్క్ పొరలో మరియు TCP / IP మోడల్ యొక్క ఇంటర్నెట్ పొరలో పనిచేస్తుంది . అందుచే ఈ ప్రోటోకాల్ వారి తార్కిక చిరునామాలపై ఆధారపడిన అతిధేయుని గుర్తించే బాధ్యత మరియు అంతర్లీన నెట్వర్క్లో వాటి మధ్య డేటాను మార్చే బాధ్యతను కలిగి ఉంటుంది .

IP provides a mechanism to uniquely identify hosts by an IP addressing scheme. IP uses best effort delivery, i.e. it does not guarantee that packets would be delivered to the destined host, but it will do its best to reach the destination. Internet Protocol version 4 uses 32-bit logical address.

Internet Protocol being a layer-3 protocol (OSI) takes data Segments from layer-4 (Transport) and divides it into packets. IP packet encapsulates data unit received from above layer and add to its own header information.

లేయర్ -3 ప్రోటోకాల్ (OSI) గా ఉన్న ఇంటర్నెట్ ప్రోటోకాల్ పొర -4 (రవాణా) నుండి డేటా సెగ్మెంట్లను తీసుకుంటుంది మరియు ప్యాకెట్లను విభజిస్తుంది. IP ప్యాకెట్ పైన పొర నుండి పొందిన డేటా యూనిట్ను encapsulates మరియు దాని స్వంత శీర్షిక సమాచారం జోడించండి.



[Image: IP Header]

The encapsulated data is referred to as IP Payload. IP header contains all the necessary information to deliver the packet at the other end.

కప్పిన డేటాను IP పేలోడ్గా సూచిస్తారు. ఇతర అంశాలలో ప్యాకెట్ను అందించడానికి అవసరమైన అన్ని అవసరమైన సమాచారాన్ని IP

హెడర్ కలిగి ఉంటుంది.

IP header includes many relevant information including Version Number, which, in this context, is 4. Other details are as follows:

ఐపి శీర్షికలో సంచిక సంఖ్యతో సహా అనేక సంబంధిత సమాచారం ఉంటుంది, ఈ సందర్భంలో, ఇది 4. ఇతర వివరాలు ఈ క్రింది విధంగా ఉన్నాయి:

- **Version:** Version no. of Internet Protocol used (e.g. IPv4).
- సంస్కరణ: సంస్కరణ సంఖ్య. ఇంటర్నెట్ ప్రోటోకాల్ ఉపయోగించారు (ఉదా. IPv4).
- **IHL:** Internet Header Length; Length of entire IP header.
- IHL: ఇంటర్నెట్ హెడర్ పొడవు; మొత్తం IP హెడర్ యొక్క పొడవు.
- **DSCP:** Differentiated Services Code Point; this is Type of Service.
- DSCP: వేరు వేరు సేవలు కోడ్ పాయింట్; ఇది సేవా పద్ధతి.
- **ECN:** Explicit Congestion Notification; It carries information about the congestion seen in the route.
- ECN: స్పష్టమైన సంకోచం నోటిఫికేషన్; ఇది మార్గంలో చూసిన రద్దీ గురించి సమాచారం ఉంది.
- **Total Length:** Length of entire IP Packet (including IP header and IP Payload).
- మొత్తం పొడవు: మొత్తం IP ప్యాకెట్ యొక్క పొడవు (IP శీర్షిక మరియు IP పేలోడ్తో సహా).
- **Identification:** If IP packet is fragmented during the transmission, all the fragments contain same identification number. to identify original IP packet they belong to.
  ఐడెంటిఫికేషన్: ప్రసార సమయములో IP ప్యాకెట్ విభజించబడినట్లయితే, అన్ని శకలాలు ఒకే గుర్తింపు సంఖ్యను కలిగి ఉంటాయి. అసలైన IP ప్యాకెట్ని వారు గుర్తించటానికి .
- **Flags:** As required by the network resources, if IP Packet is too large to handle, these 'flags' tells if they can be fragmented or not. In this 3-bit flag, the MSB is always set to '0'.
  జెండాలు: IP వనరులు నిర్వహించడానికి చాలా పెద్దదిగా ఉంటే, అవి 'ఫ్రాగ్స్' అని వివరిస్తాయి, అవి విచ్ఛిన్నం కావచ్చో లేదా చెప్పకపోవచ్చు. ఈ 3-బిట్ ఫ్లాగ్లో, MSB ఎల్లప్పుడూ '0' కు సెట్ చేయబడింది .
- **Fragment Offset:** This offset tells the exact position of the fragment in the original IP Packet.
ఫ్రాగ్మెంట్ ఆఫ్సెట్: ఈ ఆఫ్సెట్ అసలైన IP ప్యాకెట్లో ఖచ్చితమైన స్థానంతో చెబుతుంది .
- **Time to Live:** To avoid looping in the network, every packet is sent with some TTL value set, which tells the network how many routers (hops) this packet can cross. At each hop, its value is decremented by one and when the value reaches zero, the packet is discarded.
  లైవ్ టైమ్: నెట్వర్క్లో మళ్ళీ వెతికి వచ్చుటకు, ప్రతి ప్యాకెట్ కొన్ని TTL విలువ సమితితో పంపబడుతుంది, ఈ పట్టీ దాటగల ఎన్ని రౌటర్ల (హాప్లు) నెట్వర్క్ను తెలుపుతుంది. ప్రతి హాప్లో, దాని విలువ ఒకటి తగ్గిపోతుంది మరియు విలువ సున్నాకి చేరుకున్నప్పుడు, పాకెట్ విస్మరించబడుతుంది .
- **Protocol:** Tells the Network layer at the destination host, to which Protocol this packet belongs to, i.e. the next level Protocol. For example protocol number of ICMP is 1, TCP is 6 and UDP is 17.
  ప్రోటోకాల్: గమ్య హోస్ట్ వద్ద నెట్వర్క్ పొరను చెబుతుంది, ఈ ప్యాకెట్ ప్రోటోకాల్కు చెందినది, అనగా తదుపరి స్థాయి ప్రోటోకాల్. ఉదాహరణకు ICMP యొక్క ప్రోటోకాల్ సంఖ్య 1, TCP 6 మరియు UDP 17 .
- **Header Checksum:** This field is used to keep checksum value of entire header which is then used

to check if the packet is received error-free.

హెడర్ Checksum: ఈ ఫీల్డ్ మొత్తం శీర్షిక యొక్క చెక్సమ్ విలువను ఉంచడానికి ఉపయోగించబడుతుంది, ఇది పాకెట్ దోష-స్వీకరించబడిందో లేదో తనిఖీ చేయడానికి ఉపయోగించబడుతుంది .

- **Source Address:** 32-bit address of the Sender (or source) of the packet.

మూల చిరునామా: ప్యాకెట్ పంపినవారు (లేదా మూలం) యొక్క 32-బిట్ చిరునామా .

- **Destination Address:** 32-bit address of the Receiver (or destination) of the packet.

గమ్యం చిరునామా: ప్యాకెట్ యొక్క స్వీకర్త (లేదా గమ్యం) యొక్క 32-బిట్ చిరునామా .

- **Options:** This is optional field, which is used if the value of IHL is greater than 5. These options may contain values for options such as Security, Record Route, Time Stamp, etc.

ఐచ్ఛికాలు: ఐహెచ్ఎల్ యొక్క విలువ 5 కంటే ఎక్కువగా ఉంటే ఇది వాడబడే వైకల్పిక క్షేత్రం. ఈ ఐచ్ఛికాలు సెక్యూరిటీ, రికార్డ్ రూట్, టైమ్ స్టాంప్, మొదలైన వాటి కోసం విలువలను కలిగి ఉండవచ్చు .

IPv4 supports three different types of addressing modes.:

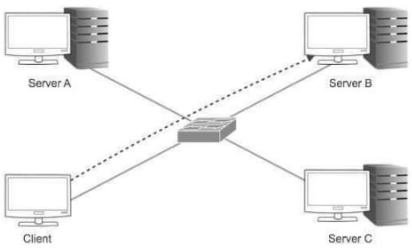
IPv4 చిరునామాలు మూడు వేర్వేరు పద్ధతులను మద్దతిస్తుంది:

Unicast Addressing Mode:

యునికస్ట్ అడ్రసింగ్ మోడ్:

In this mode, data is sent only to one destined host. The Destination Address field contains 32- bit IP address of the destination host. Here the client sends data to the targeted server:

ఈ మోడ్లో, ఒక నిర్దేశిత హోస్ట్కు మాత్రమే డేటా పంపబడుతుంది. డెస్టినేషన్ అడ్రస్ ఫీల్డ్ లో గమ్యం హోస్ట్ యొక్క 32-బిట్ IP చిరునామా ఉంటుంది. ఇక్కడ క్లయింట్ లక్ష్య సర్వర్కు డేటా పంపుతుంది:



Broadcast Addressing Mode:

In this mode, the packet is addressed to all the hosts in a network segment. The Destination Address field contains a special broadcast address, i.e. **255.255.255.255**. When a host sees this packet on the network, it is bound to process it. Here the client sends a packet, which is entertained by all the Servers:

ఈ రీతిలో, పాకెట్ నెట్వర్క్ విభాగంలోని అన్ని అతిథేయలకి ప్రసంగించబడుతుంది. డెస్టినేషన్ అడ్రస్ ఫీల్డ్ ఒక ప్రత్యేక ప్రసార చిరునామాను కలిగి ఉంది, అనగా 255.255.255.255. ఒక అతిథేయి ఈ ప్యాకెట్ను నెట్వర్క్లో చూసినప్పుడు, అది ప్రాసెస్ చేయటానికి కట్టుబడి ఉంటుంది. ఇక్కడ క్లయింట్ ప్యాకెట్ను పంపుతుంది, ఇది అన్ని సర్వర్లు వినోదం పొందుతుంది:

Multicast Addressing Mode:

This mode is a mix of the previous two modes, i.e. the packet sent is neither destined to a single host

nor all the hosts on the segment. In this packet, the Destination Address contains a special address which starts with 224.x.x.x and can be entertained by more than one host.

ఈ మోడ్ మునుపటి రెండు రీతుల్లో మిశ్రమంగా చెప్పవచ్చు, అనగా ప్యాకెట్ పంపినది ఒకే హోస్ట్ లేదా సెగ్మెంట్లోని అన్ని హోస్టకు మాత్రమే ఉద్దేశించబడింది. ఈ ప్యాకెట్లో, డెస్టినేషన్ చిరునామా 224.x.x.x తో మొదలయ్యే ప్రత్యేక చిరునామాను కలిగి ఉంటుంది మరియు ఒకటి కంటే ఎక్కువ హోస్ట్ ద్వారా వినోదం పొందవచ్చు.

Here a server sends packets which are entertained by more than one servers. Every network has one IP address reserved for the Network Number which represents the network and one IP address reserved for the Broadcast Address, which represents all the hosts in that network.

ఇక్కడ ఒక సర్వర్ ఒకటి కంటే ఎక్కువ సర్వర్లచే వినోదం పొందుతున్న ప్యాకెట్లను పంపుతుంది. ప్రతి నెట్వర్క్కు నెట్వర్కు నంబర్కు రిజర్వు చేయబడిన ఒక IP చిరునామాను కలిగి ఉంటుంది, నెట్వర్కో అన్ని హోస్టను సూచిస్తున్న బ్రాడ్కాస్ట్ చిరునామా కోసం రిజర్వు చేయబడిన నెట్వర్క్ మరియు ఒక IP చిరునామా.

Hierarchical Addressing Scheme
క్రమానుగత చిరునామా ప్రణాళిక

IPv4 uses hierarchical addressing scheme. An IP address, which is 32-bits in length, is divided into two or three parts as depicted:

IPv4 క్రమానుగత చిరునామా పథకాన్ని ఉపయోగిస్తుంది. 32-బిట్ల పొడవు గల IP చిరునామా, రెండు లేదా మూడు భాగాలుగా విభజించబడింది:

A single IP address can contain information about the network and its sub-network and ultimately the host. This scheme enables the IP Address to be hierarchical where a network can have many sub-networks which in turn can have many hosts.

ఒక IP చిరునామా నెట్వర్క్ మరియు దాని ఉప నెట్వర్క్ మరియు చివరికి హోస్ట్ గురించి సమాచారాన్ని కలిగి ఉంటుంది. ఈ పథకం IP చిరునామాను క్రమానుగత శ్రేణికి అనుమతిస్తుంది, ఇక్కడ నెట్వర్క్ అనేక ఉప-నెట్వర్క్లను కలిగి ఉంటుంది, ఇది క్రమంగా అనేక అతిధేయలను కలిగి ఉంటుంది.

Subnet Mask
సబ్నెట్ మాస్క్

The 32-bit IP address contains information about the host and its network. It is very necessary to distinguish both. For this, routers use Subnet Mask, which is as long as the size of the network address in the IP address. Subnet Mask is also 32 bits long. If the IP address in binary is ANDed with its Subnet Mask, the

						ANDed
IP	192.168.1.152	11000000	10101000	00000001	10011000	
Mask	255.255.255.0	11111111	11111111	11111111	00000000	
Network	192.168.1.0	11000000	10101000	00000001	00000000	Result

result yields the Network address. For example, say the IP Address is 192.168.1.152 and the Subnet Mask is 255.255.255.0 then:

32-bit IP చిరునామా హోస్ట్ మరియు దాని నెట్వర్క్ గురించి సమాచారాన్ని కలిగి ఉంది. ఇది రెండింటినీ గుర్తించడానికి చాలా అవసరం. దీని కొరకు, రౌటర్లు సబ్నెట్ మాస్క్ ను వుపయోగిస్తాయి, ఇది నెట్వర్కు చిరునామా యొక్క పరిమాణం వరకు ఉంటుంది ది IP చిరునామా. సబ్నెట్ మాస్క్ కూడా 32 బిట్స్ పొడవు. బైనరీలోని IP చిరునామా దాని సబ్నెట్ మాస్క్తో ముగిస్తే, ఫలితం నెట్వర్క్ చిరునామాను అందిస్తుంది. ఉదాహరణకు, IP చిరునామా 192.168.1.152 మరియు సబ్నెట్ మాస్క్ 255.255.255.0 అన్నది:

This way the Subnet Mask helps extract the Network ID and the Host from an IP Address. It can be identified now that 192.168.1.0 is the Network number and 192.168.1.152 is the host on that network.

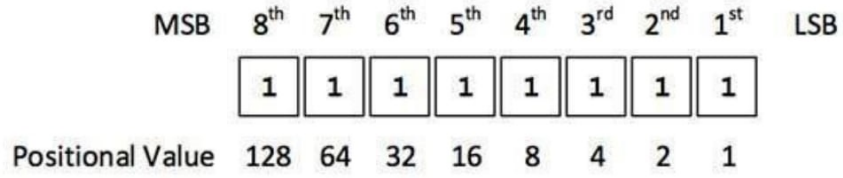
ఈ విధంగా సబ్నెట్ మాస్క్ ఒక IP చిరునామా నుండి నెట్వర్క్ ఐడి మరియు హోస్ట్ను సేకరించేందుకు సహాయపడుతుంది. ఇది 192.168.1.0 నెట్వర్క్ నంబర్ మరియు 192.168.1.152 ఆ నెట్వర్క్లో అతిధేయమని ఇప్పుడు గుర్తించవచ్చు.

Binary Representation

బైనరీ ప్రాతినిధ్యం

The positional value method is the simplest form of converting binary from decimal value. IP address is 32 bit value which is divided into 4 octets. A binary octet contains 8 bits and the value of each bit can be determined by the position of bit value '1' in the octet.

స్థాన విలువ పద్ధతి బైనరీని దశాంశ విలువ నుండి మార్చడానికి సరళమైన రూపం. IP చిరునామా 32 బిట్ విలువ, ఇది 4 ఆక్టెట్స్గా విభజించబడింది. బైనరీ ఆక్టెట్ 8 బిట్స్ కలిగి ఉంటుంది మరియు ప్రతి బిట్ యొక్క విలువ ఆక్టేట్లో బిట్ విలువ '1' యొక్క స్థానం ద్వారా నిర్ణయించబడుతుంది .



Positional value of bits is determined by 2 raised to power (position – 1), that is the value of a bit 1 at position 6 is 2^(6-1) that is 2^5 that is 32. The total value of the octet is determined by adding up the positional value of bits. The value of 11000000 is 128+64 = 192. Some examples are shown in the table below:

బిట్స్ యొక్క పొజిషన్ విలువ 2 కు అధికం (స్థానం -1) ద్వారా నిర్ణయించబడుతుంది, అది 6 వ స్థానం వద్ద బిట్ 1 యొక్క విలువ 2 ^ 5 (6-1), ఇది 2 ^ 5 గా ఉంటుంది. ఇది 32 ఆక్టేట్ బిట్స్ యొక్క స్థితి విలువను జోడించడం ద్వారా నిర్ణయించబడుతుంది. 11000000 విలువ 128 + 64 = 192. కొన్ని ఉదాహరణలు క్రింది పట్టికలో చూపించబడతాయి:

128	64	32	16	8	4	2	1	Value
0	0	0	0	0	0	0	1	1
0	0	0	0	0	0	1	0	2
0	0	0	0	0	0	1	1	3
0	0	0	0	0	1	0	0	4
0	0	0	0	0	1	0	1	5
0	0	0	0	0	1	1	0	6
0	0	0	0	0	1	1	1	7
0	0	0	0	1	0	0	0	8
0	0	0	0	1	0	0	1	9
0	0	0	0	1	0	1	0	10
0	0	0	1	0	0	0	0	16
0	0	1	0	0	0	0	0	32
0	1	0	0	0	0	0	0	64
0	1	1	0	0	1	0	0	100
0	1	1	1	1	1	1	1	127
1	0	0	0	0	0	0	0	128
1	0	1	0	1	0	0	0	168
1	1	0	0	0	0	0	0	192
1	1	1	1	1	1	1	1	255

Internet Protocol hierarchy contains several classes of IP Addresses to be used efficiently in various situations as per the requirement of hosts per network. Broadly, the IPv4 Addressing system is divided into five classes of IP Addresses. All the five classes are identified by the first octet of IP Address.

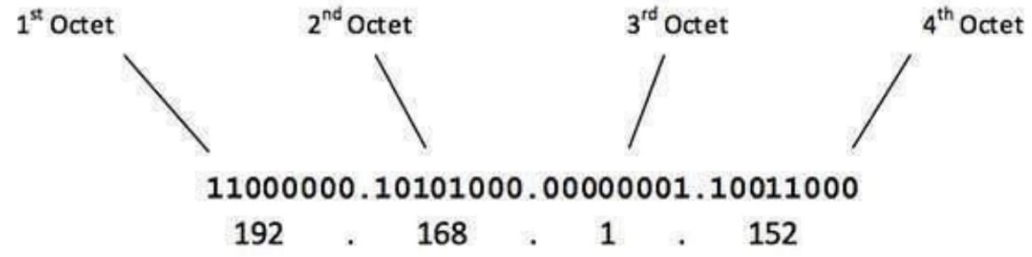
ఇంటర్నెట్ ప్రోటోకాల్ సోపానక్రమం అనేక నెట్వర్క్‌లకు అవసరమయ్యే వివిధ సందర్భాలలో సమర్థవంతంగా ఉపయోగించటానికి IP చిరునామాలు యొక్క అనేక తరగతులను కలిగి ఉంటుంది. విస్తృతంగా, IPv4 అడ్రసింగ్ విధానం ఐ.పి. చిరునామాల యొక్క ఐదు తరగతులుగా విభజించబడింది. ఐపి అడ్రస్ యొక్క మొదటి ఆక్టెట్ ద్వారా ఐదు తరగతులను గుర్తిస్తారు.

Internet Corporation for Assigned Names and Numbers is responsible for assigning IP addresses.

అసైన్డ్ నేమ్స్ అండ్ నంబర్స్ కోసం ఇంటర్నెట్ కార్పొరేషన్ IP చిరునామాలను కేటాయించడానికి బాధ్యత వహిస్తుంది.

The first octet referred here is the left most of all. The octets numbered as follows depicting dotted decimal notation of IP Address:

ఇక్కడ సూచించిన మొదటి ఆక్టెట్ ఎడమలో చాలా భాగం. IP చిరునామా యొక్క చుక్కల డెసిషన్ సంకేతాన్ని ఈ క్రింది విధంగా వివరించిన అష్టులు:



The number of networks and the number of hosts per class can be derived by this formula:

నెట్వర్క్ సంఖ్య మరియు తరగతికి హోస్ట్ల సంఖ్య ఈ సూత్రం ద్వారా ఉత్పన్నమవుతుంది :

Number of networks	= 2^network_bits
Number of Hosts/Network	= 2^host_bits – 2

When calculating hosts' IP addresses, 2 IP addresses are decreased because they cannot be assigned to hosts, i.e. the first IP of a network is network number and the last IP is reserved for Broadcast IP.

అతిథులు 'IP చిరునామాలను లెక్కిస్తున్నప్పుడు, 2 IP చిరునామాలను తగ్గిపోతుంది, ఎందుకంటే వారు హోస్ట్లకు కేటాయించలేరు, అనగా నెట్వర్క్ యొక్క మొదటి IP నెట్వర్క్ సంఖ్య మరియు చివరి ఐపి బ్రాడ్కాస్ట్ ఐపికి రిజర్వు చేయబడుతుంది.

Class A Address

The first bit of the first octet is always set to 0 (zero). Thus the first octet ranges from 1 – 127,

Class A addresses only include IP starting from 1.x.x.x to 126.x.x.x only. The IP range 127.x.x.x is reserved for loopback IP addresses.

మొదటి ఆక్టెట్ యొక్క మొదటి బిట్ ఎల్లప్పుడూ 0 (సున్నా) కు సెట్ చేయబడింది. అందుచే మొదటి ఆక్టేట్ 1 నుండి 127 వరకు ఉంటుంది, క్లాస్ ఒక చిరునామాలను మాత్రమే 1.x.x.x నుండి 126.x.x.x నుండి IP ను మాత్రమే కలిగి ఉంటుంది. IP పరిధి 127.x.x.x loopback IP చిరునామాలకు రిజర్వు చేయబడింది.

The default subnet mask for Class A IP address is 255.0.0.0 which implies that Class A addressing can have 126 networks (2^7-2) and 16777214 hosts (2^{24}-2).

తరగతి A IP చిరునామా కోసం డిఫాల్ట్ సబ్నెట్ మాస్క్ 255.0.0.0, క్లాస్ ఎ అడ్రసింగ్లో 126 నెట్వర్క్లు (27-2) మరియు 16777214 హోస్ట్లు (224-2) ఉంటాయి.

Class A IP address format is thus: **0NNNNNNN**.HHHHHHHH.HHHHHHHH.HHHHHHHH **Class**

B Address

An IP address which belongs to class B has the first two bits in the first octet set to 10

Class B IP Addresses range from 128.0.x.x to 191.255.x.x. The default subnet mask for Class B is 255.255.x.x.

తరగతి B కు చెందిన IP చిరునామా 10 మొదటి ఆక్టెట్ సెట్లో మొదటి రెండు బిట్లు కలిగి ఉంటుంది క్లాస్ B IP చిరునామాలు 128.0.x.x నుండి 191.255.x.x వరకు ఉంటాయి. క్లాస్ B కోసం డిఫాల్ట్ సబ్నెట్ మాస్క్ 255.255.x.x.

Class B has 16384 (2^{14}) Network addresses and 65534 (2^{16}-2) Host addresses.

తరగతి B 16384 (214) నెట్వర్క్ చిరునామాలు మరియు 65534 (216-2) హోస్ట్ అడ్రెస్లను కలిగి ఉంది.

Class B IP address format is: **10NNNNNN.NNNNNNNN**.HHHHHHHH.HHHHHHHH

Class C Address

The first octet of Class C IP address has its first 3 bits set to 110, that

తరగతి C IP చిరునామా యొక్క మొదటి ఆక్టెట్ దాని మొదటి 3 బిట్లను 110 కు సెట్ చేసింది

Class D Address

Very first four bits of the first octet in Class D IP addresses are set to 1110

తరగతి D IP చిరునామాలలో మొదటి ఆక్టెట్ యొక్క మొదటి నాలుగు బిట్స్ 1110 కు సెట్ చేయబడ్డాయి

Class D has IP address rage from 224.0.0.0 to 239.255.255.255. Class D is reserved for Multicasting. In multicasting data is not destined for a particular host, that is why there is no need to extract host address from the IP address, and Class D does not have any subnet mask.

క్లాస్ డి కి 224.0.0.0 నుండి 239.255.255.255 వరకు IP చిరునామా rage ఉంది. క్లాస్ డి మల్టీకస్టింగ్ కోసం కేటాయించబడింది. మల్టికస్టింగ్ డేటాలో ఒక ప్రత్యేక హోస్ట్ కోసం ఉద్దేశించబడలేదు, అందువల్ల ఐపి అడ్రస్ నుండి హోస్ట్ అడ్రస్ ను తీసివేయవలసిన అవసరం లేదు, మరియు క్లాస్ డి ఏ సబ్నెట్ మాస్క్కో లేదు.

Class E Address

This IP Class is reserved for experimental purposes only for R&D or Study. IP addresses in this class ranges from 240.0.0.0 to 255.255.255.254. Like Class D, this class too is not equipped with any subnet mask.

IPv4 - Subnetting

Each IP class is equipped with its own default subnet mask which bounds that IP class to have prefixed number of Networks and prefixed number of Hosts per network. Classful IP addressing does not provide any flexibility of having less number of Hosts per Network or more Networks per IP Class.

ప్రతి IP తరగతి దాని సొంత డిఫాల్ట్ సబ్నెట్ ముసుగుతో అమర్చబడి ఉంటుంది, ఇది IP తరగతికి పూర్వం నెట్ వర్క్ మరియు నెట్వర్క్కు ముందు హోస్ట్స్ యొక్క ప్రిఫిక్స్డ్ సంఖ్యను కలిగి ఉంటుంది. క్లాస్ఫుల్ ఐపి అడ్రసింగ్ అనేది IP క్లాస్కు నెట్వర్క్ లేదా ఎక్కువ నెట్ వర్క్ లకు తక్కువ హోస్ట్ల సంఖ్యను కలిగి ఉండదు.

CIDR or **Classless Inter Domain Routing** provides the flexibility of borrowing bits of Host part of the IP address and using them as Network in Network, called Subnet. By using subnetting, one single Class A IP address can be used to have smaller sub-networks which provides better network management capabilities.

CIDR లేదా తరగతిలేని ఇంటర్ డొమైన్ రౌటింగ్ IP చిరునామా యొక్క హోస్ట్ భాగం యొక్క రుణాలు తీసుకునే సౌకర్యాన్ని మరియు నెట్ వర్క్ ఇన్ నెట్ వర్క్, సబ్నెట్ అని పిలుస్తారు. సబ్ నెట్టిని ఉపయోగించడం ద్వారా, చిన్న నెట్వర్క్ల చిన్న నెట్వర్క్లను కలిగి ఉండటానికి ఒక సింగిల్ క్లాస్ A IP చిరునామాను ఉపయోగించవచ్చు, ఇది మెరుగైన నెట్వర్క్ నిర్వహణ సామర్థ్యాలను అందిస్తుంది.

Class A Subnets

In Class A, only the first octet is used as Network identifier and rest of three octets are used to be assigned to Hosts (i.e. 16777214 Hosts per Network). To make more subnet in Class A, bits from Host part are borrowed and the subnet mask is changed accordingly.

తరగతి A లో, మొదటి ఆక్టెట్ మాత్రమే నెట్వర్క్ ఐడెంటిఫైయర్గా ఉపయోగించబడుతుంది మరియు మిగిలిన మూడు ఆక్టేట్లు హోస్ట్లకు

కేటాయించబడ్డాయి (అనగా. నెట్వర్క్కు 16777214 హోస్ట్లు). క్లాస్ A లో మరింత సబ్నెట్ను చేయడానికి, హోస్ట్ పార్ట్ నుండి బిట్స్ అరువు తీసుకోబడి, సబ్నెట్ మాస్క్ అనుగుణంగా మార్చబడుతుంది.

For example, if one MSB (Most Significant Bit) is borrowed from host bits of second octet and added to Network address, it creates two Subnets (2^1=2) with (2^{23}-2) 8388606 Hosts per Subnet.

ఉదాహరణకు, ఒక MSB (చాలా ముఖ్యమైన బిట్) రెండవ ఆక్టెట్ యొక్క హోస్ట్ బిట్స్ నుండి స్వీకరించబడి, నెట్వర్క్ చిరునామాకు జోడించబడితే, సబ్నెట్కు 8388606 హోస్ట్లు (223-2) తో రెండు సబ్నెట్లు (21 = 2) ను సృష్టిస్తుంది.

The Subnet mask is changed accordingly to reflect subnetting.
ఉపనెట్మెంట్ను ప్రతిబింబించేలా సబ్నెట్ ముసుగు మార్చబడింది.

In case of subnetting too, the very first and last IP address of every subnet is used for Subnet Number and Subnet Broadcast IP address respectively. Because these two IP addresses cannot be assigned to hosts, sub-netting cannot be implemented by using more than 30 bits as Network Bits, which provides less than two hosts per subnet.

సబ్ నెట్ స్ట్రింగ్ విషయంలో, సబ్నెట్ నంబర్ మరియు సబ్నెట్ బ్రాడ్కాస్ట్ IP చిరునామా కోసం ప్రతి సబ్ నెట్ యొక్క మొట్టమొదటి మరియు చివరి IP చిరునామాను ఉపయోగిస్తారు. ఈ రెండు IP చిరునామాలను హోస్ట్లకు కేటాయించలేము ఎందుకంటే, నెట్వర్క్ బిట్స్గా 30 బిట్లకు పైగా ఉపబలాలను అమలు చేయడం సాధ్యం కాదు, ఇది సబ్నెట్కు రెండు కంటే తక్కువ హోస్ట్లను అందిస్తుంది.

Class B Subnets

By default, using Classful Networking, 14 bits are used as Network bits providing (2^{14}) 16384 Networks and (2^{16}-2) 65534 Hosts. Class B IP Addresses can be subnetted the same way as Class A addresses, by borrowing bits from Host bits.

డిఫాల్ట్గా, క్లాస్ఫుల్ నెట్వర్కింగ్ని ఉపయోగించి, 14 బిట్లని నెట్వర్క్ బిట్స్గా (214) 16384 నెట్వర్క్స్ మరియు (216-2) 65534 హోస్ట్లకు అందిస్తుంది. క్లాస్ B IP చిరునామాలు క్లాస్ A చిరునామాలను అదే విధంగా ఉపపట్టించబడతాయి, హోస్ట్ బిట్స్ నుండి బిట్స్ అప్పుగా తీసుకుంటారు.

Class C Subnets

Class C IP addresses are normally assigned to a very small size network because it can only have 254 hosts in a network. Given below is a list of all possible combination of subnetted Class B IP address:

తరగతి C IP చిరునామాలను సాధారణంగా చాలా చిన్న పరిమాణ నెట్వర్క్కు కేటాయించారు, ఎందుకంటే ఇది నెట్వర్క్లో 254 హోస్ట్లను మాత్రమే కలిగి ఉంటుంది. క్రింద ఇచ్చిన సబ్ నెట్టెడ్ క్లాస్ B IP చిరునామా యొక్క అన్ని కలయికల జాబితా క్రింద ఇవ్వబడింది:

IPv4 - VLSM

Internet Service Providers may face a situation where they need to allocate IP subnets of different sizes as per the requirement of customer. One customer may ask Class C subnet of 3 IP addresses and another may ask for 10 IPs. For an ISP, it is not feasible to divide the IP addresses into fixed size subnets, rather he may want to subnet the subnets in such a way which results in minimum wastage of IP addresses.

కస్టమర్ అవసరాలకు అనుగుణంగా వేర్వేరు పరిమాణాల్లో ఐపి సబ్ నెట్లను కేటాయించాల్సిన అవసరం ఉన్న పరిస్థితిని ఇంటర్నెట్

సర్వీస్ ప్రొవైడర్లు ఎదుర్కోవచ్చు. ఒక కస్టమర్ 3 IP చిరునామాల క్లాస్ సి సబ్నెట్ను అడగవచ్చు మరియు మరొకటి 10 IP లను అడగవచ్చు. ఒక ISP కోసం, ఐపి చిరునామాలను స్థిర పరిమాణ సబ్ నెట్ లకు విభజించడం సాధ్యం కాదు, బదులుగా అతను సబ్ నెట్ లను సబ్ నెట్ లను కోరుకోవచ్చు, ఇది IP చిరునామాలను కనీస వ్యర్థం చేస్తుంది.

For example, an administrator have 192.168.1.0/24 network. The suffix /24 (pronounced as "slash 24") tells the number of bits used for network address. In this example, the administrator has three different departments with different number of hosts. Sales department has 100 computers, Purchase department has 50 computers, Accounts has 25 computers and Management has 5 computers. In CIDR, the subnets are of fixed size. Using the same methodology the administrator cannot fulfill all the requirements of the network.

ఉదాహరణకు, నిర్వాహకునికి 192.168.1.0/24 నెట్వర్క్ ఉంది. అంతిమ / 24 ("స్లాష్ 24" గా ఉచ్చరిస్తారు) నెట్వర్క్ చిరునామా కోసం ఉపయోగించే బిట్ల సంఖ్యను చెబుతుంది. ఈ ఉదాహరణలో, నిర్వాహకుడికి వేర్వేరు విభాగాలు ఉన్నాయి, వేర్వేరు విభాగాలతో. సేల్స్ విభాగానికి 100 కంప్యూటర్లు, కొనుగోలు విభాగం 50 కంప్యూటర్లు, అకౌంట్స్లె 25 కంప్యూటర్లు, మేనేజ్మెంట్ 5 కంప్యూటర్లు. CIDR లో, సబ్ నెట్ లు స్థిర పరిమాణంలో ఉంటాయి. నిర్వాహకకర్త నెట్వర్క్ యొక్క అన్ని అవసరాలు నెరవేర్చలేని

దే పద్ధతిని వాడటం.

The following procedure shows how VLSM can be used in order to allocate department-wise IP addresses as mentioned in the example.

Step - 1

Make a list of Subnets possible.

Step - 2

Sort the requirements of IPs in descending order (Highest to Lowest).

- Sales 100
- Purchase 50
- Accounts 25
- Management 5

Subnet Mask	Slash Notation	Hosts/Subnet
255.255.255.0	/24	254
255.255.255.128	/25	126
255.255.255.192	/26	62
255.255.255.224	/27	30
255.255.255.240	/28	14
255.255.255.248	/29	6
255.255.255.252	/30	2

Step - 3

Allocate the highest range of IPs to the highest requirement, so let's assign 192.168.1.0 /25 (255.255.255.128) to the Sales department. This IP subnet with Network number 192.168.1.0 has 126 valid Host IP addresses which satisfy the requirement of the Sales department. The subnet mask used for this subnet has 10000000 as the last octet.

అత్యధిక అవసరాలకు IP లను అత్యధికంగా కేటాయించండి, కాబట్టి సేల్స్ విభాగానికి 192.168.1.0 / 25 (255.255.255.128) ని కేటాయించండి. నెట్వర్క్ సంఖ్య 192.168.1.0 తో ఈ IP సబ్ నెట్ 126 సేవా హోస్ట్ IP చిరునామాలు సేల్స్ డిపార్ట్మెంట్ యొక్క అవసరాన్ని సంతృప్తిపరిచేది. ఈ సబ్ నెట్ కోసం ఉపయోగించే ఉపనెట్ ముసుగు గత ఆక్టెట్ గా 10000000 ఉంది.

Step - 4

Allocate the next highest range, so let's assign 192.168.1.128 /26 (255.255.255.192) to the Purchase department. This IP subnet with Network number 192.168.1.128 has 62 valid Host IP Addresses which can be easily assigned to all the PCs of the Purchase department. The subnet mask used has 11000000 in the last octet.

తదుపరి అత్యధిక శ్రేణిని కేటాయించండి, కాబట్టి కొనుగోలు విభాగంకు 192.168.1.128 / 26 (255.255.255.192) కేటాయించండి. నెట్వర్క్ సంఖ్య 192.168.1.128 తో ఈ IP సబ్నెట్ 62 చెల్లుబాటు అయ్యే హోస్ట్ IP చిరునామాలు సులభంగా కొనుగోలు విభాగం యొక్క అన్ని PC లకు కేటాయించబడతాయి. ఉపయోగించిన ఉపనెట్ ముసుగు గత ఆక్టెట్లో 11000000 ఉంది.

Step - 5

Allocate the next highest range, i.e. Accounts. The requirement of 25 IPs can be fulfilled with 192.168.1.192 /27 (255.255.255.224) IP subnet, which contains 30 valid host IPs. The network number of Accounts department will be 192.168.1.192. The last octet of subnet mask is 11100000.
తదుపరి అత్యధిక శ్రేణి కేటాయించండి, అంటే ఖాతాలు. 25 IP ల యొక్క అవసరాన్ని 30 చెల్లుబాటు అయ్యే హోస్ట్ IP లను కలిగి ఉన్న IP సబ్ నెట్ 192.168.1.192 / 27 (255.255.255.224) తో నెరవేర్చవచ్చు. ఖాతా విభాగం యొక్క నెట్వర్క్ సంఖ్య 192.168.1.192 ఉంటుంది. సబ్నెట్ ముసుగు చివరి ఆక్టెట్ 11100000 .

Step - 6

Allocate the next highest range to Management. The Management department contains only 5 computers. The subnet 192.168.1.224 /29 with the Mask 255.255.255.248 has exactly 6 valid host IP addresses. So this can be assigned to Management. The last octet of the subnet mask will contain 11111000.

నిర్వహణకు తదుపరి అత్యధిక శ్రేణిని కేటాయించండి. నిర్వహణ విభాగం కేవలం 5 కంప్యూటర్లు మాత్రమే కలిగి ఉంది. మాస్క్ 255.255.255.248 తో సబ్నెట్ 192.168.1.224 / 29 ఖచ్చితంగా 6 చెల్లుబాటు అయ్యే హోస్ట్ IP చిరునామాలను కలిగి ఉంటుంది. కాబట్టి ఇది నిర్వహణకు కేటాయించబడుతుంది. సబ్ నెట్ ముసుగు చివరి ఆక్టెట్ 11111000 కలిగి ఉంటుంది.

By using VLSM, the administrator can subnet the IP subnet in such a way that least number of IP

addresses are wasted. Even after assigning IPs to every department, the administrator, in this example, is still left with plenty of IP addresses which was not possible if he has used CIDR.

VLSM వుపయోగించి, నిర్వాహకుడు ఐపి సబ్ నెట్ ను సబ్ నెట్ చేస్తే అతి తక్కువ సంఖ్యలో IP చిరునామాలు వృధా అవుతాయి. ప్రతి విభాగానికి IP లను కేటాయించిన తరువాత కూడా, ఈ ఉదాహరణలో, నిర్వాహకుడు ఇంకా ఐపి చిరునామాలను కలిగి ఉన్నాడు, అతను CIDR ను ఉపయోగించినట్లయితే సాధ్యం కాదు.

IPv4 - Reserved Addresses

There are a few reserved IPv4 address spaces which cannot be used on the internet. These addresses serve special purpose and cannot be routed outside the Local Area Network.

ఇంటర్నెట్లో ఉపయోగించలేని కొన్ని ప్రత్యేక IPv4 అడ్రెస్ ఖాళీలను ఉన్నాయి. ఈ చిరునామాలు ప్రత్యేక ప్రయోజనం కోసం ఉపయోగపడుతున్నాయి మరియు స్థానిక ఏరియా నెట్వర్క్ వెలుపల రద్దయింది కాదు.

Private IP Addresses

Every class of IP, (A, B & C) has some addresses reserved as Private IP addresses. These IPs can be used within a network, campus, company and are private to it. These addresses cannot be routed on the Internet, so packets containing these private addresses are dropped by the Routers.

ప్రతి తరగతి ఐపి, (A, B & C) కొన్ని IP చిరునామాలను ప్రైవేట్ IP చిరునామాలుగా కలిగి ఉంది. ఈ IP లను నెట్వర్క్, క్యాంపస్, కంపెనీలో ఉపయోగించుకోవచ్చు మరియు దానికి ప్రైవేట్గా ఉంటాయి. ఈ చిరునామాలను ఇంటర్నెట్లో రద్దీ చేయలేము, కాబట్టి ఈ ప్రైవేటు చిరునామాలను కలిగి ఉన్న ప్యాకెట్లను రూటర్లు చేస్తున్నారు.

In

Class A IP Range	Subnet Mask
10.0.0.0 – 10.255.255.255	255.0.0.0
172.16.0.0 – 172.31.255.255	255.240.0.0
192.168.0.0 – 192.168.255.255	255.255.0.0

order to communicate with the outside world, these IP addresses must have to be translated to some public IP addresses using NAT process, or Web Proxy server can be used.

వెలుపలి ప్రపంచంతో కమ్యూనికేట్ చేయడానికి, ఈ IP చిరునామాలను NAT ప్రాసెస్ను ఉపయోగించి కొన్ని పబ్లిక్ IP చిరునామాలకు అనువదించాలి, లేదా వెబ్ ప్రాక్సీ సర్వర్ని ఉపయోగించవచ్చు.

The sole purpose to create a separate range of private addresses is to control assignment of already-limited IPv4 address pool. By using a private address range within LAN, the requirement of IPv4 addresses has globally decreased significantly. It has also helped delaying the IPv4 address exhaustion.

ప్రత్యేకమైన ప్రైవేట్ చిరునామాలను రూపొందించడానికి ఏకైక ప్రయోజనం, ఇప్పటికే పరిమిత IPv4 చిరునామా పూల్ యొక్క కేటాయింపును నియంత్రించడం. LAN లో ఒక ప్రైవేట్ చిరునామా పరిధిని ఉపయోగించడం ద్వారా, IPv4 చిరునామాల అవసరం ప్రపంచవ్యాప్తంగా గణనీయంగా తగ్గింది. ఇది IPv4 చిరునామా అలసట ఆలస్యం సహాయపడింది.

IP class, while using private address range, can be chosen as per the size and requirement of the

organization. Larger organizations may choose class A private IP address range where smaller organizations may opt for class C. These IP addresses can be further sub-netted and assigned to departments within an organization.

IP తరగతి, ప్రైవేట్ చిరునామా పరిధిని ఉపయోగిస్తున్నప్పుడు, సంస్థ పరిమాణం మరియు అవసరానికి అనుగుణంగా ఎంచుకోవచ్చు. పెద్ద సంస్థలను తరగతి ఎంచుకోవచ్చు ఒక ప్రైవేట్ IP చిరునామా శ్రేణి చిన్న సంస్థలు తరగతి C. కోసం ఎంచుకోవచ్చు పేరు ఈ IP చిరునామాలను మరింత sub-netted మరియు ఒక సంస్థలో విభాగాలు కేటాయించిన చేయవచ్చు.

Loopback IP Addresses

The IP address range 127.0.0.0 – 127.255.255.255 is reserved for loopback, i.e. a Host's self-address, also known as localhost address. This loopback IP address is managed entirely by and within the operating system. Loopback addresses, enable the Server and Client processes on a single system to communicate with each other. When a process creates a packet with destination address as loopback address, the operating system loops it back to itself without having any interference of NIC.

IP చిరునామా శ్రేణి 127.0.0.0 - 127.255.255.255 loopback కోసం కేటాయించబడింది, అనగా హోస్ట్ యొక్క స్వీయ-చిరునామా, స్థానిక హోస్ట్ చిరునామాగా కూడా పిలువబడుతుంది. ఈ లూప్ బాక్ ఐపి చిరునామా ఆపరేటింగ్ సిస్టమ్ ద్వారా మరియు లోపల పూర్తిగా నిర్వహించబడుతుంది. లూప్ బ్యాక్ అడ్రెస్లు, సర్వరు మరియు క్లయింట్ ప్రాసెస్లను ఒకదానితో ఒకటి కమ్యూనికేట్ చేసేందుకు ఒకే వ్యవస్థలో ఎనేబుల్ చెయ్యండి. ఒక ప్రక్రియ లూప్బ్యాక్ చిరునామాగా గమ్య చిరునామాతో ప్యాకెట్ను సృష్టిస్తున్నప్పుడు, ఆపరేటింగ్ సిస్టం NIC యొక్క ఎటువంటి జోక్యం లేకుండా దానిని దానికి వెనక్కి తీసుకుంటుంది.

Data sent on loopback is forwarded by the operating system to a virtual network interface within operating system. This address is mostly used for testing purposes like client-server architecture on a single machine. Other than that, if a host machine can successfully ping 127.0.0.1 or any IP from loopback range, implies that the TCP/IP software stack on the machine is successfully loaded and working.

లూప్ బాక్లో పంపిన డేటా నిర్వహణ వ్యవస్థలో ఒక వర్చ్యువల్ నెట్వర్క్ ఇంటర్ఫేస్కు ఆపరేటింగ్ సిస్టమ్ ద్వారా ఫార్వార్డ్ చేయబడుతుంది. ఈ చిరునామా క్లయింట్-సర్వర్ ఆర్కిటెక్చర్ లాంటి పరీక్ష ప్రయోజనాలకు ఒకే యంత్రంలో ఉపయోగించబడుతుంది. ఇంతే కాకుండా, హోస్ట్ మెషీన్ను 127.0.0.1 లేదా లూప్ బ్యాక్ శ్రేణి నుండి ఏదైనా IP ను విజయవంతంగా పింగ్ చేయగలిగితే, మెషీన్లో TCP / IP సాఫ్ట్వేర్ స్టాక్ విజయవంతంగా లోడ్ చేయబడి పని చేస్తుంది .

Link-local Addresses

In case a host is not able to acquire an IP address from the DHCP server and it has not been assigned any IP address manually, the host can assign itself an IP address from a range of reserved Link-local addresses. Link local address ranges from 169.254.0.0 -- 169.254.255.255.

ఒక హోస్ట్ DHCP సర్వర్ నుండి IP చిరునామాని పొందలేక పోయినట్లయితే మరియు ఇది ఏ ఐపి అడ్రసును మానవీయంగా కేటాయించబడదు, రిజిస్ట్రేటెడ్ లింక్-లోకల్ అడ్రెస్ల నుండి హోస్ట్ IP చిరునామాను కూడా కేటాయించవచ్చు. 169.254.0.0 - 169.254.255.255 నుండి స్థానిక చిరునామా పరిధులను లింక్ చేయండి.

Assume a network segment where all systems are configured to acquire IP addresses from a DHCP

server connected to the same network segment. If the DHCP server is not available, no host on the segment will be able to communicate to any other. Windows (98 or later), and Mac OS (8.0 or later) supports this functionality of self-configuration of Link-local IP address. In absence of DHCP server, every host machine randomly chooses an IP address from the above mentioned range and then checks to ascertain by means of ARP, if some other host also has not configured itself with the same IP address. Once all hosts are using link local addresses of same range, they can communicate with each other.

ఒకే నెట్వర్క్ విభాగానికి అనుసంధానించబడిన DHCP సర్వర్ నుండి IP చిరునామాలను పొందేందుకు అన్ని సిస్టమ్లు కాన్ఫిగర్ చేయబడిన నెట్వర్క్ సెగ్మెంట్ను ఊహించండి. DHCP సర్వర్ అందుబాటులో లేకపోతే, సెగ్మెంట్లో హోస్ట్ ఏదీ కమ్యూనికేట్ చేయలేరు. Windows (98 లేదా తదుపరిది), మరియు Mac OS (8.0 లేదా తదుపరిది) లింక్-లోకల్ IP చిరునామా యొక్క స్వీయ-ఆకృతీకరణ యొక్క ఈ కార్యాచరణకు మద్దతు ఇస్తుంది. DHCP సర్వర్ లేకపోయినా, ప్రతి హోస్ట్ మెషీన్ను యాదృచ్ఛికంగా పైన పేర్కొన్న శ్రేణి నుండి IP చిరునామాను ఎంచుకుని ఆపై ARP ద్వారా తెలుసుకునేందుకు తనిఖీ చేస్తుంది, ఇతర హోస్ట్ కూడా అదే IP చిరునామాతో కాన్ఫిగర్ చేయకపోతే. అన్ని ఆతిథ్య లింక్లు ఒకే పరిధిలో ఉన్న స్థానిక స్థానిక చిరునామాలను ఉపయోగిస్తున్న తర్వాత, వారు ఒకరితో ఒకరు సంప్రదించవచ్చు .

These IP addresses cannot help system to communicate when they do not belong to the same physical or logical segment. These IPs are also not routable.

ఈ భౌతిక లేదా తార్కిక భాగానికి చెందినవి కానప్పుడు ఈ IP చిరునామాలు సంభాషించడానికి వ్యవస్థకు సహాయం చేయలేవు. ఈ IP లు కూడా రూట్ చేయలేవు.

Packet Flow in Network
నెట్వర్క్లో ప్యాకెట్ ఫ్లో

All the hosts in IPv4 environment are assigned unique logical IP addresses. When a host wants to send some data to another host on the network, it needs the physical (MAC) address of the destination host. To get the MAC address, the host an broadcasts ARP message and asks to give the MAC address whoever is the owner of destination IP address. All the hosts on that segment receive the ARP packet, but only the host having its IP matching with the one in the ARP message, replies with its MAC address. Once the sender receives the MAC address of the receiving station, data is sent on the physical media.

IPv4 ఎన్విరాన్మెంట్లోని అతిథేయలన్నీ ఏకైక తార్కిక IP చిరునామాలను కేటాయించబడతాయి. ఒక హోస్ట్ నెట్వర్క్లో మరొక హోస్ట్కు కొంత డేటాను పంపాలని కోరుకున్నప్పుడు, అది గమ్యం హోస్ట్ యొక్క భౌతిక (MAC) చిరునామాకు అవసరం. MAC చిరునామాను పొందడానికి, హోస్ట్ ఒక ARP సందేశాన్ని ప్రసారం చేస్తుంది మరియు గమ్య IP చిరునామా యజమాని అయిన MAC చిరునామాను ఇవ్వాలని అడుగుతుంది. ఆ విభాగంలోని అన్ని హోస్ట్లు ARP ప్యాకెట్ను అందుకుంటాయి, అయితే ARP సందేశంలోని దానితో IP తో సరిపోయే హోస్ట్ మాత్రమే దాని MAC చిరునామాతో ప్రత్యుత్తరం ఇస్తుంది. పంపేవారు స్వీకరించిన స్టేషన్ యొక్క MAC చిరునామాను అందుకున్న తర్వాత, భౌతిక మాధ్యమాల్లో డేటా పంపబడుతుంది.

In case the IP does not belong to the local subnet, the data is sent to the destination by means of Gateway of the subnet. To understand the packet flow, we must first understand the following

components:

IP స్థానిక సబ్నెట్కు చెందినది కాకపోతే, సబ్ నెట్ యొక్క గేట్ వే ద్వారా డేటాను పంపించబడుతుంది. ప్యాకెట్ ప్రవాహాన్ని అర్థం చేసుకోవడానికి, మనము మొదట ఈ కింది భాగాలను అర్థం చేసుకోవాలి:

- **MAC Address:** Media Access Control Address is 48-bit factory hard coded physical address of network device which can uniquely be identified. This address is assigned by device manufacturers.

  MAC అడ్రస్: మీడియా యాక్సెస్ కంట్రోల్ అడ్రస్ అనేది ప్రత్యేకంగా గుర్తించగలిగే నెట్వర్క్ పరికరపు 48-బిట్ ఫ్యాక్టరీ హార్డ్ కోడెడ్ భౌతిక చిరునామా. ఈ చిరునామా పరికరం తయారీదారులచే కేటాయించబడుతుంది .

- **Address Resolution Protocol:** Address Resolution Protocol is used to acquire the MAC address of a host whose IP address is known. ARP is a Broadcast packet which is received by all the host in the network segment. But only the host whose IP is mentioned in ARP responds to it providing its MAC address.

  అడ్రస్ రిజల్యూషన్ ప్రోటోకాల్: అడ్రస్ రిజల్యూషన్ ప్రోటోకాల్, దీని IP చిరునామా తెలిసిన ఒక హోస్ట్ యొక్క MAC చిరునామాను పొందేందుకు ఉపయోగిస్తారు. ARP అనేది బ్రాడ్కాస్ట్ ప్యాకెట్, ఇది నెట్వర్క్ విభాగంలోని అన్ని హోస్ట్ల నుండి పొందబడుతుంది. కానీ ARP లో దీని ఐపిని ప్రస్తావించిన అతిథేయి మాత్రమే దాని MAC అడ్రసును అందిస్తుంది .

- **Proxy Server:** To access the Internet, networks use a Proxy Server which has a public IP assigned. All the PCs request the Proxy Server for a Server on the Internet. The Proxy Server on behalf of the PCS sends the request to the server and when it receives a response from the Server, the Proxy Server forwards it to the client PC. This is a way to control Internet access in computer networks and it helps to implement web based policies.

  ప్రాక్సీ సర్వర్: ఇంటర్నెట్ను ప్రాప్తి చేయడానికి, నెట్వర్కు ఒక పబ్లిక్ IP కేటాయించిన ప్రాక్సీ సర్వర్ను ఉపయోగిస్తాయి. అన్ని PC లు ఇంటర్నెట్లో సర్వర్ కోసం ప్రాక్సీ సర్వర్ని అభ్యర్థిస్తాయి. PCS తరపున ప్రాక్సీ సర్వర్ సర్వర్కు అభ్యర్థనను పంపుతుంది మరియు అది సర్వర్ నుండి ప్రతిస్పందనను అందుకున్నప్పుడు, ప్రాక్సీ సర్వర్ ముందుకు క్లయింట్ PC కి పంపబడుతుంది. ఈ కంప్యూటర్ నెట్వర్క్లలో ఇంటర్నెట్ యాక్సెస్ నియంత్రించడానికి మరియు వెబ్ ఆధారిత విధానాలను అమలు చేయడానికి ఇది సహాయపడుతుంది .

- **Dynamic Host Control Protocol:** DHCP is a service by which a host is assigned IP address from a pre-defined address pool. DHCP server also provides necessary information such as Gateway IP, DNS Server Address, lease assigned with the IP, etc. By using DHCP services, a network administrator can manage assignment of IP addresses at ease.

  హోస్ట్ కంట్రోల్ ప్రోటోకాల్: DHCP అనేది ముందుగా నిర్వచించబడిన చిరునామా పూల్ నుండి హోస్ట్ IP చిరునామా కేటాయించిన ఒక సేవ. DHCP సర్వరు Gateway IP, DNS సర్వర్ అడ్రస్, IP తో కేటాయించిన అద్దె మొదలైనవి అవసరమైన సమాచారాన్ని అందిస్తుంది. DHCP సేవలను ఉపయోగించడం ద్వారా, నెట్వర్క్ నిర్వాహకుడు సులభంగా IP చిరునామాలను కేటాయించవచ్చు .

- **Domain Name System:** It is very likely that a user does not know the IP address of a remote Server he wants to connect to. But he knows the name assigned to it, for example, tutorialpoints.com. When the user types the name of a remote server he wants to connect to, the localhost behind the screens sends a DNS query. Domain Name System is a method to acquire the IP address of the host whose Domain Name is known.

  డొమైన్ నేమ్ సిస్టం: ఒక రిమోట్ సర్వర్ యొక్క IP చిరునామాను అతను కనెక్ట్ చేయాలనుకుంటున్న ఒక యూజర్కు ఇది తెలియదు. కానీ అతను పేరు కేటాయించిన పేరు తెలుసు, ఉదాహరణకు, tutorialpoints.com. వినియోగదారు రకాలను రిమోట్ సర్వర్ పేరుతో అతను అనుసంధానించాలనుకున్నప్పుడు, స్క్రీన్ల వెనుక ఉన్న స్థానిక హోస్ట్ DNS ప్రశ్నని పంపుతుంది. డొమైన్ నేమ్ సిస్టం అనేది హోస్ట్ యొక్క డొమైన్ పేరును పిలుస్తున్న హోస్ట్ యొక్క IP చిరునామాను పొందేందుకు ఒక పద్ధతి.

- **Network Address Translation:** Almost all PCs in a computer network are assigned private IP addresses which are not routable on the Internet. As soon as a router receives an IP packet with a private IP address, it drops it. In order to access servers on public private address, computer networks use an address translation service, which translates between public and private addresses, called Network Address Translation. When a PC sends an IP packet out of a private network, NAT changes the private IP address with public IP address and vice versa.

  నెట్వర్క్ అడ్రెస్ ట్రాన్స్లేషన్: కంప్యూటర్ నెట్వర్క్లో దాదాపు అన్ని PC లు ఇంటర్నెట్లో రూట్ చేయని ప్రైవేట్ IP చిరునామాలు కేటాయించబడతాయి. ఒక రౌటర్ ఒక ఐపి ప్యాకెట్ ను ఒక ప్రైవేట్ IP చిరునామాతో అందుకున్న వెంటనే, అది పడిపోతుంది. పబ్లిక్ ప్రైవేట్ చిరునామాలో సర్వర్లను యాక్సెస్ చేయడానికి, కంప్యూటర్ నెట్వర్కు చిరునామా చిరునామా సేవను ఉపయోగిస్తాయి, ఇది పబ్లిక్ మరియు ప్రైవేట్ అడ్రెస్ల మధ్య అనువదిస్తుంది, నెట్వర్క్ అడ్రెస్ ట్రాన్స్లేషన్ అని పిలుస్తారు. ఒక PC ఒక ప్రైవేట్ నెట్వర్క్ నుండి IP ప్యాకెట్ను పంపుతున్నప్పుడు, NAT ప్రైవేట్ IP చిరునామాను పబ్లిక్ IP చిరునామాతో మారుస్తుంది మరియు వైస్ వెర్సా.

We can now describe the packet flow. Assume that a user wants to access www.TutorialsPoint.com from her personal computer. She has internet connection from her ISP. The following steps will be taken by the system to help her reach the destination website.

ఇప్పుడు మేము ప్యాకెట్ ప్రవాహాన్ని వివరించవచ్చు. ఒక వినియోగదారు తన వ్యక్తిగత కంప్యూటర్ నుండి www.TutorialsPoint.com ను యాక్సెస్ చేయాలని అనుకుంటాను. ఆమె ISP నుండి ఇంటర్నెట్ కనెక్షన్ ఉంది. ఆమె గమ్య వెబ్సైట్ను చేరుకోవడంలో సహాయంగా ఈ క్రింది చర్యలు వ్యవస్థ ద్వారా తీసుకోబడతాయి.

Step: 1 – Acquiring an IP Address (DHCP)

దశ: 1 - IP చిరునామా (DHCP) ను పొందడం

When the user's PC boots up, it searches for a DHCP server to acquire an IP address. For the same, the PC sends a DHCPDISCOVER broadcast which is received by one or more DHCP servers on the subnet and they all respond with DHCPOFFER which includes all the necessary details such as IP, subnet, Gateway, DNS, etc. The PC sends DHCPREQUEST packet in order to request the offered IP address. Finally, the DHCP sends DHCPACK packet to tell the PC that it can keep the IP for some given amount of time that is

known as IP lease.

యూజర్ యొక్క PC బూట్ చేసినప్పుడు, అది ఒక IP చిరునామాను పొందటానికి DHCP సర్వర్ కోసం శోధిస్తుంది. అదే విధంగా, PC ఒక DHCPDISCOVER ప్రసారంను సబ్నెట్లో ఒకటి లేదా అంతకంటే ఎక్కువ DHCP సర్వర్ల ద్వారా అందుతుంది మరియు వారు అన్ని DHCPOFFER తో ప్రతిస్పందించవచ్చు, ఇందులో IP, సబ్నెట్, గేట్వే, DNS మొదలైన అన్ని అవసరమైన వివరాలను కలిగి ఉంటుంది. PC DHCPREQUEST ను పంపుతుంది ఇచ్చిన IP చిరునామాను అభ్యర్థించడానికి ప్యాకెట్. అంతిమంగా, DHCP DHCPACK ప్యాకెట్ను PC కి పంపుతుంది, ఇది ఐపి లీజ్ అని పిలవబడే కొంత సమయం కొరకు ఐపిని ఉంచుతుంది .

Alternatively, a PC can be assigned an IP address manually without taking any help from DHCP server. When a PC is well configured with IP address details, it can communicate other computers all over the IP enabled network.

ప్రత్యామ్నాయంగా, DHCP సర్వర్ నుండి ఎలాంటి సహాయం చేయకుండా ఒక PC ను మానవీయంగా IP చిరునామాను కేటాయించవచ్చు. ఐపి అడ్రెస్ వివరాలతో ఒక PC చక్కగా అమర్చినప్పుడు, ఐపి-ఎనేబుల్ నెట్వర్క్లో ఇతర కంప్యూటర్లను కమ్యూనికేట్ చేయవచ్చు.

Step: 2 – DNS Query

When a user opens a web browser and types www.tutorialpoints.com which is a domain name and a PC does not understand how to communicate with the server using domain names, then the PC sends a DNS query out on the network in order to obtain the IP address pertaining to the domain name. The pre-configured DNS server responds to the query with IP address of the domain name specified.

దశ: 2 - DNS ప్రశ్న

వినియోగదారుడు వెబ్ బ్రౌజరు మరియు రకాలు www.tutorialpoints.com ను తెరిచినప్పుడు డొమైస్ డొమైస్ పేర్లను ఉపయోగించి సర్వర్తో ఎలా కమ్యూనికేట్ చేయాలో అర్థం చేసుకోలేరు, అప్పుడు పిసి నెట్వర్క్లో ఒక DNS ప్రశ్నను నెట్వర్క్లో పంపుతుంది. డొమైస్ పేరుకు సంబంధించిన IP చిరునామా. నిర్దేశించిన DNS సర్వర్ పేర్కొన్న డొమైస్ పేరు యొక్క IP చిరునామాతో ప్రశ్నకు స్పందిస్తుంది.

Step: 3 – ARP Request

The PC finds that the destination IP address does not belong to his own IP address range and it has to forward the request to the Gateway. The Gateway in this scenario can be a router or a Proxy Server. Though the Gateway's IP address is known to the client machine but computers do not exchange data on IP addresses, rather they need the machine's hardware address which is Layer-2 factory coded MAC address. To obtain the MAC address of the Gateway, the client PC broadcasts an ARP request saying "Who owns this IP address?" The Gateway in response to the ARP query sends its MAC address. Upon receiving the MAC address, the PC sends the packets to the Gateway.

దశ: 3 - ARP అభ్యర్థన

గమ్య IP చిరునామా తన సొంత IP చిరునామా శ్రేణికి చెందినదని PC గుర్తించింది మరియు ఇది గేట్వేకు అభ్యర్థనను ముందుకు పంపాలి. ఈ సందర్భంలో గేట్వే ఒక రౌటర్ లేదా ప్రాక్సీ సర్వర్ కావచ్చు. గేట్ వే యొక్క IP చిరునామా క్లయింట్ యంత్రానికి తెలిసినప్పటికీ కంప్యూటర్లు IP చిరునామాలపై డేటాను మార్పిడి చేయవు, బదులుగా వారికి లేయర్ -

2 ఫ్యాక్టరీ MAC చిరునామా కోడ్ చేయబడిన యంత్రం యొక్క హార్డ్వేర్ చిరునామా అవసరం. Gateway యొక్క MAC చిరునామాను పొందటానికి, క్లయింట్ PC ఒక ARP అభ్యర్థనను ప్రసారం చేస్తుంది
"ఈ IP చిరునామాను ఎవరు కలిగి ఉన్నారు?" ARP ప్రశ్నకు ప్రతిస్పందనగా గేట్వే దాని MAC చిరునామాను పంపుతుంది. MAC చిరునామాను స్వీకరించిన తర్వాత, PC ప్యాకెట్లను గేట్ వేకి పంపుతుంది.

An IP packet has both source and destination addresses and it connects the host with a remote host logically, whereas MAC addresses help systems on a single network segment to transfer actual data. It is important that source and destination MAC addresses change as they travel across the Internet (segment by segment) but source and destination IP addresses never change.

ఒక IP ప్యాకెట్ మూలం మరియు గమ్య చిరునామాలు రెండింటినీ కలిగి ఉంటుంది మరియు హోస్ట్ రిమోట్ హోస్ట్తో తార్కికంగా కనెక్ట్ చేస్తుంది, అయితే అసలు డేటాను బదిలీ చేయడానికి ఒకే నెట్వర్క్ విభాగంలో MAC చిరునామాలు సహాయపడతాయి. మూలం మరియు గమ్యం MAC చిరునామాలను వారు ఇంటర్నెట్లో (సెగ్మెంట్ ద్వారా సెగ్మెంట్) ప్రయాణించేటప్పుడు మారతాయి, అయితే మూలం మరియు గమ్యస్థాన IP చిరునామాలు ఎప్పుడూ మారవు.

Medium Access Control (MAC) Protocol
మధ్యస్థ యాక్సెస్ కంట్రోల్ (MAC) ప్రోటోకాల్

MAC is a Layer 2 protocol and it resides between Physical Layer (L1) and RLC. The internal configuration of MAC is done by the RRC layer (L3). The interface between PHY and MAC are the transport channels where as the interface between RLC and MAC are the logical channels. MAC provides services to both User plane as well as Control plane. MAC takes care of circuit switched as well as packet switch traffic and signalling traffic as well.

MAC ఒక పొర 2 ప్రోటోకాల్ మరియు ఇది శారీరక లేయర్ (L1) మరియు RLC మధ్య నివసిస్తుంది. MAC యొక్క అంతర్గత ఆకృతీకరణ RRC పొర (L3) చేత చేయబడుతుంది. PHY మరియు MAC ల మధ్య ఉన్న ఇంటర్ఫేస్ అనేది రవాణా మార్గాలను RLC మరియు MAC ల మధ్య ఇంటర్ఫేస్ లాజికల్ ఛానల్స్ గా చెప్పవచ్చు. MAC వాడుకరి విమానం మరియు నియంత్రణ విమానం రెండింటికీ సేవలను అందిస్తుంది. MAC సర్క్యూట్ అలాగే అలాగే ప్యాకెట్ స్విచ్ ట్రాఫిక్ మరియు సిగ్నలింగ్ ట్రాఫిక్ అలాగే జాగ్రత్త పడుతుంది.

One important thing to remember is that the MAC is not symmetrical protocol. It is different in UL and DL.

గుర్తుంచుకోవడానికి ఒక ముఖ్యమైన విషయం ఏమిటంటే MAC సున్నితమైన ప్రోటోకాల్ కాదు. ఇది UL మరియు DL లో భిన్నంగా ఉంటుంది.

MAC Services

MAC sublayer provides following services to the upper layers:

MAC సేవలు MAC సబ్లేయర్ ఎగువ పొరలకు క్రింది సేవలను అందిస్తుంది

- Data Transfer: This service provides unacknowledged transfer of MAC SDU's between peer MAC entities.

డేటా బదిలీ: ఈ సేవ MAC SDU యొక్క పీర్ MAC ఎంటిటీల మధ్య గుర్తించబడని బదిలీని అందిస్తుంది.

- Reallocation of radio resources and MAC parameters: On request by RRC, MAC can change the identity of the UE, change the transport format set, change the transport channel type, etc.

రేడియో వనరుల మరియు MAC పారామితులను పునఃప్రారంభించడం: RRC ద్వారా అభ్యర్థనపై, MAC UE యొక్క గుర్తింపును మార్చవచ్చు, రవాణా ఆకృతి సెట్ను మార్చి, రవాణా ఛానల్ రకాన్ని మార్చవచ్చు .

- Reporting of Measurements: Traffic volume measurements are performed in MAC and reported to RRC

కొలతల రిపోర్టింగ్: ట్రాఫిక్ వాల్యూమ్ కొలతలు MAC లో నిర్వహించబడతాయి మరియు RRC కి నివేదించబడతాయి

MAC Functions

MAC Functions include:

MAC విధులు ఉన్నాయి:

- Mapping between logical channels and transport channels
- తార్కిక మార్గాల మరియు రవాణా మార్గాల మధ్య మ్యాపింగ్
- Selection of appropriate Transport Format for each Transport channel depending on instantaneous source rate. Given the Transport Format Combination Set assigned by RRC, MAC selects the appropriate transport format within an assigned transport format set for each active transport channel depending on source rate. The control of transport formats ensures efficient use of transport channels.

  ప్రతి రవాణా ఛానల్ కోసం తగిన ట్రాన్స్పోర్ట్ ఫార్మాట్ యొక్క ఎంపిక తక్షణ మూలం రేట్ ఆధారంగా. RRC చేత సమర్పించబడిన ట్రాన్స్ఫార్మ్ ఫార్మాట్ కాంబినేషన్ సెట్ ద్వారా, MAC సోర్స్ రేట్పై ఆధారపడి ప్రతి క్రియాశీల రవాణా ఛానెల్కు సెట్ చేయబడిన ఒక రవాణా రవాణా ఆకృతిలో తగిన రవాణా ఆకృతిని ఎంపిక చేస్తుంది. రవాణా ఆకృతుల నియంత్రణ రవాణా మార్గాలను సమర్థవంతంగా ఉపయోగించుకుంటుంది .

- Priority handling between data flows of one UE. When selecting between the Transport Format Combinations in the given Transport Format Combination Set, priorities of the data flows to be mapped onto the corresponding Transport Channels can be taken into account.

  ఒక UE యొక్క డేటా ప్రవాహాల మధ్య ప్రాధాన్యత నిర్వహణ. ఇచ్చిన ట్రాన్స్పోర్టేషన్ ఫార్మాట్ కాంబినేషన్ సెట్లో ట్రాన్స్పోర్ట్ ఫార్మాట్ కాంబినేషన్ల మధ్య ఎంచుకోవడం ఉన్నప్పుడు, సంబంధిత రవాణా ఛానళ్లలో డేటా యొక్క ప్రాధాన్యతలను మ్యాప్ చేయబడవచ్చు.

- Priority handling between UEs by means of dynamic scheduling. In order to utilise the spectrum resources efficiently for bursty transfer, a dynamic scheduling function may be applied. MAC realises priority handling on common and shared transport channels.

  డైనమిక్ షెడ్యూలింగ్ ద్వారా UE ల మధ్య ప్రాధాన్యత నిర్వహణ. విపరీతమైన బదిలీ కోసం స్పెక్ట్రం వనరులను సమర్థవంతంగా ఉపయోగించేందుకు, ఒక డైనమిక్ షెడ్యూలింగ్ ఫంక్షన్ వర్తించవచ్చు. MAC సాధారణ మరియు భాగస్వామ్య రవాణా మార్గాలపై ప్రాధాన్యత నిర్వహణను గుర్తిస్తుంది .

- Identification of UEs on common transport channels. When a particular UE is addressed on a common downlink channel, or when a UE is using the RACH, there is a need for inband identification of the UE. Since the MAC layer handles the access to, and multiplexing onto, the transport channels, the identification functionality is naturally also placed in MAC.

సాధారణ రవాణా మార్గాలపై UE లను గుర్తించడం. ఒక ప్రత్యేకమైన UE సాధారణ డౌన్లింక్ ఛానెల్లో ప్రసంగించబడినప్పుడు లేదా UE RACH ను ఉపయోగిస్తున్నప్పుడు, UE యొక్క ఇన్బ్యాండ్ ఐడెంటిఫికేషన్ అవసరం ఉంది. MAC లేయర్ యాక్సెస్ నిర్వహిస్తుంది కాబట్టి, రవాణా చానెళ్లకు, మల్టీప్లాక్ చేయడం వలన, గుర్తింపు కార్యాచరణ కూడా సహజంగా MAC లో ఉంచబడుతుంది.

- Multiplexing/demultiplexing of upper layer PDUs into/from transport blocks delivered to/from the physical layer on common transport channels. MAC should support service multiplexing for common transport channels, since the physical layer does not support multiplexing of these channels.

  ఎగువ లేయర్ PDU ల యొక్క మల్టిప్లెక్స్ / డెమల్టిప్లెలింగ్ సాధారణ రవాణా మార్గాలపై భౌతిక పొరకు / నుండి పంపిణీ చేయబడిన రవాణా బ్లాక్ల నుండి. భౌతిక పొర ఈ చానెల్స్ యొక్క మల్టీప్లెక్స్కు మద్దతు ఇవ్వని కారణంగా, MAC సాధారణ రవాణా ఛానెల్లకు సేవ మల్టీప్లెక్స్కు మద్దతు ఇవ్వాలి.

- Multiplexing/demultiplexing of upper layer PDUs into/from transport block sets delivered to/from the physical layer on dedicated transport channels. The MAC allows service multiplexing for dedicated transport channels. This function can be utilised when several upper layer services (e.g. RLC instances) can be mapped efficiently on the same transport channel. In this case the identification of multiplexing is contained in the MAC protocol control information.
  ఎగువ లేయర్ PDU ల యొక్క మల్టీప్లెక్స్ / డెమల్టిప్లెక్టింగ్ రవాణా బ్లాక్ల సెట్లలో / నుండి భౌతిక పొరకు ప్రత్యేక రవాణా మార్గాలపైకి పంపబడతాయి. MAC ప్రత్యేక రవాణా మార్గాల కోసం సేవ మల్టీప్లెక్స్ను అనుమతిస్తుంది. అనేక ఎగువ పొర సేవలు ఉన్నప్పుడు ఈ ఫంక్షన్ ఉపయోగించవచ్చు
  (ఉదా. RLC సందర్భాల్లో) అదే రవాణా ఛానల్లో సమర్థవంతంగా మ్యాప్ చేయవచ్చు. ఈ సందర్భంలో మల్టిప్లెక్స్ను గుర్తించడం MAC ప్రోటోకాల్ నియంత్రణ సమాచారంలో ఉంటుంది.

- Traffic volume measurement. Measurement of traffic volume on logical channels and reporting to RRC. Based on the reported traffic volume information, RRC performs transport channel switching decisions.
  ట్రాఫిక్ వాల్యూమ్ కొలత. తార్కిక చానెళ్లలో ట్రాఫిక్ వాల్యూమ్ యొక్క కొలత మరియు RRC కు నివేదించడం. నివేదించబడిన ట్రాఫిక్ వాల్యూమ్ సమాచారం ఆధారంగా, RRC రవాణా ఛానల్ మార్పిడి నిర్ణయాలు నిర్వహిస్తుంది.
- Transport Channel type switching. Execution of the switching between common and dedicated transport channels based on a switching decision derived by RRC.
  రవాణా ఛానల్ రకం మార్పిడి. RRC నుండి తీసుకున్న ఒక స్విచింగ్ నిర్ణయం ఆధారంగా సాధారణ మరియు అంకితమైన రవాణా మార్గాల మధ్య మారుతున్న అమలు.
- Ciphering. This function prevents unauthorised acquisition of data. Ciphering is performed in the MAC layer for transparent RLC mode.
  Ciphering. ఈ ఫంక్షన్ డేటా యొక్క అనధికారిక సేకరణను నిరోధిస్తుంది. పారదర్శక RLC మోడ్ కోసం MAC పొరలో కుఫెర్ను నిర్వహిస్తారు.

- Access Service Class selection for RACH and CPCH transmission. The RACH resources (i.e. access slots and preamble signatures for FDD, timeslot and channelisation code for TDD) and CPCH

resources (i.e. access slots and preamble signatures for FDD only) may be divided between different Access Service Classes in order to provide different priorities of RACH and CPCH usage. In addition it is possible for more than one ASC or for all ASCs to be assigned to the same access slot/signature space. Each access service class will also have a set of back-off parameters associated with it, some or all of which may be broadcast by the network. The MAC function applies the appropriate back-off and indicates to the PHY layer the RACH and CPCH partition associated to a given MAC PDU transfer.

RACH మరియు CPCH ట్రాన్స్మిషన్ కోసం యాక్సెస్ సర్వీస్ క్లాస్ ఎంపిక. RACH వనరులు (అనగా యాక్సెస్ స్లాట్లు మరియు TDD కొరకు FDD, సమయము మరియు ఛానలైజేషన్ కోడ్) మరియు CPCH వనరులు (ఉదాహరణకు యాక్సెస్ స్లాట్లు మరియు FDD కొరకు మాత్రమే ముందుగా సంతకాలు) వివిధ యాక్సెస్ సర్వీస్ క్లాస్ల మధ్య విభజించబడవచ్చు. మరియు CPCH వినియోగం. అదనంగా ఇది ఒకటి కంటే ఎక్కువ ASC లేదా అన్ని ASC లకు ఒకే యాక్సెస్ స్లాట్ / సంతకం స్థలానికి కేటాయించబడటం సాధ్యమవుతుంది. ప్రతి ప్రాప్తి సేవ తరగతికి దానితో అనుబంధించబడిన బ్యాక్ ఆఫ్ పారామితులను కలిగి ఉంటుంది, కొన్ని లేదా మొత్తం నెట్వర్క్ ద్వారా ప్రసారం కావచ్చు. MAC ఫంక్షన్ తగిన బ్యాక్ ఆఫ్ను వర్తిస్తుంది మరియు ఇవ్వబడిన MAC PDU బదిలీకు అనుబంధించబడిన RACH మరియు CPCH విభజన PHY కొరకు సూచిస్తుంది .

Channel Structure

ఛానెల్ నిర్మాణం

Before discussing anything further, we should look at the channel structures for Layer 1, MAC and RLC. The Transport Channels are interface between MAC and Layer 1, while Logical Channels are interface between MAC and RLC.

ఇంకా ఏదైనా చర్చించటానికి ముందు, మేము లేయర్ 1, MAC మరియు RLC కోసం ఛానల్ నిర్మాణాలను చూడాలి. MAC మరియు లేయర్ 1 మధ్య ట్రాన్స్పోర్ట్ ఛానలు ఇంటర్ఫేస్, లాజికల్ ఛానలు MAC మరియు RLC ల మధ్య అంతర్ముఖంగా ఉంటాయి .

Transport channels can be further subdivided into Common Transport Channels (where there is need for inband identification of the UEs when particular UEs are addressed); and dedicated transport channels (where the UEs are identified by the physical channel, i.e. code and frequency for FDD and code, time slot and frequency for TDD).

కామన్ ట్రాన్స్పోర్టేషన్ ఛానళ్లలో రవాణా చానెళ్లను కూడా ఉపవిభజన చేయవచ్చు (UE లలో అంతర్గతంగా గుర్తించబడే UE లలో అంతర్గతంగా గుర్తించవలసిన అవసరం ఉంది); మరియు అంకితమైన రవాణా చానెల్స్ (UE లు భౌతిక ఛానల్ ద్వారా గుర్తించబడతాయి, అంటే FDD మరియు సంకేతం, కోడ్ మరియు ఫ్రీక్వెన్సీ, సమయం స్లాట్ మరియు ఫ్రీక్వెన్సీ కోసం TDD కోసం).

Common transport channel types are:

సాధారణ రవాణా ఛానల్ రకాలు:

- Random Access Channel (RACH): A contention based uplink channel used for transmission of relatively small amounts of data, e.g. for initial access or non-real-time dedicated control or traffic data.

రాండమ్ యాక్సెస్ ఛానల్ (RACH): అతి తక్కువ పరిమాణాత్మక డేటాను ప్రసారం చేయడానికి ఉపయోగించే వివాదం ఆధారిత అప్లింక్ ఛానల్, ఉదా. ప్రారంభ ప్రాప్తి లేదా నిజ-సమయ అంకితమైన నియంత్రణ లేదా ట్రాఫిక్ డేటా కోసం .

- Common Packet Channel (CPCH): A contention based channel used for transmission of bursty data traffic. This channel only exists in FDD mode and only in the uplink direction. The common packet channel is shared by the UEs in a cell and therefore, it is a common resource. The CPCH is fast power controlled.
  సాధారణ ప్యాకెట్ ఛానల్ (CPCH): పగిలిపోయే డేటా ట్రాఫిక్ ప్రసారం కోసం ఉపయోగించే వివాదాస్పద ఆధారిత ఛానల్. ఈ ఛానల్ FDD రీతిలో మాత్రమే ఉంటుంది మరియు అప్లింక్ దిశలో మాత్రమే ఉంటుంది. సాధారణ పాకెట్ ఛానెల్ ఒక సెల్ లో UE లచే పంచుకుంటుంది మరియు అందువలన ఇది ఒక సాధారణ వనరు. CPCH వేగంగా శక్తిని నియంత్రిస్తుంది .

- Forward Access Channel (FACH): Common downlink channel without closed-loop power control used for transmission of relatively small amount of data.
  ఫార్వర్డ్ యాక్సెస్ ఛానల్ (FACH): సాపేక్షంగా తక్కువ మొత్తం డేటాను ప్రసారం చేయడానికి ఉపయోగించే మూసి-లూప్ పవర్ నియంత్రణ లేకుండా సాధారణ డౌన్లింక్ ఛానల్ .

- Downlink Shared Channel (DSCH): A downlink channel shared by several UEs carrying dedicated control or traffic data.
- డౌన్లింక్ షెడ్యూల్డ్ ఛానల్ (DSCH): ఒక డిల్లింక్ ఛానల్ అంకితమైన నియంత్రణ లేదా ట్రాఫిక్ డేటాను కలిగి ఉన్న అనేక UE ల ద్వారా భాగస్వామ్యం చేయబడింది.

- Uplink Shared Channel (USCH): An uplink channel shared by several UEs carrying dedicated control or traffic data, used in TDD mode only.

  అప్లైడ్ షేర్డ్ ఛానల్ (USCH): అండర్లింక్ ఛానల్ అనేక UE లచే అంకితమైన నియంత్రణ లేదా ట్రాఫిక్ డేటాను కలిగి ఉంది, ఇది TDD మోడ్లో మాత్రమే ఉపయోగించబడుతుంది .
- Broadcast Channel (BCH): A downlink channel used for broadcast of system information into an entire cell.
  బ్రాడ్కాస్ట్ ఛానల్ (BCH): సిస్టమ్ సమాచారాన్ని ప్రసారం చేయడానికి ఒక డెల్ లింక్ ఛానల్ మొత్తం సెల్ లోకి ఉపయోగించబడుతుంది .
- Paging Channel (PCH): A downlink channel used for broadcast of control information into an entire cell allowing efficient UE sleep mode procedures. Currently identified information types are paging and notification. Another use could be UTRAN notification of change of BCCH information.

  పేజింగ్ ఛానల్ (PCH): సమర్థవంతమైన UE నిద్ర మోడ్ విధానాలను అనుమతించే మొత్తం కణంలో నియంత్రణ సమాచారాన్ని ప్రసారం చేయడానికి ఉపయోగించే డౌన్లింక్ ఛానెల్. ప్రస్తుతం గుర్తించబడిన సమాచార రకాలు పేజింగ్ మరియు నోటిఫికేషన్. మరొక ఉపయోగం BCCH సమాచారం యొక్క మార్పు UTRAN నోటిఫికేషన్ కావచ్చు .
- High Speed Downlink Shared Channel (HS-DSCH): A downlink channel shared between UEs by allocation of individual codes, from a common pool of codes assigned for the channel.

హై స్పీడ్ డౌన్ లింక్ షెడ్డ్ ఛానల్ (HS-DSCH): ఛానల్ కోసం కేటాయించిన కోడ్ల యొక్క సాధారణ పూల్ నుండి, వ్యక్తిగత సంకేతాల కేటాయింపు ద్వారా UE ల మధ్య డౌన్లింక్ ఛానెల్ భాగస్వామ్యం చేయబడింది.

Dedicated transport channel types are:
అంకితమైన రవాణా ఛానల్ రకాలు:

- Dedicated Channel (DCH): A channel dedicated to one UE used in uplink or downlink.

అంకితమైన ఛానల్ (DCH): అప్లింక్ లేదా డౌన్ లింక్లో ఉపయోగించిన ఒక UE కు అంకితమైన ఛానెల్.

A general classification of logical channels is into two groups; Control Channels (for the transfer of control plane information) and Traffic Channels (for the transfer of user plane information).
తార్కిక చానెల్స్ యొక్క ఒక సాధారణ వర్గీకరణ రెండు సమూహాలుగా ఉంటుంది ; కంట్రోల్ ఛానెల్లు (నియంత్రణ విమానం సమాచారం బదిలీ కోసం) మరియు ట్రాఫిక్ ఛానల్స్ (యూజర్ విమానం సమాచారం బదిలీ కోసం).

Control Channels:

- Broadcast Control Channel (BCCH): A downlink channel for broadcasting system control information.
- బ్రాడ్కాస్ట్ కంట్రోల్ ఛానల్ (BCCH): ప్రసార సిస్టమ్ నియంత్రణ సమాచారం కోసం డౌన్లింక్ ఛానల్.
- Paging Control Channel (PCCH): A downlink channel that transfers paging information. This channel is used when the network does not know the location cell of the UE, or, the UE is in the cell connected state (utilising UE sleep mode procedures).
- పేజింగ్ కంట్రోల్ ఛానల్ (PCCH): పేజింగ్ సమాచారాన్ని బదిలీ చేసే డౌలింక్ ఛానల్. UE యొక్క స్థాన సెల్ను నెట్వర్క్ తెలియదు, లేదా UE కణాల కనెక్ట్ అయిన రాష్ట్రంలో (UE నిద్ర మోడ్ విధానాలను ఉపయోగించడం) ఈ ఛానెల్ ఉపయోగించబడుతుంది.
- Common Control Channel (CCCH): Bi-directional channel for transmitting control information between network and UEs. This channel is commonly used by the UEs having no RRC connection with the network and by the UEs using common transport channels when accessing a new cell after cell reselection.
  సాధారణ నియంత్రణ ఛానల్ (CCCH): నెట్వర్క్ మరియు UE ల మధ్య నియంత్రణా సమాచారాన్ని బదిలీ చేయడానికి బి-డైరెక్షనల్ ఛానల్. ఈ ఛానల్ సాధారణంగా UR లతో నెట్వర్క్ తో మరియు UE ల ద్వారా UE లను ఉపయోగించుకుంటుంది, ఇది కణ రిసెప్షన్ తర్వాత కొత్త సెల్ను ప్రాప్యత చేస్తున్నప్పుడు సాధారణ రవాణా మార్గాలను ఉపయోగిస్తుంది.
- Dedicated Control Channel (DCCH): A point-to-point bi-directional channel that transmits dedicated control information between a UE and the network. This channel is established through RRC connection setup procedure.
  అంకితమైన కంట్రోల్ ఛానల్ (DCCH): UE మరియు నెట్వర్క్ మధ్య అంకితమైన నియంత్రణ సమాచారాన్ని ప్రసారం చేసే పాయింట్ టు పాయింట్ ద్వి-డైరెక్షనల్ ఛానెల్. ఈ ఛానెల్ RRC కనెక్షన్ సెటప్ విధానం ద్వారా స్థాపించబడింది.
- Shared Channel Control Channel (SHCCH): Bi-directional channel that transmits control information for uplink and downlink shared channels between network and UEs. This channel is for TDD only.
  భాగస్వామ్యం చేయబడిన ఛానల్ కంట్రోల్ ఛానల్ (SHCCH): నెట్వర్క్ మరియు UE ల మధ్య అప్లింక్ మరియు డౌన్ లింక్ షేర్ ఛానెల్ల సమాచారాన్ని బదిలీ చేసే ద్వి-డైరెక్షనల్ ఛానెల్. ఈ ఛానెల్ TDD మాత్రమే. కోసం నియంత్రణ

Internet Protocol v6 (IPv6)

Internet Protocol version 6 (IPv6) is the latest revision of the Internet Protocol (IP) and the first version of the protocol to be widely deployed. IPv6 was developed by the Internet Engineering Task Force (IETF) to deal with the long-anticipated problem of IPv4 address exhaustion. This tutorial will help you in understanding IPv6 and its associated terminologies along with appropriate references and examples.

ఇంటర్నెట్ ప్రోటోకాల్ 6 (IPv6) అనేది ఇంటర్నెట్ ప్రోటోకాల్ (IP) యొక్క తాజా పునర్విమర్శ మరియు విస్తృతంగా అమలు చేయబడే ప్రోటోకాల్ యొక్క మొదటి వెర్షన్. IPv4 అడ్రెస్ అలసట యొక్క పొడవైన ఎదురుచూస్తున్న సమస్యను పరిష్కరించేందుకు ఇంటర్నెట్ ఇంజనీరింగ్ టాస్క్ ఫోర్స్ (IETF) చే IPv6 ను అభివృద్ధి చేసింది. ఈ ట్యుటోరియల్ మీకు IPv6 మరియు దాని అనుబంధిత పదజాలాన్ని సరైన సూచనలతో మరియు ఉదాహరణలుగా అర్థం చేసుకోవడంలో మీకు సహాయపడుతుంది .

Internet Protocol version 6 is a new addressing protocol designed to incorporate all the possible requirements of future Internet known to us as Internet version 2. This protocol as its predecessor IPv4, works on the Network Layer (Layer-3). Along with its offering of an enormous amount of logical address space, this protocol has ample features to which address the shortcoming of IPv4.
ఇంటర్నెట్ ప్రోటోకాల్ సంస్కరణ 6 ఇంటర్నెట్ సంస్కరణ 2 గా మాకు తెలిసిన భవిష్యత్ ఇంటర్నెట్ యొక్క అన్ని అవసరాలను పొందుపరచడానికి రూపొందించిన ఒక నూతన చిరునామా ప్రోటోకాల్. దాని ప్రోటోకాల్ IPv4 వలె, నెట్వర్క్ లేయర్ (లేయర్ -3) లో పనిచేస్తుంది. అపరిమితమైన లాజికల్ అడ్రస్ స్థలాన్ని అందించడంతో పాటు, ఈ ప్రోటోకాల్ IPv4 యొక్క లోపాలను పరిష్కరించడానికి సరిపోయే లక్షణాలను కలిగి ఉంది.

Why New IP Version?
కొత్త IP సంస్కరణ ఎందుకు?

So far, IPv4 has proven itself as a robust routable addressing protocol and has served us for decades on its best-effort-delivery mechanism. It was designed in the early 80's and did not get any major change afterward. At the time of its birth, Internet was limited only to a few universities for their research and to the Department of Defense. IPv4 is 32 bits long and offers around 4,294,967,296 (2^{32}) addresses. This address space was considered more than enough that time. Given below are the major points that played a key role in the birth of IPv6:

ఇప్పటివరకు, IPv4 ఒక బలమైన రౌండబుల్ అడ్రసింగ్ ప్రోటోకాల్గా నిరూపించబడింది మరియు దాని ఉత్తమ-ప్రయత్న-డెలివరీ యంత్రాంగాన్ని దశాబ్దాలుగా మాకు అందించింది. 80 ల ప్రారంభంలో దీనిని రూపొందించారు, తర్వాత ఏ పెద్ద మార్పులూ రాలేదు. దాని జన్మ సమయంలో, ఇంటర్నెట్ వారి పరిశోధన మరియు రక్షణ శాఖ కోసం కొన్ని విశ్వవిద్యాలయాలు మాత్రమే పరిమితం చేయబడింది. IPv4 32 బిట్స్ పొడవు మరియు 4,294,967,296 (232) చిరునామాలను అందిస్తుంది. ఈ అడ్రస్ స్థలం తగినంత సమయం కంటే ఎక్కువగా పరిగణించబడింది. IPv6 యొక్క జన్మలో ముఖ్య పాత్ర పోషించిన ప్రధాన అంశాల క్రింద ఇవ్వబడింది :

- Internet has grown exponentially and the address space allowed by IPv4 is saturating. There is a requirement to have a protocol that can satisfy the needs of future Internet addresses that is expected to grow in an unexpected manner.

ఇంటర్నెట్ విస్తృతంగా పెరిగింది మరియు IPv4 ద్వారా అనుమతించబడిన చిరునామా స్థలం సంతృప్తమైంది. ఊహించని రీతిలో పెరగబోయే భవిష్యత్ ఇంటర్నెట్ చిరునామాల అవసరాలను సంతృప్తిపరచగల ఒక ప్రోటోకాల్ను కలిగి ఉండవలసిన అవసరం ఉంది.

- IPv4 on its own does not provide any security feature. Data has to be encrypted with some other security application before being sent on the Internet.
  దాని సొంత IPv4 ఏ భద్రతా ఫీచర్ అందించడం లేదు. ఇంటర్నెట్ లో పంపకముందు కొన్ని ఇతర భద్రతా దరఖాస్తులతో డేటాను గుప్తీకరించాలి.
- Data prioritization in IPv4 is not up to date. Though IPv4 has a few bits reserved for Type of Service or Quality of Service, but they do not provide much functionality.
- IPv4 లో డేటా ప్రాధాన్యత తేదీ వరకు లేదు. IPv4 సేవా రకాన్ని లేదా సేవా నాణ్యత కోసం రిజర్వు చేయబడిన కొన్ని బిట్స్ ఉన్నప్పటికీ, అవి చాలా కార్యాచరణను అందించవు.
- IPv4 enabled clients can be configured manually or they need some address configuration mechanism. It does not have a mechanism to configure a device to have globally unique IP address.
- IPv4 ఎనేబుల్ క్లయింట్లు మాన్యువల్గా కన్ఫిగర్ చేయబడతాయి లేదా వారికి కొన్ని చిరునామా కాన్ఫిగరేషన్ అవసరం. పరికరాన్ని గ్లోబల్లీ ఐపి అడ్రసు కలిగి ఆకృతీకరించుటకు ఇది ఒక యంత్రాంగాన్ని కలిగి ఉండదు.

Why Not IPv5?

Till date, Internet Protocol has been recognized has IPv4 only. Version 0 to 3 were used while the protocol was itself under development and experimental process. So, we can assume lots of background activities remain active before putting a protocol into production. Similarly, protocol version 5 was used while experimenting with the stream protocol for Internet. It is known to us as Internet Stream Protocol which used Internet Protocol number 5 to encapsulate its datagram. It was never brought into public use, but it was already used.

తేదీ వరకు, ఇంటర్నెట్ ప్రోటోకాల్ గుర్తించబడింది IPv4 మాత్రమే. ప్రోటోకాల్ అనేది అభివృద్ధి మరియు ప్రయోగాత్మక ప్రక్రియలో ఉన్నప్పుడు, 0 నుండి 3 వరకు వెర్షన్ ఉపయోగించబడింది. కాబట్టి, ప్రొటోకాల్ను ఉత్పత్తిలోకి తీసుకునే ముందు మా బ్యాక్గ్రౌండ్ కార్యకలాపాలు చాలా చురుకుగా ఉంటాయి. అదే విధంగా, ఇంటర్నెట్ కోసం ప్రోటోకాల్ ప్రోటోకాల్తో ప్రయోగాలు చేస్తున్నప్పుడు ప్రోటోకాల్ వెర్షన్ 5 ఉపయోగించబడింది. ఇది ఇంటర్నెట్ ప్రోటోకాల్ నంబర్ 5 ను ఉపయోగించిన ఇంటర్నెట్ స్ట్రీమ్ ప్రోటోకాల్గా మనకు తెలిసినది. ఇది ప్రజల ఉపయోగంలోకి ఎక్కించబడలేదు, కానీ ఇది ఇప్పటికే ఉపయోగించబడింది.

Brief History

After IPv4's development in the early 80s, the available IPv4 address pool begun to shrink rapidly as the demand of addresses exponentially increased with Internet. Taking pre-cognizance of the situation that might arise, IETF, in 1994, initiated the development of an addressing protocol to replace IPv4. The progress of IPv6 can be tracked by means of the RFC published:

80 ల ప్రారంభంలో IPv4 యొక్క అభివృద్ధి తరువాత, అందుబాటులో ఉన్న IPv4 అడ్రెస్ పూల్ వేగంగా క్షీణించటం ప్రారంభించింది,

చిరునామాల డిమాండ్ ఇంటర్నెట్తో విశేషంగా పెరిగింది. తలెత్తిన పరిస్థితిని ముందుగా గ్రహించి, IETF, 1994 లో, IPv4 స్థానంలో ప్రసంగించే ప్రోటోకాల్ అభివృద్ధిని ప్రారంభించింది. IPv6 యొక్క పురోగతి RFC ద్వారా ప్రచురించబడుతుంది:

- 1998 – RFC 2460 – Basic Protocol
- 2003 – RFC 2553 – Basic Socket API
- 2003 – RFC 3315 – DHCPv6
- 2004 – RFC 3775 – Mobile IPv6
- 2004 – RFC 3697 – Flow Label Specification
- 2006 – RFC 4291 – Address architecture (revision)
- 2006 – RFC 4294 – Node requirement

On June 06, 2012, some of the Internet giants chose to put their Servers on IPv6. Presently they are using Dual Stack mechanism to implement IPv6 parallel in with IPv4.
జూన్ 06, 2012 న, ఇంటర్నెట్ జెయింట్స్ కొన్ని IPv6 పై తమ సర్వర్లను ఉంచడానికి ఎంచుకున్నారు. ప్రస్తుతం IPv4 తో IPv4 సమాంతరంగా అమలు చేయడానికి డ్యూయల్ స్టాక్ మెకానిజంను ఉపయోగిస్తున్నారు.

Features
లక్షణాలు

The successor of IPv4 is not designed to be backward compatible. Trying to keep the basic functionalities of IP addressing, IPv6 is redesigned entirely. It offers the following features:

IPv4 యొక్క వారసుడు వెనుకబడి ఉన్న అనుకూలమైనదిగా రూపొందించబడింది. IP చిరునామా యొక్క ప్రాథమిక కార్యాచరణలను ఉంచడానికి ప్రయత్నిస్తున్నప్పుడు, IPv6 పూర్తిగా పునఃరూపకల్పన చేయబడింది. ఇది క్రింది లక్షణాలను అందిస్తుంది:

Larger Address Space
In contrast to IPv4, IPv6 uses 4 times more bits to address a device on the Internet. This much of extra bits can provide approximately 3.4×1038 different combinations of addresses. This address can accumulate the aggressive requirement of address allotment for almost everything in this world. According to an estimate, 1564 addresses can be allocated to every square meter of this earth.

IPv4 కు విరుద్ధంగా, IPv6 ఇంటర్నెట్లో ఒక పరికరాన్ని పరిష్కరించడానికి 4 రెట్లు ఎక్కువ బిట్స్ను ఉపయోగిస్తుంది. అదనపు బిట్స్ యొక్క ఈ అధిక సంఖ్యలో చిరునామాలు 3.4 × 1038 వేర్వేరు కాంబినేషన్లను అందిస్తుంది. ఈ చిరునామా ఈ ప్రపంచంలో దాదాపు ప్రతిదీ కోసం కేటాయింపు యొక్క దూకుడు అవసరం కూడగట్టవచ్చు. అంచనా ప్రకారం, ఈ భూమి యొక్క ప్రతి చదరపు మీటర్కు 1564 చిరునామాలను కేటాయించవచ్చు.

Simplified Header

IPv6's header has been simplified by moving all unnecessary information and options (which are present

in IPv4 header) to the end of the IPv6 header. IPv6 header is only twice as bigger than IPv4 provided the fact that IPv6 address is four times longer.
IPv6 శీర్షిక చివరికి అన్ని అనవసరమైన సమాచారం మరియు ఐచ్ఛికాలను (IPv4 శీర్షికలో ఉన్నవి) తరలించడం ద్వారా IPv6 యొక్క శీర్షిక సరళీకృతం చేయబడింది. IPv6 శీర్షిక IPv4 కన్నా రెండు రెట్లు పెద్దది, IPv6 చిరునామా నాలుగు రెట్లు ఎక్కువ.

End-to-end Connectivity

Every system now has unique IP address and can traverse through the Internet without using NAT or other translating components. After IPv6 is fully implemented, every host can directly reach other hosts on the Internet, with some limitations involved like Firewall, organization policies, etc.
ప్రతి వ్యవస్థ ఇప్పుడు ఏకైక IP చిరునామాను కలిగి ఉంది మరియు NAT లేదా ఇతర అనువాదం భాగాలు ఉపయోగించకుండా ఇంటర్నెట్ ద్వారా ప్రయాణించవచ్చు. IPv6 పూర్తిగా అమలు చేయబడిన తరువాత, ప్రతి హోస్ట్ నేరుగా ఇంటర్నెట్లో ఇతర అతిధేయలకి చేరవచ్చు, ఫైర్వాల్, సంస్థ విధానాలు మొదలైన వాటిలో కొన్ని పరిమితులు ఉంటాయి.

Auto-configuration

IPv6 supports both stateful and stateless auto configuration mode of its host devices. This way, absence of a DHCP server does not put a halt on inter segment communication.
IPv6 దాని హోస్ట్ పరికరాల స్టేట్ఫుల్ మరియు స్థితిలేని ఆటో కాన్ఫిగరేషన్ మోడ్కు మద్దతు ఇస్తుంది. ఈ విధంగా, ఒక DHCP సర్వర్ యొక్క లేకపోవడం ఇంటర్ సెగ్మెంట్ కమ్యూనికేషన్ లో ఒక halt చాలు లేదు.

Faster Forwarding/Routing

Simplified header puts all unnecessary information at the end of the header. The information contained in the first part of the header is adequate for a Router to take routing decisions, thus making routing decision as quickly as looking at the mandatory header.
సరళీకృత శీర్షిక అన్ని అనవసరమైన సమాచారాన్ని శీర్షిక చివరిలో ఉంచుతుంది. శీర్షిక యొక్క మొదటి భాగంలో ఉన్న సమాచారం రౌటర్కు రూటింగ్ నిర్ణయాలు తీసుకోవడానికి తగినంతగా సరిపోతుంది, తద్వారా తప్పనిసరి శీర్షికను చూస్తున్నట్లుగా నిర్ణయం తీసుకోవడాన్ని రూటింగ్ చేస్తుంది.

IPSec

Initially it was decided that IPv6 must have IPSec security, making it more secure than IPv4. This feature has now been made optional.
ప్రారంభంలో IPv6 తప్పనిసరిగా IPSec భద్రతను కలిగి ఉండాలని నిర్ణయించుకుంది, ఇది IPv4 కంటే మరింత సురక్షితమైనదిగా మారింది. ఈ ఫీచర్ ఇప్పుడు ఐచ్ఛికం చేయబడింది.

No Broadcast

Though Ethernet/Token Ring are considered as broadcast network because they support Broadcasting, IPv6 does not have any broadcast support any more. It uses multicast to communicate with multiple hosts.

ఈథర్నెట్ / టోకెన్ రింగ్ బ్రాడ్కాస్టింగ్కు మద్దతిస్తున్నందున ప్రసార నెట్వర్క్గా పరిగణించబడుతున్నప్పటికీ, IPv6 కి ఏదైనా ప్రసారం లేదు. బహుళ హోస్ట్లతో కమ్యూనికేట్ చేయడానికి ఇది మల్టికాస్ట్ను ఉపయోగిస్తుంది.

Anycast Support

This is another characteristic of IPv6. IPv6 has introduced Anycast mode of packet routing. In this mode, multiple interfaces over the Internet are assigned same Anycast IP address. Routers, while routing, send the packet to the nearest destination.

ఇది IPv6 యొక్క మరొక లక్షణం. IPv6 ప్యాకెట్ రౌటింగ్ యొక్క Anycast మోడ్ను ప్రవేశపెట్టింది. ఈ మోడ్లో, ఇంటర్నెట్లో బహుళ ఇంటర్ఫేస్లు ఒకే Anycast IP చిరునామాను కేటాయించబడతాయి. రూటర్లు, రూటింగ్ చేస్తున్నప్పుడు, ప్యాకెట్ను సమీప గమ్యస్థానానికి పంపుతుంది.

Mobility

IPv6 was designed keeping mobility in mind. This feature enables hosts (such as mobile phone) to roam around in different geographical area and remain connected with the same IP address. The mobility feature of IPv6 takes advantage of auto IP configuration and Extension headers.

IPv6 అనేది చైతన్యం మనస్సులో ఉంచుతూ రూపొందించబడింది. ఈ లక్షణం ఆతిథ్య (మొబైల్ ఫోన్ వంటిది) వివిధ భౌగోళిక ప్రాంతాల్లో తిరుగుతూ మరియు అదే IP చిరునామాతో అనుసంధానించడానికి అనుమతిస్తుంది. IPv6 యొక్క కదలిక లక్షణం ఆటో IP ఆకృతీకరణ మరియు ఎక్స్టెన్షన్ శీర్షికల ప్రయోజనాన్ని పొందుతుంది.

Enhanced Priority Support

IPv4 used 6 bits DSCP (Differential Service Code Point) and 2 bits ECN (Explicit Congestion Notification) to provide Quality of Service but it could only be used if the end-to-end devices support it, that is, the source and destination device and underlying network must support it.

IPv4 సేవ యొక్క నాణ్యతను అందించడానికి 6 బిట్స్ DSCP (డిఫరెన్షియల్ సర్వీస్ కోడ్ పాయింట్) మరియు 2 బిట్లు ECN (స్పష్టమైన కన్జెషన్ నోటిఫికేషన్) ను ఉపయోగించింది, కానీ చివరికి అంతా పరికరాలకు ఇది మద్దతు ఇస్తుంది, అంటే మూల మరియు గమ్య పరికరం మరియు అంతర్లీన నెట్వర్క్ అది మద్దతు ఉండాలి.

In IPv6, Traffic class and Flow label are used to tell the underlying routers how to efficiently process the packet and route it.

IPv6 లో, ట్రాఫిక్ క్లాస్ మరియు ఫ్లో లేబుల్ అనేవి ప్యాకెట్ను ప్రాసెస్ మరియు మార్గాన్ని ఎలా సమర్థవంతంగా నిర్వహించాలో అంతర్లీన రౌటర్లకు చెప్పడానికి ఉపయోగిస్తారు.

Smooth Transition

Large IP address scheme in IPv6 enables to allocate devices with globally unique IP addresses. This mechanism saves IP addresses and NAT is not required. So devices can send/receive data among each other, for example, VoIP and/or any streaming media can be used much efficiently.

IPv6 లో IP చిరునామా పథకం ప్రపంచవ్యాప్తంగా ప్రత్యేక IP చిరునామాలతో పరికరాల కేటాయింపును అనుమతిస్తుంది. ఈ విధానం IP చిరునామాలను ఆదా చేస్తుంది మరియు NAT అవసరం లేదు. కాబట్టి పరికరాలు ప్రతి ఇతర మధ్య డేటాని పంపుతాయి / అందుకోవచ్చు, ఉదాహరణకు, VoIP మరియు / లేదా ఏదైనా స్ట్రీమింగ్ మాధ్యమం చాలా సమర్థవంతంగా ఉపయోగించబడతాయి .

Other fact is, the header is less loaded, so routers can take forwarding decisions and forward them as quickly as they arrive.

ఇతర వాస్తవం, శీర్షిక తక్కువ లోడ్ అవుతుంది, కాబట్టి రౌటర్లు నిర్ణయాలు తీసుకోవటానికి మరియు త్వరగా వచ్చినప్పుడు వాటిని ముందుకు పంపవచ్చు .

Extensibility

One of the major advantages of IPv6 header is that it is extensible to add more information in the option part. IPv4 provides only 40-bytes for options, whereas options in IPv6 can be as much as the size of IPv6 packet itself.

IPv6 హెడ్డర్ యొక్క ప్రధాన ప్రయోజనాల్లో ఒకటి, ఇది ఐచ్ఛిక భాగానికి మరింత సమాచారాన్ని జోడించడానికి విస్తరించదగినది. IPv4 ఐచ్ఛికాల కొరకు 40-బైట్లు మాత్రమే అందిస్తుంది, అయితే IPv6 లోని ఐచ్ఛికాలు IPv6 పాకెట్ యొక్క పరిమాణాన్ని కలిగి ఉంటాయి.

In computer networking, addressing mode refers to the mechanism of hosting an address on the network. IPv6 offers several types of modes by which a single host can be addressed. More than one host can be addressed at once or the host at the closest distance can be addressed.

కంప్యూటర్ నెట్వర్కింగ్లో, చిరునామా మోడ్ నెట్వర్క్లో చిరునామాను హోస్ట్ చేసే మెకానిజంను సూచిస్తుంది. IPv6 అనేక రకాలైన మోడ్లను అందిస్తుంది, దీని ద్వారా ఒకే హోస్ట్ ప్రసంగించవచ్చు. ఒకటి కంటే ఎక్కువ హోస్ట్ ఒకేసారి ప్రసంగించవచ్చు లేదా అతి దగ్గరలో అతిధేయ ప్రసంగించవచ్చు .

Unicast

In unicast mode of addressing, an IPv6 interface (host) is uniquely identified in a network segment. The IPv6 packet contains both source and destination IP addresses. A host interface is equipped with an IP address which is unique in that network segment.When a network switch or a router receives a unicast IP packet, destined to a single host, it sends out one of its outgoing interface which connects to that particular host.

చిరునామా యొక్క యునికేస్ట్ మోడ్లో, IPv6 ఇంటర్ఫేస్ (హోస్ట్) ప్రత్యేకంగా నెట్వర్క్ సెగ్మెంట్లో గుర్తించబడుతుంది. IPv6 ప్యాకెట్ మూలం మరియు గమ్య IP చిరునామాలు రెండింటినీ కలిగి ఉంటుంది. నెట్వర్క్ విభాగంలో ప్రత్యేకమైన IP చిరునామాతో ఒక అతిధేయ ఇంటర్ఫేస్ అమర్చబడి ఉంటుంది. ఒక నెట్వర్క్ స్విచ్ లేదా రూటర్ ఒక సింగిల్ హోస్ట్కు ఉద్దేశించిన ఒక యూనిట్ IP ప్యాకెట్ను స్వీకరించినప్పుడు, ఆ ప్రత్యేక హోస్ట్కు కనెక్ట్ చేసే దాని అవుట్గోయింగ్ ఇంటర్ఫేస్లో దాన్ని పంపుతుంది .

Multicast

The IPv6 multicast mode is same as that of IPv4. The packet destined to multiple hosts is sent on a special multicast address. All the hosts interested in that multicast information, need to join that multicast group first. All the interfaces that joined the group receive the multicast packet and process it, while other hosts not interested in multicast packets ignore the multicast information.

IPv6 మల్టీకాస్ట్ మోడ్ IPv4 మాదిరిగానే ఉంటుంది. బహుళ అతిధేయల కొరకు ఉద్దేశించబడిన ప్యాకెట్ ఒక ప్రత్యేక మల్టీకస్ట్

చిరునామాలో పంపబడుతుంది. ఆ మల్టికస్ట్ సమాచారం ఆసక్తి అన్ని ఆతిథ్య, ఆ చేరడానికి అవసరం మొదట బహుళ సమూహం. సమూహంలో చేరిన అన్ని ఇంటర్ఫేస్లు మల్టికస్ట్ పాకెట్ ను అందుకుంటాయి మరియు ప్రాసెస్ చేస్తాయి, మల్టికస్ట్ పాకెట్లలో ఆసక్తి లేని ఇతర అతిధేయదారులు బహుళ సమాచారాన్ని విస్మరిస్తారు

Anycast

IPv6 has introduced a new type of addressing, which is called Anycast addressing. In this addressing mode, multiple interfaces (hosts) are assigned same Anycast IP address. When a host wishes to communicate with a host equipped with an Anycast IP address, it sends a Unicast message. With the help of complex routing mechanism, that Unicast message is delivered to the host closest to the Sender in terms of Routing cost.

IPv6 ఒక కొత్త రకం చిరునామాను ప్రవేశపెట్టింది, దీనిని ఏమైనా నామకరణ చిరునామా అని పిలుస్తారు. ఈ చిరునామా మోడ్లో, బహుళ ఇంటర్ఫేస్లు (హోస్ట్స్) ఒకే Anycast IP చిరునామాను కేటాయించబడతాయి. ఒక అతిధేయుడు ఒక Anycast IP చిరునామా కలిగి హోస్ట్ కమ్యూనికేట్ కోరుకున్నప్పుడు, అది ఒక యూనికస్ట్ సందేశాన్ని పంపుతుంది. క్లిష్టమైన రౌటింగ్ మెకానిజం సహాయంతో, రసీదు ధర పరంగా పంపేవారికి అతి దగ్గరవుతున్న అతిథేయ సందేశాన్ని పంపిణీ చేస్తుంది.

Let’s take an example of TutorialPoints.com Web Servers, located in all continents. Assume that all the Web Servers are assigned a single IPv6 Anycast IP Address. Now when a user from Europe wants to reach TutorialsPoint.com the DNS points to the server that is physically located in Europe itself. If a user from India tries to reach Tutorialspoint.com, the DNS will then point to the Web Server physically located in Asia. Nearest or Closest terms are used in terms of Routing Cost.

అన్ని ఖండాల్లో ఉన్న TutorialPoints.com వెబ్ సర్వర్లు యొక్క ఉదాహరణను తీసుకుందాం. అన్ని వెబ్ సర్వర్లు ఒకే IPv6 Anycast IP చిరునామాకు కేటాయించబడతాయని అనుకోండి. ఐరోపా నుండి ఒక వినియోగదారు యూరప్లో భౌతికంగా ఉన్న సర్వర్కు DNS పాయింట్లను DNS పాయింట్లు చేరుకోవడానికి కోరుకుంటున్నప్పుడు. భారతదేశం నుండి ఒక యూజర్ Tutorialspoint.com ను చేరుకోవడానికి ప్రయత్నిస్తే, ఆసియాలో ఉన్న భౌతికంగా ఉన్న వెబ్ సర్వర్కు DNS కనిపిస్తుంది. రౌటింగ్ ఖర్చు పరంగా సమీప లేదా సమీప పదాలను ఉపయోగిస్తారు .

In the above picture, when a client computer tries to reach a server, the request is forwarded to the server with the lowest Routing Cost.

పై చిత్రంలో, ఒక క్లయింట్ కంప్యూటర్ ఒక సర్వర్ చేరుకోవడానికి ప్రయత్నించినప్పుడు, అభ్యర్థన అత్యల్ప రౌటింగ్ ధరతో సర్వర్కు ఫార్వార్డ్ చేయబడుతుంది.

Address Types & Formats Hexadecimal

Number System

Before introducing IPv6 Address format, we shall look into Hexadecimal Number System. Hexadecimal is a positional number system that uses radix (base) of 16. To represent the values in readable format, this system uses 0-9 symbols to represent values from zero to nine and A-F to represent values from ten to fifteen. Every digit in Hexadecimal can represent values from 0 to 15.

IPv6 చిరునామా ఫార్మాట్ పరిచయం ముందు, మేము హెక్సాడెసిమల్ సంఖ్య వ్యవస్థ పరిశీలిస్తాము కమిటీ. హెక్సాడెసిమల్ రీడిక్స్ ఫార్మాట్ లో విలువలు ప్రాతినిధ్యం కోసం, ఈ వ్యవస్థ పది నుండి పదిహేను వరకు విలువలు ప్రాతినిధ్యం సున్నా నుండి తొమ్మిది

మరియు A-F విలువలు ప్రాతినిధ్యం 0-9 చిహ్నాలు ఉపయోగిస్తుంది. ప్రతి అంకెల హెక్సాడెసిమల్లో 0 నుండి 15 వరకు విలువలను సూచిస్తుంది

Decimal	Binary	Hexadecimal
0	0000	0
1	0001	1
2	0010	2
3	0011	3
4	0100	4
5	0101	5
6	0110	6
7	0111	7
8	1000	8
9	1001	9
10	1010	A
11	1011	B
12	1100	C
13	1101	D
14	1110	E
15	1111	F

Address Structure

An IPv6 address is made of 128 bits divided into eight 16-bits blocks. Each block is then converted into 4-digit Hexadecimal numbers separated by colon symbols.

ఒక IPv6 చిరునామా 128 బిట్స్ ఎనిమిది 16-బిట్స్ బ్లాక్స్గా విభజించబడింది. ప్రతి బ్లాక్ అప్పుడు కోలన్ చిహ్నాలు వేరు 4- అంకెల హెక్సాడెసిమల్ సంఖ్యలు మార్చబడుతుంది.

For example, given below is a 128 bit IPv6 address represented in binary format and divided into eight 16-bits blocks:

ఉదాహరణకు, క్రింద ఇవ్వబడిన 128 బిట్ IPv6 చిరునామా బైనరీ ఆకృతిలో ప్రాతినిధ్యం మరియు ఎనిమిది 16- బిట్స్ బ్లాక్స్గా విభజించబడింది :

0010000000000001 0000000000000000 0011001000111000 1101111111100001 0000000001100011 0000000000000000 0000000000000000 1111111011111011

Each block is then converted into Hexadecimal and separated by ‘:’ symbol:

ప్రతి బ్లాక్ అప్పుడు హెక్సాడెసిమల్ గా మారుతుంది మరియు ':' గుర్తుతో వేరుచేయబడుతుంది:2001:0000:3238:DFE1:0063:0000:0000:FEFB

Even after converting into Hexadecimal format, IPv6 address remains long. IPv6 provides some rules to shorten the address. The rules are as follows:

హెక్సాడెసిమల్ ఆకృతిలోకి మారినప్పటికీ, IPv6 అడ్రెస్ చాలా పొడవుగా ఉంది. IPv6 కు కొన్ని నియమాలను అందిస్తుంది చిరునామాను

తగ్గించండి. క్రింది నియమాలు ఉన్నాయి:

Rule.1: Discard leading Zero(es):

In Block 5, 0063, the leading two 0s can be omitted, such as (5th block):

బ్లాక్ 5, 0063 లో, ప్రముఖ రెండు 0 లను విస్మరించవచ్చు, (5 వ బ్లాక్):2001:0000:3238:DFE1:63:0000:0000:FEFB

Rule.2: If two of more blocks contain consecutive zeroes, omit them all and replace with double colon sign ::, such as (6th and 7th block):

రూల్ .2: రెండు బ్లాక్స్ వరుస సున్నాలను కలిగి ఉంటే, వాటిని అన్నింటినీ వదిలివేసి డబుల్ కోలన్ తో భర్తీ చేయండి సైన్ :: :: (6 వ మరియు 7 వ బ్లాక్):2001:0000:3238:DFE1:63::FEFB

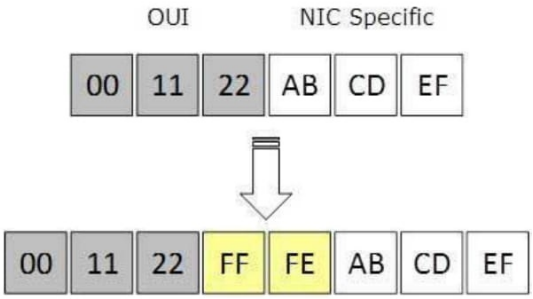
Consecutive blocks of zeroes can be replaced only once by :: so if there are still blocks of zeroes in the address, they can be shrunk down to a single zero, such as (2nd block):

సున్నాల వరుస బ్లాక్స్ను ఒకసారి మాత్రమే ఒకసారి భర్తీ చేయవచ్చు: కాబట్టి సున్నాల యొక్క బ్లాక్స్ ఇప్పటికీ ఉన్నట్లయితే చిరునామా, వారు ఒక సున్నాకి కుదించవచ్చు, (2 వ బ్లాక్):2001:0:3238:DFE1:63::FEFB

Interface ID

IPv6 has three different types of Unicast Address scheme. The second half of the address (last 64 bits) is always used for Interface ID. The MAC address of a system is composed of 48-bits and represented in Hexadecimal. MAC addresses are considered to be uniquely assigned worldwide. Interface ID takes advantage of this uniqueness of MAC addresses. A host can auto-configure its Interface ID by using IEEE's Extended Unique Identifier (EUI-64) format. First, a host divides its own MAC address into two 24-bits halves. Then 16-bit Hex value 0xFFFE is sandwiched into those two halves of MAC address, resulting in EUI-64 Interface ID.

IPv6 కి మూడు రకాల యునికస్ట్ అడ్రస్ పథకాలు ఉన్నాయి. చిరునామా యొక్క రెండవ భాగం (చివరి 64 బిట్స్) ఇంటర్ఫేస్ ID కోసం ఎల్లప్పుడూ ఉపయోగించబడుతుంది. ఒక వ్యవస్థ యొక్క MAC చిరునామా 48-బిట్స్ కలిగి ఉంటుంది మరియు హెక్సాడెసిమల్లో ప్రాతినిధ్యం వహిస్తుంది. MAC చిరునామాలు ప్రత్యేకంగా ప్రపంచవ్యాప్తంగా కేటాయించబడ్డాయి. MAC చిరునామాల యొక్క ఈ ప్రత్యేకతను ఇంటర్ఫేస్ ID ఉపయోగించుకుంటుంది. IEEE యొక్క విస్తరించిన ప్రత్యేక ఐడెంటిఫైయర్ (EUI-64) ఫార్మాట్ ఉపయోగించి ఒక హోస్ట్ ఇంటర్ఫేస్ ID ను స్వీయ-కాన్ఫిగర్ చేయవచ్చు. మొదటిది, ఒక హోస్ట్ దాని సొంత MAC చిరునామాను 24-బిట్స్ విభజనలలో విభజించింది. అప్పుడు 16-బిట్ హెక్స్ విలువ 0xFFFE అనేది MAC చిరునామా యొక్క ఆ రెండు భాగాలుగా మారిపోతుంది, ఫలితంగా EUI-64 ఇంటర్ఫేస్ ID.



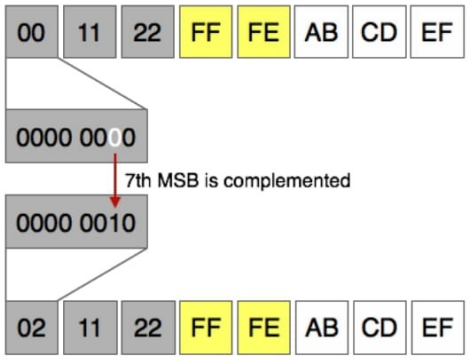
Conversion of EUI-64 ID into IPv6 Interface Identifier

EUI-64 ID మార్పిడి IPv6 ఇంటర్ఫేస్ ఐడెంటిఫయర్ లోకి మార్చబడుతుంది

To convert EUI-64 ID into IPv6 Interface Identifier, the most significant 7th bit of EUI-64 ID is complemented. For example:

EUI-64 ID ని IPv6 ఇంటర్ఫేస్ ఐడెంటిఫైయర్గా మార్చడానికి, EUI-64 ID యొక్క అత్యంత ముఖ్యమైన 7 వ బిట్ పూర్తికాబడి ఉంది.

ఉదాహరణకి:



This address type is equivalent to IPv4's public address. Global Unicast addresses in IPv6 are globally identifiable and uniquely addressable.

ఈ చిరునామా రకం IPv4 యొక్క పబ్లిక్ చిరునామాకు సమానం. IPv6 లో గ్లోబల్ యునికస్ట్ అడ్రెస్లు ప్రపంచవ్యాప్తంగా గుర్తించదగినవి మరియు ప్రత్యేకంగా చిరునామాలుగా ఉంటాయి.

Global Routing Prefix: The most significant 48-bits are designated as Global Routing Prefix which is assigned to specific autonomous system. The three most significant bits of Global Routing Prefix is always set to 001.

గ్లోబల్ రౌటింగ్ ప్రిఫిక్స్: గ్లోబల్ రౌటింగ్ ప్రిఫిక్స్లో అత్యంత ముఖ్యమైన 48- బిట్లు ప్రత్యేకమైన స్వయంప్రతిపత్త వ్యవస్థకు కేటాయించబడ్డాయి. గ్లోబల్ రౌటింగ్ ప్రిఫిక్స్ యొక్క మూడు అత్యంత ముఖ్యమైన బిట్స్ ఎల్లప్పుడూ 001 కు అమర్చబడి ఉంటుంది .

Link-Local Address

Auto-configured IPv6 address is known as Link-Local address. This address always starts with FE80. The first 16 bits of link-local address is always set to 1111 1110 1000 0000 (FE80). The next 48-bits are set to 0, thus:

స్వీయ-ఆకృతీకరణ IPv6 చిరునామాను లింక్-లోకల్ అడ్రస్ అని పిలుస్తారు. ఈ చిరునామా ఎల్లప్పుడూ FE80 తో మొదలవుతుంది.

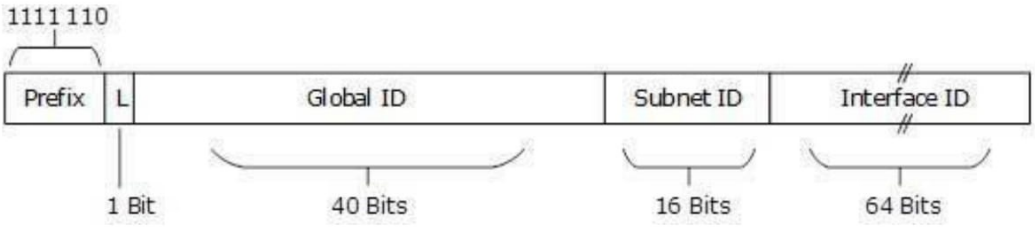
లింక్-స్థానిక చిరునామా యొక్క మొదటి 16 బిట్స్ ఎల్లప్పుడూ 1111 1110 1000 0000 (FE80) కు సెట్ చేయబడింది. తరువాతి 48-బిట్లు 0 కు సెట్ చేయబడ్డాయి, అవి:

Link-local addresses are used for communication among IPv6 hosts on a link (broadcast segment) only. These addresses are not routable, so a Router never forwards these addresses outside the link.

Unique-Local Address

type of IPv6 address is globally unique, but it should be used in local communication. The second half of this address contain Interface ID and the first half is divided among Prefix, Local Bit, Global ID and Subnet ID.

IPv6 చిరునామా రకం ప్రపంచవ్యాప్తంగా ప్రత్యేకంగా ఉంటుంది, కానీ అది స్థానిక కమ్యూనికేషన్లో వాడాలి. ఈ చిరునామా యొక్క రెండవ భాగంలో ఇంటర్ఫేస్ ID మరియు మొదటి సగం ప్రిఫిక్స్, స్థానిక బిట్, గ్లోబల్ ID మరియు సబ్నెట్ ఐడిలో విభజించబడింది.



Unique-Local Address]

Image:

Prefix is always set to 1111 110. L bit, is set to 1 if the address is locally assigned. So far, the meaning of L bit to 0 is not defined. Therefore, Unique Local IPv6 address always starts with 'FD'.

చిరునామాను స్థానికంగా కేటాయించినట్లయితే, పూర్వం ఎల్లప్పుడూ 1111 110 కు సెట్ అవుతుంది. L బిట్, 1 కు సెట్ చేయబడింది. ఇప్పటివరకు, 0 కు L బిట్ యొక్క అర్థం నిర్వచించబడలేదు. అందువల్ల, ప్రత్యేకమైన స్థానిక IPv6 చిరునామా ఎల్లప్పుడూ 'FD' తో మొదలవుతుంది .

Scope of IPv6 Unicast Addresses:

The scope of Link-local address is limited to the segment. Unique Local Address are locally global, but are not routed over the Internet, limiting their scope to an organization's boundary. Global Unicast addresses are globally unique and recognizable. They shall make the essence of Internet v2 addressing.

లింక్-లోకల్ చిరునామా యొక్క పరిధిని విభాగానికి పరిమితం చేయబడింది. ప్రత్యేక స్థానిక చిరునామా స్థానికంగా ప్రపంచంగా ఉంటుంది, అయితే ఇంటర్నెట్లో వారి వైఫల్యాన్ని పరిమితం చేయడం లేదు, వారి పరిధిని సంస్థ యొక్క సరిహద్దుకు పరిమితం చేస్తుంది. గ్లోబల్ యునికెస్ట్ అడ్రెస్లు గ్లోబల్లీ విలక్షణమైనవి మరియు గుర్తించదగినవి. వారు ఇంటర్నెట్ v2 అడ్రసింగ్ యొక్క సారాంశం చేస్తుంది.

Version 6 has slightly complex structure of IP address than that of IPv4. IPv6 has reserved a few addresses and address notations for special purposes. See the table below:

సంస్కరణ 6 IPv4 కంటే IP చిరునామా యొక్క కొంచెం క్లిష్టమైన నిర్మాణం కలిగి ఉంది. IPv6 ప్రత్యేక ప్రయోజనాల కోసం కొన్ని చిరునామాలను మరియు చిరునామా నోటిఫికేషన్లను కేటాయించింది. క్రింది పట్టికను చూడండి:

IPv6 Address	Meaning
::/128	Unspecified Address
::/0	Default Route
::1/128	Loopback Address

- As shown in the table, the address 0:0:0:0:0:0:0:0/128 does not specify anything and is said to be an unspecified address. After simplifying, all the 0s are compacted to ::/128.
  పట్టికలో చూపినట్లుగా, చిరునామా 0: 0: 0: 0: 0: 0: 0: 0: 0/128 ఏదైనా పేర్కొనలేదు మరియు పేర్కొనబడని చిరునామాగా చెప్పబడుతుంది. సరళీకరణ తరువాత, అన్ని 0 లు :: / 128 కు కుదించబడ్డాయి .
- In IPv4, the address 0.0.0.0 with netmask 0.0.0.0 represents the default route. The same concept is also applied to IPv6, address 0:0:0:0:0:0:0:0 with netmask all 0s represents the default route. After applying IPv6 rule, this address is compressed to ::/0.

  IPv4 లో, నెట్ మాస్క్ 0.0.0.0 తో 0.0.0.0 చిరునామా డిఫాల్ట్ మార్గాన్ని సూచిస్తుంది. అదే భావన IPv6 కు కూడా వర్తిస్తుంది, 0: 0: 0: 0: 0: 0: 0: 0: 0: 0 IPv6 నియమాన్ని అమలు చేసిన తరువాత, ఈ చిరునామా :: / 0 కు కంప్రెస్ చేయబడింది.

- Loopback addresses in IPv4 are represented by 127.0.0.1 to 127.255.255.255 series. But in IPv6, only 0:0:0:0:0:0:0:1/128 represents the Loopback address. After loopback address, it can be represented as ::1/128.

Reserved Multicast Address for Routing Protocols

IPv6 Address	Routing Protocol
FF02::5	OSPFv3
FF02::6	OSPFv3 Designated Routers
FF02::9	RIPng
FF02::A	EIGRP

- The above table shows the reserved multicast addresses used by interior routing protocol.
- అంతర్గత రౌటింగ్ ప్రోటోకాల్ ఉపయోగించే రిజర్వ్ మల్టీకస్ట్ అడ్రెస్లను పైన పట్టిక చూపిస్తుంది.

- The addresses are reserved following the same rules of IPv4.

Reserved Multicast Address for Routers/Node

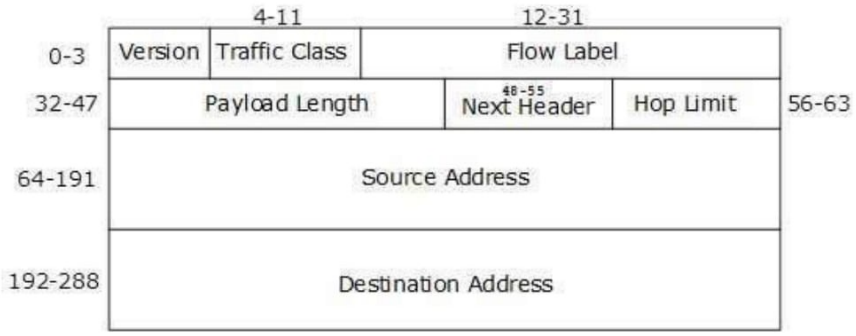
IPv6 Address	Scope
FF01::1	All Nodes in interface-local
FF01::2	All Routers in interface local
FF02::1	All Nodes in link-local
FF02::2	All Routers in link-local
FF05::2	All Routers in site-local

- These addresses help routers and hosts to speak to available routers and hosts on a segment without being configured with an IPv6 address. Hosts use EUI-64 based auto-configuration to self-configure an IPv6 address and then speak to available hosts/routers on the segment by means of these addresses.
  ఈ చిరునామాలు IPv6 చిరునామాతో కాన్ఫిగర్ చెయ్యకుండా ఒక విభాగంలో అందుబాటులో ఉన్న రౌటర్ల మరియు హోస్ట్లతో మాట్లాడటానికి రౌటర్లను మరియు హోస్ట్లకు సహాయం చేస్తుంది. హోస్ట్లు EUI-64 ఆధారిత స్వీయ-కాన్ఫిగరేషన్ను IPv6 చిరునామాను స్వీయ-కాన్ఫిగరేషన్కు ఉపయోగించుకుని ఆపై ఈ విభాగాల ద్వారా సెగ్మెంట్లో అందుబాటులో ఉన్న హోస్ట్స్ / రౌటర్లను మాట్లాడండి .

Headers

The wonder of IPv6 lies in its header. An IPv6 address is 4 times larger than IPv4, but surprisingly, the header of an IPv6 address is only 2 times larger than that of IPv4. IPv6 headers have one Fixed Header and zero or more Optional (Extension) Headers. All the necessary information that is essential for a router is kept in the Fixed Header. The Extension Header contains optional information that helps routers to understand how to handle a packet/flow.

IPv6 యొక్క అద్భుతం దాని శీర్షికలో ఉంది. IPv4 చిరునామా కంటే IPv6 చిరునామా 4 రెట్లు ఎక్కువ, కానీ ఆశ్చర్యకరంగా, IPv6 చిరునామా యొక్క శీర్షిక IPv4 కంటే 2 రెట్లు ఎక్కువగా ఉంటుంది. IPv6 శీర్షికలు ఒక స్థిర శీర్షిక మరియు సున్నా లేదా మరిన్ని ఐచ్ఛిక (పొడిగింపు) శీర్షికలు కలిగి ఉంటాయి. ఒక రౌటర్కు అవసరమైన అన్ని అవసరమైన సమాచారం స్థిర శీర్షికలో ఉంచబడుతుంది. పొడిగింపు హెడర్లో ప్యాకెట్ / ప్రవాహాన్ని ఎలా నిర్వహించాలో అర్థం చేసుకోవడానికి రౌటర్లకు సహాయపడే ఐచ్ఛిక సమాచారాన్ని కలిగి ఉంటుంది.



Fixed Header

IPv6 fixed header is 40 bytes long and contains the following information.

S.N.	Field & Description
1	**Version** (4-bits): It represents the version of Internet Protocol, i.e. 0110. సంస్కరణ (4-బిట్స్): ఇది ఇంటర్నెట్ ప్రోటోకాల్ యొక్క సంస్కరణను సూచిస్తుంది, అనగా 0110.
2	**Traffic Class** (8-bits): These 8 bits are divided into two parts. The most significant 6 bits are used for Type of Service to let the Router Known what services should be provided to this packet. The least significant 2 bits are used for Explicit Congestion Notification (ECN). ట్రాఫిక్ క్లాస్ (8-బిట్స్): ఈ 8 బిట్స్ రెండు భాగాలుగా విభజించబడ్డాయి. ఈ ప్యాకెట్కు ఏ సేవలు అందించబడాలి అనే రౌటర్ను తెలియజేయడానికి అత్యంత రకపు 6 బిట్స్ సర్వీస్ రకానికి ఉపయోగించబడతాయి. ఖచ్చితమైన కంజెషన్ నోటిఫికేషన్ (ECN) కోసం కనీసం 2 బిట్లు ఉపయోగించబడతాయి.
3	**Flow Label** (20-bits): This label is used to maintain the sequential flow of the packets belonging to a communication. The source labels the sequence to help the router identify that a particular packet belongs to a specific flow of information. This field helps avoid re-ordering of data packets. It is designed for streaming/real-time media. ఫ్లో లేబుల్ (20-బిట్లు): ఈ లేబుల్ ఒక కమ్యూనికేషన్కు చెందిన ప్యాకెట్ల వరుస ప్రవాహాన్ని నిర్వహించడానికి ఉపయోగించబడుతుంది. రౌటర్కు ఒక నిర్దిష్ట ప్యాకెట్ సమాచారాన్ని నిర్దిష్ట ప్రవాహానికి చెందినదిగా గుర్తించడంలో సహాయపడటానికి సోర్స్ లేబుల్ను సూచిస్తుంది. డేటా ప్యాకెట్లను తిరిగి క్రమం చేయకుండా ఈ ఫీల్డ్ సహాయపడుతుంది. స్ట్రీమింగ్ / రియల్-టైమ్ మీడియా కోసం ఇది రూపొందించబడింది.
4	**Payload Length** (16-bits): This field is used to tell the routers how much information a particular packet contains in its payload. Payload is composed of Extension Headers and Upper Layer data. With 16 bits, up to 65535 bytes can be indicated; but if the Extension Headers contain Hop-by-Hop Extension Header, then the payload may exceed 65535 bytes and this field is set to 0. పేలోడ్ పొడవు (16-బిట్స్): ఈ పేలుడు దాని పేలోడ్లో ఒక నిర్దిష్ట ప్యాకెట్ కలిగి ఉన్న సమాచారం ఎంత రౌటర్లకు తెలియజేయడానికి ఉపయోగిస్తారు. Payload పొడిగింపు శీర్షికలు మరియు ఉన్నత లేయర్ డేటాను కలిగి ఉంటుంది. 16 బిట్స్ తో, 65535 బైట్ల వరకు సూచించవచ్చు; కానీ పొడిగింపు శీర్షికలు హాప్-హాప్ ఎక్స్టెన్షన్ హెడర్ కలిగి ఉంటే, అప్పుడు పేలోడ్ 65535 బైట్లు మించి ఉండవచ్చు మరియు ఈ ఫీల్డ్ 0 కు సెట్ చేయబడుతుంది.
5	**Next Header** (8-bits): This field is used to indicate either the type of Extension Header, or if the Extension Header is not present then it indicates the Upper Layer PDU. The values for the type of Upper Layer PDU are same as IPv4's. తదుపరి హెడర్ (8-బిట్స్): ఎక్స్టెన్షన్ హెడర్ యొక్క రకాన్ని సూచించడానికి ఈ ఫీల్డ్ ఉపయోగించబడుతుంది, లేదా పొడిగింపు శీర్షిక లేనట్లయితే, అది ఎగువ లేయర్ PDU ని సూచిస్తుంది. ఎగువ లేయర్ PDU రకం కోసం విలువలు IPv4 యొక్క మాదిరిగానే ఉంటాయి.

6	**Hop Limit** (8-bits): This field is used to stop packet to loop in the network infinitely. This is same as TTL in IPv4. The value of Hop Limit field is decremented by 1 as it passes a link (router/hop). When the field reaches 0 the packet is discarded. 6 హాప్ పరిమితి (8-బిట్స్): ఈ ఫీల్డ్ అనంతమైన నెట్వర్క్లో లూప్కు ప్యాకెట్ను ఆపడానికి ఉపయోగించబడుతుంది. ఇది IPv4 లో TTL వలె ఉంటుంది. అది లింక్ (రౌటర్ / హాప్) ను దాటినప్పుడు హాప్ పరిమితి క్షేత్ర విలువ 1 కు తగ్గుతుంది. ఫీల్డ్ 0 చేరుకున్నప్పుడు ప్యాకెట్ విస్మరించబడుతుంది.
7	**Source Address** (128-bits): This field indicates the address of originator of the packet. మూల చిరునామా (128-బిట్స్): ఈ ఫీల్డ్ ప్యాకెట్ మూలకర్త యొక్క చిరునామాను సూచిస్తుంది .
8	**Destination Address** (128-bits): This field provides the address of intended recipient of the packet. గమ్యం చిరునామా (128-బిట్స్): ప్యాకెట్ యొక్క ఉద్దేశించిన గ్రహీత యొక్క చిరునామాను ఈ ఫీల్డ్ అందిస్తుంది.

Extension Headers

In IPv6, the Fixed Header contains only that much information which is necessary, avoiding those information which is either not required or is rarely used. All such information is put between the Fixed Header and the Upper layer header in the form of Extension Headers. Each Extension Header is identified by a distinct value.

IPv6 లో, ఫిక్స్డ్ హెడర్లో అవసరమైన చాలా సమాచారాన్ని మాత్రమే కలిగి ఉంది, అవసరమైన సమాచారాన్ని వదిలిపెట్టడం లేదా అరుదుగా ఉపయోగించడం లేదు. ఎక్స్టెన్షన్ హెడ్డర్స్ రూపంలో స్థిర శీర్షిక మరియు ఎగువ పొర శీర్షిక మధ్య ఇటువంటి అన్ని సమాచారం ఉంచబడుతుంది. ప్రతి ఎక్స్టెన్షన్ హెడర్ ఒక ప్రత్యేక విలువతో గుర్తించబడుతుంది.

When Extension Headers are used, IPv6 Fixed Header's Next Header field points to the first Extension Header. If there is one more Extension Header, then the first Extension Header's 'Next-Header' field points to the second one, and so on. The last Extension Header's 'Next-Header' field points to the Upper Layer Header. Thus, all the headers points to the next one in a linked list manner.

పొడిగింపు శీర్షికలు ఉపయోగించినప్పుడు, మొదటి పొడిగింపు శీర్షికకు IPv6 స్థిర శీర్షిక యొక్క తదుపరి హెడర్ ఫీల్డ్ పాయింట్లు. మరొక పొడిగింపు హెడర్ ఉన్నట్లయితే, మొదటి పొడిగింపు హెడర్ యొక్క 'తదుపరి-శీర్షిక' ఫీల్డ్ రెండోదానికి మరియు అందువలన న. చివరి పొడిగింపు హెడర్ యొక్క 'తదుపరి-హెడర్' ఫీల్డ్ ఎగువ లేయర్ హెడర్కు సూచిస్తుంది. అందువల్ల, అన్ని శీర్షికలు అనుసంధాన జాబితా పద్ధతిలో తదుపరి దానిని సూచిస్తాయి.

If the Next Header field contains the value 59, it indicates that there are no headers after this header, not even Upper Layer Header.

తదుపరి హెడర్ ఫీల్డ్ విలువ 59 ని కలిగి ఉంటే, అది ఈ శీర్షిక తర్వాత ఏ శీర్షికలు లేనప్పటికీ, ఎగువ లేయర్ శీర్షిక కూడా కాదు .

The following Extension Headers must be supported as per RFC 2460:

క్రింది పొడిగింపు శీర్షికలు RFC 2460 ప్రకారం మద్దతు ఇవ్వాలి:

Extension Header	Next Header Value	Description
Hop-by-Hop Options header	0	read by all devices in transit network
Routing header	43	contains methods to support making routing decision
Fragment header	44	contains parameters of datagram fragmentation
Destination Options header	60	read by destination devices
Authentication header	51	information regarding authenticity
Encapsulating Security Payload header	50	encryption information

The sequence of Extension Headers should be:

IPv6 header
Hop-by-Hop Options header
Destination Options header[1]
Routing header
Fragment header
Authentication header
Encapsulating Security Payload header
Destination Options header[2]
Upper-layer header

These headers:

- 1. should be processed by First and subsequent destinations.

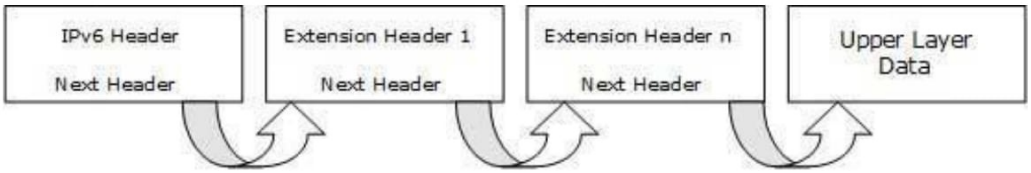
మొదటి మరియు తదుపరి గమ్యస్థానాలకు ప్రాసెస్ చేయాలి .

- 2. should be processed by Final Destination.

ఫైనల్ డెస్టినేషన్ ద్వారా ప్రాసెస్ చేయబడాలి .

Extension Headers are arranged one after another in a linked list manner, as depicted in the following diagram:

కింది రేఖాచిత్రంలో చిత్రీకరించినట్లు, పొడిగింపు శీర్షికలు అనుసంధాన జాబితా పద్ధతిలో మరొకదానిని ఏర్పాటు చేస్తాయి:



Subnetting

In IPv4, addresses were created in classes. Classful IPv4 addresses clearly define the bits used for network prefixes and the bits used for hosts on that network. To subnet in IPv4, we play with the default classful netmask which allows us to borrow host bits to be used as subnet bits. This results in multiple subnets but less hosts per subnet. That is, when we borrow host bits to create a subnet, it costs us in lesser bit to be used for host addresses.

IPv4 లో, చిరునామాలు తరగతులలో సృష్టించబడ్డాయి. క్లాస్ఫుల్ IPv4 చిరునామాలను స్పష్టంగా నెట్వర్క్ ఆదిప్రత్యేకాల కోసం ఉపయోగించిన బిట్లు మరియు ఆ నెట్వర్క్లో హోస్ట్లకు ఉపయోగించే బిట్లను స్పష్టంగా నిర్వచించవచ్చు. IPv4 లో సబ్నెట్కు డిఫాల్ట్ క్లాస్ఫుల్ నెట్ మాస్క్ తో ప్లే చేస్తాము, ఇది సబ్ నెట్ బిట్గా ఉపయోగించటానికి హోస్ట్ బిట్స్ ను అప్పుగా తీసుకునేలా అనుమతిస్తుంది. ఇది బహుళ సబ్ నెట్ లలో కానీ సబ్నెట్కు తక్కువ హోస్ట్లో ఉంటుంది. అంటే, ఒక ఉపనెట్ని సృష్టించడానికి హోస్ట్ బిట్లని మేము తీసుకుంటే, అతిధేయ చిరునామాల కోసం తక్కువ బిట్లో మాకు ఖర్చు అవుతుంది.

IPv6 addresses use 128 bits to represent an address which includes bits to be used for subnetting. The second half of the address (least significant 64 bits) is always used for hosts only. Therefore, there is no compromise if we subnet the network.

IPv6 చిరునామాలు 128 బిట్లను ఉపల్టింగ్ కోసం ఉపయోగించే బిట్లను కలిగి ఉండే చిరునామాను సూచించడానికి ఉపయోగిస్తాయి. అడ్రసు యొక్క రెండవ భాగం (అతి ముఖ్యమైన 64 బిట్స్) ఎల్లప్పుడూ హోస్ట్ల కోసం మాత్రమే ఉపయోగించబడుతుంది. అందువల్ల, మేము నెట్వర్క్ను సబ్ నెట్ చేస్తే రాజీ లేదు.

16 bits of subnet is equivalent to IPv4's Class B Network. Using these subnet bits, an organization can have another 65 thousands of subnets which is by far, more than enough.

సబ్నెట్ యొక్క 16 బిట్స్ IPv4 యొక్క క్లాస్ B నెట్వర్క్కు సమానం. ఈ సబ్నెట్ బిట్లను ఉపయోగించడం ద్వారా, ఒక సంస్థ మరో 65 వేల సబ్ నెట్లను కలిగి ఉంటుంది, ఇది చాలా కంటే ఎక్కువ.

Thus routing prefix is /64 and host portion is 64 bits. We can further subnet the network beyond 16 bits of Subnet ID, by borrowing host bits; but it is recommended that 64 bits should always be used for hosts addresses because auto-configuration requires 64 bits.

అందువలన రౌటింగ్ ఆదిప్రత్యయం / 64 మరియు హోస్ట్ భాగం 64 బిట్స్. మేము అనుసంధానిత బిట్లను అప్పుగా సబ్ నెట్ ID 16 బిట్లకు మించి నెట్ వర్క్ వేయవచ్చు. కానీ 64- బిట్లను హోస్ట్ చిరునామాలకు ఎల్లప్పుడూ ఉపయోగించాలి, ఎందుకంటే ఆటో-కాన్ఫిగరేషన్కు 64 బిట్లు అవసరం .

IPv6 subnetting works on the same concept as Variable Length Subnet Masking in IPv4.

IPv4 లో వేరియబుల్ లెంత్ సబ్నెట్ మాస్కింగ్ వలె అదే భావనపై IPv6 సబ్నెట్టింగ్ రచనలు.

/48 prefix can be allocated to an organization providing it the benefit of having up to /64 subnet prefixes, which is 65535 sub-networks, each having 2^{64}hosts. A /64 prefix can be assigned to a point-to-

point connection where there are only two hosts (or IPv6 enabled devices) on a link.

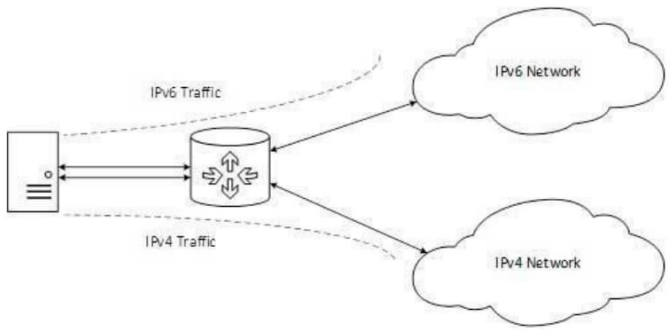
/ 48 ఉపసర్గను / సంస్థ యొక్క ఉపవ్యవస్థలకు / 64 సబ్ నెట్ పూర్వపదాలను కలిగివున్న ప్రయోజనానికి ఇది కేటాయించబడుతుంది, ఇది 65535 ఉప-నెట్వర్క్లు, ప్రతి ఒక్కటి 264 గంటలు. ఒక లింక్పై రెండు హోస్ట్ల (లేదా IPv6 ఎనేబుల్ డివైస్) ఉన్న ఒక పాయింట్-టు పాయింట్ కనెక్షన్కు A / 64 ఉపసర్గ కేటాయించవచ్చు .

Complete transition from IPv4 to IPv6 might not be possible because IPv6 is not backward compatible. This results in a situation where either a site is on IPv6 or it is not. It is unlike implementation of other new technologies where the newer one is backward compatible so the older system can still work with the newer version without any additional changes.
IPv4 నుండి IPv6 కు పూర్తి బదిలీ సాధ్యపడదు ఎందుకంటే IPv6 తిరోగమన అనుకూలతను కలిగి ఉండదు. ఇది ఒక సైట్ IPv6 లో వున్నప్పుడు లేదా అది కాదు. పాత కొత్త వ్యవస్థ ఇప్పటికీ ఏవైనా అదనపు మార్పులు లేకుండా సరికొత్త సంస్కరణతో పనిచేయగలగటంతో కొత్తగా వెనుకబడిన అనుకూలత ఉన్న ఇతర కొత్త టెక్నాలజీలను అమలు చేయకుండా ఉంటుంది.

To overcome this short-coming, we have a few technologies that can be used to ensure slow and smooth transition from IPv4 to IPv6.
ఈ స్వల్ప-రాబోయే విధానాన్ని అధిగమించడానికి, IPv4 నుండి IPv6 కు నెమ్మదిగా మరియు మృదువైన పరివర్తనను నిర్ధారించడానికి ఉపయోగించే కొన్ని సాంకేతికతలను కలిగి ఉంది.
Dual Stack Routers

A router can be installed with both IPv4 and IPv6 addresses configured on its interfaces pointing to the network of relevant IP scheme.

ఐపివి 4 మరియు IPv6 చిరునామాలతో అనుసందానించబడ్డ ఇంటర్ఫేస్లు అనుగుణంగా ఐపి స్కీమ్ యొక్క నెట్వర్క్కు గురిపెట్టి ఒక రౌటర్ను వ్యవస్థాపించవచ్చు.



In the above diagram, a server having IPv4 as well as IPv6 address configured for it can now speak with all the hosts on both the IPv4 as well as the IPv6 networks with the help of a Dual Stack Router. The Dual Stack Router, can communicate with both the networks. It provides a medium for the hosts to access a server without changing their respective IP versions.

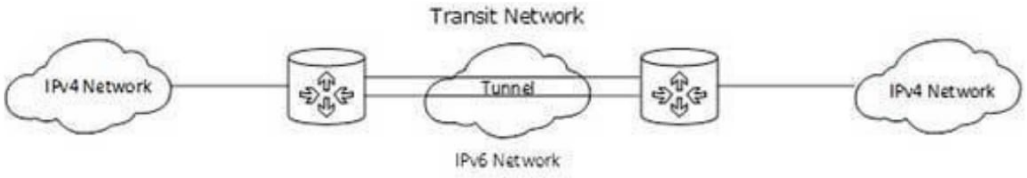
పై రేఖాచిత్రంలో, IPv4 కలిగివున్న సర్వర్ అలాగే దాని కొరకు ఆకృతీకరించిన IPv6 చిరునామా ఇప్పుడు IPv4 రెండింటిలో మరియు

హోస్ట్ డీల్ స్టాక్ రౌటర్ సహాయంతో IPv6 నెట్వర్క్లందరితో మాట్లాడవచ్చు. ద్వంద్వ స్టాక్ రూటర్, రెండు నెట్వర్క్లతో కమ్యూనికేట్ చేయవచ్చు. ఇది వారి IP సంస్కరణలను మార్చకుండా ఒక సర్వర్ను యాక్సెస్ చేయడానికి ఒక మాధ్యమం అందిస్తుంది.

Tunneling

In a scenario where different IP versions exist on intermediate path or transit networks, tunneling provides a better solution where user's data can pass through a non-supported IP version.

టన్నెలింగ్ వేర్వేరు IP సంస్కరణలు ఇంటర్మీడియట్ మార్గంలో లేదా ట్రాన్సిట్ నెట్వర్క్లలో ఉనికిలో ఉన్న సందర్భంలో, టన్నెలింగ్ యూజర్ యొక్క మద్దతు లేని IP వెర్షన్



The above diagram depicts how two remote IPv4 networks can communicate via a Tunnel, where the transit network was on IPv6. Vice versa is also possible where the transit network is on IPv6 and the remote sites that intend to communicate are on IPv4.

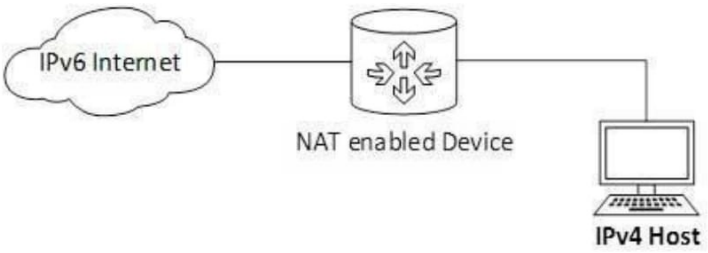
పైన రేఖాచిత్రం రెండు రిమోట్ IPv4 నెట్వర్క్ను ఒక టన్నెల్ ద్వారా ఎలా కమ్యూనికేట్ చేయగలవు, ఇక్కడ రవాణా నెట్వర్క్ IPv6 లో ఉంది. IPv6 లో రవాణా నెట్వర్క్ మరియు IPv4 లో కమ్యూనికేట్ చేయడానికి ఉద్దేశించిన రిమోట్ సైట్లు ఉన్నాయి, వైస్ వెర్సా కూడా అవకాశం ఉంది.

NAT Protocol Translation

This is another important method of transition to IPv6 by means of a NAT-PT (Network Address Translation – Protocol Translation) enabled device. With the help of a NAT-PT device, actual can take place happens between IPv4 and IPv6 packets and vice versa. See the diagram below:

NAT ప్రోటోకాల్ అనువాదం

ఇది NAT-PT (నెట్వర్క్ అడ్రెస్ ట్రాన్స్లేషన్ - ప్రోటోకాల్ ట్రాన్స్లేషన్) ఎనేబుల్ చేసిన పరికరం ద్వారా IPv6 కు మరొక ముఖ్యమైన పద్ధతి. ఒక NAT-PT పరికర సహాయంతో, IPv4 మరియు IPv6 ప్యాకెట్లను మరియు ఇదే విధంగా విరుద్ధంగా మధ్య జరుగుతుంది. దిగువన ఉన్న రేఖాచిత్రాన్ని చూడండి:



Mobility

A host with IPv4 address sends a request to an IPv6 enabled server on Internet that does not understand IPv4 address. In this scenario, the NAT-PT device can help them communicate. When the IPv4 host sends a request packet to the IPv6 server, the NAT-PT device/router strips down the IPv4 packet, removes IPv4 header, and adds IPv6 header and passes it through the Internet. When a response from the IPv6 server comes for the IPv4 host, the router does vice versa.

మొబిలిటీ

IPv4 చిరునామాతో అతిథేయ IPv6 చిరునామాను అర్థం చేసుకోని ఇంటర్నెట్లో IPv6 ప్రారంభించబడిన సర్వర్కు ఒక అభ్యర్థనను పంపుతుంది. ఈ దృష్టాంతంలో, NAT-PT పరికరం వాటిని కమ్యూనికేట్ చేయడానికి సహాయపడుతుంది. IPv4 హోస్ట్ IPv6 సర్వర్కు అభ్యర్థన ప్యాకెట్ పంపుతున్నప్పుడు, IPv4 ప్యాకెట్ పై NAT-PT పరికరం / రూటర్ స్ట్రిప్స్, IPv4 హెడర్ను తొలగిస్తుంది మరియు IPv6 శీర్షిక జతచేస్తుంది మరియు ఇంటర్నెట్ ద్వారా వెళుతుంది. IPv6 సర్వర్ నుండి ప్రతిస్పందన IPv4 హోస్ట్ కొరకు వచ్చినప్పుడు, రూటర్ వైస్ వెర్సా చేస్తుంది.

When a host is connected to a link or network, it acquires an IP address and all communication take place using that IP address on that link. As soon as, the same host changes its physical location, that is, moves into another area / subnet / network / link, its IP address changes accordingly, and all the communication taking place on the host using old IP address, goes down.

ఒక అతిథేయ లింక్ లేదా నెట్వర్కు కనెక్ట్ అయినప్పుడు, అది IP చిరునామాను పొందుతుంది మరియు అన్ని కమ్యూనికేషన్ ఆ లింక్లో ఆ IP చిరునామాను ఉపయోగించి జరుగుతుంది. వెంటనే, అదే హోస్ట్ దాని భౌతిక స్థానాన్ని మారుస్తుంది, అనగా మరొక ప్రాంతం / సబ్ నెట్ / నెట్వర్క్ / లింకు, దాని IP చిరునామా మార్పులు, మరియు పాత ఐపి చిరునామాను ఉపయోగించి హోస్ట్లో జరుగుతున్న అన్ని సంభాషణలు తరలిపోతాయి.

IPv6 mobility provides a mechanism for the host to roam around different links without losing any communication/connection and its IP address.

IPv6 చలనశీలత హోస్ట్ కోసం ఏదైనా కమ్యూనికేషన్ / కనెక్షన్ మరియు దాని IP చిరునామా కోల్పోకుండా వేర్వేరు లింకులు చుట్టూ తిరుగుతుంది.

Multiple entities are involved in this technology:
బహుళ సాంకేతికతలు ఈ టెక్నాలజీలో పాలుపంచుకున్నాయి:

- **Mobile Node**: The device that needs IPv6 mobility.

బైల్ నోడ్: IPv6 మొబిలిటీ అవసరం పరికరం.

- **Home Link**: This link is configured with the home subnet prefix and this is where the Mobile IPv6 device gets its Home Address.

హోం లింక్: ఈ లింక్ హోమ్ సబ్నెట్ ప్రిఫిక్స్తో కాన్ఫిగర్ చేయబడింది మరియు ఇది మొబైల్ IPv6 పరికరం దాని ఇంటి చిరునామాను పొందుతుంది.

- **Home Address**: This is the address which the Mobile Node acquires from the Home Link. This is the permanent address of the Mobile Node. If the Mobile Node remains in the same Home Link, the communication among various entities take place as usual.
ఇంటి చిరునామా: ఇది హోమ్ నోడ్ నుండి మొబైల్ నోడ్ పొందిన చిరునామా. ఇది మొబైల్ నోడ్ యొక్క శాశ్వత చిరునామా. మొబైల్ నోడ్ ఇదే హోమ్ లింక్లో ఉంటే, వివిధ సంస్థల మధ్య సమాచార మార్పిడి జరుగుతుంది.

- **Home Agent**: This is a router that acts as a registrar for Mobile Nodes. Home Agent is connected to Home Link and maintains information about all Mobile Nodes, their Home Addresses, and their present IP addresses.

హోం ఏజెంట్: ఇది మొబైల్ నోడ్స్ కోసం రిజిస్ట్రార్గా పనిచేసే రౌటర్. హోం ఏజెంట్ హోమ్ లింక్కు అనుసంధానించబడి, అన్ని మొబైల్ నోడ్స్, వారి ఇంటి చిరునామాలు మరియు వారి ప్రస్తుత IP చిరునామాల గురించి సమాచారాన్ని నిర్వహిస్తుంది.

- **Foreign Link**: Any other Link that is not Mobile Node's Home Link.

విదేశీ లింక్: మొబైల్ నోడ్ యొక్క హోమ్ లింక్ కాదని ఏ ఇతర లింక్.

- **Care-of Address**: When a Mobile Node gets attached to a Foreign Link, it acquires a new IP address of that Foreign Link's subnet. Home Agent maintains the information of both Home Address and Care-of Address. Multiple Care-of addresses can be assigned to a Mobile Node, but at any instance, only one Care-of Address has binding with the Home Address.

కేర్-ఆఫ్ అడ్రస్: ఒక మొబైల్ నోడ్ ఒక విదేశీ లింకుకు జతచేయబడినప్పుడు, అది ఆ విదేశీ లింక్ యొక్క సబ్ నెట్ యొక్క కొత్త IP చిరునామాను పొందుతుంది. హోం అడ్రస్ హోమ్ అడ్రస్ మరియు కేర్ ఆఫ్ అడ్రెస్ యొక్క సమాచారాన్ని నిర్వహిస్తుంది. బహుళ రక్షణ-చిరునామా చిరునామాలను మొబైల్ నోడ్కు కేటాయించవచ్చు, కానీ ఏ సందర్భంలోనైనా, ఒకే చిరునామా కేరిట్ చిరునామాతో ఇంటి చిరునామాతో బంధం ఉంది.

- **Correspondent Node**: Any IPv6 enabled device that intends to have communication with Mobile Node

కరస్పాండెంట్ నోడ్: మొబైల్ నోడ్తో సంభాషణను కలిగి ఉండే ఏదైనా IPv6 ఎనేబుల్ పరికరం

Routing

Routing concepts remain same in case of IPv6 but almost all routing protocols have been redefined accordingly. We discussed earlier, how a host speaks to its gateway. Routing is a process to forward routable data choosing the best route among several available routes or path to the destination. A router is a device that forwards data that is not explicitly destined to it.

IPv6 విషయంలో రౌటింగ్ భావనలు ఒకే విధంగానే ఉంటాయి, అయితే దాదాపు అన్ని రౌటింగ్ ప్రోటోకాల్లు దానికి అనుగుణంగా పునర్నిర్వచించబడ్డాయి. ముందుగా మేము చర్చించాము, ఒక గేట్ దాని గేట్వేకి ఎలా మాట్లాడుతుంది. రౌటింగ్ అనేది అనేక మార్గాలు లేదా గమ్యానికి మార్గం ద్వారా ఉత్తమ మార్గాన్ని ఎంచుకునే విధానాన్ని ముందుకు తీసుకువెళ్లడానికి ఒక ప్రక్రియ. ఒక రౌటర్ అనేది ఒక పరికరం, దానికి స్పష్టంగా నిర్దేశించబడని డేటా.

There exists two forms of routing protocols:
రెండు రౌటింగ్ ప్రోటోకాల్స్ ఉన్నాయి:

- **Distance Vector Routing Protocol**: A router running distance vector protocol advertises its connected routes and learns new routes from its neighbors. The routing cost to reach a destination is calculated by means of hops between the source and destination. A router generally relies on its neighbor for best path selection, also known as “routing-by-rumors”. RIP and BGP are Distance Vector Protocols.
- దూరం వెక్టర్ రూటింగ్ ప్రోటోకాల్: ఒక రౌటర్ నడుస్తున్న దూరం వెక్టార్ ప్రోటోకాల్ దాని కనెక్ట్ మార్గాలు ప్రచారం మరియు దాని పొరుగు నుండి కొత్త మార్గాలను నేర్చుకుంటుంది. ఒక గమ్యాన్ని చేరుకోవడానికి రూటింగ్ ఖర్చు మూలం మరియు గమ్యం మధ్య హాప్లు ద్వారా లెక్కిస్తారు. రౌటర్ సాధారణంగా పొరుగువారిపై ఉత్తమ మార్గం ఎంపిక కోసం ఆధారపడుతుంది, దీనిని "రూటింగ్-బై-పుకార్లు" అని కూడా పిలుస్తారు. RIP మరియు BGP దూరం వెక్టర్ ప్రోటోకాల్లు.

- **Link-State Routing Protocol**: This protocol acknowledges the state of a Link and advertises to its neighbors. Information about new links is learnt from peer routers. After all the routing information has been converged, the Link-State Routing Protocol uses its own algorithm to calculate the best path to all available links. OSPF and IS-IS are link state routing protocols and both of them use Dijkstra’s Shortest Path First algorithm.
  లింక్-స్టేట్ రౌటింగ్ ప్రోటోకాల్: ఈ ప్రోటోకాల్ లింక్ యొక్క స్థితిని తెలియజేస్తుంది మరియు దాని పొరుగువారికి ప్రచారం చేస్తుంది. కొత్త లింకుల గురించి సమాచారం పీర్ రౌటర్ల నుండి నేర్చుకుంది. అన్ని రౌటింగ్ సమాచారాన్ని సంకలనం చేసిన తర్వాత, లింక్-స్టేట్ రౌటింగ్ ప్రోటోకాల్ దాని స్వంత అల్గోరిథంను అన్ని అందుబాటులో ఉన్న లింక్లకు ఉత్తమ మార్గాన్ని లెక్కించడానికి ఉపయోగిస్తుంది. OSPF మరియు IS-IS లింక్ స్థితి రౌటింగ్ ప్రోటోకాల్లు మరియు రెండూ Dijkstra యొక్క చిన్నదైన మార్గం మొదటి అల్గోరిథంను ఉపయోగిస్తాయి .

Routing protocols can be divided in two categories:
రౌటింగ్ ప్రోటోకాల్స్ను రెండు విభాగాలలో విభజించవచ్చు:

- **Interior Routing Protocol**: Protocols in this categories are used within an autonomous system or organization to distribute routes among all routers inside its boundary. Examples: RIP, OSPF.

అంతర్గత రౌటింగ్ ప్రోటోకాల్: ఈ వర్గాలలో ప్రోటోకాల్లు దాని సరిహద్దు లోపల అన్ని రౌటర్ల మధ్య మార్గాలను పంపిణీ చేయడానికి ఒక స్వతంత్ర వ్యవస్థ లేదా సంస్థలో ఉపయోగించబడతాయి. ఉదాహరణలు: RIP, OSPF.

- **Exterior Routing Protocol**: An Exterior Routing Protocol distributes routing information between two different autonomous systems or organization. Examples: BGP.
- బయట రౌటింగ్ ప్రోటోకాల్: ఒక బాహ్య రౌటింగ్ ప్రోటోకాల్ రెండు వేర్వేరు స్వతంత్ర వ్యవస్థలు లేదా సంస్థల మధ్య రౌటింగ్ సమాచారాన్ని పంపిణీ చేస్తుంది. ఉదాహరణలు: BGP.

Network Security

నెట్వర్క్ సెక్యూరిటీ

Computer networks are an integral part of our personal and professional lives because we carry out lots of day-to-day activities through the Internet or local organizational network. The downside of this is that huge amount of data, from official documents to personal details, gets shared over the network. So it becomes necessary to ensure that the data is not accessed by unauthorized people.

ఇంటర్నెట్ లేదా స్థానిక సంస్థాగత నెట్వర్క్ ద్వారా రోజువారీ కార్యకలాపాలను నిర్వహిస్తున్నందున కంప్యూటర్ నెట్వర్క్లు మా వ్యక్తిగత మరియు వృత్తిపరమైన జీవితాల అంతర్భాగంగా ఉన్నాయి. దీని యొక్క దుష్ప్రభావం ఏమిటంటే అధిక సంఖ్యలో సమాచారం, అధికారిక పత్రాల నుండి వ్యక్తిగత వివరాలు, నెట్వర్క్లో పంచుకోబడుతుంది. కాబట్టి అనధికార వ్యక్తులచే డేటా ప్రాప్తి చేయబడదని నిర్ధారించడానికి ఇది అవసరం అవుతుంది.

Practices adopted to monitor and prevent unauthorized access and misuse of network resources and data on them is called **network security**.

అనధికార ప్రాప్యతను పర్యవేక్షించడం మరియు నిరోధించడం, వాటిపై నెట్వర్క్ వనరులు మరియు డేటాను దుర్వినియోగం చేయడం వంటి పద్ధతులు నెట్వర్క్ భద్రత అంటారు.

A network has two components – hardware and software. Both these components have their own vulnerability to threats. **Threat** is a possible risk that might exploit a network weakness to breach security and cause harm. Examples of hardware threats include –

హార్డ్వేర్ మరియు సాఫ్ట్వేర్ - నెట్వర్క్కు రెండు భాగాలుంటాయి. ఈ రెండింటికీ బెదిరింపులకు వారి సొంత బలహీనత ఉంది. భద్రత భంగం మరియు హాని కలిగించడానికి ఒక నెట్వర్క్ బలహీనతను దోపిడీ చేసే ప్రమాదం ముప్పు. హార్డ్వేర్ బెదిరింపులు ఉదాహరణలు ఉన్నాయి -

- Improper installation
- అక్రమ సంస్థాపన
- Use of unsecure components
- అసురక్షిత భాగాల ఉపయోగం
- Electromagnetic interference from external sources
- బాహ్య మూలాల నుండి విద్యుదయస్కాంత జోక్యం
- Extreme weather conditions
- తీవ్ర వాతావరణ పరిస్థితులు
- Lack of disaster planning

- విపత్తు ప్రణాళిక లేకపోవడం

Hardware threats form only 10% of network security threats worldwide because the components need to be accessed physically. 90% threats are through software vulnerabilities. Here we discuss the major types of software security threats.

ప్రపంచవ్యాప్తంగా నెట్వర్క్ భద్రతా బెదిరింపుల్లో కేవలం 10% మాత్రమే హార్డ్వేర్ బెదిరింపులు ఏర్పడుతున్నాయి, ఎందుకంటే భాగాలు భౌతికంగా ప్రాప్తి చెయ్యాలి. 90 % బెదిరింపులు సాఫ్ట్వేర్ దుర్బలత్వాలు. ఇక్కడ మేము ప్రధానంగా సాఫ్ట్వేర్ భద్రతా బెదిరింపులను చర్చించాము.

Virus (వైరస్)

A **virus** is a malicious program or **malware** that attaches itself to a host and makes multiple copies of itself (like a real virus!), slowing down, corrupting or destroying the system.

ఒక వైరస్ ఒక హానికర కార్యక్రమం లేదా మాల్వేర్ అనేది అతిథేయకు జోడించబడి, పలు కాపీలను (నిజమైన వైరస్ వంటిది) చేస్తుంది, మందగించడం, వ్యవస్థను నాశనం చేయడం లేదా వ్యవస్థ నాశనం చేస్తుంది.

Some harmful activities that can be undertaken by a virus are –

ఒక వైరస్ ద్వారా చేపట్టే కొన్ని హానికరమైన కార్యకలాపాలు -

- Taking up memory space
- మెమరీ స్థలాన్ని తీసుకొని
- Accessing private information like credit card details
- క్రెడిట్ కార్డు వివరాలు వంటి ప్రైవేటు సమాచారాన్ని యాక్సెస్ చేస్తోంది
- Flashing unwanted messages on user screen
- యూజర్ తెరపై అవాంఛిత సందేశాలను ఫ్లాషింగ్
- Corrupting data
- డేటాను అరికట్టడం
- Spamming e-mail contacts
- ఇ-మెయిల్ పరిచయాలను స్పామ్ చేస్తోంది

Viruses mostly attack Windows systems. Till a few years ago, Mac systems were deemed immune from viruses, however now a handful of viruses for them exist as well.

వైరస్లు ఎక్కువగా Windows వ్యవస్థలను దాడి చేస్తాయి. కొన్ని సంవత్సరాల క్రితం వరకు, మాక్ వ్యవస్థలు వైరస్ల నుండి రోగనిరోధక శక్తిగా భావించబడ్డాయి, అయితే ఇప్పుడు వాటి కోసం కొన్ని వైరస్లు కూడా ఉన్నాయి.

Viruses spread through e-mails and need a host program to function. Whenever a new program runs on the infected system, the virus attaches itself to that program. If you are an expert who tinkers with the OS files, they can get infected too.

వైరస్లు ఇ-మెయిల్స్ ద్వారా వ్యాప్తి చెందుతాయి మరియు పని చేయడానికి హోస్ట్ ప్రోగ్రామ్ అవసరం. ఒక కొత్త కార్యక్రమం సోకిన వ్యవస్థలో నడుస్తున్నప్పుడు, వైరస్ ఆ ప్రోగ్రామ్కు జోడించబడుతుంది. మీరు OS ఫైళ్ళతో టింకర్స్ అయిన నిపుణుడు అయితే, వారు చాలా బారిన పడతారు.

Trojan Horse

Trojan horse is a malware that hides itself within another program like games or documents and harms

the system. As it is masked within another program that appears harmless, the user is not aware of the threat. It functions in a way similar to **viruses** in that it needs a host program to attach itself and harms systems in the same ways.

ట్రోజన్ హార్స్

ట్రోజన్ హార్స్ గేమ్లు లేదా డాక్యుమెంట్ల వంటి మరొక కార్యక్రమంలో దాక్కున్న ఒక మాల్వేర్ మరియు వ్యవస్థను హానికరం చేస్తుంది. హానిరహితంగా కనిపించే మరొక ప్రోగ్రామ్లో ఇది మూసివేయబడితే, వినియోగదారు ముప్పు గురించి తెలియదు. ఇది వైరస్ల మాదిరిగా పనిచేస్తుంది, అదే విధంగా దానికి అనుగుణంగా వ్యవస్థలను దెబ్బతీస్తుంది మరియు వ్యవస్థలను పాడుచేస్తుంది.

Trojan horses spread through emails and exchange of data through hard drives or pen drives. Even worms could spread Trojan horses.

ట్రోజన్ హార్స్ హార్డ్ డ్రైవ్లు లేదా పెన్ డ్రైవ్ల ద్వారా ఇమెయిల్స్ ద్వారా మరియు డేటాను మార్పిడి చేస్తాయి. కూడా పురుగులు ట్రోజన్ హార్స్ వ్యాప్తి కాలేదు.

Worms

Worms are autonomous programs sent by the attacker to infect a system by replicating itself. They usually infect multitasking systems that are connected to a network. Some of the harmful activities undertaken by worms include –

వార్మ్స్

వార్మ్స్ స్వయంగా పునరుత్పత్తి ద్వారా వ్యవస్థ హాని దాడిచేత పంపిన స్వతంత్ర కార్యక్రమాలు. వారు సాధారణంగా నెట్వర్క్కి అనుసంధానించబడిన బహువిధి వ్యవస్థలను హాని చేస్తారు. పురుగులచే హానికరమైన కార్యకలాపాలలో కొన్ని ఉన్నాయి -

- Accessing and relaying back passwords stored on the system
వ్యవస్థలో నిల్వ చేసిన రహస్యపదాలను యాక్సెస్ చేయడం మరియు రిలే చేయడం
- Interrupt OS functioning
అంతరాయం ఆపరేటింగ్ సిస్టమ్
- Disrupt services provided by the system
సిస్టమ్ అందించిన సేవలను అశుద్ధం చేస్తుంది
- Install viruses or Trojan horses
ఇన్స్టాల్ వైరస్లు లేదా ట్రోజన్ హార్స్

Spams

Electronic junk mail, unsolicited mail or junk newsroom postings are called spam. Sending multiple unsolicited mails simultaneously is called **spamming**. Spamming is usually done as part of marketing tactics to announce a product or share political or social views with a wide base of people.

ఎలక్ట్రానిక్ వ్యర్థ మెయిల్, అయాచిత మెయిల్ లేదా జంక్ న్యూస్ రూమ్ పోస్టింగ్స్ స్పామ్ అంటారు. అనేక అయాచిత మెయిల్లను ఒకే సమయంలో పంపడం స్పామింగ్ అని పిలుస్తారు. స్పామింగ్ సాధారణంగా ఒక మార్కెటింగ్ వ్యూహంలో భాగంగా జరుగుతుంది, ఇది ఒక ఉత్పత్తిని ప్రకటించడానికి లేదా రాజకీయ లేదా సాంఘిక అభిప్రాయాలను ప్రజల విస్తృత స్థానాలతో పంచుకునేందుకు.

The first spam mail was sent by Gary Thuerk on ARPANET in 1978 to announce launch of new model of

Digital Equipment Corporation computers. It was sent to 393 recipients and together with lots of hue and cry it generated sales for the company as well.

డిజిటల్ స్పెషల్ కార్పోరేషన్ కార్పోరేషన్ కంప్యూటర్ల కొత్త మోడల్ను ప్రకటించడానికి 1978 లో ARPANET పై గ్యారీ థుర్మ్ మొదటి స్పామ్ మెయిల్ను పంపించారు. ఇది 393 గ్రహీతలకు మరియు పలు రంగులతో కలిసి మరియు సంస్థ కోసం అమ్మకాలను కూడా ఉత్పత్తి చేసింది.

Almost all mail servers give you the option of stopping spams by marking a received mail as junk. You should take care to share your email ID only with trusted people or websites, who will not sell them to spammers.

దాదాపుగా అన్ని మెయిల్ సర్వర్లు మీరు అందుకున్న మెయిల్ను వ్యర్థంగా గుర్తించడం ద్వారా స్పామ్లను ఆపే అవకాశం ఇస్తుంది. మీరు మీ ఇమెయిల్ ID ను విశ్వసనీయ వ్యక్తులు లేదా వెబ్సైట్లతో మాత్రమే పంచుకునేందుకు శ్రద్ధ వహించాలి, వారిని స్పామర్లకు విక్రయించదు.

Firewall

There exist multiple approaches to counter or at least reduce security threats. Some of these are –

ఎదుర్కోవడానికి లేదా కనీసం భద్రతా బెదిరింపులను తగ్గించడానికి బహుళ విధానాలు ఉన్నాయి. వీటిలో కొన్ని -

- Authenticating users accessing a service
- సేవను యాక్సెస్ చేసే వినియోగదారులను గుర్తించడం
- Providing access to authorized users
- అధీకృత వినియోగదారులకు యాక్సెస్ను అందించడం
- Using encrypted passwords for remote log on
- రిమోట్ లాగ్ కోసం గుప్తీకరించిన పాస్వర్డ్లను ఉపయోగించడం
- Using biometric authorization parameters
- బయోమెట్రిక్ ప్రామాణీకరణ పారామితులను ఉపయోగించడం
- Restricting traffic to and from
- ట్రాఫిక్ ను నియంత్రిస్తుంది

Firewalls are the first line of defense against unauthorized access to private networks. They can be used effectively against virus, Trojan or worm attacks.

ప్రైవేట్ నెట్వర్క్లకు అనధికారిక ప్రాప్యతకు వ్యతిరేకంగా ఫైర్వాల్స్ రక్షణ యొక్క మొదటి మార్గం. అవి వైరస్, ట్రోజన్ లేదా వార్మ్ దాడులకు వ్యతిరేకంగా సమర్థవంతంగా ఉపయోగించబడతాయి.

How Firewalls Work

Dictionary defines **firewall** as a wall or partition designed to inhibit or prevent spread of fire. In networks, a system designed to protect an intranet from **unauthorized access** is called firewall. A private network created using World Wide Web software is called an **intranet**. Firewall may be implemented in both hardware and software.

ఎలా ఫైర్‌వాల్స్ పని చేస్తాయి ?

నిఘంటువు ఫైర్ లేదా అగ్ని వ్యాప్తి నిరోధించడానికి లేదా నిరోధించడానికి రూపొందించిన ఒక గోడ లేదా విభజన నిర్వచిస్తుంది. నెట్వర్క్లలో, అనధికార ప్రాప్యత నుండి ఇంట్రానెట్ను రక్షించడానికి రూపొందించిన వ్యవస్థను ఫైర్వాల్ అని పిలుస్తారు. వరల్డ్ వైడ్ వెబ్ సాఫ్ట్వేర్ను ఉపయోగించి సృష్టించబడిన ఒక ప్రైవేట్ నెట్వర్క్ను ఇంట్రానెట్ అని పిలుస్తారు. ఫైర్వాల్ హార్డ్వేర్ మరియు సాఫ్ట్వేర్ రెండింటిలోనూ అమలు చేయబడవచ్చు.

All traffic to and from the network is routed through the firewall. The firewall examines each message and blocks those that does not meet the **pre-defined security criteria**.

నెట్వర్క్ నుండి మరియు అన్ని ట్రాఫిక్ను ఫైర్వాల్ ద్వారా రద్దయింది. ఫైర్వాల్ ప్రతి సందేశమును పరిశీలిస్తుంది మరియు ముందే నిర్వచించిన భద్రతా ప్రమాణంను చేరుకోని వాటిని అడ్డుకుంటుంది.

These are some of the prevalent techniques used by firewalls –

ఈ ఫైర్వాల్స్ ఉపయోగించే ప్రబలమైన పద్ధతులు కొన్ని –

- **Packet level filtering** – Here each packet is examined depending on user-defined rules. It is very effective and transparent to users, but difficult to configure. Also, as IP address is used to identify users, **IP spoofing** by malicious parties can prove counterproductive.

  ప్యాకెట్ స్థాయి వడపోత - ఇక్కడ ప్రతి ప్యాకెట్ యూజర్ నిర్వచించిన నిబంధనలను బట్టి పరీక్షించబడుతుంది. ఇది వినియోగదారులకు చాలా ప్రభావవంతమైనది మరియు పారదర్శకంగా ఉంటుంది, కానీ ఆకృతీకరించడం కష్టం. అలాగే, IP చిరునామాను వినియోగదారులు గుర్తించడానికి ఉపయోగిస్తారు, హానికరమైన పార్టీల ద్వారా IP స్పూఫింగ్ ప్రతికూలమైనదిగా నిరూపించగలదు .

- **Circuit level filtering** – Like good old telephone connections, circuit level filtering applies security mechanisms while connection between two systems is being established. Once the connection is deemed secure, data transmission can take place for that session.

  సర్క్యూట్ స్థాయి ఫిల్టరింగ్ - మంచి పాత టెలిఫోన్ కనెక్షన్ల వలె, సర్క్యూట్ స్థాయి ఫిల్టరింగ్ రెండు వ్యవస్థల మధ్య కనెక్షన్ ఏర్పాటు చేస్తున్నప్పుడు భద్రతా వ్యవస్థలను వర్తింపచేస్తుంది. కనెక్షన్ సురక్షితంగా భావించిన తర్వాత, ఆ సెషన్కు డేటా ట్రాన్స్మిషన్ జరుగుతుంది .

- **Application level filtering** – Here, security mechanisms are applied to commonly used applications like Telnet, FTP servers, storage servers, etc. This is very effective but slows down performance of the applications.

  స్థాయి వడపోత - ఇక్కడ, టెల్నెట్, FTP సర్వర్లు, స్టోరేజ్ సర్వర్లు మొదలైనవి సాధారణంగా ఉపయోగించిన అనువర్తనాలకు భద్రతా విధానాలు వర్తిస్తాయి. ఇది చాలా ప్రభావవంతంగా ఉంటుంది కానీ అనువర్తనాల పనితీరు నెమ్మదిస్తుంది .

- **Proxy server** – As the name suggests, proxy server is used to interrupt all incoming and outgoing messages and mask the true server address.

ప్రాక్సీ సర్వర్ - పేరు సూచించినట్లు, ప్రాక్సీ సర్వర్ అన్ని ఇన్కమింగ్ మరియు అవుట్గోయింగ్ సందేశాలు అంతరాయం మరియు నిజమైన సర్వర్ చిరునామాను ముసుగు చేయడానికి ఉపయోగించబడుతుంది .

A firewall may use a combination of two or more techniques to secure the network, depending on extent of security required.
అవసరమయ్యే భద్రత మేరకు, ఫైర్వాల్ నెట్వర్క్ను సురక్షితంగా ఉంచడానికి రెండు లేదా అంతకంటే ఎక్కువ సాంకేతికతలను కలయికగా ఉపయోగించవచ్చు .

Cookies

Cookies are small text files with their **unique ID** stored on your system by a website. The website stores your browsing details like preferences, customizations, login ID, pages clicked, etc. specific to that website. Storing this information enables the website to provide you with a customized experience the next time you visit it.

కుకీలు ఒక ప్రత్యేకమైన ID తో మీ టెక్స్ట్ మీద నిల్వవున్న చిన్న టెక్స్ట్ ఫైల్స్. వెబ్ సైట్ కు నిర్దిష్టమైన ప్రాధాన్యతలు, అనుకూలీకరణలు, లాగిన్ ID, పేజీలు క్లిక్ చేయడం, మొదలైనవి వంటి మీ బ్రౌజింగ్ వివరాలను వెబ్సైట్ నిల్వ చేస్తుంది. ఈ సమాచారాన్ని నిల్వ చేయడం, మీరు సందర్శించే తదుపరిసారి అనుకూలీకరించిన అనుభవాన్ని మీకు అందించడానికి వెబ్సైట్ను అనుమతిస్తుంది .

How Cookies Work

When you visit a website through your browser, the website creates and stores a cookie file in your browser or program data folder/sub-folder. This cookie may be of two types –
మీరు మీ బ్రౌజర్ ద్వారా ఒక వెబ్సైట్ను సందర్శించినప్పుడు, వెబ్ సైట్ మీ బ్రౌజర్ లేదా ప్రోగ్రామ్ డేటా ఫోల్డర్ / సబ్-ఫోల్డర్లో కుకీ ఫైల్ని సృష్టిస్తుంది మరియు నిల్వ చేస్తుంది. ఈ కుకీ రెండు రకాలు కావచ్చు

- **Session cookie** – It is valid only till the session lasts. Once you exit the website the cookie is automatically deleted.
- సెషన్ కుకీ - సెషన్ వరకు మాత్రమే ఇది చెల్లుతుంది. మీరు వెబ్సైట్ నుండి నిష్క్రమించిన తర్వాత కుకీ స్వయంచాలకంగా తొలగించబడుతుంది.
- **Persistent cookie** It is valid beyond your current session. Its expiration date is mentioned within the cookie itself.
  సెషన్ కుకీ - సెషన్ వరకు మాత్రమే ఇది చెల్లుతుంది. మీరు వెబ్సైట్ నుండి నిష్క్రమించిన తర్వాత కుకీ స్వయంచాలకంగా తొలగించబడుతుంది .

A cookie stores these information –
కుకీ ఈ సమాచారాన్ని నిల్వ చేస్తుంది -

- Name of website server
- Cookie expiration date/time
- Unique ID

A cookie is meaningless by itself. It can be read only by the server that stored it. When you visit the website subsequently, its server matches cookie ID with its own database of cookies and loads webpages according to your browsing history.

ఒక కుక్కీ స్వయంగా అర్థం కాదు. ఇది నిల్వ చేసిన సర్వర్ ద్వారా మాత్రమే చదవబడుతుంది. మీరు ఈ వెబ్సైట్ను సందర్శిస్తున్నప్పుడు, మీ బ్రౌజింగ్ చరిత్ర ప్రకారం దాని సర్వర్ కుకీలు మరియు లోడ్లు వెబ్పేజీలతో దాని సర్వర్ కుకీ ఐడితో సరిపోలుతుంది.

Handling Cookies

Cookies were initially designed to enhance user's web browsing experience. However, in the current aggressive marketing scenario, **rogue cookies** are being used to create your profile based on your browsing patterns without consent. So you need to be wary of cookies if you care about your privacy and security.

కుకీలను నిర్వహించడం

వినియోగదారుల వెబ్ బ్రౌజింగ్ అనుభవాన్ని మెరుగుపరచడానికి కుకీలు ప్రారంభంలో రూపొందించబడ్డాయి. అయితే, ప్రస్తుత ఉగ్రమైన మార్కెటింగ్ దృష్టాంతంలో, అనుమతి లేకుండా మీ బ్రౌజింగ్ నమూనాల ఆధారంగా మీ ప్రొఫైల్ను రూపొందించడానికి రోగ్ కుకీలను ఉపయోగిస్తున్నారు. కాబట్టి మీరు మీ గోప్యత మరియు భద్రత గురించి పట్టించుకోనట్లయితే మీరు కుకీలను జాగ్రత్త వహించాలి.

Almost all modern-day browsers give you options to allow, disallow or limit cookies on your system. You can view the cookies active on your computer and make decisions accordingly.

దాదాపు అన్ని ఆధునిక-రోజు బ్రౌజర్లు మీ సిస్టమ్పై కుక్కీలను అనుమతించవద్దు, అనుమతించవద్దు లేదా పరిమితం చేయడానికి మీకు ఎంపికలను అందిస్తాయి. మీరు మీ కంప్యూటర్లో చురుకుగా ఉన్న కుక్కీలను చూడవచ్చు మరియు తదనుగుణంగా నిర్ణయాలు తీసుకోవచ్చు.

Hacking

Unauthorized access to data in a device, system or network is called **hacking**. A person hacking another person's system is called hacker. A hacker is a highly accomplished computer expert who can exploit the smallest of vulnerabilities in your system or network to hack it.

పరికరం, వ్యవస్థ లేదా నెట్వర్క్లో డేటాకు అనధికార ప్రాప్యత హ్యాకింగ్ అని పిలుస్తారు. మరొక వ్యక్తి యొక్క వ్యవస్థను హ్యాకింగ్ చేస్తున్న వ్యక్తి హ్యాకర్ అని పిలుస్తారు. హ్యాకర్ అనేది మీ వ్యవస్థలో లేదా హాక్ చేయడానికి నెట్వర్క్లో ఉన్న దుర్బలత్వాలను అతిక్రమించే అత్యంత నైపుణ్యం కలిగిన కంప్యూటర్ నిపుణుడు .

A hacker may hack due to any of the following reasons −

- Steal sensitive data
- Take control of a website or network

- Test potential security threats
- Just for fun
- Broadcast personal views to a large audience

Types of Hacking

Depending on the application or system being broken into, these are some categories of hacking common in the cyber world –

రకాలు హ్యాకింగ్

దరఖాస్తు లేదా వ్యవస్థ విచ్ఛిన్నం అవుతోంది, ఈ సైబర్ ప్రపంచంలో సాధారణ హ్యాకింగ్ కొన్ని వర్గాలు ఉన్నాయి -

- Website hacking
- Network hacking
- Email hacking
- Password hacking
- Online banking hacking

Ethical Hacking

As iron sharpens iron, hacking counters hacking. Using hacking techniques to identify potential threats to a system or network is called **ethical hacking**. For a hacking activity to be termed ethical, it must adhere to these criteria –

నైతిక హ్యాకింగ్ ఇనుము

ఇనుము పదునుగా, హ్యాకింగ్ కౌంటర్లు హ్యాకింగ్. వ్యవస్థ లేదా నెట్వర్క్కు సంభావ్య బెదిరింపులను గుర్తించడానికి హ్యాకింగ్ పద్ధతులను ఉపయోగించి నైతిక హ్యాకింగ్ అంటారు. ఒక హ్యాకింగ్ సూచించే నైతిక అని పిలుస్తారు, అది ఈ ప్రమాణాలను కట్టుబడి ఉండాలి -

- Hacker must have written permission to identify potential security threats
- సంభావ్య భద్రతా బెదిరింపులను గుర్తించడానికి హ్యాకర్కు వ్రాతపూర్వక అనుమతి ఉండాలి
- Individual's or company's privacy must be maintained
- వ్యక్తి లేదా సంస్థ యొక్క గోప్యతను నిర్వహించాలి
- Possible security breaches discovered must be intimated to the concerned authorities
- గుర్తించదగిన భద్రతా ఉల్లంఘనలను సంబంధిత అధికారులకు తెలియజేయాలి
- At a later date, no one should be able to exploit ethical hacker's inroads into the network
- తరువాతి రోజున, ఎవరూ నెట్వర్క్ లోకి నైతిక హ్యాకర్ యొక్క ప్రవేశాలు దోపిడీ చెయ్యలేరు

Cracking

A term that goes hand in glove with hacking is cracking. Gaining unauthorized access to a system or network with malicious intent is called **cracking**. Cracking is a crime and it may have devastating impact on its victims. Crackers are criminals and strong cyber laws have been put into place to tackle them.

హ్యాకింగ్ తో చేతి తొడుగు లోకి వెళ్లిన ఒక పదాన్ని క్రాకింగ్ చేస్తుంది. హానికరమైన ఉద్దేశ్యంతో వ్యవస్థ లేదా నెట్వర్క్కు అనధికార ప్రాప్యతను పొందడం అనేది క్రాకింగ్ అంటారు. క్రాకింగ్ ఒక నేరం మరియు దాని బాధితులపై వినాశకరమైన ప్రభావాన్ని కలిగి ఉండవచ్చు. క్రాకర్స్ నేరస్తులు మరియు బలమైన సైబర్ చట్టాలు వాటిని పరిష్కరించడానికి స్థానంలో ఉంచబడ్డాయి.

Security Acts And Laws

Cyber Crimes

Any unlawful activity involving or related to computer and networks is called **cybercrime**. Dr. K. Jaishankar, Professor and Head of the Department of Criminology, Raksha Shakti University, and Dr. Debarati Halder, lawyer and legal researcher, define cybercrime thus –

సైబర్ క్రైమ్స్

కంప్యూటర్ మరియు నెట్వర్క్లతో సంబంధం ఉన్న ఏదైనా అశాస్త్రీయ కార్యకలాపం సైబర్క్రైమ్ అంటారు. డాక్టర్ K. జైషంకర్, క్రిమినోల విభాగం యొక్క ప్రొఫెసర్ మరియు అధిపతి, రక్షా శక్తి యూనివర్శిటీ, మరియు డాక్టర్ డిబరతి హాలేడర్, న్యాయవాది మరియు న్యాయ పరిశోధకుడు, సైబర్క్రైమ్ను ఈ విధంగా నిర్వచించారు -

Offences that are committed against individuals or groups of individuals with a criminal motive to intentionally harm the reputation of the victim or cause physical or mental harm, or loss, to the victim directly or indirectly, using modern telecommunication networks such as Internet (networks including but not limited to Chat rooms, emails, notice boards and groups) and mobile phones (Bluetooth/SMS/MMS).

బాధితుడి యొక్క ఖ్యాతికి ఉద్దేశపూర్వకంగా హాని కలిగించే లేదా శారీరక లేదా మానసిక హాని లేదా నష్టాన్ని కలిగించే ఒక నేర ఉద్దేశ్యంతో వ్యక్తులు లేదా సమూహాలకు వ్యతిరేకంగా కట్టుబడి ఉన్న నేరాలు బాధితులకు ప్రత్యక్షంగా లేదా పరోక్షంగా, ఇంటర్నెట్ వంటి ఆధునిక టెలికమ్యూనికేషన్ నెట్వర్క్లను (చాట్ గదులు, ఇమెయిల్లు, నోటీసు బోర్డులు మరియు సమూహాలకు మాత్రమే పరిమితం కాకుండా) మరియు మొబైల్ ఫోన్లు (బ్లూటూత్ / SMS / MMS)

This definition implies that any crime perpetrated on the Internet or using computers is a cybercrime.

ఈ డెఫినిషన్ ఇంటర్నెట్లో జరిగే నేరాలు లేదా కంప్యూటర్లు ఉపయోగించడం అనేది ఒక సైబర్క్రైమ్ అని సూచిస్తుంది.

Examples of cybercrimes include –

- Cracking
- Identity theft
- Hate crime
- E-commerce fraud

- Credit card account theft
- Publishing obscene content
- Child pornography
- Online stalking
- Copyright infringement
- Mass surveillance
- Cyber terrorism
- Cyber warfare

Cyber Law

Cyber law is a term that encompasses legal issues related to use of **Internet**and **cyberspace**. It is a broad term that covers varied issues like freedom of expression, internet usage, online privacy, child abuse, etc. Most of the countries have one or the other form of cyber law in place to tackle the growing menace of cybercrimes.

సైబర్ లా

సైబర్ చట్టం ఇంటర్నెట్ మరియు సైబర్స్పేస్ను ఉపయోగించే చట్టపరమైన సమస్యలను కలిగి ఉంటుంది. వ్యక్తీకరణ స్వేచ్ఛ, ఇంటర్నెట్ వినియోగం, ఆన్లైన్ గోప్యత, పిల్లల దుర్వినియోగం మొదలైనవి వంటి పలు అంశాలని ఇది విస్తృతపరుస్తుంది. చాలా దేశాలలో సైబర్క్రైమ్స్ యొక్క పెరుగుతున్న ప్రమాదం పరిష్కరించడానికి ఒకటి లేదా ఇతర సైబర్ చట్టాన్ని కలిగి ఉన్నాయి.

A major issue here is that in any crime perpetrator, victim and instruments used might be spread across multiple locations nationally as well as internationally. So investigating the crime needs close collaboration between computer experts and multiple government authorities, sometimes in more than one country.

ఇక్కడ ఒక ప్రధాన సమస్య ఏమిటంటే ఏ నేరం నేరస్తుడు, బాధితుడు మరియు సాధన వంటివి దేశీయంగా మరియు అంతర్జాతీయంగా బహుళ ప్రదేశాలలో వ్యాప్తి చెందుతాయి. కాబట్టి నేర దర్యాప్తు కంప్యూటర్ నిపుణులు మరియు అనేక ప్రభుత్వ అధికారుల మధ్య సన్నిహిత సహకారం అవసరం, కొన్నిసార్లు ఒకటి కంటే ఎక్కువ దేశాల్లో .

Indian IT Act

Information Technology Act, **2000** is the primary Indian law dealing with **cybercrime** and **e-commerce**. The law, also called **ITA-2000** or **IT Act**, was notified on 17th October 2000 and is based on the United Nations Model Law on Electronic Commerce 1996 recommended by the UN General Assembly on 30th January 1997.

భారత ఐటి చట్టం

సమాచార సాంకేతిక చట్టం, 2000 సైబర్క్రైమ్ మరియు ఇ-కామర్స్తో వ్యవహరించే ప్రాధమిక భారతీయ చట్టం. ఐటీఏ-2000 లేదా ఐటి చట్టం అని కూడా పిలవబడే ఈ చట్టం 17 అక్టోబరు 2000 న ప్రకటించబడింది మరియు ఇది యునైటెడ్ మీద ఆధారపడిందిఎలక్ట్రానిక్ కామర్స్పై నేషన్స్ మోడల్ లా 1996 జనవరి 30 న UN జనరల్ అసెంబ్లీచే సిఫార్సు చేయబడింది.

The IT Act covers whole of India and recognizes electronic records and digital signatures. Some of its prominent features include –

ఐటీ చట్టం భారతదేశం మొత్తాన్ని వర్తిస్తుంది మరియు ఎలక్ట్రానిక్ రికార్డులను మరియు డిజిటల్ సంతకాలను గుర్తిస్తుంది. దాని ప్రముఖ లక్షణాలలో కొన్ని ఉన్నాయి -

- Formation of Controller of Certifying Authorities to regulate issuance of digital signatures
- డిజిటల్ సంతకాల జారీని నియంత్రించడానికి సర్టిఫైయింగ్ అధికారుల కంట్రోలర్ యొక్క నిర్మాణం
- Establishment of Cyber Appellate Tribunal to resolve disputes due to the new law
- కొత్త చట్టం కారణంగా వివాదాలను పరిష్కరించేందుకు సైబర్ అప్పీలేట్ ట్రిబ్యునల్ ఏర్పాటు
- Amendment in sections of Indian Penal Code, Indian Evidence Act, Banker's Book Evidence Act and RBI Act to make them technology compliant
- ఇండియన్ పీనల్ కోడ్, ఇండియన్ ఎవిడెన్స్ యాక్ట్, బ్యాంకర్స్ బుక్ ఎవిడెన్స్ యాక్ట్ మరియు ఆర్బిఐ యాక్ట్ లలో సవరణలు

The IT Act was framed to originally to provide legal infrastructure for e-commerce in India. However, major amendments were made in 2008 to address issues like cyber terrorism, data protection, child pornography, stalking, etc. It also gave authorities the power to intercept, monitor or decrypt any information through computer resources.

భారతదేశంలో ఇ-కామర్స్ కోసం చట్టపరమైన మౌలిక సదుపాయాలను అందించడానికి మొదట ఐటి చట్టం రూపొందించబడింది. అయితే, 2008 లో సైబర్ టెర్రరిజం, డేటా రక్షణ, పిల్లల అశ్లీలత, స్టాకింగ్ వంటి అంశాలపై ప్రధాన సవరణలు జరిగాయి. కంప్యూటర్ వనరుల ద్వారా ఏదైనా సమాచారాన్ని అడ్డగించడం, మానిటర్ చేయడం లేదా వ్యక్తీకరించడం వంటి అధికారాలను కూడా ఇది అధికారాన్ని ఇచ్చింది.

IPR Issues

IPR stands for **Intellectual Property Rights**. IPR is legal protection provided to creators of **Intellectual Property (IP)**. IP is any creation of the intellect or mind, like art, music, literature, inventions, logo, symbols, tag lines, etc. Protecting the rights of intellectual property creators is essentially a moral issue. However, law of the land does provide legal protection in case of violation of these rights.

IPR విషయాలు

IPR మేధో సంపత్తి హక్కులని సూచిస్తుంది. IPR అనేది మేధో సంపత్తి సృష్టికర్తలకు (IP) అందించిన చట్టపరమైన రక్షణ. కళ, సంగీతం,

సాహిత్యం, ఆవిష్కరణలు, లోగో, చిహ్నాలు, ట్యాగ్ లైన్లు లాంటి మేధస్సు లేదా మనస్సు యొక్క ఏవైనా సృష్టి. IP మేధో సంపత్తి సృష్టికర్తల హక్కులను రక్షించడం అనేది నైతిక సమస్య. అయినప్పటికీ, ఈ హక్కుల ఉల్లంఘన విషయంలో భూమి యొక్క చట్టం చట్టపరమైన రక్షణను అందిస్తుంది.

Intellectual Property Rightsinclude–

- Patents
- Copyrights
- Industrial design rights
- Trademarks
- Plant variety rights
- Trade dress
- Geographical indications
- Trade secrets

Violation of Intellectual Property Rights is called **infringement** in case of patents, copyrights and trademarks, and **misappropriation** in case of trade secrets. Any published material that you view or read on the Internet is copyright of its creator and hence protected by IPR. You are legally and morally obliged not to use it and pass it off as your own. That would be infringement of creator's copyright and you may incur legal action.

మేధోసంపత్తి హక్కుల ఉల్లంఘనను పేటెంట్స్, కాపీరైట్ల మరియు ట్రేడ్మార్క్లు, మరియు వాణిజ్య రహస్యాలు విషయంలో దుర్వినియోగం జరిగిన సందర్భంలో ఉల్లంఘన అంటారు. ఇంటర్నెట్లో మీరు వీక్షించిన లేదా చదివే ఏదైనా ప్రచురించిన విషయం దాని సృష్టికర్త యొక్క కాపీరైట్ మరియు అందుకే IPR ద్వారా రక్షించబడుతుంది. మీరు దాన్ని చట్టబద్ధంగా మరియు నైతికంగా ఉపయోగించుకోవడం లేదు, దాన్ని మీ స్వంతం చేసుకోవడం లేదు. అది సృష్టికర్త యొక్క కాపీరైట్ ఉల్లంఘన మరియు మీరు చట్టపరమైన చర్యలు జరగవచ్చు.

UPS (uninterruptible power supply)

UPS (uninterruptible power supply) systems are a critical component of your data center, whether you're running just a couple computers or numerous servers. When selecting a UPS, you'll have to choose among a number of options, but if you can differentiate between the various available configurations, you'll be better able to choose the right system to meet your needs.

UPS (నిరంతర విద్యుత్ సరఫరా) వ్యవస్థలు మీ డేటా కేంద్రానికి ఒక కీలక భాగం, మీరు కేవలం జంట కంప్యూటర్లను లేదా అనేక సర్వర్లను అమలు చేస్తున్నారని. UPS ని ఎంపికచేసినప్పుడు, మీరు అనేక ఎంపికలలో ఎంపిక చేసుకోవాలి, కానీ వివిధ అందుబాటులో ఉన్న కాన్ఫిగరేషన్ల మధ్య మీరు వేరు చేయగలిగితే, మీ అవసరాలను తీర్చడానికి సరైన వ్యవస్థను ఎంచుకోగలుగుతారు.

Why a UPS?

Imagine if your heart decided to quit beating for a while, of if it all of the sudden slowed way down or sped up in a sharp burst. Not a very appealing scenario, is it? Now, imagine that the power supply to your company's IT equipment failed, or if it sent large spikes to your equipment. Although this situation isn't as macabre as the metaphor of a heart, it nonetheless spells trouble for your business. Power is the lifeblood of your data center, and your IT equipment is designed to be supplied with a steady flow.
మీ గుండె కొంచెం కొట్టడం విడిచిపెట్టాలని నిర్ణయించుకుంటే, ఊహిస్తే అకస్మాత్తుగా పదునైన పేలవమైన మార్గంలో అది పడిపోతుంది. చాలా ఆకర్షణీయమైన దృశ్యం కాదు, ఇది? ఇప్పుడు, మీ కంపెనీ యొక్క ఐటి పరికరాలకు విద్యుత్ సరఫరా విఫలమైంది, లేదా అది మీ పరికరాలకు పెద్దగా వచ్చే చిక్కులు పంపినట్లయితే ఊహించుకోండి. ఈ పరిస్థితి హృదయ రూపకం వంటి భ్రమకరంగా లేనప్పటికీ, ఇది మీ వ్యాపారానికి ఇబ్బందినిస్తుంది. శక్తి మీ డేటా సెంటర్ యొక్క జీవనాడిగా ఉంది, మరియు మీ ఐటి పరికరాలు స్థిరమైన ప్రవాహంతో సరఫరా చేయబడతాయి.

Unfortunately, the power delivered from your utility isn't as steady as you'd like it to be. Brief power outages, power sags and power surges/spikes can cause more than just a hassle—they can cause damage to your IT equipment. Although backup power generators can supply your data center in the case of an extended outage (hours or even days), they are no help when you're faced with transient power fluctuations. For example, if another utility customer starts a large inductive load, you may feel the effects down the line in the form of a short lived, but potentially harmful, power event. In such a case, you wouldn't have any warning—let alone time to switch to a backup generator.

దురదృష్టవశాత్తూ, మీ ప్రయోజనం నుండి పంపిణీ చేయబడిన శక్తి అది మీకు కావలసినంత నిలకడగా ఉండదు. క్లుప్తంగా విద్యుత్ వైఫల్యాలు, పవర్ సాగ్స్ మరియు పవర్ సర్జ్ / వచ్చే చిక్కులు కేవలం ఒక అవాంతరం కంటే ఎక్కువగా ఉంటాయి-అవి మీ ఐటి పరికరాలకు నష్టం కలిగించవచ్చు. బ్యాకప్ శక్తి జనరేటర్లు మీ డేటా సెంటర్ను పొడిగించిన విరామ సందర్భంలో (గంటలు లేదా రోజులు) సరఫరా చేయగలవు, మీరు తాత్కాలిక శక్తి హెచ్చుతగ్గులు ఎదుర్కొంటున్నప్పుడు వారు ఎటువంటి సహాయం చేయలేరు. ఉదాహరణకు, మరొక ప్రయోజన కస్టమర్ ఒక పెద్ద ప్రేరక లోడ్ను ప్రారంభించినట్లయితే, మీరు తక్కువ కాలం గడిపిన, కాని హానికర, శక్తి ఘటన రూపంలో ఈ క్రింది ప్రభావాలను అనుభవిస్తారు. అలాంటి సందర్భంలో, మీకు బ్యాకప్ జెనరేటర్కు మారడానికి ఏవైనా హెచ్చరికలు ఉండవు.

To deal with these short-lived power events, a UPS is critical. These systems not only provide temporary backup power for brief outages, but many also provide protection against transient power events like spikes and sags, thereby supplying your equipment with clean, high-quality power. Essentially, a UPS is a power storage device that cleans your power supply or takes over in the event of a power failure, giving you time to switch to your backup generators if the outage is expected to last more than some short period of time (like a minute or two, depending on your UPS's capacity).

ఈ స్వల్ప కాలిక శక్తి సంఘటనలను ఎదుర్కోవటానికి, ఒక UPS క్లిష్టమైనది. ఈ వ్యవస్థలు క్లుప్త వైఫల్యాల కోసం తాత్కాలిక బ్యాకప్ శక్తిని అందించడం మాత్రమే కాదు, అయితే పలువురు కూడా స్పైక్లు మరియు సాక్స్ వంటి తాత్కాలిక పవర్ ఈవెంట్లకు వ్యతిరేకంగా రక్షణను అందిస్తారు, తద్వారా మీ సామగ్రిని శుభ్రంగా, అధిక నాణ్యత గల శక్తితో సరఫరా చేస్తుంది. అత్యవసరంగా, UPS మీ విద్యుత్ సరఫరాను శుభ్రపరుస్తుంది లేదా విద్యుత్తు వైఫల్యం సందర్భంగా తీసుకుంటుంది, మీ బ్యాకప్ జెనరేటర్లకు కొంత సమయం తక్కువగా

ఉన్నట్లయితే, ఒక నిమిషం లేదా రెండు, మీ UPS యొక్క సామర్థ్యాన్ని బట్టి).

Energy Storage: Battery or Flywheel

UPSs store power either in the form of chemical energy (as in a battery) or energy of motion (as in a flywheel). The case of the battery is familiar: your notebook computer, for instance, can run off standard AC power, all while charging the battery, but if AC power fails or is disconnected, the notebook then switches seamlessly to the battery. A UPS performs a similar function, although it does so as a separate unit rather than being integrated into a computer or server. The UPS's ability to power your equipment in the event of an outage depends, of course, on how much equipment you're powering and on the capacity of the battery.

రసాయన శక్తి (బ్యాటరీలో) లేదా కదలిక శక్తి (ఫ్లైవీహిల్లో) వంటి రూపంలో UPS లు నిల్వ శక్తిని కలిగి ఉంటాయి. బ్యాటరీ విషయంలో తెలిసినది: మీ నోట్బుక్ కంప్యూటర్, ఉదాహరణకు, బ్యాటరీ ఛార్జింగ్ చేస్తున్నప్పుడు, ప్రామాణిక AC శక్తిని అమలు చేయగలదు, అయితే AC శక్తి విఫలమైతే లేదా డిస్కనెక్ట్ అయినట్లయితే, నోట్బుక్ బ్యాటరీకి సజావుగా మారుతుంది. ఒక UPS ఒక ఇదే పనితీరును ప్రదర్శిస్తుంది, అయితే ఒక కంప్యూటర్ లేదా సర్వర్లో విలీనం కాకుండా ఇది ఒక ప్రత్యేక యూనిట్ వలె ఉంటుంది. అవుట్ అయ్యే సందర్భంలో మీ పరికరాలను అధికారం చేయడానికి UPS యొక్క సామర్థ్యాన్ని, మీరు ఎంత శక్తిని ఉపయోగిస్తున్నారనే దానిపై మరియు బ్యాటరీ సామర్థ్యంపై ఆధారపడి ఉంటుంది.

An alternative energy storage approach is the flywheel. The flywheel is a rotating mechanical wheel that stores energy in the form of motion (angular momentum). When an outage occurs, for example, the flywheel's energy of motion is converted back to electrical energy to supply the equipment (the flywheel then slows as more energy is removed). Some flywheels are heavy and slowly rotating, but some are lighter and run at much higher speeds. Although flywheels generally do not store as much energy as a battery, they do offer some advantages. Processor.com ("UPS Flywheel Technology") notes, for instance, that the flywheel offers "superior performance without the high cost of ownership and the environmental impacts that lead batteries present." Furthermore, its "rapid recharging and broad operating temperature range...allow it to be used where batteries cannot operate. The footprint of flywheels is also much smaller and lighter than a battery's footprint."

ప్రత్యామ్నాయ శక్తి నిల్వ విధానం ఫ్లైవీల్. ఫ్లైవీల్ మోషన్ రూపంలో శక్తిని నిల్వ చేసే తిరిగే యాంత్రిక చక్రం (కోణీయ మొమెంటం). ఉదాహరణకు ఒక ఔట్టేజ్ ఏర్పడుతుంది, ఉదాహరణకు, ఫ్లైవీల్ యొక్క శక్తి శక్తిని తిరిగి సరఫరా చేయడానికి విద్యుత్ శక్తిగా మార్చబడుతుంది (మరింత శక్తిని తొలగించినప్పుడు ఫ్లైవీల్ తగ్గిపోతుంది). కొన్ని ఫ్లైవీల్స్ భారీ మరియు నెమ్మదిగా తిరిగేవి, కానీ కొన్ని ఉన్నాయి తేలికైన మరియు అధిక వేగంతో అమలు. ఫ్లైవీల్స్ సాధారణంగా బ్యాటరీగా ఎక్కువ శక్తిని నిల్వ చేయకపోయినప్పటికీ, వారు కొన్ని ప్రయోజనాలను అందిస్తారు. ఉదాహరణకి, ఫ్లైవీల్ "యాజమాన్యం యొక్క అధిక వ్యయం మరియు బ్యాటరీలను అందించే పర్యావరణ ప్రభావాలు లేకుండా ఉన్నత పనితీరును అందిస్తుంది" అని ప్రాసెసర్.కామ్ ("UPS ఫ్లైవీల్ టెక్నాలజీ") పేర్కొంది. అంతేకాకుండా, దాని "వేగవంతమైన రీఛార్జింగ్ మరియు విస్తృత

ఆపరేటింగ్ ఉష్ణోగ్రత పరిధి. బ్యాటరీలు ఆపరేట్ చేయలేని వాటిని ఉపయోగించుకోండి. ఫ్లైవీల్స్ యొక్క పాద ముద్ర బ్యాటరీ యొక్క పాద ముద్ర కంటే చాలా చిన్నది మరియు తేలికైనది.

Regardless of the means of energy storage, however, a UPS is essentially a short-term backup power supply, although many also add in power quality improvement features.

అయినప్పటికీ ఎనర్జీ స్టోరేజ్తో సంబంధం లేకుండా, UPS తప్పనిసరిగా స్వల్పకాలిక బ్యాకప్ విద్యుత్ సరఫరా, అయితే అనేకమంది విద్యుత్ నాణ్యతా మెరుగుదల లక్షణాల్లో చేర్చారు.

What's in a UPS?

A UPS takes AC power, stores a portion of the energy in the backup battery but otherwise transfers the AC power (possibly after cleaning it up) to the connected equipment. To perform this function, the UPS needs three basic components: a charger/rectifier, a battery (or flywheel apparatus—but the focus here is on the case of a battery) and an inverter. The charger (or rectifier) converts the input AC power to DC for battery charging, and the inverter converts battery power (DC) to AC power during an outage. The configuration of these main components, as well as additional design aspects, determines how the UPS functions.

ఒక UPS AC శక్తిని తీసుకుంటుంది, బ్యాకప్ బ్యాటరీలో శక్తి యొక్క భాగాన్ని నిల్వ చేస్తుంది, అయితే కనెక్ట్ చేయబడిన పరికరాలకు AC శక్తిని (దానిని శుభ్రపరిచిన తర్వాత) బదిలీ చేస్తుంది. ఈ విధిని నిర్వహించడానికి, UPS కు మూడు ప్రాథమిక భాగాలు అవసరం: ఒక ఛార్జర్ / రిక్టిఫైయర్, ఒక బ్యాటరీ (లేదా ఫ్లైవీల్ ఉపకరణం-కానీ ఇక్కడ దృష్టి బ్యాటరీ విషయంలో ఉంటుంది) మరియు ఇన్వర్టర్. ఛార్జర్ (లేదా రెక్టిఫైయర్) బ్యాటరీ ఛార్జింగ్ కోసం డిసికి ఇన్పుట్ AC పవర్ను మారుస్తుంది మరియు ఇన్వర్టర్ బ్యాటరీ శక్తిని (DC) మినహాయింపు సమయంలో AC పవర్కు మారుస్తుంది. ఈ ప్రధాన భాగాల ఆకృతీకరణ, అలాగే అదనపు రూపకల్పన అంశాలు, ఎలా UPS విధులు నిర్ణయిస్తుంది.

Types of UPS

UPSs come in several basic varieties, each with its own advantages and disadvantages (such as features, cost and so on). Here are the three main types:

UPS లు అనేక ప్రాథమిక రకాలు, వాటి సొంత ప్రయోజనాలు మరియు అప్రయోజనాలు (లక్షణాలు, ధర మరియు మొదలైనవి) కలిగి ఉంటాయి. ఇక్కడ మూడు ప్రధాన రకాలు:

Standby (offline) UPS. The least expensive variation, the standby UPS charges its battery when main power is active, but it is otherwise inactive until a power outage strikes. When this occurs, the UPS switches to backup battery power, giving the user time to switch to a longer-term backup supply or to properly shut down the connected equipment. This type of UPS doesn't provide protection from power sags and surges, however, so it isn't fit for applications where high availability is required or where protection from such power events is otherwise required.

స్టాండ్బై (ఆఫ్లైన్) UPS. ప్రధాన వ్యయం క్రియాశీలంగా ఉన్నప్పుడు అతి తక్కువ ఖరీదైన వైవిధ్యం, స్టాండ్బై యుపిఎస్ బ్యాటరీని చెల్లిస్తుంది, అయితే విద్యుత్తు అంతరాయం దాడుల వరకు అది క్రియారహితంగా ఉంటుంది. ఇది సంభవించినప్పుడు, బ్యాటరీ బ్యాటరీ

శక్తిని బ్యాకప్ చేయడానికి UPS మారుతుంది, దీర్ఘకాలిక బ్యాకప్ సరఫరాకు మారడానికి లేదా కనెక్ట్ చేయబడిన పరికరాన్ని సరిగా మూసివేయడానికి వినియోగదారుని సమయం ఇవ్వడం. ఈ రకమైన UPS పవర్ సాగ్స్ మరియు సర్జెస్ నుండి రక్షణను అందించదు, అయితే, అధిక లభ్యత అవసరమయ్యే అనువర్తనాలకు సరిపోదు లేదా అలాంటి పవర్ ఈవెంట్ల నుండి రక్షణ అవసరం లేకపోతే.

Advantages:

- Low cost(తక్కువ ధర)
- Silent operation when in standby(నిశ్శబ్ద ఆపరేషన్లో ఉన్నప్పుడు)
- Efficient(సమర్ధవంతమైన)

Disadvantages:

- Minimal power protection - only protects against a small percentage of problems
- కనీసపు శక్తి రక్షణ - ఒక చిన్న శాతం సమస్యల నుండి మాత్రమే రక్షించబడుతుంది
- Poor output voltage regulation - sags and surges will be passed straight to the load
- తక్కువ ఉత్పత్తి వోల్టేజ్ నియంత్రణ - సాగ్గులు మరియు కదలికలు నేరుగా లోడ్ చేయబడతాయి
- Break transfer to battery mode
- మోడ్కు బదిలీని బ్రేక్ చేయండి
- No failsafe - UPS will drop the load if there is a high start-up current, overload or inverter failure
- విఫలమైనది - అధిక ప్రారంభ-ప్రస్తుత, ఓవర్లోడ్ లేదా ఇన్వెస్టర్ వైఫల్యం ఉన్నట్లయితే యుపిఎస్ లోడ్ తగ్గిపోతుంది

Line interactive UPS. This type of UPS combines the inverter and charger in the power supply line for both the main AC power and the backup battery power. This configuration limits transient events when switching and also speeds the changeover from main power to battery power in the event of an outage. A line interactive UPS thus provides more protection than a standby UPS, but it is also more expensive.

లైస్ ఇంటరాక్టివ్ UPS. ఈ రకం UPS ప్రధాన AC పవర్ మరియు బ్యాకప్ బ్యాటరీ శక్తి రెండింటి కోసం విద్యుత్ సరఫరా లైన్లో ఇన్వర్టర్ మరియు ఛార్జర్లను మిళితం చేస్తుంది. ఈ కాన్ఫిగరేషన్ ట్రాన్సియంట్ ఈవెంట్స్ను పరిమితం చేసేటప్పుడు పరిమితం చేస్తుంది మరియు ప్రధాన విద్యుత్తు నుండి బ్యాటరీ శక్తికి మించిపోయే సందర్భంలో మార్పును వేగవంతం చేస్తుంది. ఒక లైన్ ఇంటరాక్టివ్ UPS విధంగా స్టాండ్బై యుపిఎస్ కంటే ఎక్కువ రక్షణను అందిస్తుంది, కానీ ఇది చాలా ఖరీదైనది.

Advantages:

- Lower cost than on
- ఆన్లైన్ కంటే తక్కువ ఖర్చు
- Gives better protection than offline
- ఆఫ్లైన్ కంటే మెరుగైన రక్షణను ఇస్తుంది
- Silent operation when in standby
- నిశ్శబ్ద ఆపరేషన్లో ఉన్నప్పుడు
- Efficient
- సమర్ధవంతమైన

Disadvantages:

- Fluctuations, such as spikes, can still be passed straight to the load
- వచ్చే చిక్కులు వంటి ఫ్లుక్యువేషన్లు ఇప్పటికీ లోడ్కు నేరుగా పంపబడతాయి
- Break on transfer to battery mode.
- బ్యాటరీ మోడ్కు బదిలీపై బ్రేక్.
- No failsafe - UPS will drop the load if there is a high start-up current, overload or inverter failure
- విఫలమైనది - అధిక ప్రారంభ-ప్రస్తుత, ఓవర్లోడ్ లేదా ఇన్వెస్టర్ వైఫల్యం ఉన్నట్లయితే యుపిఎస్ లోడ్ తగ్గిపోతుంది

Double conversion (online) UPS. This variation provides the most protection from outages and power quality problems. Instead of switching from main power to backup (battery) power as needed, this UPS simply converts all AC power to DC. Some of the DC power charges the battery, and the rest is converted back to AC to power the connected equipment. This double conversion process essentially prevents any power event from reaching the equipment, thus yielding the greatest protection level. In addition to being the most expensive option, however, double conversion UPSs also decrease operating efficiency owing to the conversion of AC to DC and then back to AC during normal operation. Some power is always lost in this process; the other UPS types, on the other hand, essentially feed AC power directly (possibly with some filtering) to equipment when main power is functioning, avoiding the inefficiencies of power conversion. Furthermore, double conversion UPS systems also operate at higher temperatures, increasing the cooling load in a data center, for example.

డబుల్ మార్పిడి (ఆన్లైన్) UPS . ఈ వైవిధ్యం వైఫల్యం మరియు శక్తి నాణ్యత సమస్యల నుండి అత్యధిక రక్షణను అందిస్తుంది. అవసరమైనప్పుడు బ్యాకప్ (బ్యాటరీ) శక్తికి ప్రధాన శక్తి నుండి మారడానికి బదులుగా, ఈ యుపిఎస్ అన్ని AC శక్తిని DC కి మారుస్తుంది. DC పవర్లో కొన్ని బ్యాటరీని ఛార్జ్ చేస్తాయి, మిగిలినవి కనెక్ట్ చేయబడిన సామగ్రిని శక్తివంతం చేయడానికి AC కి తిరిగి మార్చబడతాయి. ఈ డబుల్ మార్పిడి ప్రక్రియ తప్పనిసరిగా పరికరాన్ని చేరుకోకుండా ఏ పవర్ ఈవెంట్ను నిరోధిస్తుంది, తద్వారా అత్యధిక రక్షణ స్థాయిని అందిస్తుంది. అయితే, అత్యంత ఖరీదైన ఎంపికగా ఉండటంతో పాటు, డబుల్ మార్పిడి UPS లు కూడా ఆపరేటింగ్ సామర్థ్యాన్ని తగ్గిస్తాయి, ఎందుకంటే AC కి DC మారిపోవడం మరియు సాధారణ ఆపరేషన్ సమయంలో AC కి తిరిగి వెళ్లడం. ఈ ప్రక్రియలో కొంత శక్తి ఎల్లప్పుడూ కోల్పోతుంది; మరోవైపు ఇతర UPS రకాలు ప్రధాన విద్యుత్ శక్తి పనితీరు అయినప్పుడు, విద్యుత్ శక్తి మార్పిడి యొక్క తప్పించుకోకుండా తప్పనిసరిగా ఎసి విద్యుత్ను నేరుగా (బహుశా కొన్ని ఫిల్టరింగ్తో) పరికరానికి తిండిస్తుంది. అంతేకాకుండా, డబుల్ మార్పిడి UPS వ్యవస్థలు కూడా అధిక ఉష్ణోగ్రతల వద్ద పనిచేస్తాయి, ఉదాహరణకి డేటా సెంటర్లో శీతలీకరణ లోడ్ పెరుగుతుంది .

If you're just running a single machine, say in a SOHO situation, then a standby UPS might just fit the bill. But for corporate data centers, where downtime is unacceptable and expensive equipment must be protected from power quality problems, standby and even line interactive UPSs are insufficient. In these situations, some form of double conversion is crucial.

మీరు ఒకే యంత్రాన్ని అమలు చేస్తే, ఒక SOHO పరిస్థితిలో చెప్పండి, అప్పుడు స్టాండ్బై యుపిఎస్ బిల్లుకు సరిపోతుంది. కానీ కార్పోరేట్ డేటా కేంద్రాల కోసం, సమయములో మందమైన సమయం ఉండదు మరియు ఖరీదైన పరికరాలు పవర్ నాణ్యత సమస్యల నుండి కాపాడబడాలి, స్టాండ్బై మరియు లైన్ ఇంటరాక్టివ్ UPS లు సరిపోవు. ఈ పరిస్థితులలో, కొన్ని రకపు డబుల్ మార్పిడి కీలకం .

UPS systems are a critical part of a data center's power infrastructure. Although they do cannot keep a facility running during a long outage, they provide the short-term protection necessary to avoid damage equipment and to give the facility manager time to activate diesel backup generators if needed

డేటా సెంటర్ యొక్క శక్తి అవస్థాపనలో UPS వ్యవస్థలు కీలకమైన భాగంగా ఉన్నాయి. సుదీర్ఘ కాల వ్యవధిలో పనిచేసే సదుపాయాన్ని వారు నిర్వహించలేనప్పటికీ, హానిని నివారించడానికి అవసరమైన స్వల్ప-కాలిక రక్షణను వారు అందిస్తారు పరికరాలు మరియు అవసరమైతే డీజిల్ బ్యాకప్ జనరేటర్లు సక్రియం చేయడానికి సౌకర్యం మేనేజర్ సమయం ఇవ్వాలని

Although this article only provides basic details of how UPSs operate, it serves as a jumping off point if you're investigating a particular solution for your data center.

ఈ వ్యాసం UPS లు ఎలా పనిచేస్తుందో అనే ప్రాథమిక వివరాలను మాత్రమే అందిస్తున్నప్పటికీ, మీరు మీ డేటా సెంటర్ కోసం ఒక ప్రత్యేక పరిష్కారం గురించి దర్యాప్తు చేస్తే, ఇది ఒక జంపింగ్ పాయింట్ వలె పనిచేస్తుంది.

Advantages:

ప్రయోజనాలు:

- Continuous & total power conditioning
- నిరంతర మరియు మొత్తం శక్తి కండిషనింగ్
- Failsafe/overload protection with static bypass facility
- స్థిర బైపాస్ సదుపాయంతో ఫెయిల్సేఫ్ / ఓవర్లోడ్ రక్షణ
- No break on mains failure
- మెయిన్స్ వైఫల్యం మీద విరామం లేదు
- Wide input voltage tolerance
- వైడ్ ఇన్పుట్ వోల్టేజ్ టాలరెన్స్
- Recommended with Generator sets
- జనరేటర్ సెట్లతో సిఫార్సు చేయబడింది

Disadvantages:

ప్రతికూలతలు:

- More expensive than other types of UPS technology
- ఇతర రకాల UPS టెక్నాలజీ కంటే మరింత ఖరీదైనది

How do I select the right size UPS for my equipment?

నా పరికరాల కోసం సరైన పరిమాణ UPS ను ఎలా ఎంచుకోవాలి?

As far as SBS and UPS equipment is concerned "size does matter, but bigger is not necessarily better".In choosing SBS and UPS equipment, selecting a model of the proper size is central. Selecting an SBS or UPS that is too small to provide enough power for the equipment you need protected should be avoided. It may result in having to return the unit for a larger model, or cause the SBS or UPS to fail. As a good portion of the purchase price of an SBS or UPS is directly related to its size or output capacity, selecting one that is too large for your needs will be a waste of money. More important it may be the difference between buying an over-sized SBS providing limited protection, or the correct size On-line UPS, which gives a much greater level of power protection.

SBS మరియు UPS పరికరాలకు సంబంధించి "పరిమాణాన్ని కలిగి ఉంటుంది, కానీ పెద్దది తప్పనిసరిగా మంచిది కాదు." SBS మరియు UPS పరికరాన్ని ఎంచుకుని, సరైన పరిమాణంలోని నమూనాను ఎంచుకోవడం కేంద్రం. మీరు రక్షించాల్సిన అవసరం కోసం తగినంత శక్తిని అందించడానికి చాలా తక్కువగా ఉండే SBS లేదా UPS ను ఎంచుకోవడం తప్పనిసరిగా దూరంగా ఉండాలి. ఇది పెద్ద మోడల్ కోసం యూనిట్ను తిరిగి పొందడం లేదా SBS లేదా UPS విఫలం కావడానికి కారణం కావచ్చు. SBS లేదా UPS యొక్క కొనుగోలు ధర యొక్క ఒక మంచి భాగాన్ని నేరుగా దాని పరిమాణం లేదా అవుట్పుట్ సామర్థ్యంతో అనుసంధానించడం వలన, మీ అవసరాలకు చాలా పెద్దదిగా ఎంచుకోవడం డబ్బును కోల్పోతుంది. మరింత ముఖ్యమైనది, అధిక-పరిమాణం గల SBS ని పరిమిత రక్షణను అందించే లేదా సరైన పరిమాణంలో ఆన్ లైన్ UPS ని అందించే మధ్య వ్యత్యాసం కావచ్చు, ఇది అధిక స్థాయి రక్షణ శక్తిని ఇస్తుంది.

The size of SBS and UPS units indicates their output power capacity. This rating is in VA (volt/amperes) or kVA (thousand volt amperes) which is preceded by a number like 500VA or 2kVA. To the lay person this can be confusing, because the power consumption label located on most equipment is typically rated in watts or amps, not VA. When the rating is specified in VA, it can become more confusing, as the input power factor of the equipment must also be considered. Most SBS and UPS manufacturers state the output power of their UPS products in Watts or Amps somewhere on their product box or in their published specifications. Most manufacturers make their product specifications available on their web sites.

SBS మరియు యుపిఎస్ విభాగాల పరిమాణాన్ని వారి అవుట్పుట్ పవర్ సామర్థ్యాన్ని సూచిస్తుంది. ఈ రేటింగ్ VA (వోల్ట్ / ఆంపియర్స్) లేదా kVA (వేల వోల్ట్ ఆంపియర్) లో ఉంది, ఇది 500VA లేదా 2kVA వంటి సంఖ్యతో ముగుస్తుంది. లే వ్యక్తికి ఇది గందరగోళంగా ఉంటుంది, ఎందుకంటే చాలా పరికరాల్లో విద్యుత్ వినియోగ లేబుల్ సాధారణంగా వాట్స్ లేదా ఆప్లలో రేట్ చేయబడుతుంది, VA కాదు. రేటింగ్ VA లో పేర్కొన్నప్పుడు, అది మరింత గందరగోళంగా తయారవుతుంది, ఎందుకంటే పరికరం యొక్క ఇన్పుట్ పవర్ ఫాక్టర్ కూడా పరిగణనలోకి తీసుకోవాలి. చాలా ఎస్బిఎస్ మరియు యుపిఎస్ తయారీదారులు వారి యుపిఎస్ ఉత్పత్తుల ఉత్పాదక శక్తిని వాట్స్ లేదా ఆంప్స్లో తమ ఉత్పత్తి పెట్టెలో లేదా వారి ప్రచురించిన వివరణల్లో ఎక్కడో చెపుతారు. చాలామంది తయారీదారులు తమ వెబ్ సైట్లలో తమ ఉత్పత్తి వివరణలను అందుబాటులోకి తీసుకుంటారు.

To determine the input watts required to power a specific piece of equipment, multiply the input current (in AMPS) required operating the equipment times the utility voltage. In the United States the utility voltage is 120Vac, so for a piece of equipment requiring 5 Amps, one would multiply (5 x 120) = 600 watts. Do not confuse the input plug rating of a piece of electrical equipment, (15, 20 or 30 Amps) as the actual current required to operate the equipment. The actual input current required is usually specified on a label located somewhere on the equipment.

పరికరానికి ఒక ప్రత్యేకమైన పరికరాన్ని అవసరమయ్యే ఇన్పుట్ వాట్లను గుర్తించేందుకు, పరికరాలను వినియోగించే వోల్టేజ్ సమయాల్లో అవసరమైన ఇన్పుట్ కరెంట్ (AMPS లో) గుణించండి. యునైటెడ్ స్టేట్స్ యుటిలిటీ వోల్టేజ్ 120Vac, కాబట్టి 5 ఆంప్ల అవసరం ఉన్న పరికరాల భాగానికి, ఒకటి (5 x 120) = 600 వాట్స్. విద్యుత్ పరికరాల యొక్క ఇన్పుట్ ప్లగ్ రేటింగ్ కంగారుపడకండి, (15, 20 లేదా 30 ఆంప్స్) పరికరాలను ఆపరేట్ చేయడానికి అవసరమైన వాస్తవమైన ప్రవాహం. అవసరమయ్యే అసలు ఇన్పుట్

ప్రస్తుత సాధారణంగా పరికరంలో ఎక్కడా ఉన్న లేబుల్పై పేర్కొనబడుతుంది

Determining the power requirements for computers (the simple rule of thumb) For the majority of PC and Mac based computers having up to a combination of four hard and one CDROM drive, with one monitor(up to 19"), one network router or modem, selecting a UPS with a

350 watt output will be more than adequate.

కంప్యూటర్ల కోసం పవర్ అవసరాలు (thumb యొక్క సాధారణ నిబంధన) నిర్ణయించడం PC మరియు Mac ఆధారిత కంప్యూటర్ల కోసం ఒక హార్డ్వేర్ మరియు ఒక CDROM డ్రైవ్ కలయికతో, ఒక మానిటర్ (19 వరకు వరకు), ఒక నెట్వర్క్ రౌటర్ లేదా మోడెమ్ , 350 U వాట్ అవుట్పుట్తో UPS ను ఎంచుకోవడం తగినంతగా సరిపోతుంది.

Determining the power requirements for your computers (the absolutely safe method) Should you have more equipment that needs to be protected, or are unsure of the previous method do the following? 1. Write down all of the stated input currents and wattage requirement for every piece of equipment to be protected and convert any current ratings to watts, add them up to determine the total wattage requirement. Be suspect of any individual current ratings that state 15 amps as it is highly unlikely that any office equipment would require that much current. This usually represents the full current rating of the typical electrical outlet found in most households and offices in the U.S.

మీ కంప్యూటర్లు (ఖచ్చితంగా సురక్షితమైన పద్ధతి) కోసం విద్యుత్ అవసరాలకు నిర్ణయించడం మీరు రక్షించాల్సిన మరింత సామగ్రిని కలిగి ఉండాలి లేదా మునుపటి పద్ధతిని ఖచ్చితంగా తెలియదా? 1. పేర్కొన్న ఇన్పుట్ ప్రవాహాలు మరియు వాటేజ్ అవసరాలు అన్ని రక్షక సామగ్రి కోసం వ్రాసి, వాట్లకు ప్రస్తుత రేటింగ్లను మార్చడానికి, మొత్తం వాటేజ్ అవసరాన్ని గుర్తించడానికి వారిని జోడిస్తాయి. ఏ వ్యక్తి ప్రస్తుత రేటింగ్స్ యొక్క అనుమానితుడిగా ఉండండి, ఆ 15 amps ను ఏ కార్యాలయ సామగ్రి అయినా చాలా అవసరం అని చాలా అరుదుగా ఉంటుంది. ఇది సాధారణంగా U.S. లోని చాలా కుటుంబాలు మరియు కార్యాలయాలలో కనిపించే సాధారణ విద్యుత్ ఔట్లెట్ యొక్క పూర్తి ప్రస్తుత రేటింగ్ను సూచిస్తుంది.

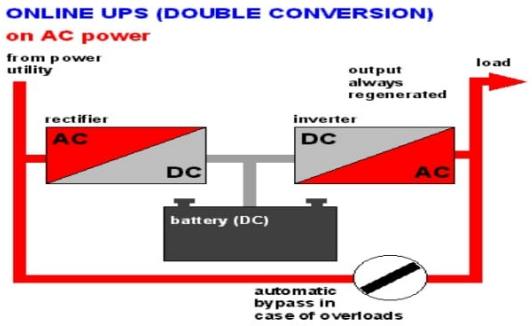
Remember the stated input rating on computers and other electrical equipment in most cases represents the worst case requirements.

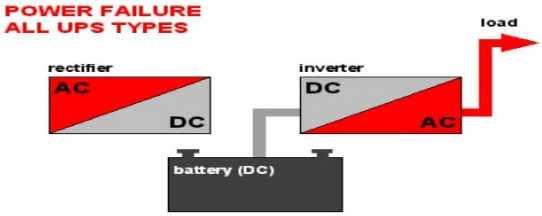
చాలా సందర్భాలలో కంప్యూటర్లు మరియు ఇతర ఎలక్ట్రికల్ పరికరాలపై పేర్కొన్న ఇన్పుట్ రేటింగ్ను గుర్తుంచుకోండి, చెత్త కేసుల అవసరాలను సూచిస్తుంది.

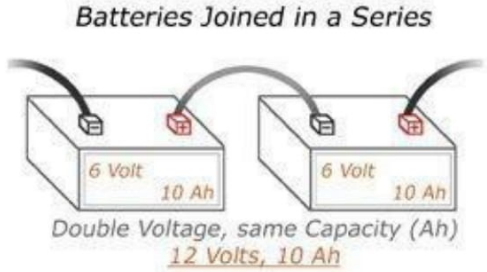
What you should know about laser printers, laser copiers and faxes machines. Incorporating a laser printer, copier or any other equipment incorporating a heating element called a "fuser" can cause SBS and UPS unit problems. The best approach is to avoid connecting them to any SBS or UPS. The fuser randomly switches on and off, requiring a substantial amount of current with every on cycle. We have determined that to successfully power a typical laser printer requires an SBS or UPS capable of more that 1200 watts. Additionally many or these devices do not work properly with a SBS or UPS that does not have a true sinewave output. Should it be necessary to protect this type of equipment, install a separate over sized SBS or UPS that powers only that piece of equipment?

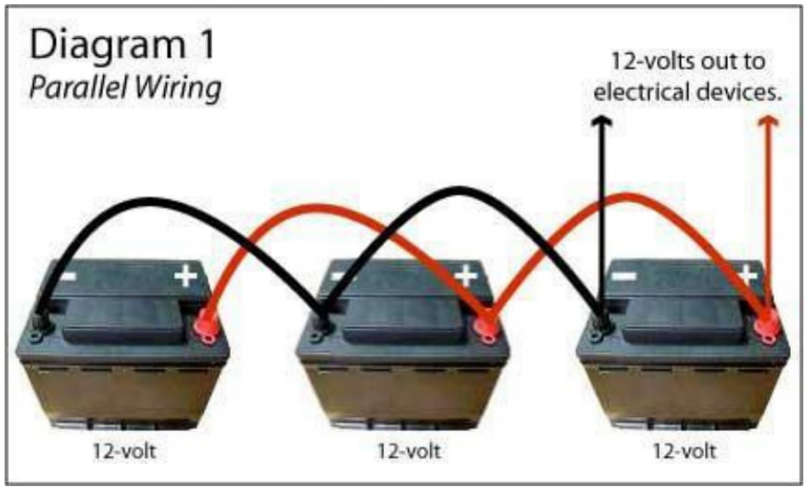
మీరు లేజర్ ప్రింటర్లు, లేజర్ కాపీయర్లు మరియు ఫ్యాక్స్ మెషీన్స్ గురించి తెలుసుకోవాలి. లేజర్ ప్రింటర్, కాపియర్ లేదా ఏ ఇతర

పరికరాలను కలుపుతూ ఒక "ఫ్యూజర్" అని పిలిచే హీటింగ్ ఎలిమెంట్ను SBS మరియు UPS యూనిట్ సమస్యలను కలిగించవచ్చు. ఎటువంటి SBS లేదా UPS లను కనెక్ట్ చేయకుండా ఉండటానికి ఉత్తమ మార్గం. ఫ్యూసర్ యాదృచ్ఛికంగా ఆన్ మరియు ఆఫ్ స్విచ్లు, ప్రతి చక్రంలో ప్రస్తుత గణనీయమైన మొత్తం అవసరం. మేము ఒక విజయవంతమైన శక్తిని లేజర్ ప్రింటర్కు 1200 వాట్ల సామర్థ్యం కలిగిన SBS లేదా UPS కి అవసరమని మేము గుర్తించాము. అదనంగా లేదా ఈ పరికరములు నిజమైన Sinewave అవుట్పుట్ లేని SBS లేదా UPS తో సరిగా పనిచేయవు. పరికరాల ఈ రకాన్ని కాపాడటానికి అవసరమైనప్పుడు, పరిమాణ SBS లేదా UPS పై ప్రత్యేకమైన పరికరాలను మాత్రమే అధికారంగా ఇన్స్టాల్ చేయాలా?









WISH YOU ALL THE BEST