# NAME: - KAMLESH KUMAR SAHU

DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING, DIPLOMA

SEMSETER: **4TH SEM**

SUBJENCT NAME: - **COMPUTER NETWORK**

SUBJECT CODE: - **2033472(033)**

**CHHATTISGARH INSTITUTE OF TECHNOLOGY, JASHPUR**

SESSION 2025-26

# UNIT 01
# BASICS OF COMPUTER NETWORKING

**COMPUTER NETWORK (कम्प्यूटर नेटवर्क): -**

जब दो या दो से अधिक Device आपस में Connect होकर Information Share करती है तो उसे हम नेटवर्क कहते है। यह Devices जैसे Computers, Servers, Mobiles, Routers आदि कोई भी Electronic Device हो सकते है। कम्प्यूटर नेटवर्क, कम्यूनिकेशन के उद्देश्य के लिए कम्प्यूटर और अन्य डिवाइसेस का एक ग्रुप होता है, जो वायर्ड (लैन), वायरलेस या इंटरनेट से कनेक्ट होते हैं।

**NETWORK SERVICES (नेटवर्क सर्विस): -**

कम्प्यूटर नेटवर्क में के विभिन्न रिसोर्सेस जैसे हार्ड-डिस्क, सीडी-ड्राइव, प्रिंटर आदि को शेयर करने के लिए नेटवर्क सर्विस ही जिम्मेदार होती हैं। नेटवर्क में प्रयोग होने वाली प्रमुख सर्विसेस निम्न हैं: -

1. फाइल सर्विस: - नेटवर्क में किसी फाइल को एक कम्प्यूटर से दुसरे कम्प्यूटर पर ट्रान्सफर, मूव या कॉपी करने के लिए फाइल सर्विस प्रयोग में आती है। फाइल सर्विस ही नेटवर्क में बैकअप की सुविधा प्रदान करती है। FTP प्रोटोकॉल इंटरनेट का मुख्य उपयोग, फाइलो को डाउनलोड करना है अर्थात इंटरनेट पर एक कम्प्यूटर से दूसरे कम्प्यूटर पर फाईलो को ट्रांसफर करना है।
2. प्रिंट सर्विस: - प्रिंट सर्विस का कारण नेटवर्क में किसी एक कम्प्यूटर पर लगे प्रिंटर को नेटवर्क के अन्य कम्प्यूटर के लिए उपलब्ध करवाना होता है अर्थात प्रिंट सर्विस के कारण ही एक प्रिंटर का प्रयोग नेटवर्क में सभी कम्प्यूटर यूजर कर पाते हैं। प्रिंट सर्विस का कार्य नेटवर्क में प्रिंटर की संख्या को कम करना होता है। इस सर्विस के कारण ही नेटवर्क में प्रिंटर को कहीं भी स्थापित किया जा सकता है।
3. मेसेज सर्विस: - मेसेज सर्विस का कार्य एक कम्प्यूटर का मेसेज दूसरे कम्प्यूटर तक पहुचना होता है। इसके साथ हम डाटा, ऑडियो, विडियो, टेक्स्ट आदि इनफार्मेशन को भी भेज सकते हैं। एक प्रकार से मेसेज सर्विस, फाइल सर्विस की तरह ही कार्य करती है। लेकिन यह डाइरेक्ट कम्प्यूटर के बीच कार्य न करके User Application के बीच कार्य करती है। Email व Voice Mail इसके उदहारण हैं।
4. डाटाबेस सर्विस: - यह सर्विस नेटवर्क में सर्वर आधारित डाटाबेस की सुविधा प्रदान करती है अर्थात नेटवर्क में जब कोई क्लाइंट रिक्वेस्ट करता है तो उसे आवश्यक जानकारी डाटाबेस सर्वर के द्वारा प्रदान कर दी जाती है। यह सर्विस डाटा सिक्योरिटी प्रदान करती है और इसके कारण ही डाटाबेस की लोकेसन केन्द्रित हो पाती है।
5. एप्लीकेशन सर्विस: - कम्प्यूटर नेटवर्क में वे सर्विस जो नेटवर्क क्लाइंट के लिए Software चलाती हैं एप्लीकेशन सर्विस कहलाती हैं। यह सर्विस केवल डाटा शेयर के साथ उनकी Processing Power भी शेयर करने की अनुमति प्रदान करती है। इसका सबसे अच्छा उदाहरण लैन गेमिंग है, जिसमे एक गेम को कई यूजर एक साथ खेलते हैं।
6. सिक्योरिटी सर्विस: - नेटवर्क तथा नेटवर्क पर उपलब्ध सूचना, डाटा या सॉफ्टवेयर को अनाधिकृत व्यक्तियों (Unauthorized Persons) की पहुंच से दूर रखना तथा केवल विश्वसनीय उपयोगकर्ताओं द्वारा ही इनका उपयोग सुनिश्चित करना भी नेटवर्क सर्विस का महत्वपूर्ण कार्य है।

**INTERNET AND INTRANET (इंटरनेट एवं इंट्रानेट): -**

1. इंटरनेट: - Internet आपस में जुडे हुए कम्प्युटरों का ग्लोबल नेटवर्क हैं। जो Standard Internet Protocol का इस्तेमाल करता हैं। इंटरनेट में उपस्थित समस्त जानकारी सभी लोगों के लिए उपलब्ध है और इसे इंटरनेट से जुडे हुए किसी भी डिवाईस के माध्यम से Access किया जा सकता हैं।
2. इंट्रानेट: - Intranet भी आपस में जुडे हुए Computers का Private Network होता हैं। जिसे किसी कंपनी, संस्थान, संगठन विशेष द्वारा आंतरिक संचार और डाटा आदान-प्रदान के लिए बनाया जाता हैं। इंट्रानेट का उपयोग केवल कंपनी विशेष से संबंधित लोग यथा कर्मचारी, सदस्य, डायरेक्टर आदि ही कर सकते हैं, क्योंकि इंट्रानेट को Firewall द्वारा Global Network से अलग रखा जाता हैं और इसे Access करने के लिए पासवर्ड की जरूरत भी पडती हैं।

इंटरनेट एवं इंट्रानेट में समानताएं: - इंटरनेट और इंट्रानेट दोनों एक नेटवर्क ही हैं।

i. इंटरनेट और इंट्रानेट दोनों में समान तकनीक Internet Technology का इस्तेमाल होता हैं।
ii. दोनों को वेब ब्राउजर द्वारा Access किया जा सकता हैं।
iii. इंटरनेट और इंट्रानेट दोनों किसी नेटवर्क को Represent करते हैं।

इंटरनेट एवं इंट्रानेट में अंतर: -

| क्र. | इंटरनेट | इंट्रानेट |
|---|---|---|
| 01. | इंटरनेट एक Global Network हैं। | इंट्रानेट केवल एक Private Network होता हैं। |
| 02. | इंटरनेट को कोई भी व्यक्ति Access कर सकता हैं। | लेकिन इंट्रानेट केवल कंपनी, संगठन विशेष से जुडे हुए लोग ही Access कर सकते हैं। |
| 03. | इंटरनेट से लाखों-करोडों कम्प्युटर जुडे होते हैं। | इंट्रानेट में कम्प्युटरों की संख्या सीमित और बहुत कम होती हैं। |
| 04. | इंटरनेट पर असीमित सूचना उपलब्ध हो सकती हैं। | एक इंट्रानेट पर सीमित लेकिन विशेष सूचना ही उपलब्ध होती हैं। |
| 05. | इंटरनेट कम सुरक्षित हैं। | इंट्रानेट सुरक्षित नेटवर्क हैं। |
| 06. | इंटरनेट का कोई मालिक नही होता है। | एक इंट्रानेट नेटवर्क का कोई ना कोई मालिक अवश्य होता हैं। |
| 07. | इंटरनेट LAN, MAN, WAN आदि नेटवर्कों से मिलकर बना होता हैं। | इंट्रानेट अधिकतर LAN यानि Local Area Network पर निर्भर होता हैं। |
| 08. | इंटरनेट पर हजारों सर्वर कार्य कर रहे हैं। | इंट्रानेट में सर्वर की संख्या सीमित होती हैं। |
| 09. | इंटरनेट पर किसी साइट को चलाने के लिये पहले इस साइट को वेब सर्वर पर अपलोड करने के लिये Web Space की आवश्यकता होती हैं। | इंट्रानेट पर किसी साइट को अपलोड करने के लिए Web Space की आवश्यकता नहीं होती हैं। |

**APPLICATION OF COMPUTER NETWORK (कम्प्यूटर नेटवर्क के अनुप्रयोग): -**

a. डाटा प्रोसेसिंग (Data Processing) - बडें और विशाल पैमाने पर डाटा प्रोसेसिंग (Data Processing) करने के लिये और सूचना तैयार करने के लिये कम्प्यूटर का प्रयोग किया जाता है इससे डाटा इकट्ठा करना उसका विश्लेषण करना और सूचना प्राप्त करना बहुत आसान हो जाता है, जो कम्प्यूटर नेटवर्क की महत्वपूर्ण विशेषता है।

b. शिक्षा (Education) - कम्प्यूटर नेटवर्क के द्वारा आज इन्टरनेट के माध्यम से हम किसी भी विषय की जानकारी कुछ ही क्षणों में प्राप्त कर सकते हैं, स्कूल और कॉलेजों को भी इंटरनेट से जोड दिया गया है तथा कई जगहों पर स्मार्ट क्लास पर जोर दिया जा रहा है जो कम्प्यूटर नेटवर्क की वजह से ही संभव है।

c. बैंक (Bank)- बैंकिंग क्षेत्र में तो कम्प्यूटर नेटवर्क के उपयोग ने क्रांति ही ला दी है, पुराने जमाने के बही खाते और रजिस्टर की जगह कम्प्यूटर ने ले ली है। बैंकों के अधिकांश कार्य कम्प्यूटर के माध्यम से ही हो रहे हैं। जैसे पैसे निकालना और जमा करना के लिए भी कम्प्यूटरीकृत मशीने उपलब्ध हैं, जो कम्प्यूटर नेटवर्क से जुडी रहती है।

d. संचार (Communication)- 4जी इंटरनेट को आज प्रत्येक व्यक्ति प्रयोग कर रहा है कम्प्यूटर तकनीक ने ही संचार के क्षेत्र में इन्टरनेट के प्रयोग को संभव बनाया है और इन्टरनेट ने संचार क्रांति को जन्म दिया।

e. मनोरंजन (Recreation) - मल्टीमिडिया के प्रयोग ने तो कम्प्यूटर नेटवर्क को बहुयामी बना दिया है, कम्प्यूटर नेटवर्क का प्रायः सिनेमा, टेलीविजन, वीडियो गेम खेलने के लिये भी किया जाता है।

f. प्रशासन (Governance) - हर एक संस्थान में अपना एक आंतरिक प्रशासन होता है और प्रशासनिक कार्य कम्प्यूटर नेटवर्क से ही किये जाते हैं, साथ ही साथ सरकारी योजनओं का लाभ भी ई-शासन (E-Governance) के रूप में कम्प्यूटर नेटवर्क की सहायता से आज जनों के घरो तक पहुँच रहा है।

g. सुरक्षा (Security) - आज बिना कम्प्यूटर नेटवर्क के हमारी सुरक्षा व्यवस्था बिलकुल कमजोर हो जाएगी। एयरक्राफ्ट ट्रैक करने में, हवाई हमल, सीसीटीवी कैमरे में कम्प्यूटर नेटवर्क का उपयोग होता है।

h. वाणिज्य (Commerce) - दुकान, बैंक, बीमा, क्रेडिट कंपनी, आदि में कम्प्यूटर का अधिकतम उपयोग होता है। कम्प्यूटर नेटवर्क के बिना काम करना वितीय दुनिया के लिए असंभव हो गया है।

i. उद्योग (Industry) - बहुत सारे औधोगिक संस्थान; जैसे – स्टील, कैमिकल, तेल कंपनी आदि कम्प्यूटर पर निर्भर हैं | संयंत्र प्रक्रियाओं के वास्तविक नियंत्रण के लिए भी कम्प्यूटर का उपयोग करते हैं।

j. चिकित्सा (Medicine) - चिकित्सा के क्षेत्र में कम्प्यूटर का अनुप्रयोग विभिन्न शारीरिक रोगों का पता लगाने के लिए किया जाता है, रोगों का विश्लेषण और निदान भी कम्प्यूटर के द्वारा संभव है, आधुनिक युग में एक्स रे, सिटी स्कैन, अल्ट्रासाउंड इत्यादि विभिन्न क्षेत्र में कम्प्यूटर नेटवर्क का व्यापक उपयोग हो रहा है।

**NETWORKING (नेटवर्किंग): -**

नेटवर्किंग एक प्रोसेस होती है जिसमें नेटवर्क को Create और Configure किया जाता है। यह कार्य हार्डवेयर और सॉफ्टवेयर दोनों के उपयोग से किया जाता है। नेटवर्क को Create करने के लिए हार्डवेयर के रूप में अलग अलग नेटवर्किंग डिवाइसेज जैसे की Hub, Switch, Router आदि Use किए जाते हैं।

**NETWORK TOPOLOGY (नेटवर्क टोपोलॉजी): -**

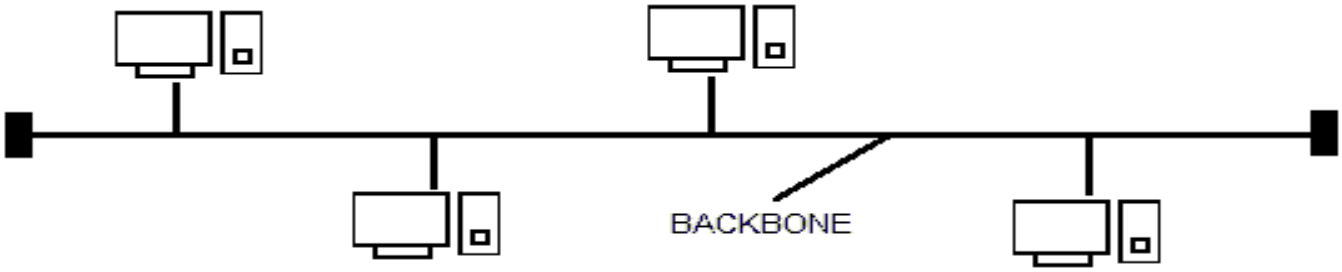
कंप्यूटर नेटवर्क की भाषा में दो या दो से अधिक कंप्यूटर को आपस में जोड़ना नेटवर्क कहलाता है। टोपोलॉजी नेटवर्क की आकृति या लेआउट को कहा जाता है। नेटवर्क के विभिन्न नोड किस प्रकार एक दुसरे से जुड़े होते है तथा कैसे एक दुसरे के साथ कम्युनिकेशन स्थापित करते है, उस नेटवर्क को टोपोलॉजी ही निर्धारित करता है। टोपोलॉजी फिजिकल या लौजिकल होता है।

नेटवर्क टोपोलॉजी सामान्यत: निम्न प्रकार की होती है:-

i. बस टोपोलॉजी (Bus Topology)
ii. रिंग टोपोलॉजी (Ring Topology)
iii. स्टार टोपोलॉजी (Star Topology)
iv. मेश टोपोलॉजी (Mesh Topology)
v. ट्री टोपोलॉजी (Tree Topology)
vi. हाइब्रिड टोपोलॉजी (Hybrid Topology)

1. **BUS TOPOLOGY (बस टोपोलॉजी): -**

Bus Topology में एक विशेष प्रकार के केबल का प्रयोग किया जाता है जिसे Backbone Cable कहते है। इसमें नेटवर्क के सारे Node इसी केबल से जुड़े होते है। केबल के प्रारंभ व अंत में एक विशेष प्रकार का डिवाईस लगा होता है जिसे Terminator कहते है। इसका कार्य Signals के नियंत्रित करना होता है। Bus Topology में Sender से Receiver तक डेटा व सूचना सदैव Backbone से होकर पहुँचता है।




Advantages of Bus Topology (बस टोपोलॉजी से लाभ): -

i. बस नेटवर्क स्थापित करना और विस्तार करना आसान है।
ii. इसमें स्टार व अन्य नेटवर्क की तुलना में कम केबल लगती है।
iii. बस टोपोलॉजी की लागत बहुत कम है।
iv. रैखिक (Linear) बस नेटवर्क का उपयोग ज्यादातर छोटे नेटवर्क में किया जाता है।

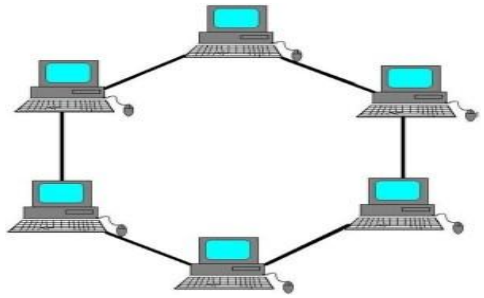
Disadvantages of Bus Topology (बस टोपोलॉजी से हानि): -

i. एक कम्प्यूटर के ख़राब होने से सारा डाटा संचार रुक जाता है।
ii. समय के साथ रखरखाव लागत अधिक हो सकती है।
iii. बस नेटवर्क की दक्षता नए नोड जुड़ने पर कम हो जाती है।
iv. यह भारी यातायात वाले नेटवर्क के लिए उपयुक्त नहीं है।
v. सुरक्षा बहुत कम है क्योंकि सभी कंप्यूटर स्रोत से भेजे गये सिग्नल प्राप्त करते हैं।

2. **RING TOPOLOGY (रिंग टोपोलॉजी): -**

इस कम्प्यूटर में कोई होस्ट, मुख्य या कंट्रोलिंग कम्प्यूटर नही होता। इसमें सभी कम्प्यूटर एक गोलाकार आकृति में लगे होते है प्रत्येक कम्प्यूटर अपने अधीनस्थ (Subordinate) कम्प्यूटर से जुड़े होते है, किन्तु इसमें कोई भी कम्प्यूटर स्वामी नही होता है। इसे सर्कुलर (Circular) भी कहा जाता है।

रिंग नेटवर्क (Ring Network) में साधारण गति से डाटा का आदान-प्रदान होता है तथा एक कम्प्यूटर से किसी दुसरे कम्प्यूटर को डाटा (Data) प्राप्त करने पर उसके मध्य के अन्य कंप्यूटरो को यह निर्धारित करना होता है कि उक्त डाटा उनके लिए है या नही। यदि यह डाटा उसके लिए नही है तो उस डाटा को अन्य कम्प्यूटर में आगे (Pass) कर दिया जाता है।



Advantages of Ring Topology (रिंग टोपोलॉजी से लाभ): -

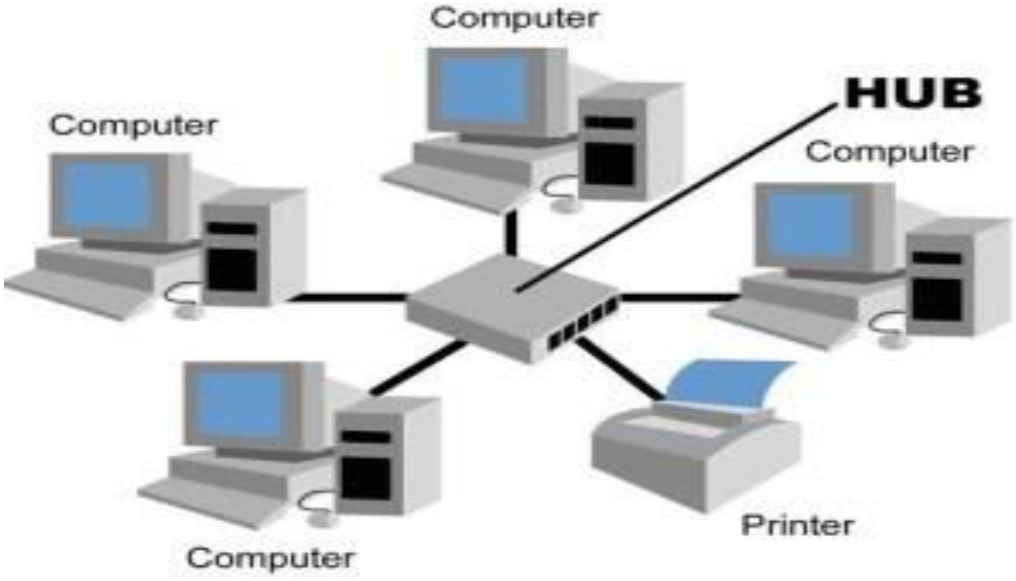
i. रिंग टोपोलॉजी को बस टोपोलॉजी की तुलना में Manage करना आसान है।
ii. नेटवर्क में ट्रैफिक की बड़ी मात्रा को संभाल सकता हैं।
iii. बहुत Reliable है और नेटवर्क में अच्छी Speed प्रदान करता है।
iv. सभी कंप्यूटर अपने आप में सम्पूर्ण होते है कोई किसी को कण्ट्रोल नही कर रहा है।
v. एक ही दिशा में सभी डेटा प्रवाह करता है जिससे पैकेट टकराव होने की संभावना न के बराबर होगी।
vi. डेटा उच्च गति पर वर्कस्टेशन के बीच ट्रान्सफर हो जाता है।
vii. एक लाइन होने के कारण Installation में खर्च कम आता है।

Disadvantages of Ring Topology (रिंग टोपोलॉजी से हानि): -

i. Ring Topology में Troubleshooting करना काफी Difficult है।
ii. रिंग टोपोलॉजी में डिवाइस को कनेक्ट य डिसकनेक्ट करने से सारा नेटवर्क Disturbs होता हैं।
iii. एक दुसरे पर निर्भरता के कारन एक ख़राब डिवाइस सारे नेटवर्क को फेल कर सकती हैं।
iv. डाटा लक्ष्य तक पहुँचने के लिए सभी कंप्यूटर से होकर जायेगा जब तक लक्ष्य तक पहुँच न जाये चाहे डाटा दुसरे कंप्यूटर से सम्बंधित हो या न हो।

3. **STAR TOPOLOGY (स्टार टोपोलॉजी): -**

Star Topology में सभी Node एक Star की आकृति में एक दूसरे से जुड़े होते है। इस प्रकार के नेटवर्क टोपोलाजी में एक Host या Controling कम्प्यूटर होता है जो नेटवर्क का सबसे प्रमुख कम्प्यूटर होता है। नेटवर्क के बाकी सभी Node इसी Host कम्प्यूटर से जुड़े होते है जो इन्हें Control करने का कार्य करता है। इसमें Sender से Receiver तक डेटा व सूचना सदैव Host कम्प्यूटर से होकर पहुँचता है।




Advantages of Satr Topology (स्टार टोपोलॉजी से लाभ): -

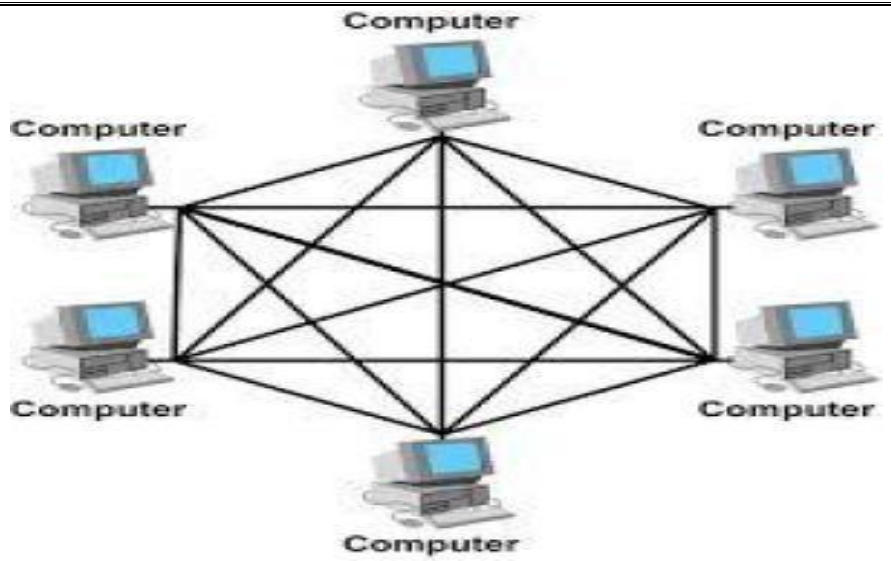
i. इसको Install करना काफी आसान हैं।
ii. Star Topology के द्वारा सारे नेटवर्क को Centralized Manage किया जा सकता हैं |
iii. यदि नेटवर्क पर एक कंप्यूटर ख़राब हो जाता है, तो बाकी नेटवर्क सामान्य रूप से कार्य करना जारी रखता है।
iv. Star Topology के द्वारा नेटवर्क को आसानी से बड़ा किया जा सकता हैं।
v. चलते हुए नेटवर्क में डिवाइस को कनेक्ट और रिमूव करने से नेटवर्क पर कोई फर्क नहीं पड़ता।
vi. यह नेटवर्क अधिकतम उपयोग में लिया जाता है।

Disadvantages of Star Topology (स्टार टोपोलॉजी से हानि): -

i. अगर केंद्रीय कंप्यूटर, हब, या स्विच विफल हो जाता है, तो पूरा नेटवर्क और सभी कंप्यूटर नेटवर्क से डिस्कनेक्ट हो जाते हैं।
ii. नेटवर्क को बनाने के लिए ज्यादा केबल्स की आवश्यकता पड़ती है।
iii. स्विच या राउटर काफी महंगे डिवाइस हैं। जिससे लागत बढ़ जाती है।
iv. केंद्रीय नेटवर्क डिवाइस (स्विच या राउटर या हब) नेटवर्क में कंप्यूटरों की संख्या को निर्धारित करता है।

4. **MESH TOPOLOGY (मेश टोपोलॉजी): -**

मेश टोपोलॉजी को मेश नेटवर्क (Mesh Network) या मेश भी कहा जाता है। मेश एक नेटवर्क टोपोलॉजी है जिसमे संयंत्र (Devices) नेटवर्क नोड (Nodes) के मध्य कई अतिरिक्त अंत: सम्बन्ध (Interconnections) से जुड़े होते है। अर्थात मेश टोपोलॉजी में प्रत्येक नोड नेटवर्क के अन्य सभी नोड से जुड़े होते है। मेश टोपोलॉजी में सारे कंप्यूटर कही न कही एक दूसरे से जुड़े रहते हैं और एक दूसरे से जुड़े होने के कारण ये अपनी सूचनाओ का आदान प्रदान आसानी से कर सकते हैं। इसमें कोई होस्ट कंप्यूटर नहीं होता हैं।




Advantages of Mesh Topology (मेश टोपोलॉजी से लाभ): -

i. नेटवर्क में इनफार्मेशन को शेयर करने के लिए बहुत सारे रास्ते मिल जाते हैं।
ii. प्रत्येक कनेक्शन अपना डेटा लोड ले सकता है।
iii. यह मजबूत है।
iv. सुरक्षा और गोपनीयता प्रदान करता है।

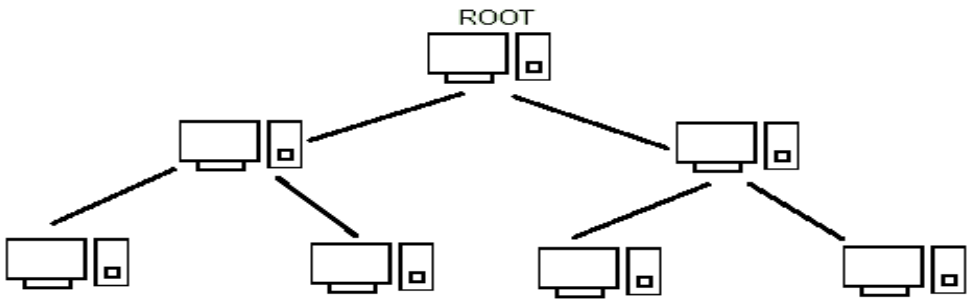
Disadvantages of Mesh Topology (मेश टोपोलॉजी से हानि): -

i. यदि कंप्यूटर अधिक हो जाते है तो Install करना मुश्किल है ।
ii. पूरी तरह कनेक्टेड मेश टोपोलॉजी के मामले में केबल की लागत अधिक है और सबसे ज्यादा है।
iii. मेश टोपोलॉजी के लागत बाकि अन्य टोपोलॉजी की तुलना में बहुत अधिक होती है।
iv. खराबी का आसानी से पता नहीं चल पाता है।

5. **TREE TOPOLOGY (ट्री टोपोलॉजी): -**

ट्री टोपोलॉजी में स्टार तथा बस दोनों टोपोलॉजी के लक्षण विधमान होते है। इसमें स्टार टोपोलॉजी की तरह एक होस्ट कम्प्यूटर होता है और बस टोपोलॉजी की तरह सारे कम्प्यूटर एक ही केबल से जुड़े रहते हैं। यह नेटवर्क एक पेड़ के समान दिखाई देता हैं।

Tree Topology में एक Root Node होता है एवं बाकी सभी Node एक वृक्ष की शाखाओं की आकृति में इससे जुड़े होते है। इसे Hierarchical Network भी कहा जाता है। इस नेटवर्क टोपोलाजी में Root Node ही Host या Controling कम्प्यूटर होता है जो नेटवर्क का सबसे प्रमुख कम्प्यूटर होता है। नेटवर्क के एक Branch से दूसरे Branch में डेटा व सूचना Root Node से होकर ही पहुँचता है।



Advantages of Tree Topology (ट्री टोपोलॉजी से लाभ): -

i. इसको Install करना काफी आसान हैं।
ii. अगर नेटवर्क ने कोई समस्या आती है तो Faulty Devices को ढूढ़ना आसान हैं।
iii. नेटवर्क को बढ़ाना आसान है क्योंकि चाइल्ड के नीचे भी कंप्यूटर को जोड़ना आसान है।

Disadvantages of Tree Topology (ट्री टोपोलॉजी से हानि): -

i. विशाल केबलिंग की आवश्यकता है।
ii. एक कंप्यूटर या नोड के ख़राब होने पर सभी चाइल्ड नोड का नेटवर्क भी काम नहीं कर पाता है।
iii. रखरखाव बहुत ज्यादा है।

6. **HYBRID TOPOLOGY (हाइब्रिड टोपोलॉजी):** -

एक टोपोलॉजी जो बस टोपोलॉजी, रिंग टोपोलॉजी, ट्री टोपोलॉजी, स्टार टोपोलॉजी और मैश टोपोलॉजी में से किसी भी दो या अधिक अन्य नेटवर्क टोपोलॉजी का उपयोग करती है। इस मिली जुली टोपोलॉजी को हाइब्रिड टोपोलॉजी कहंगे। इस टोपोलॉजी को अपनी आवश्यकता अनुसार उपयोग में लगा जा सकता है और लाभ और हानियाँ भी उपयोग करने वाली टोपोलॉजी पर निर्भर करता है।

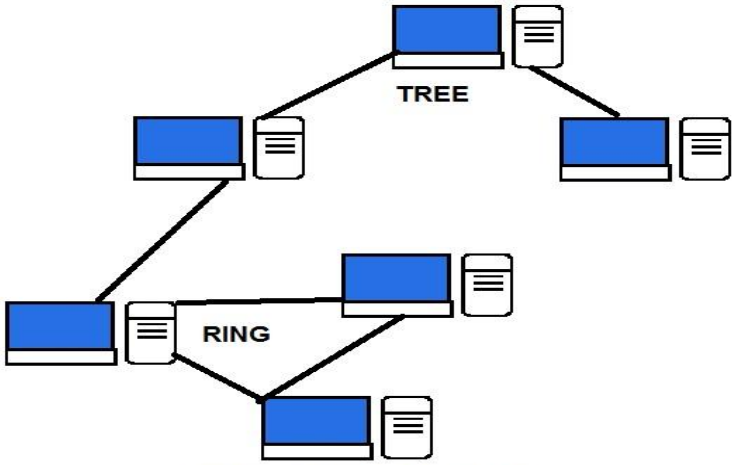


FIG: HYBRID TOPOLOGY

Advantages of Hybrid Topology (हाइब्रिड टोपोलॉजी से लाभ): -

i. यह टोपोलॉजी बड़े ऑफिस के नेटवर्क के लिए काफी अच्छी हैं।
ii. बड़े volume of traffic को हैंडल करने में काफी सहायक हैं।
iii. नेटवर्क में faulty device को ढूढना आसान हैं।

Disadvantages of Hybrid Topology (हाइब्रिड टोपोलॉजी से हानि): -

i. काफी Expensive हैं।
ii. इसकी Structure काफी Complex होता हैं।
iii. Installation और Configuration करना बहुत ही Difficult हैं।

**NETWORK ARCHITECTURES (नेटवर्क आर्किटेक्चर): -**

नेटवर्क आर्किटेक्चर को दो प्रकार से विभाजित किया जाता है: -

1. Based on Network Architecture.
    a. Client Server Architecture. (क्लाइंट - सर्वर आर्किटेक्चर).
    b. Peer To Peer Network (पीयर तो पीयर नेटवर्क).
2. Based on Geographical Architecture.
    a. Local Area Network (LAN) (लोकल एरिया नेटवर्क).
    b. Metropolitan Area Network. (MAN) (मेट्रोपोलिटन एरिया नेटवर्क).
    c. Wide Area Network (WAN) (वाइड एरिया नेटवर्क).

**LAN (Local Area Network) लोकल एरिया नेटवर्क: -**

यह एक ऐसा नेटवर्क है जिसका प्रयोग दो या दो से अधिक कम्प्यूटर को जोड़ने के लिए किया जाता है। लोकल एरिया नेटवर्क स्थानीय स्तर पर काम करने वाला नेटवर्क है इसे संक्षेप में लेन कहा जाता हैं। यह एक ऐसा कम्प्यूटर नेटवर्क है जो स्थानीय इलाकों जैसे- घर, कार्यालय, या भवन समूहों को कवर करता है। **विशेषतायें:-**

1. यह एक कमरे या एक बिल्डिंग तक सीमित रहता है।
2. इसकी डाटा हस्तांतरित (Data Transfer) Speed अधिक होती है।
3. इसमें बाहरी नेटवर्क को किराये पर नहीं लेना पड़ता है।
4. इसमें डाटा सुरक्षित रहता है।
5. इसमें डाटा को व्यवस्थित करना आसान होता है।
6. LAN का उपयोग कम्प्यूटर्स के बीच प्रिंटर, Hard Disc, स्कैनर आदि Share करने के लिए किया जाता है।
7. इसकी स्पीड 10 MBPS से 1GBPS तक होती है।
8. उदहारण - ईथरनेट।

**MAN (Metropolitan Area Network) मेट्रोपोलिटन एरिया नेटवर्क : -**

यह एक ऐसा उच्च गति वाला नेटवर्क है जो आवाज, डाटा और इमेज को 200 मेगाबाइट प्रति सेकंड या इससे अधिक गति से डाटा को 75 कि.मी. की दूरी तक ले जा सकता है। यह लेन (LAN) से बड़ा तथा वेन (WAN) से छोटा नेटवर्क होता है। इस नेटवर्क के द्वारा एक शहर को दूसरे शहर से जोड़ा जाता है। इसके अंतर्गत दो या दो से अधिक लोकल एरिया नेटवर्क एक साथ जुड़े होते हैं। यह एक शहर के सीमाओ के भीतर का स्थित कम्प्यूटर नेटवर्क होता हैं। **विशेषतायें:-**

1. इसका रखरखाव कठिन होता है।
2. इसकी गति उच्च होती है।
3. इसकी स्पीड 10 MB से 100 MB तक होती है।
4. यह 75 कि.मी. की दूरी तक फैला रहता है।
5. उदहारण : City Cable TV network।
6. इसमें बाहरी नेटवर्क को किराये पर लेना पड़ता है।

**WAN (Wide area Network) वाइड एरिया नेटवर्क: -**

इसका पूरा नाम Wide Area Network होता है। यह क्षेत्रफल की द्रष्टि से बड़ा नेटवर्क होता है। यह नेटवर्क पूरे विश्व को जोड़ने का कार्य करता है अर्थात् यह सबसे बड़ा नेटवर्क होता है इसमें डाटा को सुरक्षित भेजा और प्राप्त किया जाता है। इस नेटवर्क मे कम्प्यूटर आपस मे लीज्ड लाइन या स्विच सर्किट के द्वारा जुड़े रहते हैं। इस नेटवर्क की भौगोलिक परिधि बड़ी होती है जैसे पूरा शहर, देश या महादेश मे फैला नेटवर्क का जाल। बैंको का ATM सुविधा वाईड एरिया नेटवर्क का उदाहरण हैं।

**विशेषताये:-**

1. यह तार रहित नेटवर्क होता है।
2. इसमें डाटा को संकेतो (Signals) या उपग्रह (Satellite) के द्वारा भेजा और प्राप्त किया जा सकता है।
3. यह सबसे बड़ा नेटवर्क होता है।
4. इसके द्वारा हम पूरी दुनिया में डाटा ट्रान्सफर कर सकते है।
5. WAN की डेटा रेट सबसे ज्यादा होता है।
6. इसकी स्पीड 10 MBPS से 100 MBPS तक होती है।
7. इसमें बाहरी नेटवर्क को किराये पर लेना पड़ता है।

**लेन, मैन और वेन का तुलना चार्ट: -**

| तुलना का आधार | LAN | MAN | WAN |
|---|---|---|---|
| पूरा नाम | लोकल एरिया नेटवर्क | मेट्रोपॉलिटन एरिया नेटवर्क | वाइड एरिया नेटवर्क |
| क्षेत्र | यह नेटवर्क एक छोटे भौगोलिक क्षेत्र में कंप्यूटर को ग्रुप में जोड़ कर रखता है। | यह नेटवर्क एक मध्यम भौगोलिक क्षेत्र को कवर करता है। | यह नेटवर्क बहुत बड़े भौगोलिक क्षेत्र को कवर करता है। |
| नेटवर्क का मालिक | प्राइवेट। | प्राइवेट और पब्लिक। | प्राइवेट और पब्लिक। |
| नेटवर्क को डिजाइन और प्रबंधन करना | यह आसान होता है। | यह कठिन होता है। | यह कठिन होता है। |
| स्पीड | ज्यादा | मध्यम | कम |
| नेटवर्क के बीच ट्रैफिक | कम | ज्यादा | ज्यादा |
| नेटवर्क का इस्तेमाल | अस्पताल, स्कूल, कॉलेज, बैंकों आदि में। | शहर में। | देशों और महाद्वीपों में। |
| सहनशीलता | कम | ज्यादा | ज्यादा |

# UNIT 02
# REFERENCE MODEL FOR NETWORK COMMMUNICATION

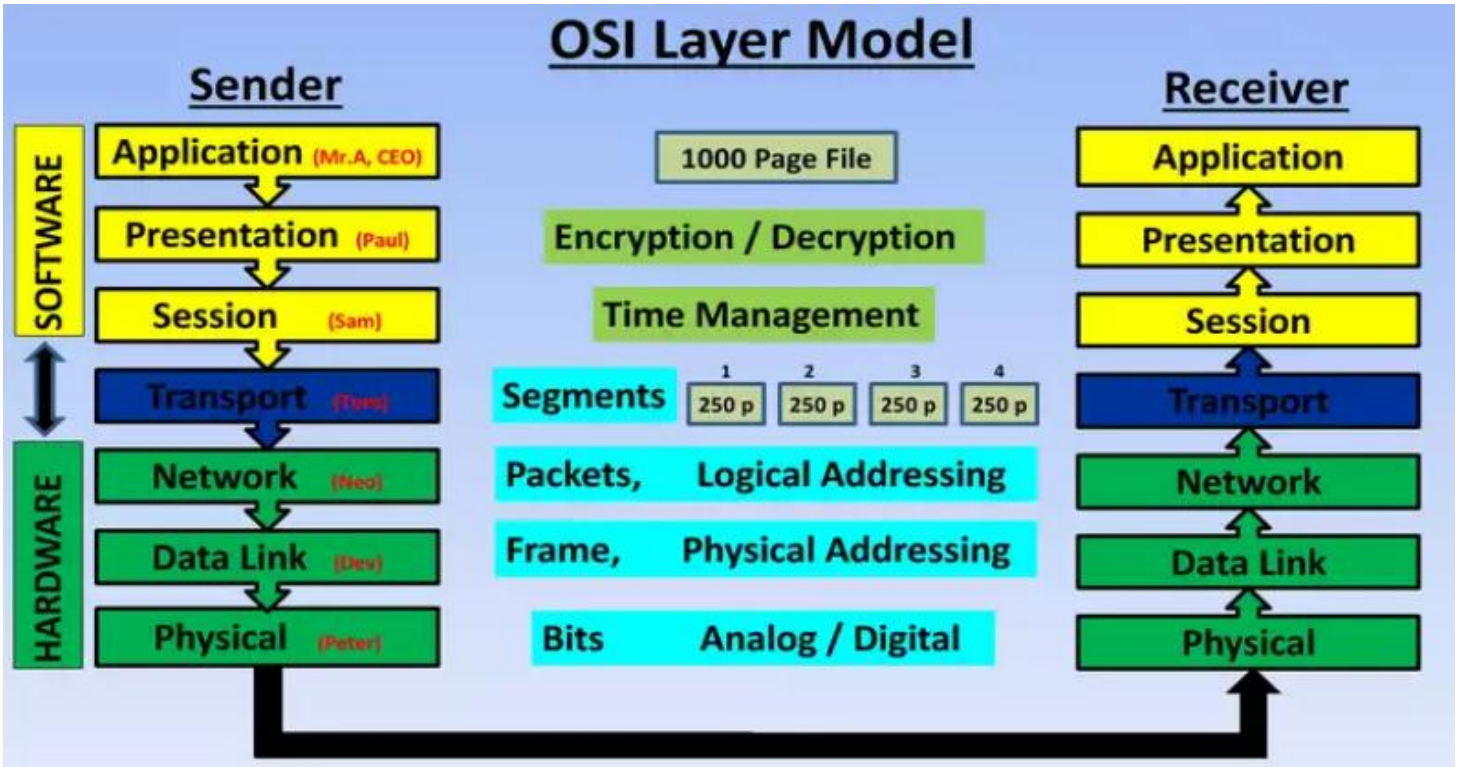
**OSI Model**

OSI model को ISO (International Organization for Standardization) ने 1984 में डेवलप किया था।

ये एक Reference Model है, यानि इसका Real Life में कोई यूज़ नहीं होता है। Real Life में आप इसी के Base पर बना हुआ TCP/IP (Transmission Control Protocol / Internet Protocol) Model यूज़ करते है।

OSI Model को Data की Journey को समझने के लिए बनाया गया है। OSI Model के माध्यम से आप समझ सकते है की Data कैसे एक Network से दूसरे Network में जाता है। और इस दौरान डेटा के साथ क्या क्या Processing होती है।

OSI Model 7 Layers से मिलकर बना होता है। ये सभी Layers डेटा के साथ कुछ ना कुछ Processing करती है। और जब Data दूसरी तरफ उसी Layer में पहुँचता है तो ये Processing डेटा से हट जाती है। हर Layer पर Data को अलग अलग नामों से जाना जाता है।




**PHYSICAL LAYER (फिजिकल लेयर): -**

OSI Model में Physical लेयर सबसे निम्नतम लेयर है। यह लेयर फिजिकल तथा इलेक्ट्रिकल कनेक्शन के लिए जिम्मेदार रहता है जैसे:- वोल्टेज, डेटा रेट्स आदि। इस लेयर में डिजिटल सिग्नल, इलेक्ट्रिकल सिग्नल में बदल जाता है। इस लेयर में नेटवर्क की Topology अर्थात Layout of Network (नेटवर्क का आकार) का कार्य भी इसी लेयर में होता है। फिजिकल लेयर यह भी Describe करता है कि कम्युनिकेशन Wireless होगा या Wired होगा। इस लेयर को बिट यूनिट भी कहा जाता है। फिजिकल लेयर के बेसिक फंक्शन: -

a. यह फिजिकल कनेक्शन को एक्टिवेट करता है, मैंटेन रखता है और डिएक्टिवेट करता है।
b. यह नेटवर्क पर अनस्ट्रक्चर्ड रॉ डेटा के ट्रांसमिशन और रिसीविंग के लिए जिम्मेदार है।

c. ट्रांसमिशन के लिए आवश्यक वोल्टेज और डाटा रेट फिजिकल लेयर में डिफाइन किए जाते है।
d. यह डिजिटल सिग्नल या ऑप्टिकल सिग्नल में डिजिटल / एनालॉग बिट्स को कन्व र्ट करता है।
e. डाटा एन्कोडिंग भी इस लेयर में किया जाता है।
f. Computer आपस मे किस Topology से Physically Connect है इस बात की Responsibility भी Physical Layers पर ही होती है।

**DATA LINK LAYER (डाटा लिंक लेयर): -**

Physical Layer से डेटा प्राप्त करते समय, Data Link Layer फिजिकल ट्रांसमिशन एरर को चेक करता हैं और बिट्स को डेटा "फ्रेम" में पैकेट करता है। Data Link Layer ईथरनेट नेटवर्क के लिए मैक एड्रेस जैसे फिजिकल एड्रेसिंग स्किम को मैनेज भी करता है, फिजिकल मीडियम के लिए किसी भी विभिन्न नेटवर्क डिवाइसेस के एक्सेस को कंट्रोल करता है। चूंकि Data Link Layer, OSI मॉडल में एक सबसे कॉम्प्लेक्स लेयर है, इसे अक्सर दो भागों में विभाजित किया जाता है, "Media Access Control" सबलेयर और "Logical Link Control" सबलेयर।

डाटा लिंक लेयर के बेसिक फंक्शन: -

a. इस लेयर का मुख्य कार्य यह सुनिश्चित करना है कि फिजिकल लेयर पर एक नोड से दूसरे में डेटा ट्रांसफर एरर फ्री हो।
b. Physical Layer से 0 1 की फॉर्म में Data Link Layer पर आता है तो वह यह Frame में Convert हो जाता है।
c. Data Link Layer उस इनफॉर्मेशन को सिंक्रनाइज़ करता है जो फिजिकल लेयर पर ट्रांसमिट होती है।
d. अनुक्रमिक रूप से प्राप्त ट्रांसमिशन और डेटा फ्रेम्स इस लेयर द्वारा मैनेज किया जाता है।
e. Data Link Layers, Network Topology को भी Define करती है।

**NETWORK LAYER (नेटवर्क लेयर): -**

Network Layer डेटा लिंक लेयर के ऊपर राउटिंग की कांसेप्ट को एड करता है। जब डेटा नेटवर्क लेयर पर आता है, तो प्रत्येक फ़्रेम के अंदर स्थित सोर्स और डेस्टिनेशन एड्रेस कि जाँच करता हैं ताकि यह सुनिश्चित किया जा सकते कि डेटा उसके फाइनल डेस्टिनेशन तक पहुंच गया है या नहीं। अगर डेटा फाइनल डेस्टिनेशन तक पहुंच गया है, तो यह लेयर 3 ट्रांसपोर्ट लेयर तक पहुंचने वाले पैकेटों में डेटा को फॉर्मेट करता है। अन्यथा, नेटवर्क लेयर डेस्टिनेशन एड्रेस को अपडेट करता है और फ्रेम को नीचे की लेयर में वापस पुश कर देता है।

राउटिंग को सपोर्ट करने के लिए, नेटवर्क लेयर नेटवर्क पर डिवाइसेस के लिए IP Address जैसे लॉजिकल एड्रेस मेंटेन करता है। नेटवर्क लेयर इन लॉजिकल एड्रेस और फिजिकल एड्रेस के बीच मैपिंग भी मैनेज करता है। आईपी नेटवर्किंग में, यह मैपिंग एड्रेस रिज़ॉल्यूशन प्रोटोकॉल (ARP) के माध्यम से पूरा किया जाता है। नेटवर्क लेयर के बेसिक फंक्शन: -

a. नेटवर्क लेयर में डाटा फ्रेम को पैकेट में परिवर्तित किया जाता है।
b. Source to Destination यह एक नोड से अन्य नोड तक विभिन्न चैनलों के माध्यम से सिग्नल को राउट करता है।
c. यह एक नेटवर्क कंट्रोलर के रूप में कार्य करता है। यह सबनेट ट्रैफिक मैनेज करता है।
d. यह तय करता है कि डेटा को किस रूट को लेना चाहिए।
e. यह आउटगोइंग मैसेजेस को पैकेट में बांटता है और इनकमिंग पैकेट को हाइर लेवर के लिए मैसेजेस को अस्सेम्बल करता है।
f. दो या दो से अधिक Network के बीच Data का का Communication करता है।
g. लॉजिकल एड्रेस को फिजिकल एड्रेस से तथा इसके विपरीत परिवर्तन करता है।

**TRANSPORT LAYER (ट्रांसपोर्ट लेयर): -**

ट्रांसपोर्ट लेयर डेटा को नेटवर्क कनेक्शन में भेजता है। TCP, ट्रांसपोर्ट लेयर 4 नेटवर्क प्रोटोकॉल का सबसे आम उदाहरण है। अलग-अलग ट्रांसपोर्ट प्रोटोकॉल वैकल्पिक क्षमताओं की एक रेंज को सपोर्ट कर सकते हैं जिसमें एरर रिकवरी, फ्लो कंट्रोल और रि-ट्रांसमिशन के लिए सपोर्ट शामिल हैं।ट्रांसपोर्ट लेयर के बेसिक फंक्शन: -

a. ट्रांसपोर्ट लेयर सेगमेंटेशन के द्वारा बड़े Data को छोटे-छोटे Block में Divide करने की प्रक्रिया करता है।
b. End to End सिस्टम के बीच डेटा के ट्रांसपरेंट ट्रांसफर के लिए जिम्मेदार।
c. End to End एरर रिवकरी और फ्लो कंट्रोल के लिए जिम्मेदार।
d. संपूर्ण डेटा ट्रांसफर के लिए जिम्मेदार।
e. Transport Layer Multiplexing और,Demultiplexing का काम करती है।
f. Transport layer application और Service को Connection provide करती है।
g. यहां SMTP, TCP, UDP जैसे प्रोटोकॉल काम करते हैं।

**SESSION LAYER (सेशन लेयर): -**

जब दो डिवाइसेस, कंप्यूटर या सर्वर को एक-दूसरे के साथ कम्युनिकेट की आवश्यकता होती है, तो Session बनाना आवश्यक होता है, और यह Session Layer पर किया जाता है। इस लेयर के फंक्शन में सेटअप, कोआर्डिनेशन (उदाहरण के लिए रिस्पांस के लिए सिस्टम को कितनी कितनी देर तक प्रतीक्षा करनी होगी) और सेशन के प्रत्येक एंड पर एप्लीकेशन के बीच टर्मिनेशन शामिल हैं। सेशन लेयर के बेसिक फंक्शन: -

a. Authentication: - Session Layer Data को Access करने की Permission Check करती है।
b. एप्लीकेशन के बीच एस्टैब्लिशमेंन्ट, मैनेजमेंट और कनेक्शन के टर्मिनेशन के लिए जिम्मेदार।
c. Session Layer प्रत्येक एंड पर एप्लीकेशन के बीच कोऑर्डिनेशन, एक्सचेंज और डाइलॉग सेटअप करता है।
d. यह सेशन और कनेक्शन कोऑर्डिनेशन के साथ काम करता है।
e. इस लेयर पर NFS, NetBios Names, RPC, SQL जैसे प्रोटोकॉल काम करते हैं।

**PRESENTATION LAYER (प्रेजेंटेशन लेयर): -**

Presentation Layer को Translation Layer भी कहा जाता है। एप्लिकेशन लेयर से डेटा यहां Extract किया जाता है और नेटवर्क पर ट्रांसमिट करने के लिए आवश्यक फॉर्मेट के अनुसार मैनिपुलेट किया जाता है। प्रेजेंटेशन लेयर के फंक्शन: -

a. Presentation layer यह ध्यान रखता है कि डेटा इस तरह से भेजा जाएं, ताकि रिसिवर इनफॉर्मेशन (डेटा) को समझ सके और डेटा का उपयोग करने में सक्षम हो।
b. डेटा प्राप्त करते समय, Presentation लेयर एप्लीकेशन के लिए डेटा ट्रांसफॉर्म कर रेडी करता हैं।
c. दो कम्युनिकेशन सिस्टम में लैंग्वेज (सिंटैक्स) भिन्न हो सकती हैं। इस स्थिति के अंतर्गत Presentation Layer ट्रांसलेटर की भूमिका निभाता है।
d. यह डाटा कंप्रेशन, डाटा एन्क्रिप्शन, डेटा कन्वर्शन इत्यादि परफॉर्म करता है।

**APPLICATION LAYER (एप्लीकेशन लेयर): -**

OSI Reference Model के टॉप पर Application layer होता हैं, जो नेटवर्क ऐप्लीकेशन द्वारा इम्प्लीमेंट किया जाता है। यह ऐप्लीकेशन डेटा को प्रोडयुस करते हैं, जिसे नेटवर्क पर ट्रांसफर किया जाता हैं। यह लेयर नेटवर्क एक्सेस के लिए ऐप्लीकेशन सर्विसेस के लिए विंडो के रूप में कार्य करता हैं और यूजर्स को प्राप्त इनफॉर्मेशन को दिखाता हैं। वेब

ब्राउज़र (गूगल क्रोम, फायरफॉक्स, सफारी, आदि) या अन्य ऐप – स्काइप, आउटलुक, ऑफिस यह सभी लेयर 7 एप्लीकेशन के उदाहरण हैं। एप्लीकेशन लेयर के फंक्शन: -

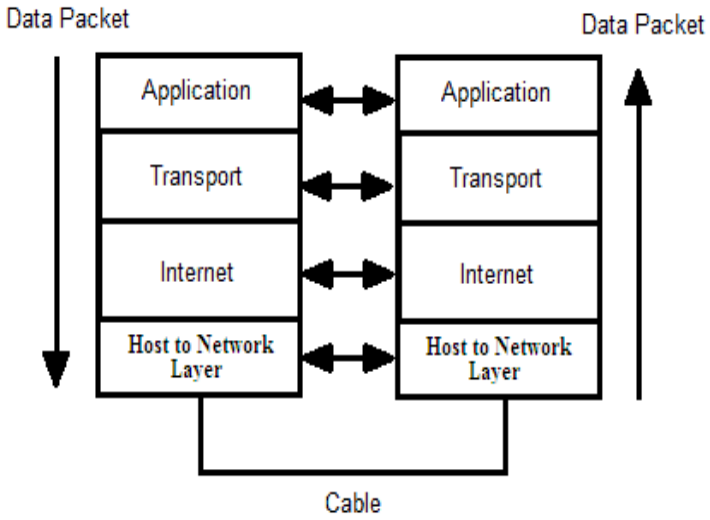
a. एप्लीकेशन लेयर एप्लीकेशन, ऐप्स और एंड यूजर्स प्रोसेसेस को सपोर्ट करता है।
b. सर्विस की क्वालिटी को मैंटेन करता है।
c. यह लेयर फ़ाइल ट्रांसफर, ई-मेल और अन्य नेटवर्क सॉफ़्टवेयर सर्विसेस के लिए एप्लीकेशन सर्विसेस के लिए ज़िम्मेदार है।
d. इस लेयर पर Telnet, FTP, HTTP जैसे प्रोटोकॉल काम करते हैं।

**TCP / IP MODEL: -**

- TCP/IP Model का पूरा नाम Transmission Control Protocol (TCP) तथा Internet Protocol (IP) है।
- TCP/IP Model को सबसे पहले एक संस्था नें रिमोट मशीन के नेटवर्क को नियंत्रण करने के लिए बनाया था। इस मॉडल को इसलिए बनाया गया था, ताकि एक कंप्यूटर के किसी एप्लीकेशन से दुसरे कंप्यूटर के किसी अन्य एप्लीकेशन से संपर्क जोड़ा जा सके।
- ये वर्ल्ड वाइड वेब का एक प्रोटोकॉल है जिसे हम इंटरनेट कहते है।यह मॉडल End-to-End कम्युनिकेशन उपलब्ध कराता है।
- टीसीपी/आईपी मॉडल की निम्न विशेषताएं थी: -
  - यह हर संरचना को सपोर्ट करता था।
  - इसके नेटवर्क में ज्यादा मशीनें भी जोड़ी जा सकती थी।
  - इसका नेटवर्क बहुत जबरदस्त था और कनेक्शन बहुत मजबूत थे।

TCP/IP मॉडल में 4 लेयर होती है जो निम्न है:-

1. Host-To-Network (Network Access) Layer
2. Internet Layer (Network Layer)
3. Transport Layer
4. Application Layer




1. **HOST –TO-NETWORK / NETWORK INTERFACE (होस्ट टू नेटवर्क लेयर): -**

- सबसे नीचे की लेयर।
- इसमें प्रोटोकॉल का इस्तेमाल होस्ट से कनेक्ट होने के लिए किया जाता है, जिससे पैकेट भेजे जा सके।
- यह लेयर विभिन्न होस्ट और मॉडल में अलग अलग होती है।

2. **INTERNET / NETWORK LAYER (इन्टरनेट लेयर): -**

- किसी इन्टरनेट के नेटवर्क पर किसी पैकेट नेटवर्क को सेलेक्ट करना, इन्टरनेट लेयर कहलाता है।
- यह लेयर पूरी संरचना को बाँध कर रखती है।
- यह लेयर पैकेट के आवागमन को ध्यान में रखती है।
- जिस क्रमांक में पैकेट भेजे जाते हैं, उससे अलग क्रमांक में पैकेट वापस आते हैं।
- आईपी (Internet Protocol) का इस्तेमाल इस लेयर में किया जाता है।
- इन्टरनेट लेयर के विभिन्न उपयोग निम्न हैं:
  - आईपी पैकेट को भेजना
  - रूटिंग करना
  - भीड़-भाड़ से बचाना

3. **TRANSPORT LAYER (ट्रांसपोर्ट लेयर): -**

- यह लेयर यह निश्चित करती है, कि डेटा का आवागमन एक ही रास्ते पर होना चाहिए, या अन्य पर भी।
- डेटा को बांटने आदि का काम ट्रांसपोर्ट लेयर करती है।
- यह लेयर डेटा पर हैडर सुचना जोडती है।
- ट्रांसपोर्ट लेयर डेटा को छोटे-छोटे भागों में बाँट देती है, जिससे नेटवर्क लेयर डेटा को अच्छे से ले जा सके।
- इसके अलावा, ट्रांसपोर्ट लेयर डेटा को एक क्रमांक में फिक्स कर देता है।
- यह लेयर दो प्रोटोकॉल की जानकारी देती है, टीसीपी और युडीपी (TCP and UDP)
  - TCP (Transmission Control Protocol): - यह एक ऐसा प्रोटोकल है, जो सोर्स और मंजिल के बीच बाईट स्ट्रीम को हैंडल करता है।
  - UDP (User Datagram Protocol): - युडीपी प्रोटोकॉल (UDP Protocol) एक ऐसा प्रोटोकॉल है, जिसमें क्रमांक, सूचि आदि की जरूरत नहीं होती है।

4. **APPLICATION LAYER (एप्लीकेशन लेयर): -**

- टीसीपी/आईपी मॉडल कई प्रकार के एप्लीकेशन का इस्तेमाल करता है, जिसमें से कुछ महत्वपूर्ण निम्न हैं:
  - TELNET एक दोतरफा कम्युनिकेशन प्रोटोकॉल है, जो रिमोट मशीन को जोड़ता है, और उनपर एप्लीकेशन चलाता है।
  - DNS (Domain Name Server): डीएनएस (DNS) किसी भी आईपी एड्रेस को शब्दों में बदल देता है, जिससे होस्ट को आसानी हो।
  - FTP (File Transfer Protocol) एक ऐसा प्रोटोकॉल होता है, जो एक नेटवर्क से जुड़े विभिन्न कंप्यूटर में फाइल ट्रांसफर करता है। यह एक सुलभ और आसान प्रोटोकल है।
  - SMTP (Simple Mail Transport Protocol) एक ऐसा प्रोटोकल है, जो किसी भी सोर्स और मंजिल के बीच इलेक्ट्रॉनिक मेल भेजने के काम आता है।

Advantage of TCP / IP Model (टीसीपी/आईपी मॉडल के लाभ): -

- यह मॉडल स्वतंत्र रूप से काम करता है।
- इस मॉडल को बड़ा बनाया जा सकता है।

- इस मॉडल में क्लाइंट सर्वर (client server) की संरचना बनायीं जा सकती है।
- यह मॉडल बहुत से रूटिंग प्रोटोकॉल को सपोर्ट करता है।
- इस मॉडल को दो कंप्यूटर के बीच कनेक्शन बनाने के लिए इस्तेमाल किया जा सकता है।

Disadvantage of TCP / IP Model (टीसीपी/आईपी मॉडल के हानि): -

- इस मॉडल को बदलना बहुत मुश्किल है।
- इस मॉडल को किसी दुसरे एप्लीकेशन में इस्तेमाल नहीं किया जा सकता है।
- इस मॉडल में, ट्रांसपोर्ट लेयर पैकेट की डिलीवरी को सुनिश्चित नहीं करती है।
- इस मॉडल में सेवाओं और प्रोटोकॉल के बीच कोई खास अंतर नहीं है।

| S.No. | OSI Model | TCP / IP Model |
|---|---|---|
| 01. | यह एक 7 Layer Model है। | यह एक 4 Layer Model है। |
| 02. | इसको सामन्यतयः एक Reference Model के तोर पर ही जाना जाता है। | TCP/IP Model, OSI Model के Function और Task को Real में Implement करने का तरीका है। |
| 03. | यह Model एक Vertical Approach को Follow करता है। | यह एक Horizontal Approach को Follows करता है। |
| 04. | Protocol OSI Model में Hide रहते है। जिसको आसानी है Technology में परिवर्तित किया गया है। | TCP / IP Model में Protocol को Refresh करना आसान नहीं है। |
| 05. | OSI मॉडल का ट्रांसपोर्ट लेयर पैकेट के डिलीवरी की गारन्टी देता है। | TCP/IP मॉडल का ट्रांसपोर्ट लेयर पैकेट के डिलीवरी की गारन्टी नहीं देता है। |
| 06. | इसका ट्रांसपोर्ट लेयर केवल कनेक्शन ओरिन्टेड होता है। | इसका ट्रांसपोर्ट लेयर कनेक्शन ओरिन्टेड एवं कनेक्शन लेस्स दोनों होता है। |
| 07. | इसका नेटवर्क लेयर कनेक्शन ओरिन्टेड एवं कनेक्शन लेस्स दोनों होता है। | इसका नेटवर्क लेयर केवल कनेक्शन लेस्स दोनों होता है। |
| 08. | यह International Organization for Standardization द्वारा 1980 में विकसित किया गया है। | इसको संयुक्त राज्य अमेरिका के रक्षा विभाग की एक एजेंसी, DARPA ने 1970 में इसे बनाया गया था। |
| 09. | OSI Model, Service Interface और Protocol को स्पष्ट रूप से परिभाषित करता है और उनके बीच अंतर स्पष्ट करता है। | TCP /IP मॉडल, Service interface और Protocol एक ही बात होती है, अर्थात इसकी Service को Protocol के नाम से ही जाना जाता है। |

**BASIC PROTOCOLS of DATA LINK LAYER (डाटा लिंक लेयर के बेसिक प्रोटोकॉल): -**

1. Sliding Window Protocol.
2. SDLC Protocol.
3. HDLC Protocol.
4. CSMA And CSMA/CD Protocol.
5. IEEE Standards 802.3, 802.4 and 802.5.

**FRAMING (फ्रेमिंग): -**

फिजिकल लेयर से प्राप्त इनफार्मेशन बिट्स के फॉर्म में रहते है। जिसे एक निश्चित प्रारूप (Format) में परिवर्तित किया जाता है जिसे फ्रेम (Frame) कहते है। डाटा लिंक लेयर फ्रेमिंग करने के लिए जिम्मेदार होती है। फ्रेमिंग से सूचनाओं को एक निश्चित फ्रेम सीमा में स्टोर किया जाता है। फ्रेमिंग करने के लिए सूचनाओं के सामने एवं पीछे कुछ स्पेशल बिट पैटर्न को जोड़ा जाता है। डाटा लिंक लेयर में सामन्तयः चार प्रकार से किया जाता है: -

1. Character Count Method.
2. Starting and Ending Character, With Character Stuffing.
3. Starting and Ending Flags, With Bit Stuffing.

**1. Character Count Methods (करैक्टर काउंट मेथड): -**

इस मेथड में सभी फ्रेम के सामने में एक हैडर फिल्ड का उपयोग किया जाता है जो उस फ्रेम में उपस्थित कैरेक्टर की साइज की संख्या को दर्ज किया जाता है। इसकी सहायता से जब फ्रेम को डेस्टिनेशन एड्रेस में भेजा जाता है तब इस फील्ड के माध्यम से ही फ्रेम में उपस्थित कैरेक्टर की संख्या ज्ञात की जाती है और एक्चुअल फ्रेम को प्राप्त किया जाता है।

इस मेथड्स का सबसे बड़ा नुकसान यह है की जब हैडर फील्ड के वैल्यू नेटवर्क में कम्युनिकेशन के दौरान बदल जाती है तो फ्रेम की सही सूचनाओं को प्राप्त करना मुश्किल हो जाता है। इस कारण इस मेथड को बहुत ही कम उपयोग किया जाता है।

उदाहरण: -

a. Information: "a boy was going to school"

Sender Message:

b.

| 1 | a | 3 | b | o | y | 3 | w | a | s | 5 | g | o | i | n | g | 2 | t | o | 6 | s | c | h | o | o | l |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|

Reciver Correct Reciving Message

c.

| 1 | a | 3 | b | o | y | 3 | w | a | s | 5 | g | o | i | n | g | 2 | t | o | 6 | s | c | h | o | o | l |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|

Reciver Right Recived Message is "a boy was going to school"

Reciver Wrong Reciving Message

d. Error

| 1 | A | 3 | b | o | y | **4** | w | a | s | 5 | g | o | i | n | g | 2 | t | o | 6 | s | c | h | o | o | l |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|

Reciver got wrong message is "a boy was5 to school"

**2. Starting and Ending Character, With Character Stuffing: -**

इस मेथड में प्रत्येक फ्रेम एक ASCII कैरेक्टर सिक्वेंस से प्रारंभ एवं उसी प्रकार के सिक्वेंस ASCII कैरेक्टर से अंत करता है। यह कैरेक्टर सीक्वेंस प्राय: DLE STX तथा DLE ETX होते हैं। इसमें DLE का तात्पर्य Data Link Escape, तथा STX का तात्पर्य Start of Text एवं ETX का तात्पर्य End of Text होता है।

यह मेथड कैरक्टर काउंट मेथड के ड्रॉबैक को कम करने के लिए उपयोग किया जाता है। इस मेथड में DLE STX तथा DLE ETX के माध्यम से कम्युनिकेशन को Synchonization किया जाता है। कभी-कभी बायनरी सूचनाओं के कम्युनिकेशन के दौरान STX ETX तथा DLE सूचनाओं के होने की संभावना रहती है। इन स्पेशल ASCII कैरेक्टर के होने पर उन सूचनाओं के पूर्व में एक एक्स्ट्रा DLE कैरेक्टर का प्रयोग किया जाता है।

सेंडर मशीन के द्वारा यह जोड़े गए एक्स्ट्रा DLE को रिसीवर एंड में मूल सूचनाओं को प्राप्त करने के लिए हटाया जाता है और इस प्रकार इन स्पेशल कैरेक्टर का उपयोग कर डाटा लिंक लेयर से सूचनाओं को नेटवर्क लेयर में भेजा जाता है।

यह मेथड भेजे जाने वाले सूचनाओं में बहुत अधिक एक्स्ट्रा कैरेक्टर को इंक्लूड करता है जिस कारण इसमें मैसेज की लंबाई बहुत अधिक हो जाती है जो इस मेथड का मुख्य ड्रॉबैक है।

उदाहरण: -

| S.No | **Orignal Message** | **Sending Message** |
|---|---|---|
| 01 | A B C | DLE STX A B C DLE ETX |
| 02 | A DLE C | DLE STX A DLE DLE C DLE ETX |
| 03 | A DLE STX C | DLE STX A DLE DLE DLE STX C DLE ETX |

**3. Starting and Ending Flags, With Bit Stuffing: -**

यह मेथड कैरक्टर स्टफिंग मेथड के ड्रॉबैक को दूर करने के लिए उपयोग में लाया गया। इस मेथड में STX and ETX को हटाकर स्पेशल बिट पैटर्न "01111110" एवं DLE के बदले में एक '0' बिट फ्लैग पैटर्न का प्रयोग किया जाता है।

इस मेथड में सूचनाएं बायनरी फॉर्म में भेजा जाता है। सेंडर जब भी लगातार पांच 1's की पहचान करता है तब वह स्पेशल बिट पैटर्न से भिन्न करने के लिए एक '0' बिट स्टफ करता है। इसी प्रकार रिसीवर रिसीव किए गए मैसेज में लगातार पांच 1's की पहचान करता है तब वह अगले बिट में उपस्थित '0' को हटा देता है।

उदाहरण: -

| | | | | | | | | | | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Orignal | 0 | 1 | 0 | 1 | 1 | 0 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 0 | 1 | 1 | 1 | 1 | 1 | 0 | 0 | 0 | 1 | 1 |
| Sender | 0 | 1 | 0 | 1 | 1 | 0 | 1 | 1 | 1 | 1 | 1 | 0 | 1 | 1 | 1 | 0 | 1 | 1 | 1 | 1 | 1 | 0 | 0 | 0 | 0 | 1 | 1 |
| Reciver | 0 | 1 | 0 | 1 | 1 | 0 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 0 | 1 | 1 | 1 | 1 | 1 | 0 | 0 | 0 | 1 | 1 |

**SLIDING WINDOW PROTOCOL (स्लाइडिंग विंडो प्रोटोकॉल): -**

स्लाइडिंग विंडो प्रोटोकॉल सेन्डर के द्वारा बहुत सारे फ्रेम को एक साथ भेजने के लिए उपयोग किया जाता है। इस मेथड में भेजे गए फ्रेम का Acknowldgement आवश्यक होता है। इसमें सेन्डर एवं रिसीवर के पास आभाषी फ्रेम होते है जिसका उपयोग फ्रेम को भेजने एवं रिसीव करने लिए किया जाता है। ये प्रोटोकॉल निम्न प्रकार से विभाजित किये जाते है: - Sliding Window Protocol

1. **Single Bit: -**
   a. Stop and Wait ARQ Protocol
2. **Multiple Bit: -**
   a. Go – Back – N ARQ Protocol.
   b. Selective Repeat / Request ARQ Protocol.

**A. STOP AND WAIT ARQ PROTOCOL (स्टॉप एंड वेट ARQ प्रोटोकॉल): -**

इसका प्रयोग Connection oriented कम्युनिकेशन में किया जाता है तथा इसका प्रयोग डेटा लिंक लेयर में होता है। Stop & Wait Protocol में सेन्डर एक समय में केवल एक डेटा फ्रेम को ही रिसीवर को Send करता है और रिसीवर को जब डेटा फ्रेम प्राप्त होता है तो वह Sender को Acknowledgement भेजता है। Sender दूसरा फ्रेम तभी Send करता है जब पिछले वाले फ्रेम की Acknowledgement उसके पास आ गयी हो।

Stop & Wait Protocol का मुख्य फायदा है इसकी Accuracy। क्यूंकि यह अगला डेटा फ्रेम तभी भेजता है जब पिछले वाले की acknowledgement मिल गयी हो। इससे डेटा फ्रेम के Lost हो जाने की संभावना खत्म हो जाती है।

Stop & Wait Protocol का सबसे बड़ा नुकसान यह है कि यह डेटा फ्रेम के ट्रांसमिशन की गति को बहुत धीमा (slow) कर देता है। क्योंकि Sender अगला फ्रेम तब तक नहीं भेजता जब तक उसे पहले वाले की Acknowledgement प्राप्त नही हो जाती। इस कारण Sender तथा Reciever दोनों को Infinite समय के लिए इन्तजार करना पड़ता है। डेटा फ्रेम भेजने की यह प्रक्रिया तब तक चलती रहती है जब तक की Sender के पास भेजने के लिए डेटा होता है।

**B. <u>GO – BACK – N ARQ PROTOCOL (गो बैक अन प्रोटोकॉल): -</u>**

- इसमें Sender Window का Size 'N' होता है। उदाहरण:- Go Back 7, तो Sender Window का Size 7 होगा। Receiver Window का Size हमेशा 1 होता है।
- इसमें Receiver एक Acknowledgement Timer को Maintain करता है। जब भी Receiver कोई Frame प्राप्त (Receive) करता है तो वह एक नए Acknowledgement Timer को शुरू कर देता है। जब Timer खत्म (Expire) हो जाता है तो Receiver उन सभी Frames के लिए Sender को Acknowledgement भेज देता है जिनका उस समय तक Acknowledge नही भेजा गया था।
- Go Back N का प्रयोग Independent Acknowledgement भेजने के लिए भी किया जा सकता है। Independent Acknowledgement का प्रयोग जरूरत पड़ने पर किया जाता है।
- यदि Receiver किसी Corrupt हुए F0rame को प्राप्त करता है तो वह उसे रद्द (Discard) कर देता है। अर्थात् रिसीवर Corrupt हुए Frame को Accept नही करता है। जब Timer Expire हो जाता है तो Correct Frame को Sender दुबारा भेजता है।
- यदि Receiver किसी ऐसे Frame को Receive करता है जिसका Sequence नंबर सही नहीं है तो वह ऐसे Frames को सीधे Discard कर देता है। और उसके पीछे से आने वाले सभी Frames को भी Discard कर दिया जाता है। ऐसा इसलिए होता है क्योंकि Receiver Window का Size 1 होता है और वह क्रम (Order) में नहीं होने वाले Frames को Accept नहीं कर सकता है।
- यदि किसी विशेष Frame के लिए सेन्डर Acknowledgement प्राप्त नहीं करता है तो यह समझा जाता है कि वह Frame तथा उसके बाद आने वाले सभी Frames को Receiver के द्वारा Discard कर दिया गया है। इसलिए Sender को उन सभी Frames को दुबारा भेजना पड़ता है। अर्थात् Sender को पूरी Window ही दुबारा Send करनी पड़ती है। इसीलिए इस Protocol का नाम Go Back N ARQ पड़ा।
- यदि कोई Frame रिसीवर तक पहुँचने से पहले ही Lost हो जाती है तो उस Frame को दुबारा वापस तभी भेजा जा सकता है जब उसका Timer Expire होगा।

**C. SELECTIVE REPEAT / REQUEST ARQ PROTOCOL (सेलेक्टिव रिपीट रिक्वेस्ट प्रोटोकॉल): -**

Selective Repeat ARQ (Automatic Repeat reQuest) एक डेटा लिंक लेयर प्रोटोकॉल है जो कि Sliding Window विधी का प्रयोग करता है। Go Back N प्रोटोकॉल में Errors अधिक होने पर फ्रेम्स को दुबारा भेजने में बहुत सारीं Bandwidth का नुकसान होता है। इसलिए हम Selective Repeat / Request ARQ का प्रयोग करते है।

- इसमें Sender Window Size हमेशा Receiver Window Size के बराबर होता है। (Sender Window का Size = Receiver Window का Size) इनका Size हमेशा 1 से बड़ा होता है अन्यथा यह प्रोटोकॉल Stop and Wait Protocol बन जायेगा। यदि Sequence नंबर के लिए 'n' bits उपलब्ध है तो, Sender Window का Size = Receiver Window का Size = 2n/2 = 2(n-1) होता है।
- Receiver प्रत्येक Frame को Independent (स्वत्रंत) रूप से Acknowledge करता है। जब भी रिसीवर, सेन्डर से कोई Frame रिसीव करता है तो वह इसका Acknowledgement भेजता है।
- यदि Receiver किसी ऐसे Frame को Receive करता है जो Corrupt हो तो, वह उसे सीधे Discard नही करता बल्कि Sender को एक Negative Acknowledgement भेजता है। Negative Acknowledgement मिलते ही Sender उस Frame को दुबारा भेज सकता है और उसे किसी Timer के Expire होना का इन्तजार नही करना पड़ता।
- यदि किसी Frame का Sequence नंबर गलत होता है तो रिसीवर उस Frame को Discard नहीं करता। वह इस Frame को अपने Window में रख लेता है।
- Selective Repeat/Request में, Receiver Window को एक Linked List की तरह Implement किया जाता है। जब Receiver कोई नया Frame रिसीव करता है तो वह इस नए Frame को Linked List के अंत में डाल देता है। जब भी किसी Frame का Sequence नंबर गलत होता है अर्थात् Frames अपने क्रम (Order) में नहीं होते है तो रिसीवर Sorting को परफॉर्म करता है। Sorting के द्वारा क्रम (Order) को सही कर लिया जाता है।
- यदि Sender कोई Frame भेजता है और वह बीच में कही Lost हो जाता है। तो सेन्डर Searching ऑपरेशन को परफॉर्म करता है और उस खोये हुए फ्रेम को Search करता है और जब फ्रेम मिल जाता है तो Sender उसे Select करके दुबारा भेज देता है। इसमें पूरी Window को भेजने की जरूरत नही पड़ती। इसलिए इस प्रोटोकॉल को Selective Repeat कहते है।
- यदि कोई Frame रिसीवर तक पहुँचने से पहले ही खो जाती है तो उसे केवल तब ही दुबारा भेजा जा सकता है जब इस फ्रेम के लिए Time Out Timer खत्म (Expire) हो जाता है।

**SDLC (SYNCHRONOUS DATA LINK CONTROL) PROTOCOL: -**

सिंक्रोनस डाटा लिंक प्रोटोकॉल को आईबीएम के द्वारा डेवलप किया गया। डाटा लिंक लेयर प्रोटोकोल है जिसका उपयोग सिस्टम नेटवर्क आर्किटेक्चर एनवायरनमेंट में किया जाता है। इस प्रोटोकॉल में नेटवर्क के सभी फंक्शन को विभिन्न लेयर में विभाजित किया जाता है। यह लेयर फिजिकल कंट्रोल लेयर और लॉजिकल लेयर कहलाते हैं।

यह प्रोटोकॉल विभिन्न प्रकार के डाटा लिंक एवं टोपोलॉजी को सपोर्ट करता है। उदाहरण के लिए पॉइंट टू पॉइंट लिंक, मल्टी लिंक, स्विच नेटवर्क, एवं पैकट नेटवर्क। इसमें दो प्रकार के नेटवर्क पाए जाते हैं पहला प्राइमरी नोड दूसरा सेकेंडरी नोड। प्राइमरी नोड का कार्य सेकेंडरी नोड को कंट्रोल करना होता है। जबकि सेकेंडरी नोड सारी सूचनाओं को प्राइमरी नोड में भेजने के लिए जिम्मेदार होता है।

**HDLC (HIGH LEVEL DATA LINK CONTROL) PROTOCOL: -**

High-level Data Link Control (HDLC) प्रोटोकॉल Network Points या Nodes के बीच डेटा संचारित करने के लिए Data Link Layer के Communication Protocols का एक समूह है। HDLC एक Bit – Oriented Protocol है। HDLC Protocol को ISO द्वारा Point to Point Data Links पर इस्तेमाल करने के लिए बनाया गया है। HDLC को IBM द्वारा बनाये गए Synchronous Data Link Control (SDLC) Protocol के आधार पर बनाया गया है। यह Cisco की सभी Routers पर By Default Configure होता है इसलिए इसे अलग से Configure करने की आवश्यकता नहीं होती है।

यह प्रोटोकॉल Full Duplex Communication को Support करता है। HDLC प्रोटोकॉल Data को एक Data Frame में डालता है जो Devices को Data Flow Control और Error Corrections की Capabilities Provide करता है।

HDLC दो प्रकार के Transfer Modes, Normal Response Mode और Asynchronous Balanced Mode का समर्थन करता है।

a. Normal Response Mode (NRM): – यहां, दो प्रकार के स्टेशन हैं, एक Primary Station जो Commands को Send करता है और Secondary Station प्राप्त कमांड का जवाब देता हैं। इसका उपयोग Point – to – Point और Multi Point Communications के लिए किया जाता है।
b. Asynchronous Balanced Mode (ABM): – यहां, कॉन्फ़िगरेशन संतुलित है, यानी प्रत्येक स्टेशन कमांड भेज सकता है और कमांड का जवाब दे सकता है। इसका उपयोग केवल Point – to – Point Communication के लिए किया जाता है।

**CSMA Carrier Sensed Multiple Accesses (कैरियर सेंस मल्टीपल एक्सेस): -**

यह एक नेटवर्क एक्सेस मेथड है जो शेयर्ड नेटवर्क टेक्नोलॉजी जैसे की इथरनेट में नेटवर्क एक्सेस को कंट्रोल करने के लिए प्रयोग किया जाता है। इस मेथड में बहुत सारे डिवाइस एक नेटवर्क केबल में अटैच होते हैं जो किसी डेटाफ्रेम को ट्रांसमिट करने के पूर्व चैनल के आइडियल होने की स्थिति की जांच करता है। यह प्रक्रिया बहुत सारे डिवाइस के द्वारा एक साथ ट्रांसमिशन के पूर्व किया जाता है इसलिए इस मेथड को कैरियर सेंस मल्टीपल एक्सेस कहते हैं।यह प्रोटोकॉल तीन प्रकार का होता है

1.1-Persitent CSMA (1-परसिस्टेंट CSMA).
2.Non-Persistent CSMA (नॉन परसिस्टेंट CSMA).
3.P-Persistent CSMA (P-परसिस्टेंट CSMA).

1. **1-Persitent CSMA (1-परसिस्टेंट CSMA): -** इस मेथड में जो डिवाइस डाटा फ्रेम को ट्रांसमिट करना चाहता है वह कम्युनिकेशन चैनल को लगातार उसके बिजी या आइडियल होने की स्थिति की जांच करता है। यदि जब तक चैनल बिजी आता है तब तक डिवाइस चैनल के आइडियल होने की स्थिति तक इंतजार करता है और जैसे ही चैनल आइडियल मिलता है वह डिवाइस तुरंत ही डेटाफ्रेम को ट्रांसमिट कर देता है। इसके इसी गतिविधि के कारण डाटा फ्रेम के भेजने की प्रायिकता एक (01) होती है और इसीलिए इसे 1-परसिस्टेंट CSMA कहते हैं।

2. **Non-Persistent CSMA (नॉन परसिस्टेंट CSMA): -** इस मेथड में जो डिवाइस डेटाफ्रेम को ट्रांसमिट करना चाहता है वह कम्युनिकेशन चैनल को उसके बिजी या आइडियल होने की स्थिति की जांच किसी रेंडम अमाउंट ऑफ़ टाइम में करता है। जब चैनल आइडियल मिलता है तब वह डेटाफ्रेम को तत्काल भेज देता है और यदि कम्युनिकेशन चैनल बिजी मिलता है तब यह अनिश्चित समय अंतराल में चैनल की आइडियल होने की स्थिति की जांच करता है। अनिश्चित समय अंतराल के कारण इसे नॉन परसिस्टेंट CSMA कहते हैं।

3. **P-Persistent CSMA (P-परसिस्टेंट CSMA): -** इस मेथड में जो डिवाइस डेटाफ्रेम को ट्रांसमिट करना चाहता है वह कम्युनिकेशन चैनल को एक निश्चित समय अंतराल में चैनल की आइडियल होने की स्थिति की जांच करता है। यदि डिवाइस को चैनल बिजी मिलता है तब वह नेक्स्ट स्लॉट के लिए इंतजार करता है और जैसे ही डिवाइस को चैनल आइडियल मिलता है तब वह डेटाफ्रेम को प्रायिकता P के साथ डेटाफ्रेम को उस स्लॉट में प्रेषित करता है।

**CSMA/CD Carrier Sensed Multiple Accesses / Collision Detection: -** कैरियर सेन्स मल्टीपल एक्सेस (Collision डिटेक्शन) एक मीडिया एक्सेस कण्ट्रोल मेथड है जिसका ईथरनेट / LAN तकनीक में काफी प्रयोग किया जाता है। एक ऐसी स्थिति जहां किसी लिंक में 'n' संख्या में स्टेशन हैं और वो सभी इस चैनल द्वारा डाटा को भेजने का इन्तजार कर रहे हैं। ऐसी स्थिति में वो सभी 'n' संख्या में स्टेशन चैनल में अपने-अपने डाटा को भेजने का प्रयास करेंगे। अब अगर एक से ज्यादा स्टेशन ने डाटा को एक साथ भेज दिया तो वहीं समस्या खड़ी हो जाएगी और ऐसी स्थिति में ही विभिन्न स्टेशन के डाटा के बीच एक Collision होगा।

CSMA/CD एक ऐसी तकनीक है जहां विभिन्न स्टेशन डाटा का अच्छे से ट्रांसमिशन के लिए जो इस प्रोटोकॉल को मानते हैं। ये प्रोटोकॉल ये निर्णय लेता है कि कौन सा कौन सा स्टेशन कब डाटा ट्रान्सफर शुरू करेगा जिस से डाटा बिना corrupt हुए डेस्टिनेशन तक पहुंचे।

**IEEE 802.3 ETHERNET (ईथरनेट): -**

ईथरनेट भी IEEE स्टैण्डर्ड 802.3 के अंतर्गत काम करने वाला एक LAN तकनीक ही है जो बड़े स्तर पर प्रयोग में आता है। इस Technology की मदद से Computers और Networking Devices को आपस में Connect किया जाता है और Information को Share किया जाता है। "Ethernet" TCP/IP Stack के Data Link Layer का Protocol है।

Ethernet Data Transmission में दो तरह के यूनिट का इस्तेमाल करता है पहला Frame और दूसरा Packet। Frame केवल Payload को ले के नहीं जाता बल्कि वो MAC Address को भी साथ में ले के जाता है। MAC Address Computer का Address होता है, जिससे की वो Sender और Receiver Computers का पता प्राप्त कर सके।

**IEEE 802.4 TOKEN BUS (टोकन बस): -**

IEEE 802.4 को Token Bus भी कहते हैं। इस प्रोटोकॉल का उपयोग LAN में वर्चुअल रिंग बनाने के लिए किया जाता है। इसमें बस या ट्री टोपोलॉजी में फिजिकल मीडिया के लिए कोएक्सियल केबल का प्रयोग किया जाता है। एक वर्चुअल रिंग का निर्माण विभिन्न स्टेशन को आपस में एक सिक्वेंस में कनेक्ट किया जाता है जिसमें एक स्टेशन अपने पड़ोसी स्टेशन के फिजिकल ऐड्रेस की जानकारी रखते हैं।

इस प्रोटोकॉल में किसी मैसेज को भेजने के पूर्व एक टोकन (स्मॉल मैसेज) को उस रिंग में उपस्थित समस्त स्टेशन के मध्य ट्रांसमीट किया जाता है। इस टोकन के माध्यम से जिस स्टेशन को डाटा ट्रांसमीट करना होता है वह स्टेशन टोकन को रिसीव कर लेता है तत्पश्चात स्टेशन अपना डाटा मैसेज को ट्रांसमीट करना प्रारंभ करता है।

**IEEE 802.5 TOKEN RINGS (टोकन रिंग): -**

टोकन रिंग को IBM द्वारा 1980 में ईथरनेट के विकल्प के रूप में विकसित किया गया था। ये LAN के लिए एक डाटा लिंक तकनीक है जिसमे Devices को एक स्टार या रिंग टोपोलॉजी में कनेक्ट करते हैं। ये OSI के नेटवर्क लेयर में काम करता है। एक स्टैण्डर्ड टोकन रिंग केवल 16 Mbps तक की गति को सम्भाल सकता है। बाद में इसे विकसित कर के इसकी गति को 100 Mbps तक किया गया ताकि ये ईथरनेट को टक्कर दे सके।

**Woring Methods of Token Ring (टोकन रिंग की कार्यप्रणाली): -**

LAN इंटरकनेक्शन के बाकी सारे तकनीक के विपरीत टोकन रिंग एक या एक से ज्यादा डाटा फ्रेम को मेन्टेन करता है जो लगातार नेटवर्क में घूमते रहते हैं। इन फ्रेम्स को सभी कनेक्टेड Devices द्वारा नेटवर्क में शेयर किया जाता है जिसकी प्रक्रिया निम्नलिखित है: -

i. रिंग सीक्वेंस में एक फ्रेम यानी की पैकेट अगले डिवाइस पर आता है।
ii. वो डिवाइस इस बात की जांच करता है कि इस फ्रेम में कोई मैसेज, सूचना या पता है की नही। अगर ऐसा है तो डिवाइस मैसेज को फ्रेम से निकाल कर हटा देता है। अगर ये सब नही है तो वो फ्रेम खाली है इसी यहाँ एम्प्टी फ्रेम कहा जाता है।
iii. जिस डिवाइस ने फ्रेम रख रखा है वो ये निर्णय लेता है कि मैसेज भजना है या नहीं। अगर ऐसा है तो ये मैसेज डाटा को टोकन फ्रेम में डालता है और उसे वापस LAN में भेज देता है। अगर मैसेज नही भेजना है तो डिवाइस उस टोकन फ्रेम को रिलीज़ कर देता है जिसे सीक्वेंस में अगला फ्रेम उठा लेता है।

दूसरे शब्दों में कहें तो नेटवर्क Congestion को कम करने के लिए एक समय पर सिर्फ एक डिवाइस का प्रयोग किया जाता है। उपर वाले सभी स्टेप्स को सभी Devices के लिए लगातार रिपीट किया जाता है। टोकन तीन बाइट के होते हैं जिसमे Start और End डिलिमिटर होते हैं और वह ये बताते हैं कि फ्रेम शुरू कहाँ से हो रहा है और कहाँ पर ख़त्म हो रहा है। टोकन के अंदर एक्सेस कण्ट्रोल बाइट भी होता है। डाटा फील्ड का अधिकतम Length 4500 बाइट हो सकता है।

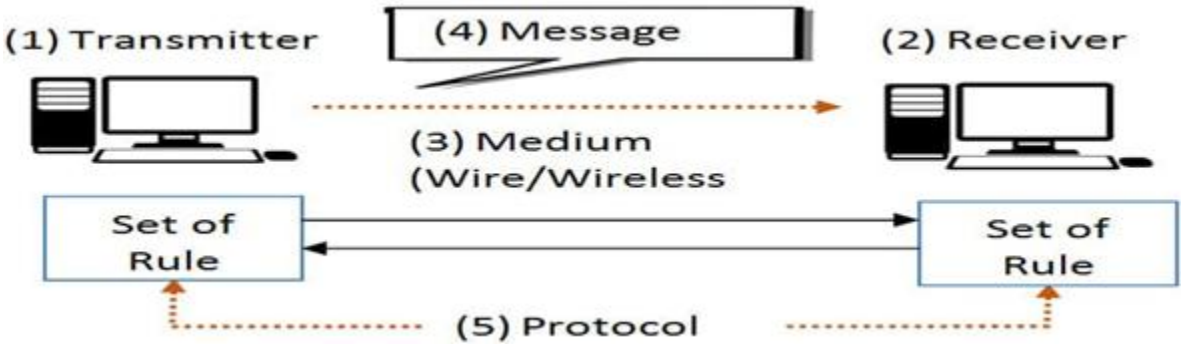
# UNIT 03
# TRANSMISSION MEDIA AND MODE

**DATA COMMUNICATION (डेटा कम्युनिकेशन): -**

डेटा कम्युनिकेशन, ट्रांसमिशन मीडियम के माध्यम से दो डिवाइसेस के बीच डेटा का एक्सचेंज हैं। नेटवर्किंग में कम्प्यूटिंग डिवाइसेस के बीच फिजिकल कनेक्शन केबल मीडिया या वायरलेस मीडिया के माध्यम से स्थापित किया जाता है। इसका सबसे अच्छा उदाहरण इंटरनेट है।

कंप्यूटर का उपयोग, इनफॉर्मेशन को उत्पन्न करने के लिए किया जाता है। इस इनफॉर्मेशन को एक स्थान से दूसरे स्थान पर ट्रांसमिट किया जाना चाहिए। इस प्रोसेस को Data Communication कहा जाता है।

इन डेटा व सूचनाएँ के आदान-प्रदान के लिए बहुत सारे सिस्टम बनाए गए है जिन्हें Communication System कहते है। रेडियो, टीवी, टेलीफोन, मोबाईल, इंटरनेट आदि वर्तमान के महत्वपूर्ण Communication System है।




1) Transmitter: - ट्रांसमीटर डिवाइस मैसेज भेजता है। यह एक कंप्यूटर, वर्कस्टेशन, टेलिफोन हैंडसेट, वीडियो कैमरा और कुछ भी हो सकता है।

2) Receiver: - रिसीवर ट्रांसमीटर द्वारा भेजे गए मैसेज को रिसिव करता है। यह भी एक कंप्यूटर, वर्कस्टेशन, टेलिफोन हैंडसेट, टेलीविज़न, और कुछ भी हो सकता है।

3) Message: - मैसेज एक ट्रांसमिशन (डेटा) है जिसे Communicate किया जाना है। इसमें टेक्स्ट, नंबर्स, इमेज, साउंड, या वीडियो या कुछ भी हो सकते हैं।

4) Medium: - इसे Communication Media या Transmission Media भी कहा जाता है। यह Wired या Wireless दोनों हो सकता है। Medium वह माध्यम या मार्ग होता है जिसके द्वारा Message को Sender से Receiver तक ले जाया जाता है। इसमें ट्विस्टेड पेयर वायर, कोएक्सिअल केबल, फाइबर ऑप्टिक केबल, लेजर या रेडियो वेव (स्थलीय या सैटेलाइट माइक्रोवेव) हो सकता हैं।

5) Protocol: - प्रोटोकॉल नियमों का एक ग्रुप है जो डेटा कम्युनिकेशन को कंट्रोल करता है। यह कम्युनिकेशन डिवाइसेस के बीच एक एग्रीमेंट को रिप्रेसेंट है। प्रोटोकॉल के बिना, दो डिवाइस कनेक्ट किए जा सकते हैं, लेकिन कम्युनिकेशन नहीं कर सकते।

**COMMUNICATION CHANNEL CHARACTERSTICS (कम्युनिकेशन चैनल के गुणधर्म): -**

1. Delivery (डिलीवरी): - डिलीवरी से तात्पर्य डाटा को एक जगह से दूसरे जगह सही रूप से प्रेषित करने से है। सिस्टम को सही डेस्टिनेशन पर डेटा को डिस्ट्रीब्यूट करना चाहिए।
2. Accuracy (शुद्धत्ता): -यह डाटा की गुणवत्ता या डाटा की सत्यता होने को दर्शाता है। सिस्टम को सही ढंग से डेटा डिलीवर करना चाहिए। यदि डेटा को ट्रांसमिशन में बदल दिया गया तो वह अनुपयोगी है।
3. Timeliness (समयबद्धता): - यह गुण डाटा के सही समय में पहुँचाने की स्थिति को बताता है। सिस्टम को समय पर डेटा डिलीवर करना चाहिए। देर से डिलीवर किया गया डेटा बेकार है।
4. Connection Type (कनेक्शन टाइप): - एक चैनल Wired या Wireless दोनों हो सकता है।
5. Channel Noise (चैनल नॉइज़): - किसी कम्युनिकेशन चैनल में नॉइज़ की मात्रा कम से कम होनी चाहिए।
6. Channel Bandwidth (चैनल बैंडविड्थ): - बैंडविड्थ अधिक होना चाहिए। अच्छे डाटा फ्लो स्पीड के लिए जितना अधिक बैंडविड्थ होगा उतना ही गति से सूचनाओं का कम्युनिकेशन हो सकेगा।
7. Channel Capacity (चैनल कैपेसिटी): - किसी समय में चैनल में communicate होने वाली सूचना की मात्रा को प्रदर्शित करता है। अतः चैनल की कैपेसिटी अधिक होनी चाहिए।
8. Transmission Time (ट्रांसमिशन टाइम): - यह वह टाइम होता है जिसमे कोई मैसेज चैनल में भेजने के लिए तैयार होता है। चैनल की अच्छी गुणवत्ता के लिए ट्रांसमिशन टाइम कम होना चाहिए।
9. Prapogation Time (प्रपोगेशन टाइम): - सोर्स पॉइंट से डेस्टिनेशन पॉइंट तक चैनल के माध्यम से किसी मैसेज को भेजने में लगने वाले समय को प्रपोगेशन टाइम कहते है। चैनल की अच्छी गुणवत्ता के लिए प्रपोगेशन टाइम कम होना चाहिए।

**BANDWIDTH (बैंडविड्थ): -**

निश्चित समय में ट्रांसमिट होने वाले डेटा को Bandwidth कहा जा सकता हैं। Bandwidth, विशिष्ट समय में वेबसाइट या इंटरनेट सर्विस से आपके कंप्यूटर पर डेटा ट्रांसफर के रेट को डिस्क्राइब करता है। Bandwidth को बिट्स प्रति सेकंड में मापा जाता है। बैंडविड्थ को किसी भी युनिट (Bytes, KiloBytes, MegaBytes, GigaBytes आदि) में एक्सप्रेस किया जा सकता है।

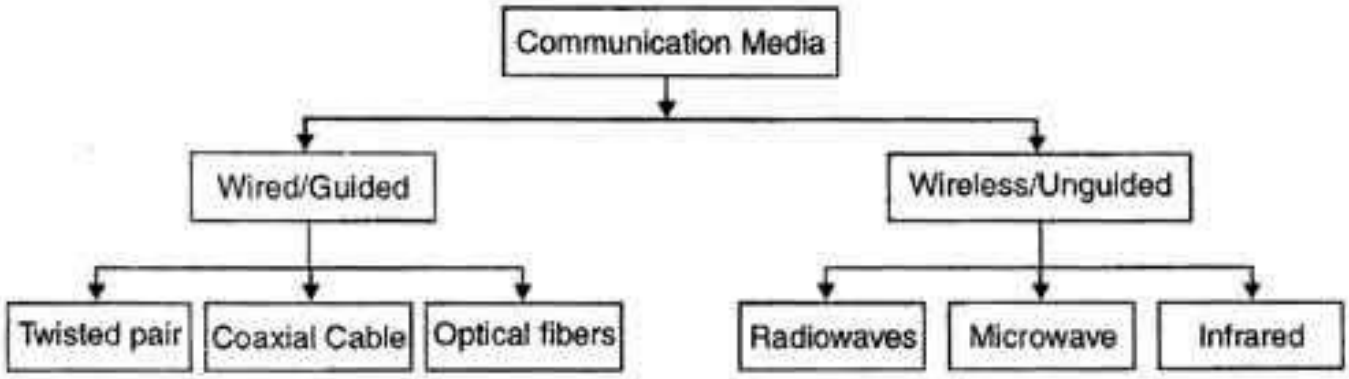
यह जानना महत्वपूर्ण है कि मेगा "बिट्स" और मेगा "बाइट्स" के बीच बहुत बड़ा अंतर है। एक बाइट (B) में 8 बिट्स (b) होते हैं। उदाहरण के लिए, 15 MBps 15 Mbps के समान नहीं है (लोअरकेस b पर ध्यान दें) । पहला 15 MegaBYTES के रूप में पढ़ा जाता हैं जबकि दूसरा 15 MegaBITS है।

**BIT RATE OR DATA RATE (बिट रेट या डाटा रेट): -**

Data Rate वह Rate होती है जिस पर सूचना को ट्रांसफर किया जाता है। इसे सूचना की मात्रा प्रति यूनिट टाइम के रूप में व्यक्त किया जाता है। Bit Rate आधारित फॉर्मेट सबसे सरल होते हैं जब एक फाइल साइज कैलकुलेट की जाती है ऐसा इसलिए क्योंकि Bit Rate वाकई में डेटा Rate होती है खासतौर से Bit Rate वह Data Rate है जो प्रति यूनिट समय में bits की संख्या के रूप में निर्धारित की जाती हैं। डिजिटल मल्टीमीडिया में, Bit Rate सूचना की मात्रा को दर्शाता है या संपूर्ण जानकारी जो रिकॉर्डिंग के समय के प्रत्येक यूनिट में स्टार्ट होती हैं।

**COMMUNICATION OR TRANSMISSION MEDIA (कम्युनिकेशन या ट्रांसमिशन मीडिया): -**

Communication Media वह माध्यम या मार्ग होता है जिसके द्वारा डेटा व सूचनाओं को Sender से Receiver तक ले जाया जाता है। इसे Transmission Media भी कहा जाता है। यह निम्नलिखित दो प्रकार का होता है।

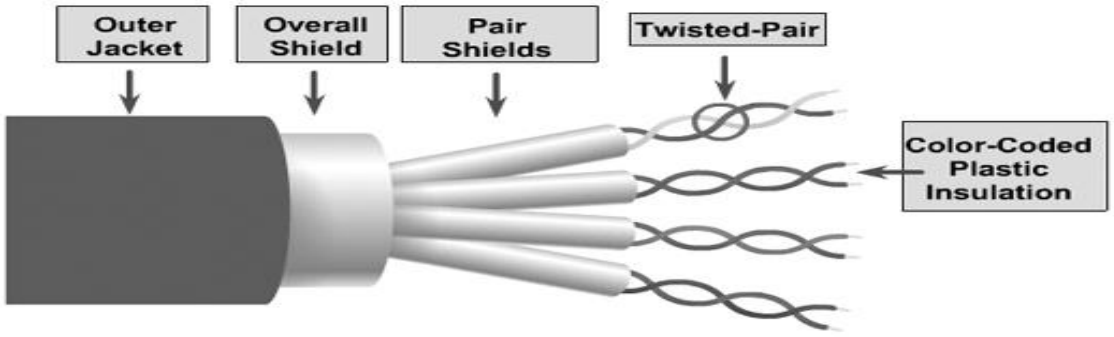



**GUIDED MEDIA: -** मुख्यतः Point to Point कम्युनिकेशन के लिए प्रयोग होता है, कंप्यूटर नेटवर्क में विभिन्न प्रकार के फिजिकल चैनल या कम्युनिकेशन होते है, उन्हीं में से Guided Media भी एक है। इस माध्यम में कंप्यूटरो को नेटवर्क से अथवा परस्पर संयोजित करने के लिए धात्विक तार अथवा कांच की प्रकाशीय फाइबर का प्रयोग किया जाता है। तार माध्यम अथवा संचार का निर्देशित संचार माध्यम ही Guided Media (Wired) कहलाता है। इस मीडिया में Sender और Receiver दोनों ही एक निश्चित स्थान पर होते है, और इनके बीच डाटा को ट्रांसफर करने के लिए भौतिक तारो का उपयोग करते है। ये भौतिक तार तीन प्रकार के होते है।

1. **TWISTED PAIR CABLE (ट्विस्टेड पेअर केबल): -**

ट्विस्टेड पेअर केबल का प्रयोग LAN (Local Area Network) में सबसे ज्यादा किया जाता है। यह केबल दो Insulated कॉपर की तारो से मिलकर बनी होती है। यह परस्पर लिपटे होते है। यह तकनीकी बहुत पहले से प्रयोग की जा रही है।

ट्विस्टेड पेअर केबल का प्रयोग करना आसान होता है, क्योकि यह मार्किट में आसानी से उपलब्ध हो जाती है तथा यह सबसे सस्ती केबल होती है। कंप्यूटर से टेलीफ़ोन लाइन का संयोजन करने के लिए मॉडेम को इस तार से संयोजित किया जाता है। इस तार का उपयोग दूरभाष, अधिकांश आतंरिक संचार, कंप्यूटर के स्थानीय नेटवर्क को स्थापित करने के लिए, आदि जगह इसी केबल का प्रयोग किया जाता है।




दो प्रमुख तरह की ट्विस्टेड पेअर केबल होती है, Unshielded Twisted Pair (UTP) और Shielded Twisted Pair (STP), जिनकी आवश्यकता अनुसार हम प्रयोग करते है।

a. **Unshielded Twisted pair:** Unshielded Twisted pair में दो Wire एक दूसरे से में सर्पीले आकर में लिपटी होती है। यह Cable आम तोर पर 100 से 150 meters तक Data को Travel करा सकती है इस Cable में Data 1 GB से 10 GBPS की Speed से Travel कर सकता है।

b. **Shielded Twisted Pair: -** Shielded Twisted Pair में Wires के ऊपर एक Shield होती है जससे इस Wire में Transfer हो रहे Data को थोड़ी Speed मिलती है क्योंकि यह Shield Data के Electromagnetic Field को कम कर देती है, जिससे Data Signal की Travel करने की Speed बढ़ जाती है।

Advantage of Twisted Pair Cable (ट्विस्टेड पेअर केबल के लाभ): -

1. यह Cable लागत में किसी अन्य Cable की तुलना में बहुत ही सस्ती होती है।
2. इसका Installation बहुत सरल (Easy) होता है। इसको RJ 45 ( Registered Jack type 45 ) जैसे Plug के साथ आसानी से Connect किया जासकता है।
3. इसमें किसी भी Node को Easily Network में Connection दिया जा सकता है।

Disadvantage of Twisted Pair Cable (ट्विस्टेड पेअर केबल की हानियाँ): -

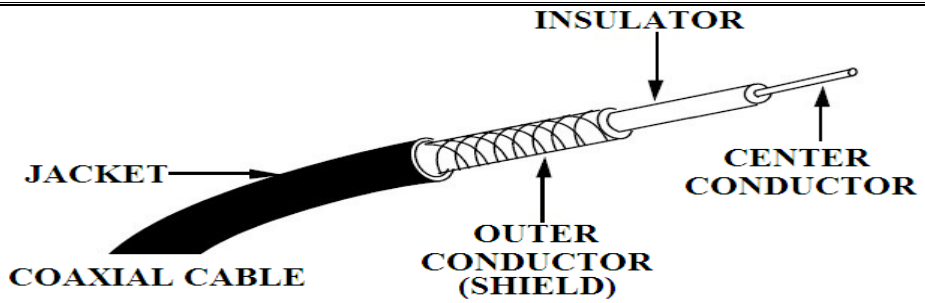
1. इस Cable से Data को ज्यादा Long Distance तक Travel नहीं कराया जा सकता है।
2. यह Cable बाहरी वातावरण से Effective होती है क्योंकि इसमें Electromagnetic Field बनता है जिससे Electrical नॉइज़ व Interference होता है।
3. इस Cable में किसी भी Node को Connection देना बहुत ही Easy होता है अतः यह सुरक्षा के लिहाज से अधिक सुरक्षित नहीं होती है।
4. इस Cable में Connection बढ़ने पर Data transfer की स्पीड भी कम हो जाती है।

2. **CO-AXIAL CABLE (कोएक्सिअल केबल): -**

ट्विस्टेड पेअर केबल को आसानी से तोडा जा सकता है अर्थात यह सुरक्षा के लिए बहुत कमजोर होती है। ट्विस्टेड पेअर केबल के इस Drawback को दूर करने के लिए Co-axial Cable का प्रयोग किया जाता है।

Co-Axial केबल Center Copper Conductor (Core) से मिलकर बनी होती है। यह Core Second Conductor इंसुलेशन से ढकी होती है। जो पुनः प्लास्टिक की कवर से ढकी होती है। Co-axial केबल को इनके Impedance के अनुसार वर्गीकृत किया जाता है। 50 Ohms डिजिटल ट्रांसमिशन तथा 75 Ohms एनालॉग ट्रांसमिशन के रूप में कोएक्सिअल केबल को वर्गीकृत किया गया है।

- इसके तार का व्यास लगभग 0.4 इंच से 1 इंच तक होता है।
- ट्विस्टेड पेअर केबल की तुलना में यह अत्यंत सुरक्षित होती है एवं इन्हे आसानी से तोडा नहीं जा सकता है।
- इनकी स्पीड ट्विस्टेड पेअर केबल की तुलना में तेज होती है।
- कोएक्सिअल केबल को लम्बी दुरी के लिए प्रयोग किया जाता है।




Co-Axial केबल दो प्रकार की होती है Thin Net Cable और Thick Net Cable

a. **Thin Net Cable: -**

- यह Thick Net Cable का एक Update और विकसित रूप (Version) है।
- इसकी Data Transfer करने की दूरी 500 मीटर तक है, क्योंकि इसमें Inter Connector के व्यास को बढ़ाकर Shield और Insulation को कम कर दिया गया, जिससे Signal ज्यादा दूरी तक Strong होने लगे।
- इसका Installation थोड़ा Hard था और यह मोटी होने के कारण थोड़ी कठोर है। जिससे इसके टूटने का डर नहीं रहता है।
- वर्तमान में इसका प्रयोग Cable TV में किया जाता है।

b. **Thick Net Cable: -**

- यह एक Original और पहला Coaxial Cable है।
- इसकी Data transfer करने की दूरी (Distance)185 मीटर तक है।
- इसका Installation थोड़ा Easy था और यह लचीली-और कमजोर थी जिससे टूटने का ज्यादा डर रहता था।
- इसका यूज़Computer में मुख्यत Bus topology में किया जाता था वर्तमान समय में इसका उपयोग Computer में न के बराबर है ।

Advantage of Coaxial Cable (कोएक्सिअल केबल के लाभ): -

1. इस केबल के बैंडविड्थ अधिक होती है।
2. इनकी स्पीड ट्विस्टेड पेअर केबल की तुलना में तेज होती है।
3. डिजिटल सिग्नल्स का ट्रांसमिशन तेज गति से होता है।
4. नॉइज़ का प्रभाव कम होता है तथा बिना किसी परिवर्तन के डाटा का प्रसार होता है।
5. कोएक्सिअल केबल को लम्बी दुरी के लिए प्रयोग किया जाता है।

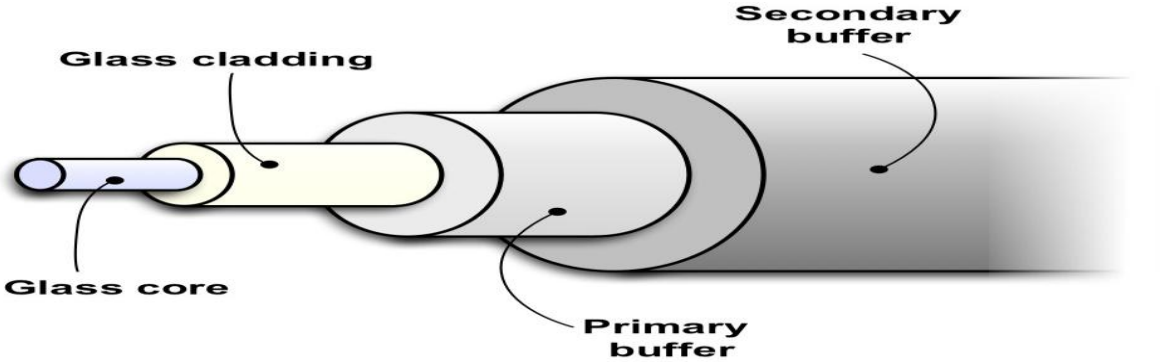
Disadvantage of Coaxial Cable (कोएक्सिअल केबल की हानियाँ): -

1. यदि यह केबल बंद हो जाये तो पूरा नेटवर्क भी बंद हो जाता है।
2. इसे Install करना ट्विस्टेड पेअर केबल की तुलना में कठिन और महंगा होता है।
3. यदि शील्ड सही जगह न हो तो केबल Ground Loop में जा सकता है।

**3. OPTICAL FIBER CABLE (फाइबर ऑप्टिकल केबल ): -**

तीसरी प्रकार की प्रमुख्य केबल फाइबर ऑप्टिक्स केबल होती है। फाइबर ऑप्टिक्स केबल फाइबर से मिलकर बनी होती है, जो लाइट को कंडक्ट करती है। यह तार कांच के हजारो रेशो से निर्मित होती है। यह फाइबर गिलास और प्लास्टिक के रूप में हो सकती है। इसमें प्रत्येक कांच का रेशा एक बाल के सामान बारीक़ होता है।

फाइबर ऑप्टिक्स केबल में डाटा का ट्रांसमिशन काफी तेज होता है। यह केबल सभी केबल की तुलना में होती है। इस केबल में सबसे इनर कोर, ऑप्टिक्स फाइबर कोर होती है, जो प्लास्टिक तथा कांच से मिलकर बनी होती है। जिसमे डाटा प्रकाश की स्पीड के तुलना में ट्रांसफर होता है। यह Core, ऑप्टिक्स बफर Tube से घिरी होती है। इसके ऊपर Protective Outer Jacket की लेयर होती है। यह केबल सुरक्षा के लिए अधिक मजबूत होती है। इसे छोटी तथा लम्बी दुरी दोनों के लिए प्रयोग किया जाता है।




Advantage of Fiber Optical Cable (कोएक्सिअल केबल के लाभ): -

1. इस केबल के बैंडविड्थ अधिक होती है।
2. Electromagnetic Interface का प्रभाव काम पड़ता है।
3. जंग लगने की सम्भावना कम होती है।
4. वजन में हल्का होता है।

Disadvantage of Fiber Optical Cable (कोएक्सिअल केबल की हानियाँ): -

1. इसे Install करना कठिन और महंगा होता है।
2. यह केबल अन्य केबल की तुलना में अधिक महंगा है।
3. लाइट का ट्रांसमिशन सिर्फ एक ही डायरेक्शन में होता है।

**UNGUIDED MEDIA (): -** Unguided Media को Wireless Media भी कहा जाता है। एक ऐसा medium जिसमे Data के Communication में Wire का यूज़ नहीं किया जाता है यह एक Wireless Communication होता है। Wireless Communication मुख्य रूप से Electromagnetic Wave के माध्यम से होता है ! Electromagnetic Wave को Electric और Magnetic Fields के Combination से Generate किया जाता है। Unguided Media भी निम्नलिखित तीन प्रकार का होता है: -

1. **Radio Waves (रेडियो वेव्स):-**

- इनकी आवृत्ति 3 KHz से 1 GHz तक होती है। इन्हें आसानी से स्थापित किया जा सकता है तथा इनका एटेनुऐशन भी उच्च होता है। रेडियो तरंगे ज्यादातर Omni Directional होती है। जब एक Antenna रेडियो तरंगों को ट्रांसमिट करता है तो ये सभी दिशाओं में फैल जाते है।
- रेडियो तरंगों का प्रयोग टेलीविज़न, मोबाइल तथा रेडियो के Communication में होता है। इनमे एक Radio Tuner होता है जो कि रेडियो तरंगो को Receive करता है तथा स्पीकर में इन तरंगों को Mechanical Vibration में बदल देता है जिससे हमें स्पीकर से आवाज़ सुनाई देती है।

2. **Microwaves (माइक्रोवेव्स):-**

- इसमें सूचना का ट्रांसमिशन इलेक्ट्रोमैग्नेटिक तरंगों द्वारा किया जाता है जिसकी Wavelength को सेंटीमीटर में मापा जाता है।
- Microwave Communication में 16 Gigabit / Second Data को Transfer करने की Speed होती है। यह एक Unidirection Communication होता है इसके लिए ऊचे और बड़े Tower लगाने की जरूरत होती है।
- इन Tower के ऊपर Parabolic Antenna का Use किया जाता है। और दोनों Parabolic Antenna को बिलकुल एक दूसरे के सामने की Direction में रखा जाता है जिससे Micro Wave बीम Travel कर सके।
- इनकी आवृत्ति 1GHz से अधिक होती है तथा ये अनेक प्रकार के ट्रांसमिट से निर्मित होती है। Microwaves का प्रयोग खाना पकाने तथा मोबाइल आदि में किया जाता है तथा Wi-Fi में भी इसका प्रयोग किया जाता है।

3. **Infrared Waves (इंफ्रारेड वेव्स):-**

- सन् 1800 में सर्वप्रथम सर william herschel ने infrared को विकसित किया था।
- Infrared Communication एक Unidirection Communication होता है।यह दीवार या किसी भी Physical अवरोध को पार नहीं कर सकता है और ना ही यह ज्यादा दूर तक Travel कर सकता है।
- यह एक विशेष तरंगदैर्ध्य का विधुतचुम्ब्कीय विकीरण होता है जिन्हें हम Infrared कहते हैं। इन तरंगो को मनुष्य देख नहीं सकता है परन्तु Skin में Heat के रूप में महसूस अवश्य कर सकता है।
- इनका प्रयोग TV रिमोट कण्ट्रोल, Wireless LAN, CCTV, Automatic Door, Remote Control तथा मिसाइल गाइडेंस सिस्टम आदि में किया जाता है।

4. **SATELLITE COMMUNICATION (सैटेलाइट कम्युनिकेशन): -**

- यह भी एक Microwave Communication का ही दूसरा रूप है परन्तु इस Process में जमीन पर लगे Parabolic Antenna सीधे अंतरिक्ष की Orbit में स्थापित Satellite से Communication करते है। उनका भी Communication करने का माध्यम Uni Direction ही होता है।
- सैटेलाइट पृथ्वी के वातावरण की और पृथ्वी की हर छोटी से बड़ी चीजों की मॉनीटरिंग करता है। यह पृथ्वी के चक्कर लगाती है, सैटेलाइट को हिंदी में उपग्रह भी कहते है।
- Satellite Communication का सबसे बड़ा फायदा यह होता है की इससे एक Country से दूसरी Country तक भी Communication किया जा सकता है। इसका सबसे अच्छा उदहारण आज के आज के वक्त में लाइव TV Streams और Dish TV है जिसमे Micro Wave का Use होता है ।

सैटेलाइट कम्युनिकेशन के प्रकार: -

a. लो अर्थ ऑरबिट सैटेलाइट: - ये उपग्रह पृथ्वी की कक्षा के सबसे पास होते है। इनकी ऊंचाई 160 से 1600 किलोमीटर तक होती है। इनकी गति तेज होती है। यह तेज गति से पृथ्वी के चक्कर लगाते है। इस वजह से दिन में यह कई बार पृथ्वी के चक्कर पूरे कर लेते है। और इन्हें धरती को स्कैन करने में समय बहुत कम लगता है और इनका अधिकतर उपयोग इमेज और स्कैनिंग के लिए किया जाता है।

b. मीडियम अर्थ ऑरबिट सैटेलाइट: - यह उपग्रह ज्यादा तेज गति से पृथ्वी के चक्कर नहीं लगाते है। यह 12 घंटे में धरती का एक चक्कर पूरा कर लेती है। यह उपग्रह किसी जगह से एक निश्चित समय से होकर गुजरता है। इन उपग्रह की ऊंचाई 10 हजार किलोमीटर से 20 हजार किलोमीटर होती है। इनका उपयोग नेवीगेशन के लिए किया जाता है।

c. हाई अर्थ ऑरबिट सैटेलाइट: - यह उपग्रह धरती से करीब 36 हजार किलोमीटर दूर होते है। यह पृथ्वी की गति के साथ ही पृथ्वी का चक्कर लगाते है। इन उपग्रहों का प्रयोग कम्युनिकेशन के लिए किया जाता है।

**सैटेलाइट के प्रयोग: -**

i. टेलीविजन: - सैटेलाइट घरों में सीधे टीवी सिग्नल भेजते हैं, ये सैटेलाइट "किसी भी दृश्य में" समाचार प्रसारण, चाहे वह इलेक्शन पर लाइव रिपोर्टिंग या एक ट्रैफिक दुर्घटना के दृश्य हो, क्षेत्र से स्टूडियो तक सैटेलाइट के माध्यम से भेजे जाते हैं।

ii. टेलीफोन: - सैटेलाइट अक्सर ग्रामीण क्षेत्रों और उन क्षेत्रों के लिए वॉइस कम्युनिकेशन का मुख्य केंद्र होता है जहाँ आपदा के बाद फ़ोन लाइनें क्षतिग्रस्त हो जाती हैं। सैटेलाइट फोन और मोबाइल के लिए प्राथमिक समय स्रोत भी प्रदान करते हैं।

iii. नेविगेशन: - Global Positioning Systems (GPS) जैसे सैटेलाइट-आधारित नेविगेशन सिस्टम किसी को भी कुछ मीटर के भीतर उसके स्थान को निर्धारित करने के लिए सक्षम करते हैं। जीपीएस-बेस सिस्टम का उपयोग नागरिकों और सेना द्वारा भूमि, समुद्र और हवा पर नेविगेशन के लिए किया जाता है।

iv. व्यापार और वित्त: - कम्युनिकेशन सैटेलाइट में व्यापक रूप से अलग-अलग स्थानों के बीच तेजी से कम्युनिकेशन करने की क्षमता होती है। यह एक महत्वपूर्ण टूल है।

v. मौसम: - सैटेलाइट मौसम विज्ञानियों को वैश्विक स्तर पर मौसम को देखने की क्षमता प्रदान करते हैं, जिससे उन्हें ज्वालामुखी विस्फोट, गैस और तेल क्षेत्रों जैसी घटनाओं के प्रभावों का पता लगाने, तूफान और अल नीनो जैसी बड़ी दुर्घटना का पता लगाने के लिए प्रयोग किया जाता है।

vi. जलवायु और पर्यावरण निगरानी: - जलवायु परिवर्तन अनुसंधान के लिए उपग्रहों में से कुछ डेटा के सबसे अच्छे स्रोत हैं। सैटेलाइट समुद्र के तापमान और प्रचलित धाराओं की निगरानी करते हैं।

vii. सुरक्षा: - अर्थ ऑब्जरवेशन सैटेलाइट समुद्र और हवा की धाराओं के साथ-साथ जंगल की आग, तेल फैल और वायु प्रदूषण की सीमा की निगरानी कर सकते हैं; साथ में यह रिमोट क्षेत्रों में संकटग्रस्त लोगों के लिए सैटेलाइट "खोज और बचाव" में "खोज" कर सकते हैं।

viii. जमीन का परिचारक: - सैटेलाइट पानी और खनिज स्रोतों का पता लगा सकते हैं; भूमि से जलमार्ग में पोषक तत्वों और दूषित पदार्थों के ट्रांसफर की निगरानी करते हैं; और भूमि और पानी के तापमान, समुद्रों में शैवाल की वृद्धि, और भूमि से टोपोसिल के क्षरण को मापते हैं।

ix. विकास: - विकासशील देशों में कम्युनिकेशन सैटेलाइट शिक्षा और चिकित्सा विशेषज्ञता तक पहुँच प्रदान करते हैं, जो अन्यथा उन तक नहीं पहुँचते।

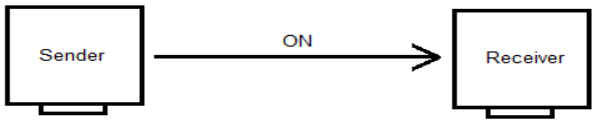
x. अंतरिक्ष विज्ञान: - सैटेलाइट दूरबीनों को पल्सर और ब्लैक होल जैसी घटनाओं को समझने के साथ-साथ ब्रह्मांड की आयु को मापने के लिए भी महत्वपूर्ण है।

## COMMUNICATION OR TRANSMISSION MODE (कम्युनिकेशन या ट्रांसमिशन मोड): -

Communication Mode का अर्थ दो Device के मध्य Signal Flow की दिशा से होता है। Communication में एक Device Signal को भेजने वाला तथा दूसरा Device इसे प्राप्त करने वाला हो सकता है। साथ ही दोनों के दोनों Device भी Signal को भेजने व प्राप्त करने वाले हो सकते है। इसके अनुसार Communication Mode निम्नलिखित तीन प्रकार का होता है—

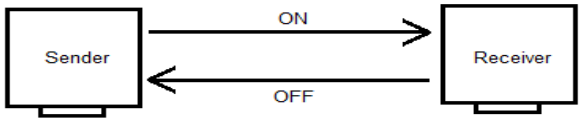
1. Simplex (सिम्पलेक्स): -

Simplex Communication Mode में डेटा व सिग्नल सदैव एक ही दिशा में Transmit होते है। अर्थात हम अपनी सूचनाओ को केवल भेज सकते है प्राप्त नहीं कर सकते सिम्पलेक्स कम्युनिकेशन कहलाता हैं। इसीलिए इसे One-Way Communication भी कहा जाता है। इसमें सामान्यतः एक डिवाईस सिग्नल की भेजने वाला तथा एक या एक से अधिक डिवाईस इसे प्राप्त करने वाले होते है। उदाहरण— कीबोर्ड, कीबोर्ड से हम केवल सूचनाये भेज सकते है प्राप्त नहीं कर सकते। अन्य उदाहरण—Radio, TV, Remote आदि।



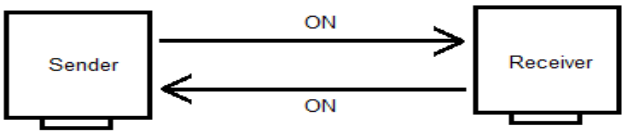

2. Half Duplex (हाफ डुप्लेक्स): -

Half Duplex Communication Mode में डेटा व सिग्नल सदैव दोनों दिशा में Transmit होते है। इसे Alternative Two-Way Communication भी कहा जाता है। इसमें जब एक डिवाईस सिग्नल को भेज रहा होता है तो दूसरा डिवाईस उसे प्राप्त कर रहा होता है। इसी प्रकार जब दूसरा डिवाईस सिग्नल को भेज रहा होता है तो पहला डिवाईस उसे प्राप्त कर रहा होता है। किन्तु दोनों डिवाईस एक ही समय में सिग्नल का आदान-प्रदान नहीं कर सकते है। उदाहरण— हार्डडिस्क (Hard Disk), हार्डडिस्क से डाटा का आदान प्रदान Half Duplex अवस्था में होता है। जब हार्डडिस्क पर डाटा संगृहीत (Save) किया जाता है तो उस समय डाटा को हार्डडिस्क से पढ़ा नहीं जा सकता है और जब हार्डडिस्क से डाटा को पढ़ा जाता है तो उस समय हम डाटा को संगृहीत (Save) नहीं कर सकते। अन्य उदाहरण— Walkie-Talkie, Citizen's Band आदि।




3. Full Duplex (फुल डुप्लेक्स): -

Full Duplex Communication Mode में डेटा व सिग्नल दोनों दिशा में Transmit होते है। इसे Full Two-Way Communication भी कहा जाता है। अर्थात हम एक ही समय में सूचनाएं भेज भी सकते है और प्राप्त भी कर सकते है पूर्ण ड्यूप्लेक्स (Full Duplex) कहलाता हैं। इसमें दोनों डिवाईस एक ही समय में सिग्नल का आदान-प्रदान कर सकते है। इसमें Communication सबसे तेज गति से होता है इसीलिए इसका प्रयोग वर्तमान में सबसे ज्यादा किया जा रहा है। उदाहरण— Computer, Mobile, Landline आदि।



# UNIT 04
# NETWORKING DEVICES

**NETWORKING DEVICES (नेटवर्किंग डिवाइसेस): -** Networking Devices वे Equipment होते है जिनके द्वारा दो या दो से अधिक कंप्यूटर या इलेक्ट्रॉनिक डिवाइस को आपस में Connect किया जाता है। जिससे की वे आपस में डेटा Share कर सकें तथा कम्युनिकेशन कर सकें। Networking Devices निम्नलिखित प्रकार के है: -

1. Repeater.
2. Hub.
3. Switch.
4. Bridge.
5. Router.
6. Gateways.

## 1. REPEATER (रिपीटर): -

Repeater का मतलब होता है Network रिपीट। ये एक ऐसा Powerful Network Device होता है जिसका इस्तेमाल Signal को Regenerate करने में किया जाता है। सिग्नल जब लंबी दूरी तय करते है तब इनकी Strength समान रहे यही Repeater का काम होता है। रिपीटर Signal को Amplify नहीं करते बल्कि Signal के Weak होने पर उन्हें Bit By Bit कॉपी करते हैं फिर उसे Regenerate करते हैं।

रिपीटर्स का इस्तेमाल Ethernet नेटवर्क को Establish करने में भी किया जाता है। रिपीटर OSI Layer के First Layer में स्थित होता है। रिपीटर्स में उन Cable का इस्तेमाल किया जाता है जो कम से कम 100 मीटर की दूरी को कवर करती हो। इनके लिए Optical Fiber, Copper, Coaxial का इस्तेमाल होता है।

यह OSI मॉडल के लेयर 1 (Physical Layer) में कार्य करता है। Repeater का प्रयोग सिग्नलों को एक सीमा तक नष्ट होने से पहले Regenerate करने के लिए किया जाता है। सिग्नल को Regenerate इसलिए किया जाता है क्योंकि जब सिग्नल एक जगह से दूसरी जगह में जाते है तो वह Weak होते जाते है इसलिए सिग्नल के नष्ट होने से पहले दुबारा Generate किया जाता है जिससे की सिग्नल नष्ट ना हो।

यह डिजिटल तथा एनालॉग दोनों प्रकार के सिग्नलों को Replicate तथा Regenerate कर सकता है। Repeater दो प्रकार का होता है Analog Repeater तथा Digital Repeater. Analog Repeater सिग्नल को केवल Regernrate करता है। जबकि Digital Repeater सिग्नल को Reconstruct करके उसमें से Errors को हटा के आगे भेजते है।


Advantage of Repeater (रिपीटर के लाभ): -

a. रिपीटर के माध्यम से सिग्नल को Regenerate करके लम्बी दुरी तक ट्रांसमिट किया जा सकता है।
b. Repeater एक Intelligent डिवाइस है यह सिग्नल को Regenerate करने के साथ साथ सिग्नल में उपस्थित Noise और Error को भी Repair करता है।
c. रिपीटर एक Simple Device है अतः इसके उपयोग करने के लिए टेक्निकल स्किल की जरुरत नहीं होती है।
d. रिपीटर की कीमत ज्यादा नहीं होती है अतः इस नेटवर्क में उपयोग करने से नेटवर्क की Cost में ज्यादा फर्क नहीं पड़ता है।

e. रिपीटर वायर्ड और वायरलेस दोनों प्रकार के आते है अतः यूज़र अपने सुविधा के अनुरूप उपयोग कर सकता है।
f. रिपीटर का उपयोग करके नेटवर्क के साइज़ को बड़ा करने पर उसके परफॉरमेंस में कोई फर्क नहीं पड़ता है।
g. रिपीटर अलग अलग प्रकार के मीडिया से कनेक्ट होकर कार्य कर सकता है जैसे ट्विस्टेड पेअर केबल , कोएक्सीयल केबल, फाइबर ऑप्टिक्स इत्यादि।

Disadvantage of Repeater (रिपीटर से हानि): -

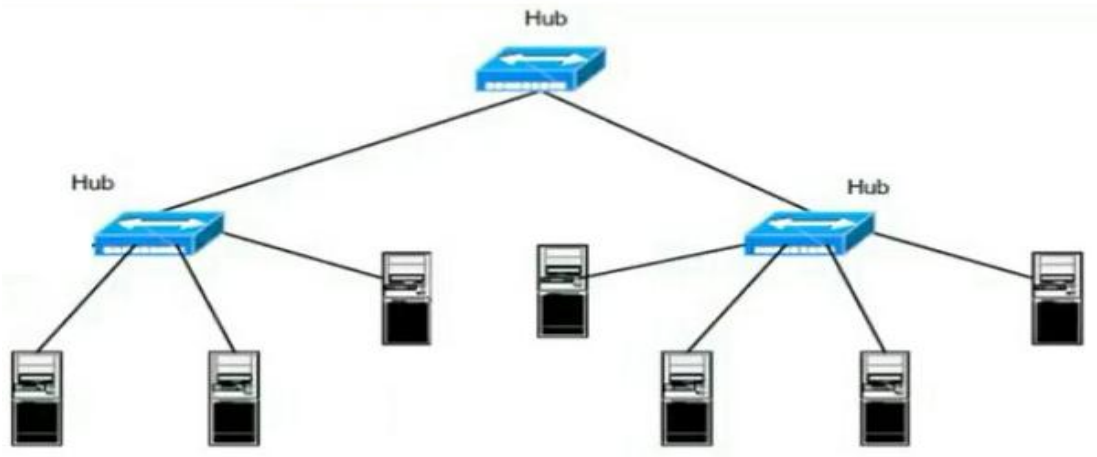
a. Repeater में नेटवर्क को मॉनिटर करने एवम् उनको ठीक करने की फंक्शन नहीं होती है।
b. रिपीटर का उपयोग केवल डिजिटल सिग्नल के लिए किया जाता है यह एनालॉग सिग्नल के लिए कार्य नहीं करता है।
c. Repeater का उपयोग करके दो अलग-अलग LAN को कनेक्ट नहीं किया जा सकता है इसके द्वारा केवल एक ही LAN के अलग-अलग सिग्मेंट को जोड़ा जा सकता है।
d. Repeater नेटवर्क के ट्रैफिक को फ़िल्टर नहीं कर सकता है।
e. Repeater केवल एक ही प्रकार के प्रोटोकॉल पर कार्य कर सकता है।

**2. HUB (हब): -**

Hub एक ऐसा Device होता है जो की एक Network Connection को Multiple Computers में Split करता है। यह एक Distribution Center के जैसा होता है। जब एक Computer Information के लिए किसी एक Network से या एक Specific Computer से Request करता है, तब Hub उस Request को एक Cable के माध्यम से Send करता है।

Network Hubs की अलग अलग Speeds भी होते हैं। जहाँ पहले के Older Network Hubs केवल 10 Mbps Speeds प्रदान करते थे, वहीँ अभी के Hubs 100 Mbps तक की Speed प्रदान करते हैं। अभी के बड़े Networks में, ये जरुरी होता है की एक Dual Speed Network Hub का उपयोग किया जाता है, और ये दोनों 10 और 100 Mbps में आता है जो की Computers और Printers को Connection Points प्रदान करता है। एक USB hub में हम 127 Devices कनेक्ट कर सकते है और नेटवर्क हब में 32 Devices। एक Network Hub एक Variable Port Repeater की तरह होता है, इसमें Cluster of Computers के लिए केवल एक Common Link होता है यह आमतौर पर Information प्राप्त कर उन्हें ये आगे, सभी PC Terminals में Attached होते हैं, Forward कर देता है। इसमें Data की Repetition होती है जिससे की Unnecessary Data Traffic को Network में Sent किया जाता है। Network Hub के Features क्या होते हैं: -

- ये Half Duplex Mode में Operate होती है।
- ये 4 से लेकर 24 Port Sizes में Available होती है।
- इसमें अगर कोई Collision Detection और Re-transmission of Packets होता है तब Hosts ही Responsible होते हैं।



Hub दो प्रकार का होता है: -

- Passive Hub: - यह सिग्नल को जैसा है उसी स्थिति में आगे भेज देता है इसलिए इसे Power Supply की जरुरत नहीं होती है।
- Active Hub:- इसमें सिग्नल को दुबारा Generate किया जाता है, इसलिए ये भी Repeater की तरह कार्य करते है। इन्हें Multiport Repeater कहते है। इसमें Power Supply की जरुरत होती है।

Advantage of HUB (हब से लाभ): -

a. ये आसानी से Network के पुरे Distance में Extend हो सकता है।
b. यह दूसरी devices की तुलना में सस्ता होता है।
c. यह बहुत सारीं Network Media को Support करता है। इनके साथ बहुत से अलग अलग Media Types को आसानी से Connect किया जा सकता है।
d. यह नेटवर्क की कुल दूरी (Total Distance) को बढ़ा सकता है।
e. एक हब Internet के Traffic को Monitor कर सकता है और उसे Analyze कर सकता है।
f. यह Network की Performance को बाधित (Disturb) नही करता।

Disadvantage of HUB (हब से हानि): -

a. हब Network Traffic को फ़िल्टर नहीं कर सकता है।
b. हब नेटवर्क के Best Path का Selection नहीं कर सकता है।
c. अलग अलग प्रकार के Network Architecture को Connect नहीं कर सकता है।
d. Network को Segment में Divide नहीं कर सकता है।
e. नेटवर्क ट्रैफिक को Reduce नहीं कर सकता है।

**3. SWITCH (स्विच): -**

Switch एक ऐसा Networking Device होता है जो की Network में Devices को एक दुसरे के साथ Connect होने में मदद करता है, जिससे की वो Data का Transfer network में कर सकें। ये Network Switches पूरी तरह से Network Hubs के समान Identical होते हैं, लेकिन एक स्विच, हब की तुलना में ज्यादा Intelligent होती है ।

Intelligence का तात्पर्य यह है की Network Switch आये हुए Frames को पहले Inspect करता है, उसकी Source और Destination Address को Determine करता है और फिर उस फ्रेम को Accordingly सही जगह को Route करता है। स्वीट्चेस, फ्रेम को आगे Forward करने के लिए मुख्य रूप से 4 Methods का उपयोग करते हैं।

1. Store और Forward करना – इस Method में, Switches प्रत्येक Frame को Buffer करती है और उन्हें आगे Forward करने के पूर्व उसमें Checksum Perform करती है।

2. Cut Through करना – इस Method में, कोई भी Error Check Perform नहीं किया जाता है। इसमें मुख्य रूप से Switch, Frame की Hardware Address को Read करती है और फिर उसे Forward करती है।

3. Fragment Free – यह Method ऊपर दोनों Methods का Combination होता है अर्थात Store and Forward और Cut Through. इस Method में पहले Frame की First 64 Bytes को Check करती है जिससे Addressing Information प्राप्त हो जाता है। इससे Switch को Frame के Destination के विषय में पता चल जाता है।

4. Adaptive Switching – इस Method का उपयोग बाकि तीनों Modes के बीच Automate Switching के लिए किया जाता है।

Type of Switch (स्विच के प्रकार): -

1. Unmanaged स्विच: - इन Switches का ज्यादातर प्रयोग Home Networks और Small Businesses में होता है क्यूंकि ये Plug-in होते हैं और इन्हें तुरंत ही उपयोग में किया जा सकता है। इन Switches को Configure करना पड़ता है। इनमें केवल छोटे Cable Connections की जरुरत होती है। ये Network में Devices को एक दुसरे के साथ Connect होने में Allow करता है।

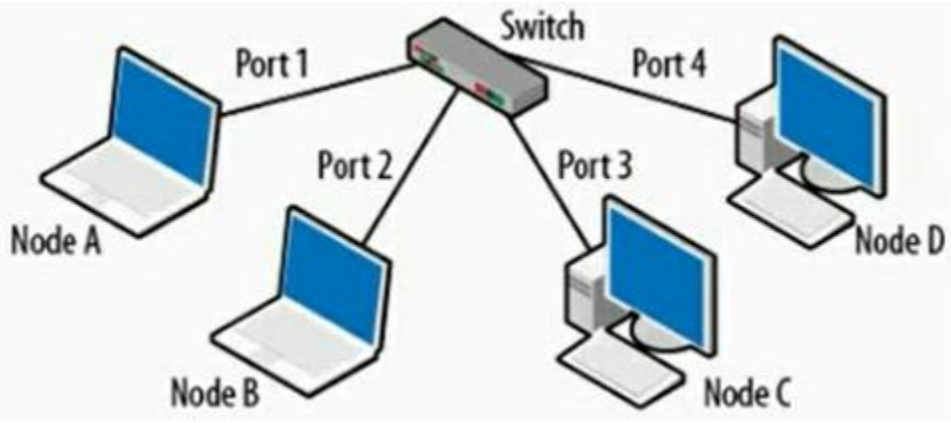
2. Managed स्विच: - इस प्रकार की Switches में कई प्रकार के Features होते हैं जैसे की Highest Levels की Security, Precision Control और Network की Full Management का होना। इन्हें अक्सर उन Organisations में प्रयोग में लाया जाता है जहाँ की एक बहुत ही बड़ी Network होती है और इन्हें आसानी से Customised किया जा सकता है जिससे की किसी एक Network की Functionality को Enhance किया जा सके।

Advantages of Switch (स्विच से लाभ): -

a. इसका उपयोग Network की Available Bandwidth को बढ़ाने के लिए होता है।
b. इसके उपयोग से Individual Host PCs के Workload को कम किया जा सकता है।
c. ये Network के Performance को बढ़ाने में मदद करते हैं।
d. Networks जिनमें Switches का उपयोग होता है उनमें बहुत ही कम Frame Collisions होते हैं। ऐसा इसलिए क्यूंकि Switches प्रत्येक Connection में Collision Domains Create करते हैं।
e. ये Hubs की तुलना में ज्यादा Intelligent होते हैं।
f. Switches को Directly Workstation के साथ में Connect किया जा सकता है।

Disadvantages of Switch (स्विच से हानि): -

a. ये Network Bridges की तुलना में बहुत ही ज्यादा Expensive (कीमती) होते हैं।
b. Network Switch के माध्यम से Network Connectivity Issues को Trace करना बहुत ही Difficult होता है।
c. Traffic को Broadcast करना ज्यादा Troublesome काम हो सकता है।
d. Multicast Packets को Handle करने के लिए Proper Design और Configuration की जरुरत होती है।
e. जब Broadcasts को Limit करने की बारी आती है, तब वो Routers के समान उतने बेहतर कार्य नहीं करते हैं।




Diffence Between HUB and Switch (हब और स्विच में अंतर): -

| S.N | HUB | SWITCH |
|---|---|---|
| 01 | फिजिकल लेयर पर काम करता है। | डेटा लिंक लेयर पर काम करता है। |
| 02 | ब्रॉडकास्ट ट्रांसमिशन का प्रकार है। | यूनिकैस्ट, मल्टिकास्ट और ब्रॉडकास्ट टाइप ट्रांसमिशन है। |

| | | |
|---|---|---|
| 03 | अधिकतम 4 पोर्ट होते हैं। | 24 से 48 पोर्ट हो सकते हैं। |
| 04 | केवल एक collision domain है। | अलग-अलग पोर्ट का अपना Collision Domain होता है। |
| 05 | एक हाफ डुप्लेक्स ट्रांसमिशन मोड है। | एक Full Duplex ट्रांसमिशन मोड है। |
| 06 | पैकेट फ़िल्टरिंग प्रदान नहीं किया गया है। | पैकेट फ़िल्टरिंग प्रदान किया जाता है। |
| 07 | हब को रिपीटर के रूप में उपयोग नहीं किया जा सकता है। | स्विच को रिपीटर के रूप में इस्तेमाल किया जा सकता है। |
| 08 | हब एक इंटेलीजेंट डिवाइस नहीं है, इसलिए यह तुलनात्मक रूप से सस्ती है। | स्विच एक इंटेलीजेंट डिवाइस है इसलिए यह महंगा है। |
| 09 | हब एक पुरानी डिवाइस है और आमतौर पर अब इसका उपयोग नहीं किया जाता है। | स्विच बहुत परिष्कृत उपकरण है और व्यापक रूप से उपयोग किया जाता है। |

**4. <u>BRIDGE (ब्रिज): -</u>**

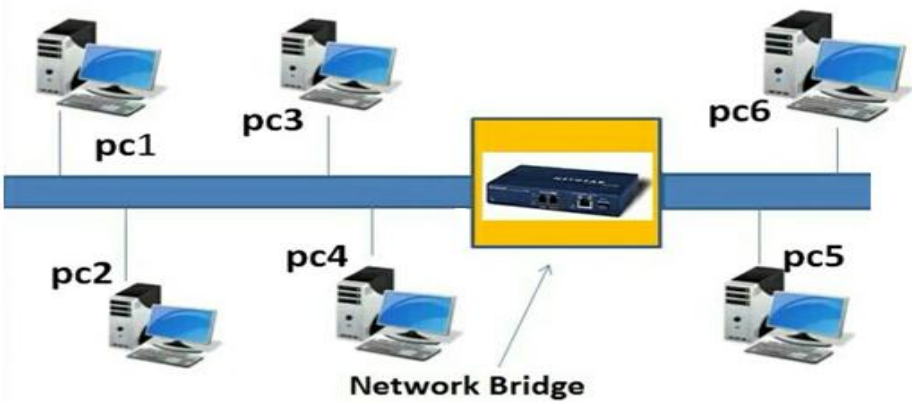
- यह एक Networking Device है जो की नेटवर्क सेगमेंट्स को आपस में जोड़ता है तथा डेटा फ़िल्टरिंग का कार्य भी करता है।
- Bridge में केवल दो पोर्ट होते हैं एक Incoming (आने वाला) और Outgoing (जाने वाला)।
- Bridge डेटा को भेजने से पहले Destination एड्रेस को Check करता है। यदि Bridge को डेस्टिनेशन एड्रेस मिल जाता है तो वह डेटा को भेजता है अन्यथा वह डेटा को ट्रांसमिट नहीं करेगा।
- Bridges का उपयोग डेटा Signals और ट्रैफिक को Maintain करते हुए नेटवर्क को बढ़ाने के लिए किया जाता है।
- यह OSI Model के लेयर 2 (डेटा लिंक लेयर) पर काम करता है। इसमें डेटा Frames के रूप में जाता है।

<u>Advnatage of Bridge (ब्रिज से लाभ): -</u>

a. ये Bridges बहुत ही Simple होते हैं Repeaters and Swtich की तुलना में ये बहुत ही सस्ते होते हैं।
b. यह Switches का एक बहुत ही बेहतरीन विकल्प है और इनकी मदद से Micro Segmentation किया जा सकता है।
c. इनकी मदद से Data Link Layer के ऊपर के Load को Lower किया जा सकता है।
d. Bridges बहुत ही ज्यादा Reliable होते हैं।

<u>Disadvantage of Bridge (ब्रिज से हानि): -</u>

a. कुछ Specific IP Address को Read करने में ये असक्षम होते हैं; वो ज्यादा MAC Addresses के साथ Concerned होते हैं।
b. ये Repeaters और Hubs की तुलना में थोड़े Expensive होते है ।
c. ये Repeaters की तुलना में थोड़े Slow काम करते हैं क्योंकि इसमें Filtering होती है।



**5. ROUTER (राऊटर): -**

यह OSI Model के लेयर 3 (नेटवर्क लेयर) में कार्य करता है। Router एक Hardware Networking Device है। इसका उपयोग Network में किया जाता है। जब भी कोई Data जो एक Packet के रूप में एक Network से दुसरे Network में Travel करता है, तब Router, Packet Data को Receive करता है, और Data Packet में जो भी छुपी हुई Information है, उसको Analyze करने के बाद Destination Device को Forward करता है। इस Networking Device को अलग अलग Networks को अपसा में Wire या Wirelessly जोड़ने के लिया किया जाता है।

Router छोटे इलेक्ट्रॉनिक उपकरण होते हैं जो कई Computer Networks को Wired या Wireless Connection के माध्यम से एक साथ जोड़ते हैं। अर्थात Router एक Computer Network को दूसरे Computer Network से Cconnect करता हैं। इसलिए इसे Inter Networking Device भी कहा जाता हैं।

Network को Internet से Connect करने के लिए Router का Modem से Connect होना चाहिए। इसलिए, अधिकांश Router में एक विशिष्ट ईथरनेट पोर्ट होता है जिसे Cable या DSL Modem के ईथरनेट पोर्ट से कनेक्ट करने के लिए डिज़ाइन किया गया है। Types of Router: -

a. Wired Router
b. Wireless Router

a. Wired Router: - आमतौर पर बॉक्स के आकार वाले डिवाइस होते हैं जो सीधे "हार्ड-लाइन"या वायर्ड कनेक्शन के माध्यम से कंप्यूटर से कनेक्ट होते हैं।Wired Router पर एक कनेक्शन पोर्ट राउटर को इंटरनेट डेटा पैक प्राप्त करने के लिए मॉडेम से कनेक्ट करने की इजाजत देता है, जबकि Ports का एक और सेट एक Wired Router को इंटरनेट Data Packet वितरित करने के लिए कंप्यूटर से कनेक्ट करने की अनुमति देता है। कुछ Wired Router फ़ैक्स मशीनों और टेलीफ़ोन पर Data Packet वितरित करने के लिए Port भी प्रदान करते हैं।

b. Wireless Router: - Wifi Router एक ऐसा डिवाइस है जो Internet चलाने के लिए Use किया जाता है Wifi Router DSL Internet के साथ प्रयोग किया जाता है| DSL का अर्थ Direct Subscribe Line होता है जो हर कंपनी में ISP कंपनी द्वारा प्रोवाइड किया जाता है| ISP एक Internet Service Provider कंपनी होती है जो users के लिए Internet की सुविधा उपलब्ध कराती है| Wired Router की तरह, एक Wireless Router भी इंटरनेट डेटा पैकेट प्राप्त करने के लिए सीधे केबल के माध्यम से मॉडेम से जोड़ता है।

Diffence Between Router and Bridge (ब्रिज और राऊटर में अंतर): -

| S.N | BRIDGE | ROUTER |
|---|---|---|
| 01 | Bridge डेटा लिंक लेयर पर काम करता है। | Router नेटवर्क लेयर पर काम करता है। |
| 02 | इस पर डेटा Frame के फॉर्मेट में होता है। | इस पर डेटा Packet के फॉर्मेट में होता है। |
| 03 | Bridge में केवल 2 पोर्ट होते है। | Router में दो से अधिक Port होते है। |
| 04 | Bridge दो LAN को आपस में जोड़ता है। | दो अलग अलग नेटवर्क को आपस में कनेक्ट करता है। |
| 05 | Bridge में कोई Routing Table का उपयोग नहीं होता। | Router में Routing Table का उपयोग किया जाता है। |
| 06 | Bridge सिंगल ब्रॉडकास्ट डोमेन पर काम करता है। | राउटर सिंगल ब्रॉडकास्ट डोमेन से अधिक पर काम करता है। |
| 07 | Bridges को कॉन्फ़िगर करना काफी आसान है। | Routers को कॉन्फ़िगर करना काफी Difficult है। |
| 08 | Bridge MAC address पर काम करता है। | Router IP Address पर काम करता हैं। |
| 09 | Bridge सस्ता होता है। | राऊटर महंगा होता है। |

**6. GATEWAY (गेट्वे): -**

- Gateway का मतलब "इंटरनेट या किसी अन्य नेटवर्क से कनेक्ट करने के लिए दो कंप्यूटरों के बीच के लिंक को Gateway कहा जाता है।"
- यह Gateway एक हार्डवेयर है जो फ़ायरवॉल, राउटर या सर्वर के रूप में आ सकता है। दो नेटवर्क के लिए, यह एक होम या ऑफिस नेटवर्क और इंटरनेट की तरह एक Wider Area Network हो सकता है।
- Gateway एक नेटवर्क नोड है जो दो नेटवर्क को अलग-अलग प्रोटोकॉल का उपयोग करके कनेक्ट करता है।
- एक नेटवर्क Gateway दो नेटवर्क को कनेक्ट करता है ताकि एक नेटवर्क के डिवाइस दूसरे नेटवर्क के पर डिवाइसेस के साथ कम्यूनिकेट कर सकें।
- Gateway पूरी तरह से सॉफ्टवेयर, हार्डवेयर, या दोनों के कॉम्बिनेशन में लागू किया जा सकता है। क्योंकि एक नेटवर्क Gateway फ़ायरवॉल और प्रॉक्सी सर्वर इसके साथ इंटिग्रेटेड होते हैं।
- Gateway को प्रोटोकॉल कनवर्टर के रूप में भी जाना जाता है जो OSI मॉडल लेयर पर परफॉर्म कर सकता है।

Types of Gateways (गेटवे के प्रकार): - Gateway कई फॉर्म में हो सकता हैं और कई प्रकार के कार्य कर सकता हैं।

i. Web Application firewall: – वेब सर्वर से ट्रैफ़िक को फ़िल्टर करता है और एप्लिकेशन-लेयर डेटा को देखता है।
ii. API, SOA or XML Gateway: – अंदर या बाहर फ्लो रही ट्रैफिक को मैनेज करता हैं, माइक्रो-सर्विस-ओरिएंटेड आर्किटेक्चर या XML-बेस वेब सर्विसेस को मैनेज करता हैं।
iii. Cloud Storage Gateway: – विभिन्न क्लाउड स्टोरेज सर्विस API कॉल के साथ स्टोरेज रिक्वेस्ट को ट्रांसलेट करता है।
iv. Media Gateway: – एक प्रकार के नेटवर्क के लिए आवश्यक फॉर्मेट से डेटा को दूसरे के लिए आवश्यक फॉर्मेट में कन्वर्ट करता है।
v. VoIP Trunk Gateway: – IP (VoIP) नेटवर्क पर वॉइस के साथ सादे पुराने टेलीफोन सर्विस (POTS) उपकरण, जैसे लैंडलाइन फोन और फैक्स मशीन के उपयोग की सुविधा प्रदान करता है।
vi. Email Security Gateway: – कंपनी पॉलिसी को तोड़ने वाले या दुर्भावनापूर्ण इरादे से ट्रांसफर होने वाले ईमेल के प्रसारण को रोकता है।

**7. ACCESS POINT (एक्सेस पॉइंट): -**

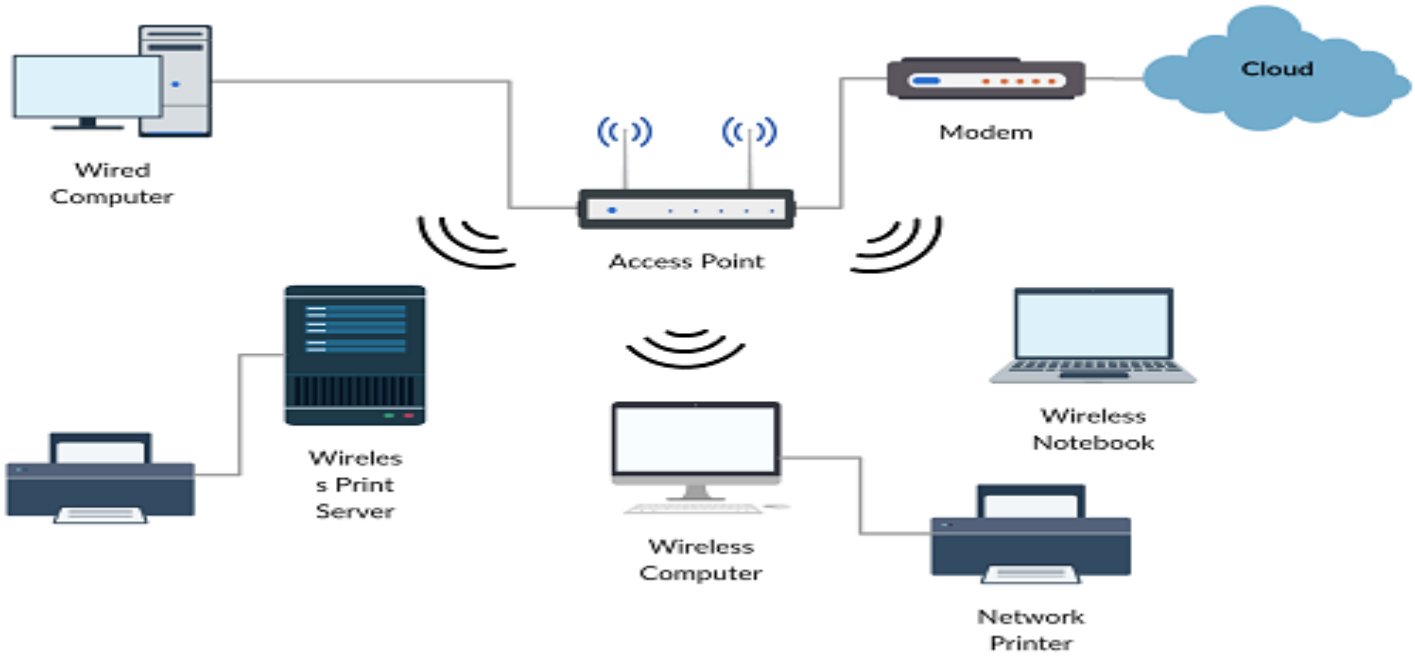
Access Point को शार्ट में (AP) कहा जाता है, यह एक नेटवर्किंग हार्डवेयर डिवाइस है, जिसका उपयोग Wireless LAN Connectivity के लिए किया जाता है। यानि Access Point एक वायरलेस प्लेटफार्म देता है, जिससे कनेक्ट होकर आप LAN या इंटरनेट से जुड़ सकते हैं।

एक्सेस पॉइंट Access Point एक वायरलेस राऊटर की तरह डिवाइस होता है, जो की वायरलेस डिवाइसेस को किसी नेटवर्क के साथ कनेक्ट होने में मदद करता है। ज्यादातर एक्सेस पॉइंट्स बिल्ट इन राऊटर होते हैं, वहीं दूसरे डीवाईसेस को नेटवर्क एक्सेस प्रदान करने के लिए किसी राऊटर के साथ कनेक्ट होना पड़ेगा। किसी भी स्थिति की बात करें, एक्सेस पॉइंट को Typically हार्ड वायर्ड किया जाता है दुसरे डिवाइसेस के साथ, जैसे की नेटवर्क Swithc या ब्रॉडबैंड मॉडेम।

Access Point को Wireless Router का बड़ा रूप भी कह सकते हैं, जो Router के सभी काम तो करता ही है, साथ ही इसकी Wireless Range भी काफी ज्यादा होती है और इसमें ज्यादा Network Traffic Control करने की क्षमता होती है।

Access Point का इस्तेमाल ज्यादा बड़े Area जैसे कि बड़े Corporate Offices, Colleges, School या फिर बड़ी Buildings इत्यादि में बेहतर Wireless Connectivity के लिए किया जाता है, जिससे Wireless LAN और Internet की अच्छी स्पीड बनी रहे।

इसके लिए किसी भी Area के अनुसार एक या उससे कई अधिक (AP) Wireless Access Point लगाए जा सकते हैं, जिनको किसी एक जगह जैसे Server Room से नेटवर्क Admin द्वारा Manage किया जाता है। जहाँ एक Access Point को डायरेक्ट कंट्रोल किया जा सकता है, वहीँ एक से अधिक Wireless Access Point होने पर इनको कंट्रोल या मैनेज करने के लिए Centralized Solution यानि Controller Software या कंट्रोलर हार्डवेयर डिवाइस की मदद भी ली जा सकती है। जिससे इन एक्सेस पॉइंट को मैनेज करना आसान हो जाता है, और वायरलेस Uses में पॉलिसी लगाई जा सकती हैं, जैसे सीमित इंटरनेट डाटा की अनुमति देना, Downloading खोलना या बंद करना इत्यादि।




**8. CONNECTOR (कनेक्टर): -**

सूचना विज्ञान में कनेक्टर्स, जिन्हें आमतौर पर इनपुट-आटपुट कनेक्टर्स (या संक्षिप्त में I/O) कहते हैं, वैसे इन्टरफेस हैं जो केबल की मदद से उपकरणों को जोड़ते हैं। कनेक्टर्स में आमतौर पर पिन बाहर निकले होते हैं। जिसे प्लग के Socket में डालना होता है, जिसमें पहले से पिन के प्रवेश करने लायक छेद बने होते हैं। कनेक्टर्स कई प्रकार के होते है जिनमे से दो प्रकार के कनेक्टर्स निम्नानुसार है: -

a. RJ11
b. RJ45

a. RJ11: - (Register Jack 11) RJ जो है वह रजिस्टर जैक होता है, मानक फोन के लिए प्रयोग किया जाता है। यह एक अंतरराष्ट्रीय मानक है जो दूरसंचार नेटवर्क के लिए एक डिवाइस कनेक्ट करने के लिए प्रयोग किया जाता है। यह (Digital Subscriber Line) (DSL) या एनालॉग हो सकता है।

यह कनेक्टर टेलीफोन केबल लाइन में प्रयोग किया जाता है। आम तौर इसमें 3 ट्विस्टेड पेअर केबल होते है जिसमे से दो जोड़ी प्रयोग किया जाता है।

RJ11 के दो पेअर केबल 2 और 3, फोन लाइन के लिए उपयोग किया जाता है और रंग उपयोगकर्ता गाइड करने के लिए मदद करते हैं।

b. RJ45: - (Register Jack 45) में जो कि डेटा Equipments को आपस में जोड़ने के लिए प्रयोग किया जाता है। RJ45 एक प्रकार का कनेक्टर है जो सामन्यतया ईथरनेट नेटवर्किंग के लिए प्रयोग किया जाता है। RJ45 का प्रयोग ईथरनेट पर आधारित लोकल एरिया नेटवर्क (LAN) में कंप्यूटरों को जोड़ने के लिए किया जाता है। RJ45 एक फिजिकल नेटवर्क कनेक्टर है। ये टेलीफोन Jack के समान ही है परन्तु ये उससे थोडा चौडा होता है।

RJ 45 में 8 पिन होती है अर्थात् इसमें 8 अलग अलग वायर होती है। जो कि अलग अलग रंगों की होती है जिसमें 4 में ठोस रंग होते है जबकि 4 में हल्के धारीदार रंग होते है। RJ45 की हम दो तरीकों से वायरिंग कर सकते है।

- T-568A
- T-568B

T-568B वायरिंग जो है वह सबसे ज्यादा प्रयोग की जाती है। क्योंकि ज्यादातर नेटवर्किंग डिवाइस इसी वायरिंग को सपोर्ट करती है।

लेकिन कुछ devices T-568A का भी प्रयोग करती है। कुछ ऐसी Networking एप्लीकेशन होती है जिसमें एक तरफ तो T-568A का प्रयोग करना पड़ता है और दूसरी तरफ तो T-568B वायरिंग का प्रयोग करना पड़ता है। ऐसा LAN में उन कंप्यूटर को कंप्यूटर से जोड़ने के लिए किया जाता है जहाँ पर कोई स्विच, हब, ब्रिज नहीं होता है।

## 9. NETWORK INTERFACE CARD NIC (नेटवर्क इंटरफ़ेस कार्ड): -

नेटवर्क इंटरफ़ेस कार्ड को NIC या नेटवर्क कार्ड के नाम से जानते है। NIC मुख्यतः एक सर्किट बोर्ड या चिप है जो नेटवर्क पर दो कंप्यूटर के बीच कम्युनिकेशन स्थापित करने में सहायक होते है। इस बोर्ड को इनस्टॉल करने के बाद रिसोर्स, इनफार्मेशन या कंप्यूटर हार्डवेयर को नेटवर्क पर शेयर कर कर सकते है। इनका प्रयोग लोकल या वाइड एरिया नेटवर्क में होता है।

NIC कैसे कार्य करता है: -

जब एक यूजर कोई भी वेबसाइट या वेबपेज विजिट करता है तो जब यूजर किसी Link पर Click करता है तो कम्प्यूटर उस Click को Request के रूप में नेटवर्क कार्ड में पास करता है। ये Request Signal के रूप Send किया जाता है जिसको Web Server Internet की मदद से Receive करते है। यही Signal Web Server से Web Page के रूप में नेटवर्क कार्ड से हो कर वापस Send किया जाता है और वापस Send किये गये Signals को Electrical Signal कहते है।

जब कम्प्यूटर User के द्वारा Request Send करता है वह Humans के लिए Unreadable होता है। जब यही Signal Web Server से नेटवर्क कार्ड से होकर वापस Send किया जाता है तो ये Electrical Signals को नेटवर्क इंटरफेस कार्ड NIC की मदद से ट्रांसलेट कर देता है जिसको Humans Read कर सकते है।

इंस्टालेशन प्रोसेस: -

कम्प्यूटर में मदरबोर्ड पर इनको PCI Expantion Slot पर लगया जाता है, हालाकि पहले इन्हें ISA स्लॉट पर लगाया जाता था। आज भी कुछ कंप्यूटर में ISA Compatible NIC देखने को मिल जाती है लेकिन आजकल बनने वाली सभी NIC, PCI स्लॉट का हो प्रयोग करती है क्योंकि ISA स्टैण्डर्ड स्लॉट मदरबोर्ड पर लगने बंद हो चुके है। नेटवर्क इंटरफ़ेस कार्ड की मदद से एक कम्प्यूटर, दुसरे कम्प्यूटर के साथ कम्यूनिकेट करने के लिए एक और चीज की मांग करती है और वो है कम्युनिकेशन का माध्यम। यदि हम वायरलेस नेटवर्क का प्रयोग नहीं कर पा रहे है तो एक NIC से दुसरे NIC के बीच नेटवर्क में लाने के लिए उन्हें आपस में जोड़ना पड़ेगा। इसके लिए हमें केबल को आवश्यकता पड़ेगी।

Testing NIC card using Ping Command: -

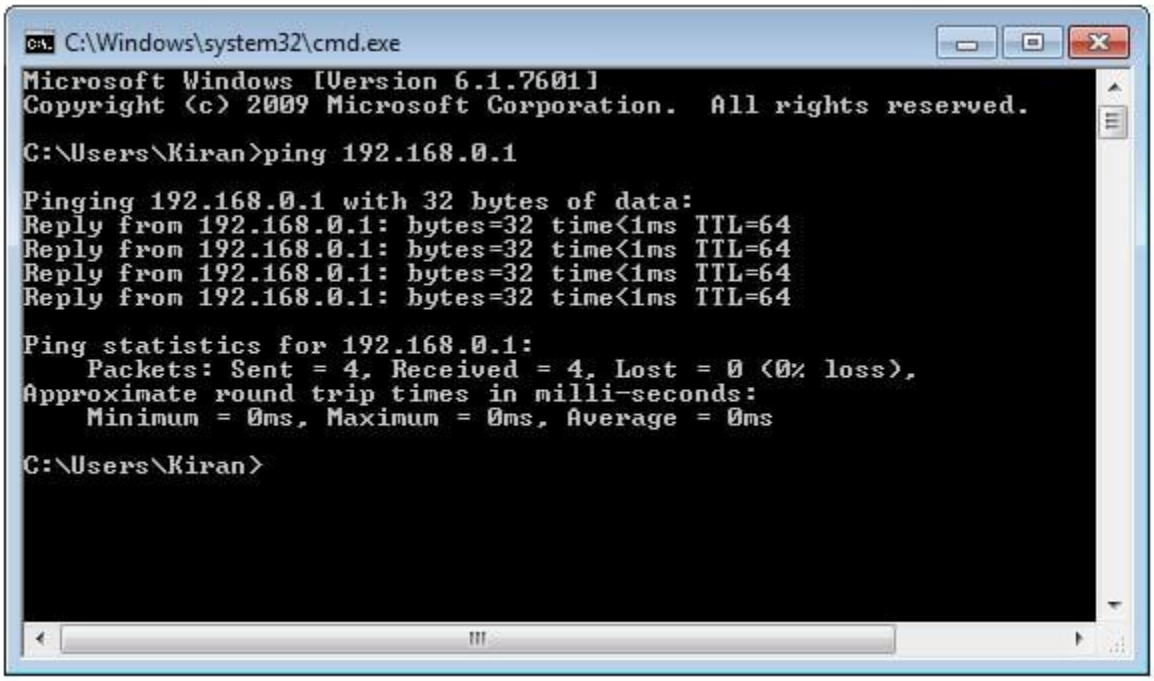
पिंग: - पिंग एक यूटिलिटी है यह Verify करने के लिए कि नेटवर्क, डेटा पैकेट को बिना Error के एक एड्रेस पर डिस्ट्रिब्यूट करने में सक्षम है या नहीं। पिंग यूटिलिटी सामान्यतः नेटवर्क Error को चेक करने के लिए उपयोग की जाती है।

पिंग TCP / IP Model में IP Address के द्वारा NIC Card के कनेक्शन को Test करता है। Ping टेस्ट यह निर्धारित करती है कि आपका क्लाइंट (Computer, Server या अन्य डिवाइस) किसी नेटवर्क पर किसी अन्य डिवाइस के साथ Communication कर सकता है या नहीं।

विंडोज ऑपरेटिंग सिस्टम में, पिंग कमांड का उपयोग पिंग टेस्ट रन करने के लिए किया जाता है। यह सिस्टम में इन-बिल्ट है और कमांड प्रॉम्प्ट के माध्यम से इसे एक्सिक्यूट किया जाता है। कमांड प्रॉम्प्ट ओपन करें और Ping के आगे IP एड्रेस टाइप करें। फिर Enter किज प्रेस करें।

उदाहरण – 192.168.0.1 आईपी एड्रेस वाले राउटर के लिए पिंग टेस्ट रन करने के लिए विंडोज कमांड इस प्रकार होगी:

ping 192.168.0.1 ┘ <Enter>




Ping रिजल्ट के परिणामों की व्याख्या: -

a. Reply From: डिफ़ॉल्ट रूप से, माइक्रोसॉफ्ट विंडोज में एड्रेस पर पिंग कमांड चार मैसेज की एक सिरिज भेजता हैं।प्रोग्राम का आउटपूट हर एक प्राप्त मैसेज का Response होता हैं, जो टार्गेट कम्प्यूटर से आता हैं।
b. Bytes: प्रत्येक पिंग Request डिफ़ॉल्ट रूप से 32 बाइट साइज का होता है।
c. Time: request भेजने और रिस्पॉस प्राप्त करने के बीच के समय (मिलीसेकंड में) का Ping रिपोर्ट।
d. TTL (Time-to-Live): 1 और 128 की Value का काउंट होता है जो TTL टार्गेट तक पहुंचने से पहले पिंग मैसेज कितने अलग-अलग नेटवर्कों से गुजरता हैं।128 नंबर इंडिकेट करता है की डिवाइस लोकल नेटवर्क पर है, जिसमें से 0 अन्य नेटवर्क हैं।

## 10. BLUETOOTH (ब्लूटूथ): -

Bluetooth एक ऐसी Wireless Technology है जिसका प्रयोग Electronic Devices के बीच Data Transfer करने के लिए किया जाता है। इस Technology में Data Transmission होने का Distance बहुत कम होता है। इसके उपयोग में Users को कोई भी Cords, Cables, Adapters की जरुरत ही नहीं पड़ती है और ये उन्हें Wirelessly ही Communicate करने की Permission प्रदान करता है।

इसकी Physical Range 10m से लेकर 50m तक ही है। ये Bluetooth Device ज्यादा से ज्यादा सात Devices में ही Connect हो सकता है और इनका मुख्य प्रयोग Smartphones, Personal Computers, और Gaming Consoles में किया जाता है। IEEE ने Bluetooth को IEEE 802.15.1 के रूप में Standardized किया है।

Features of Bluetooth Technology (ब्लूटूथ टेक्नोलॉजी की विशेषताएं): -

- Less Ccomplication: - इसमें ज्यादा Complication नहीं होती है, ये बहुत ही Simple Technology है।
- Less Power Consumption: - इसमें ज्यादा Power की Consumption नहीं होती है। जो की इसे ज्यादा Popular बनाता है।
- Cheaper Rates: - दुसरे Similar Technologies के तुलना में ये ज्यादा सस्ते होते हैं।
- Robustness: – ये बहुत ही Robust होते हैं। कहीं और कभी भी इनका प्रयोग किया जा सकता है।
- Distance: इनका इस्तमाल 10 से 50 meters तक के बीच किया जा सकता है।
- Data Rate: इनका Data Rate 1 Mbps तक होता है। जो की बहुत ही Fast होता है।

Advantages (लाभ): -

a. इसके उपयोग में Users को कोई भी Cords, Cables, Adapters की जरुरत ही नहीं पड़ती है और ये उन्हें Wirelessly ही Communicate करने की Permission प्रदान करता है।
b. इसमें Low Power Consumption होता है।
c. Data Transfer दीवारों के बीच से भी हो सकता है।
d. इसकी Range Infrared Communication की तुलना में बेहतर होती है।
e. इसका उपयोग Voice और Data Transfer के लिए होता है।
f. चूँकि इस Technology में FHSS का इस्तमाल होता है इसलिए यहाँ पर Data Communication बहुत ही Secure होता है।
g. इस Technology का उपयोग बहुत से Products जैसे की Head Set, Car System, Printer, Web Cam, GPS System, Keyboard और Mouse में होते हैं।

Disadvantages (हानि): -

a. इसका सबसे बड़ा Disadvantage इसकी Security हैं। ये दीवारों को आसानी से Penetrate भी कर सकता है। इसलिए इसका उपयोग Critical Business या Personal Data Transfer के लिए न ही करें।
b. चूँकि HomeRF Technology भी इसी Frequency पर Operate करती है, इसलिए कई बार एक दुसरे के साथ Interference भी हुआ करती है।
c. इसकी Bandwidth Wi-Fi के Compare में काफी Lower होती है।

**11. WiFi: -**

WiFi का पूरा नाम है Wireless Fidelity। यह एक लोकप्रिय Wireless Networking Technology है। एक एसी Technology है, जिसके जरिए आज हम Internet और Network Connection का उपयोग रहे है। WiFi एक मानक (Standard) है। जिस Standard को हम Follow करके Computers को Wireless Network से जोड़ते हैं। अभी के समय में जितने भी Smartphone, Laptop, Printer और Computer हैं। इन सभी में एक WiFi Chip रहता है। जिसके जरिए हम और आप Wireless Router से Connect करते हैं और Internet का उपयोग करते हैं।

WiFi Standard (वाई-फाई मानक): -

IEEE 802.11a: - वर्ष 1999 में IEEE द्वारा बनाया गया था, जो 5 GHz आवर्ती पर 54 Mbps गति से 115 फ़ीट तक काम करता हैं।

IEEE 802.11b: - यह 1999 में घरेलू उपयोग के लिए बना था, जो 5 GHz आवर्ती पर 11 Mbps गति से 115 फ़ीट तक काम करता हैं।

IEEE 802.11g: - वर्ष 2003 में 802.11a व 802.11b को मिलाकर बनाया गया था, जो 2.4 GHz आवर्ती पर 54 Mbps गति से 125 फ़ीट तक काम करता हैं।

IEEE 802.11n: - यह वर्ष 2009 में 2.4 GHz व 5 GHz दोनों आवर्ती राऊटर (Dual Band Router) पर काम करने के लिए बनाया गया था। इसकी डाटा भेजने की गति 54 Mbps और 230 फ़ीट तक काम करता हैं।

IEEE 802.11ac: - यह वर्ष 2009 में बनाया गया था, जो 5 GHz आवर्ती पर 1.3 Gbps की गति से 115 फ़ीट तक काम करता हैं।

Advanctages (लाभ): -

a. ऐसे वायरलेस नेटवर्क के यूजर किसी भी सुविधाजनक लोकेशन से इंटरनेट को Access कर सकते हैं। लैपटॉप या मोबाइल के लिए यह उपयुक्तहैं।
b. यूजर अपने मोबाइल को घर के प्राइवेट और पब्लीक वायरलेस नेटवर्क को कभी भी Connect कर इंटरनेट का उपयोग कर सकते हैं। उदाहरण के लिए, अधिकांश चेन कॉफी शॉप या मॉल, अपने कस्टमर्स को फ्री में इंटरनेट एक्सेस देते हैं।
c. एक वायरलेस नेटवर्क से Connect यूजर लगभग हर जगह अपने लैपटॉप को प्राइवेट या पब्लीक वायरलेस नेटवर्क को Connect कर अपनी प्रोडक्टिविटी को बढा सकते हैं।
d. वायरलेस नेटवर्क के लिए आपको किसी फिजिकल केबल की आवश्यकता नहीं होती जिससे नेटवर्क का खर्च बचता हैं। साथ ही लेबर कॉस्ट की भी बचत होती हैं।
e. वायर कनेक्शन के मुकाबले आपको वायरलेस नेटवर्क में यूजर्स की संख्या बढ़ने पर अतिरिक्त खर्च करने की आवश्यकता नहीं होती। एक ही राउटर को एक साथ कई यूजर्स Connect होते हैं।

Disadvantages (हानि): -

a. Security: वायर्ड नेटवर्क के मुकाबले वायरलेस नेटवर्क को हैक करना आसान होता हैं।
b. Range: वाई-फाई सिग्नल की रेंज आपके राऊटर के मॉडल पर निर्भर होती हैं। आमतौर पर घर पर उपयोग किए जाने वाले राउटर की रेंज 150 फीट से 300 फीट तक हो सकती हैं। ज्यादा रेंज के लिए Repeaters या Access Points का प्रयोग किया जाता है।

# UNIT 05
# NETWORK PROTOCOL & APPLICATIONS

**PROTOCOL (प्रोटोकॉल): -** कंप्यूटर नेटवर्क में सूचनाओं के सही तरीके से आदान-प्रदान के लिए कुछ नियम बनाये गये हैं इन नियमों के समूह को प्रोटोकॉल कहा जाता है। किसी नेटवर्क से जुड़े डिवाइस आपस में कैसे Communicate करेंगे, उनके बीच डाटा किस Format में और किस तरह से ट्रान्सफर होगा और डाटा Receive होने के बाद क्या होगा यह Protocol द्वारा ही निर्धारित होता है।

**01. INTERNET PROTOCOL (IP) (इंटरनेट प्रोटोकॉल): -**

किसी भी नेटवर्क पर इस्तेमाल किए जाने वाले आईपी एड्रेस के 2 स्टैण्डर्ड हैं: -

a. **IP VERSION 4 (IPv4):** Internet Protocol Version 4 (IPv4) यह इंटरनेट प्रोटोकॉल (IP) का चौथा वर्जन हैं, जिसे नेटवर्क के डिवाइस की पहचान करने के लिए इस्तेमाल किया जाता हैं। IPv4 एड्रेस 32 bit (04 Byte) लंबा होता हैं और यह 4,294,967,296 एड्रेसेस को सपोर्ट करता हैं (हालांकि इनमे से कई विशेष उद्देश्यों के लिए आरक्षित हैं, जैसे 10.0.0.0 (प्राइवेट एड्रेस) और 127.0.0.0 (लूपबैक एड्रेस) । **IPv 4 HEADER FORMAT (IPv4 का हैडर फॉर्मेट): -**

Internet Protocol (IP) Version 4 (IPv4) 32 बिट का होता है। IP Layer 3 (Network Layer) पर काम करता है। ये Layer 4 (Transport Layer) के द्वारा भेजे गए Segments (TCP Protocol) या Datagram (UDP Protocol) को Packets में Break करती है। इन Packets के साथ IP Header Attach किया जाता है। ये Header, Packet से Related आवश्यक Information Receiver Side को Provide करता है। IP Header में ये Information Different Fields के द्वारा Represent किया जाता है।

| | | | | | |
|---|---|---|---|---|---|
| Version (4) | Header Length (4) | Types of Services (8) | Total Lengh (16) | | 4 Byte |
| Indentification (16) | | | Flags (3) | Fragment Offset (13) | 4 Byte |
| Time To Live (8) | | Protocol (8) | Header Checksum (16) | | 4 Byte |
| Source IP Address (32) | | | | | 4 Byte |
| Destination IP Address (32) | | | | | 4 Byte |
| Option & Data | | | | | |

- Version Number (04 bit): – Version Number Field के द्वारा Internet Protocol का Version Number Define किया जाता है। यँहा पर IPV4 header की बात की जा रही है इसलिए Version भी 4th ही होगा।
- Header Length (04 bit): – इस Field के द्वारा IP Header की Length Define की जाती है। IPV4 Header की Length 32 bit Words (With Options & Data) के द्वारा दर्शायी जाती है। यदि Header में कोई Options Defined ना हो तो इस Filed की Value 05 Set होती है।
- Types of Service (08 bit): – ये Field वो तरीका Define करता है जिससे Router को Packets को Queue करना चाहिए जब Packets Forward होने के लिए Wait कर रहे हो। यदि किसी Packet की Priority ज्यादा हो तो इस Field की Value '1' होती है। Regular Packets के लिए इस Field की value '0' होती है।
- Total Length (16 bit): – ये Field IP Datagram की Total Length को दर्शाता है। ऊपर Define किया गया Header Length Field, Header की Length को Define करता है और ये Field Data और Header सहित Datagram की Total Length को Define करता है। इसकी वैल्यू 20 से 65535 तक होता है।

- Identification (16 bit): – ये Field एक Packet का Identification होता है। ये एक 16 bit का Number होता है जो Source Address के साथ मिलकर किसी Packet को Uniquely Identify करता है।
- Flags (03 bit): – ये Field दर्शाता है कि क्या Router किसी Segment को Fragment कर सकते है। इस Field में 3 bits होती है। पहली bit Reserved होती है। यदि इस Field में Second bit Set '1' हो तो उसका मतलब होता है Don't Fragment और यदि इस Field में Third bit Set '1' हो तो उसका मतलब होता है की Segment Fragmented है।
- Fragment Offset (13 bit): – यदि Packet Fragmented है तो ये Field Original Packet की शुरू की 8 bits को दर्शाता है। ये Field 13 bits का होता है।
- Time to Live (8 bit): – ये Field एक Limit Set करता है। यह फील्ड किसी पैकेट के नेटवर्क में उपस्थित रहने की अधिकतम समय सीमा को निश्चित करता है। मान लीजिये इस Field की Value 15 है। यदि Packet 15 Routers से Pass होने के बाद भी Destination तक नहीं पहुँचता है तो उस Packet को Discard कर दिया जाता है। Authenticity के नजरिए से ये एक महत्वपूर्ण Field है।
- Protocol (8 bit): – इस Field में उस Protocol का नाम होता है जिसने Packet Network Layer को Pass किया क्योंकि Receiver Side पर De - Multiplexing के लिए ये पता होना चाहिए की कौन से Protocol को Data Pass करना है।
- Header Checksum (16 bit): – ये Field Errors को Check करने के लिए यूज़ किया जाता है। जब Packet Source से Send किया जाता है तो इस Field में एक Value होती है जो Algorithm के द्वारा Header से Calculate की जाती है। जब ये Packet Receiver Side पर पहुँचता है तो उसी Algorithm के द्वारा Value को वापस Header से Calculate किया जाता है यदि Value Source Side से Match करती है तो माना जाता है की Packet Error Free है।
- Source IP Address (32 bit): – ये Field Source के IP Address को Represent करता है।
- Destination IP Address (32 bit): – ये Field Destination के IP Address को Represent किया जाता है।
- Options & Data (): – ये Field कुछ Options को Represent करता है जो कुछ Packets Use कर सकते है। हालाँकि इस Field को यूज़ नहीं किया जाता है लेकिन जब भी इसे यूज़ किया जाता है इससे Header की Length 32 bits से ज्यादा हो जाती है। इस Field में मुख्य Data होता है जो Transport Layer Protocols द्वारा IP को Pass किया जाता है।

b. **IP VERSON 6 (IPv6):** इंटरनेट के लोकप्रिय विकास के कारण IPv4 के संभावीत एड्रेस भविष्य में समाप्त होने की चिंता से Internet Protocol Version 6 (IPv6) का नया वर्जन विकसित किया गया। यह IPv4 का नया और उन्नत वर्जन हैं। इसे IPng (IP New Generation) के रूप में भी जाना जाता है IPv6 128 Bits (16 Bytes) लंबा होता हैं। इसलिए, यह $2^{128}$ इंटरनेट एड्रेस को सपोर्ट करता हैं, यह बहुत सारे एड्रेस हैं और वे बहुत लंबे समय तक इंटरनेट ऑपरेशनल जारी रखने के लिए पर्याप्त से अधिक हैं। **IPv 6 HEADER FORMAT (IPv6 का हैडर फॉर्मेट):**

<table>
<tr><td>VER (4)</td><td>TRAFFIC CLASS (8)</td><td colspan="3">FLOW LOAD (20)</td></tr>
<tr><td colspan="2">PAYLOAD LENGTH (16)</td><td colspan="2">NEXT HEADER (8)</td><td>HOP COUNT (8)</td></tr>
<tr><td colspan="5">SOURCE IP ADDRESS (128 )</td></tr>
<tr><td colspan="5">DESTINATION IP ADDRESS (128)</td></tr>
</table>

- Version (4 बिट): - ये इन्टरनेट प्रोटोकॉल के वर्जन को दिखाता है l जैसे कि, 0110.
- Traffic Class (8 बिट): - इन 8 बिट को दो भागों में बांटा गया है। मोस्ट Significant 6 बिट्स का प्रयोग सर्विस का टाइप दिखाने के लिए किया जाता है जिस से राऊटर को ये पता चलता है कि किस तरह की सर्विस दी जाये। लीस्ट Significant 2 बिट को ECN यानि Explicit Congention Notification के लिए प्रयोग किया जाता है।

- Flow Label (20 बिट): - इस लेवल का प्रयोग संचार में पैकेट के फ्लो को कण्ट्रोल रखने के लिए किया जाता है। सोर्स सीक्वेंस को लेबल कर देता है ताकि राऊटर ये पहचान सके कि कोण सा पैकेट किस फ्लो या सूचना से सम्बन्ध रखता है। ये क्षेत्र एक ही डाटा पैकेट को बार-बार भेजने से छुटकारा देता है। इसे स्ट्रीमिंग यानि कि वास्तविक समय मीडिया के लिए डिजाईन किया गया है।
- Payload Length (16 बिट): - इस क्षेत्र का प्रयोग राऊटर को ये बताने के लिए किया जाता है कि पेलोड में कोई खास पैकेट कितनी सूचना रखे हुए है। पेलोड में एक्सटेंशन हेडर और उपरी लेयर का डाटा होता है। 16 बिट्स के साथ 65,535 बाइट तक दिखाए जा सकते हैं लेकिन अगर एक्सटेंशन हेडर के पास Hop by Hop एक्सटेंशन हेडर है तो पेलोड 65,535 बाइट से ज्यादा भी हो सकता है और इस क्षेत्र को 0 सेट कर दिया जाता है।
- Next Header (8 बिट): - इस फील्ड का प्रयोग या तो एक्सटेंशन हेडर का टाइप बताने में किया जाता है या फिर अपर-लेयर PDU बताने में (अगर एक्सटेंशन हेडर उपस्थित नही हो तो)
- Hop Limit (8 बिट): - इस क्षेत्र का प्रयोग पैकेट को हमेशा के लिए रोक देने के लिए किया जाता है।
- Source Address (128 बिट): - ये क्षेत्र इस बारे में सूचना देता है कि पैकेट को कहाँ से भेजना शुरू किया गया है।
- Destination Address (128 बिट): - ये क्षेत्र ये बताता है कि इस पैकेट को कहाँ भेजा जाने वाला है।

**02. IP ADDRESSING: -**

- Internet Protocol (IP) यह एक मेथड या प्रोटोकॉल है, जिसके द्वारा डाटा इंटरनेट पर एक डिवाइस से दूसरे डिवाइस पर भेजा जाता है।
- IP address, को Simply "IP" भी कह सकते हैं। यह एक Unique Address होता है जिससे की एक Device को Internet या एक Local Network में आसानी से Identify किया जा सकता है।
- नेटवर्क से जुड़े हर डिवाइस को एक यूनिक आईपी एड्रेस होना चाहिए। आपके डिवाइस के यूनिक एड्रेस के बिना, आप नेटवर्क या इंटरनेट पर अन्य डिवाइसेस, युजर और कम्प्यूटर के साथ कम्युनिकेशन नहीं कर सकते। आईपी एड्रसेस बाइनरी वैल्यू का बना हुआ होता है और नेटवर्क या इंटरनेट पर सभी डेटा को रूटिंग करता हैं।

**TYPES OF IP ADDRESS (आई.पी.एड्रेस के प्रकार): -**

आई.पी.एड्रेस 4 प्रकार के होते है: -

a. Private IP Address: - इन्हें एक Network के "Inside" में प्रयोग किया जाता है, इस प्रकार की IP Addresses का प्रयोग आपके Devices को Router के साथ एक Private Network में दुसरे Devices के साथ Communicate करने के लिए किया जाता है। Private IP Addresses को Manually Set किया जाता है या आपके Router के द्वारा Automatically ही Assign किया जा सकता है।
b. Public IP Address: - इस प्रकार के IP Addresses का प्रयोग Network के "Outside" में किया जाता है, जिन्हें की ISP द्वारा Assign किया गया हो। ये वही Main Address होता है जिसे की आपके Home या Business Network में प्रयोग दुनिया भरके Networked Devices के साथ Communicate करने के लिए किया जाता है। Private IP Address's और Public IP Addresses दोनों या तो Dynamic हो सकते हैं या Static भी हो सकते हैं।
c. Dynamic IP Address: - एक IP Address जिसे की Assigned किया जाता है एक DHCP Server के द्वारा उसे एक Dynamic IP address कहते हैं।
d. Static IP Address: - वहीँ अगर एक device में DHCP enabled नहीं होती है या उसे Support नहीं करती है तब IP Address को Manually Assigned किया जाता है, इसी Case में IP Address को एक Static IP Address कहा जाता है।

**Classes of IP Address**

IPV4 Addresses को 05 Classes में Divide किया गया है।

i. Class A: - Class A की Network Range 1 से 126 होती है। इस Class का Default Subnet Mask 255.0.0.0 होता है। इस Class के IP Addresses में Only First Octet ही Network को शो करता है और बाकी के 3 Octets Hosts को शो करते है। इस क्लास में ($2^{8-1}$- 2 = 126) Network होते है और हर Network में ($2^{24}$- 2) 1, 67, 77, 214 Hosts हर Network में होते है।

ii. Class B: - Class B की Network Range 128 से 191 होती है। इस Class के IP Addresses का Default Subnet Mask 255.255.0.0 होता है। इस class के IP Addresses में पहले 2 Octet Network को Represent करते है और आखिरी 2 Octet Hosts को Define करते है। इस क्लास में ($2^{16-2}$- 2 = 16384) Networks होते है ($2^{16}$- 2) और 65534 Hosts हर Network में होते है।

iii. Class C: - Class C की Network Range 192 से 223 होती है। इस Class के IP Addresses का Default Subnet Mask 255.255.255.0 होता है। इस Class के IP Addresses में पहले 3 Octet Network को Represent करते है और आखिरी एक Octet Hosts को Represent करता है। इस Class में ($2^{24-3}$- 2 = 2097152) Network होते है और ($2^{8}$- 2) 254 Hosts हर Network में होते है।

iv. Class D: - Class D की Network Range 224 से 239 होती है। Class D का उपयोग Network Multicast के लिए Reserved होते है। इस Class के Addresses का कोई Subnet Mask नहीं होता है।

v. Class E: - Class E की Network Range 240 से 255 होती है। Class E का उपयोग Millitry, Army etc. के लिए Reserved होते है। इस Class के Addresses का भी कोई Subnet Mask नहीं होता है।

**03. SUBNETTING (सबनेटिंग): -**

Subnetting की जरुरत इसलिए पड़ी क्योंकि जब इन्टरनेट Popular हुआ तो सभी IP एड्रेस Consume होने वाले थे। अर्थात् उस समय IP एड्रेस की Shortage (कमी) हो गयी थी। जिससे इन्टरनेट का भविष्य खतरे में था और यह खत्म हो जाता। इसी परेशानी से बचने के लिए Subnetting को बनाया गया।

Subnetting एक ऐसी विधि है जिसमें एक बड़े नेटवर्क को दो या दो से अधिक छोटे लॉजिकल नेटवर्कों में विभाजित कर दिया जाता है। इन छोटे नेटवर्कों को Subnetwork या Subnet कहा जाता है। इन Subnet का अपना अलग-अलग एड्रेस होता है। इन छोटे नेटवर्कों को बनाने के लिए Subnet Mask का प्रयोग किया जाता है। Subnet Mask को IP एड्रेस में Network Address तथा Host Address के बीच Differentiate (अंतर) करने के लिए किया जाता है। Subnet Mask का उद्देश्य यह Identify करना कि IP Address का कौन सा भाग Network Address है और कौन सा भाग Host Address।

Advantage of Subnetting (सबनेटिंग से लाभ): -

i. इसमें नेटवर्क की Security बेहतर होती है क्योंकि हम प्रत्येक Subnet को मैनेज कर सकते है।

ii. नेटवर्क छोटे होने से Collision डोमेन और Broadcast डोमेन भी छोटे हो जाते है। जिससे ट्रैफिक और ब्रेकडाउन की समस्या में कमी आती है।

iii. इसमें Administrative Control बेहतर हो जाता है क्योंकि बड़े नेटवर्क की तुलना में छोटे नेटवर्क को मैनेज तथा Administrate करना आसान होता है।

iv. इसमें हम एक ही नेटवर्क में दो या दो से अधिक LAN Technology का प्रयोग कर सकते है।

v. Subnetting इन्टरनेट में IP Addresses की समस्या को Solve करने में बहुत ही सहायक होते है।

vi. Subnets इन्टरनेट में Routing Tables के Size को Minimize करता है।

Disadvantage of Subnetting (सबनेटिंग से हानि): -

i. यह बहुत ही Expensive होता है क्योंकि इसमें Routers, Switches, Hubs, Bridge आदि Networking Devices का प्रयोग किया जाता है जो कि बहुत महंगे होते है।

ii. इसमें Subnets को मैनेज करने के लिए Experienced Administrative की जरुरत होती है।

**04. ARP (ADDRESSES RESOLUTION PROTOCOL) (एड्रेस रेसोलुशन प्रोटोकॉल): -**

ARP एक Network Layer Protocol है। TCP/IP Protocol Suit में ये एक बहुत ही Important Protocol है। ARP को IPv4, X.25, Frame Relay, ATM जैसी महत्वपूर्ण Technologies के साथ Implement किया गया है।

ARP Protocol IP Address के Base पर MAC Address को Resolve करता है। Application Layer पर किसी भी Device से Communicate करने के लिए IP Address Use किया जाता है। लेकिन Data Link Layer (LAN) पर किसी Device से Communicate करने या फिर उसे Data Send करने के लिए MAC Address की आवश्यकता होती है। ARP Protocol, Logical Address को Mac Address में परिवर्तित करता है।

Working of ARP (ARP की कार्यपद्धति): -

- जब एक Sender किसी Receiver से Communicate करना चाहता है तो Sender सबसे पहले अपना ARP Cache में Receiver का MAC Address को Check करता है। यदि Receiver का MAC Address पहले से ARP Cache में मौजूद है तो Sender उस MAC Address को Use करते हुए Receiver से Communicate करता है।
- यदि Receiver Device का MAC Address ARP Cache में पहले से मौजूद नहीं है तो Sender Device द्वारा एक ARP Request Message तैयार कर LAN में Broadcast कर देता है। सभी Devices इस Request Message के Receiver IP Address को स्वयं के IP Address से Match करते है। जिन Devices का ये IP Address Match नहीं होता है वे इस Request Message को Drop कर देते है।
- जिस Device के IP Address से इस Request Message का Receiver IP Address Match करता है वह इस Message को Receive करता है और ARP Reply Message तैयार कर Sender को Unicast Message भेजा जाता है।
- जैसे ही Sender Device ARP Reply Message Receive करता है तो वह अपने ARP Cache को नयी Information (Receiver का MAC Address) के साथ Update कर लेता है। अब Sender बिना किसी परेशानी के Data Send और Receiver कर सकता है।

Header Format of ARP (ARP का हैडर फॉर्मेट): -

<table>
<tr><td colspan="2">HARDWARE TYPE (16 bit)</td><td>PROTOCOL TYPE (16 bit)</td></tr>
<tr><td>HARDWARE LENGTH (08 bit)</td><td>PROTOCOL LENTH (08 bit)</td><td>OPCODE (16 bit)</td></tr>
<tr><td colspan="3">SENDER MAC (HARDWARE) ADDRESS (0 – 6 Bytes)</td></tr>
<tr><td colspan="3">SENDER LOGICAL (IP) ADDRESS (0 – 4 Bytes)</td></tr>
<tr><td colspan="3">TARGET MAC (HARDWARE) ADDRESS (0 – 6 Bytes)</td></tr>
<tr><td colspan="3">TARGET LOGICAL (IP) ADDRESS (0 – 4 Bytes)</td></tr>
</table>

- Hardware Type (16 bits): – इस Field की Size 2 Bytes होती है। ये Field Define करता है की ARP Message को Transmit करने के लिए किस प्रकार का Hardware Type Use किया गया है। सबसे Common Hardware Type Ethernet है। Ethernet की Value 1 होती है।

- Protocol Type (16 bits): – ये Field बताता है की ARP Message की Transmitting के लिए किस Protocol को Use किया गया है। ज्यादातर इस Field की Value 2048 होती है जो की IP v 4 को दर्शाती है।
- Hardware Address Length (08 bits): – ये Field Hardware Address की Length Bytes में दर्शाता है। Ethernet MAC Address की Size 6 Bytes होती है।
- Protocol Address Length (08 bits): – ये Field IP Address की Size Bytes में दर्शाता है। IP Address की Size 4 Bytes होती है।
- OP Code (16 bits): – ये Field ARP Message के Type को बताता है। यदि इस Field की Value 1 है तो यह Request Message है और यदि इस Field की Value 2 है तो यह Reply Message है।
- Sender Hardware Address (0-6 Bytes): – इस Field में Message Send करने वाले Device का MAC Address होता है।
- Sender Protocol Address (0-4 Bytes): – इस Field में Message Send करने वाले Device का IP Address होता है।
- Target Hardware Address (0-6 Bytes): – Request Message में यह Field खाली होता है। इस Field में Receiving Device का Hardware Address होता है।
- Target Protocol Address (0-4 Bytes): – इस Field में Receiving Device का IP Address होता है।

**RARP (REVERSE ADDRESSES RESOLUTION PROTOCOL) (रिवर्स एड्रेस रेसोलुशन प्रोटोकॉल): -**

RARP Protocol MAC Address के Base पर IP Address को Resolve करता है। RARP Protocol, Mac Address को Logical Address में परिवर्तित करता है।

Working of RARP (RARP की कार्यपद्धति): -

- जब एक Sender किसी Receiver से Communicate करना चाहता है तो Sender सबसे पहले अपना RARP Cache में Receiver का IP Address को Check करता है। यदि Receiver का IP Address पहले से RARP Cache में मौजूद है तो Sender उस IP Address को Use करते हुए Receiver से Communicate करता है।
- यदि Receiver Device का IP Address RARP Cache में पहले से मौजूद नहीं है तो Sender Device द्वारा एक RARP Request Message तैयार कर LAN में Broadcast कर देता है। सभी Devices इस Request Message के Receiver MC Address को स्वयं के MAC Address से Match करते है। जिन Devices का ये MAC Address Match नहीं होता है वे इस Request Message को Drop कर देते है।
- जिस Device के MAC Address से इस Request Message का Receiver MAC Address Match करता है वह इस Message को Receive करता है और RARP Reply Message तैयार कर Sender को Unicast Message भेजा जाता है।
- जैसे ही Sender Device RARP Reply Message Receive करता है तो वह अपने RARP Cache को नयी Information (Receiver का IP Address) के साथ Update कर लेता है। अब Sender बिना किसी परेशानी के Data Send और Receiver कर सकता है।

Header Format of RARP (RARP का हैडर फॉर्मेट): -

<table>
<tr><td colspan="2">HARDWARE TYPE (16 bit)</td><td>PROTOCOL TYPE (16 bit)</td></tr>
<tr><td>HARDWARE LENGTH (08 bit)</td><td>PROTOCOL LENTH (08 bit)</td><td>OP CODE (16 bit)</td></tr>
<tr><td colspan="3">SENDER MAC (HARDWARE) ADDRESS (0 – 6 Bytes)</td></tr>
</table>

| SENDER LOGICAL (IP) ADDRESS (0 – 4 Bytes) |
|---|
| TARGET MAC (HARDWARE) ADDRESS (0 – 6 Bytes) |
| TARGET LOGICAL (IP) ADDRESS (0 – 4 Bytes) |

- Hardware Type (16 bits): – इस Field की Size 2 Bytes होती है। ये Field Define करता है की RARP Message को Transmit करने के लिए किस प्रकार का Hardware Type Use किया गया है। सबसे Common Hardware Type Ethernet है। Ethernet की Value 1 होती है।
- Protocol Type (16 bits): – ये Field बताता है की RARP Message की Transmitting के लिए किस Protocol को Use किया गया है। ज्यादातर इस Field की Value 2048 होती है जो की IP v 4 को दर्शाती है।
- Hardware Address Length (08 bits): – ये Field Hardware Address की Length Bytes में दर्शाता है। Ethernet MAC Address की Size 6 Bytes होती है।
- Protocol Address Length (08 bits): – ये Field IP Address की Size Bytes में दर्शाता है। IP Address की Size 4 Bytes होती है।
- OP Code (16 bits): – ये Field RARP Message के Type को बताता है। यदि इस Field की Value 1 है तो यह Request Message है और यदि इस Field की Value 2 है तो यह Reply Message है।
- Sender Hardware Address (0-6 Bytes): – इस Field में Message Send करने वाले Device का MAC Address होता है।
- Sender Protocol Address (0-4 Bytes): – इस Field में Message Send करने वाले Device का IP Address होता है।
- Target Hardware Address (0-6 Bytes): – इस Field में Receiving Device का MAC Address होता है।
- Target Protocol Address (0-4 Bytes): – Request Message में यह Field खाली होता है। इस Field में Receiving Device का IP Address होता है।

**05. ICMP (INTERNET CONTROL MESSEGING PROTOCOL) (इंटरनेट कण्ट्रोल मेसेजिंग प्रोटोकॉल): -**

Internet Protocol की 2 महत्वपूर्ण कमियां है।

i. No Error Reporting: – यदि किसी Error की वजह से कोई Packet Router द्वारा Discard हो जाए तो इसके लिए Internet Protocol में ऐसा कोई Mechanism नहीं है जिससे की Sender को इस Error के बारे में Report किया जा सके।

ii. No Communication: – कई बार ऐसा हो सकता है कि एक Device को दूसरे Device से Communicate करने की आवश्यकता हो तो ऐसी Situation के लिए भी Internet Protocol में ऐसा कोई Mechanism नहीं है जिससे Devices आपस में Communicate कर सके।

Internet Protocol की इन कमियों को दूर करने के लिए ICMP को Design किया गया है। ICMP और IP दोनों एक साथ काम करते है। ICMP में Message Mechanism होता है जिससे Hosts को Error और Status के बारे में Notify किया जाता है। ICMP Header Format (ICMP हैडर फॉर्मेट): -

| TYPE (8 bits) | CODE (8 bits) | CHECKSUM (16 bits) |
|---|---|---|
| REST OF THE HEADER (IP HEADER) (32 bits) | | |
| DATA SECTION | | |

- Type (8 bits): – ये Field Message का Type Define करता है। उदाहरण के लिए किसी प्रकार की Error Report करते समय उस Error से सम्बंधित Code इस Field में Define किया जाता है। उसी प्रकार यदि Query Message है तो इस Field में उस Query का Code आएगा। इस फील्ड के लिए 03 प्रकार के Query मैसेज होते है।
- Code (08 bits): – Query Messages के लिए इस Field की Value Zero होती है। Error Messages के लिए ये Field Error के Sub Type को Define करता है। इस फील्ड के लिए 05 प्रकार के Error मैसेज होते है।
- Checksum (16 bits): – Header और Data के द्वारा Checksum Calculate किया जाता है जिसे Errors को Detect करने के लिए Use किया जाता है।
- Rest of the Header: – ICMP Message को IP Datagram में Encapsulate किया जाता है। ICMP Message में Rest of The Header Section Remaining IP Header को दर्शाता है।
- Data: – Error Messages के सन्दर्भ में इस Section में जिस Packet के द्वारा Error आयी है उस Packet की Complete Information होती है।

ICMP द्वारा Create किये जाने वाले Messages को 2 Categories में Divide किया गया है।

1. **Error Reporting Messages: -** ये वे Messages होते है जिनसे ICMP Errors को Report करता है।

a. Destination Unreachable (Code 3): – यदि कोई Router किसी Packet के लिए Destination नहीं ढूँढ पाता है तो ऐसी Situation में Packet को Discard कर दिया जाता है और Source को Destination Unreachable Message Send किया जाता है।

b. Source Quench (Code 4): – जब Sending Device की Speed अधिक होती है तो IP कुछ Packets को Discard कर देता है। इस Situation में ICMP Flow Control Provide करता है और Sender को Source Quench Eessages Send करता है।

c. Redirect (Code 5): – जब यह Host कोई Data Send करेगा तो Data उस Router के Through Correct Router तक जाएगा। इस Situation में Router, Redirection Message Send करेगा ताकि Host की Routing Information Update की जा सके और Host Directly Correct Router को Data Send कर सके।

d. Time Exceeded (Code 11): – यदि Routing Table Correct नहीं है तो ऐसी Situation में Packet Loop में ही घूमता रहता है। इस Situation से बचने के लिए हर Packet में एक Time To Live Field होता है। जैसे ही इस Field की Value Zero होती है तो Router द्वारा इस Packet को Discard कर दिया जाता है। इस Situation में Router Source को Time Exceeded Message Send करता है।

e. Parameter Unintelligible (Code 12): – यदि कोई Router या Destination Host Packet के किसी Field को Empty पाता है तो उस Packet को Discard कर देता है और Source को Parameter Unintelligible Message Send करता है।

2. **Query Messages: -** इसमें ICMP किसी Host के Status के लिए Query करता है।

a. Echo Request (Code 8) & Echo Reply (Code 9): – Query Messages का ये Pair Network में Problems को Diagnose करने के लिए Use किया जाता है। ये दोनों Messages ये Determine करते है की क्या दो Hosts आपस में Communicate कर सकते है?

b. Time-Stamp Request (Code 13) & Time Stamp Reply (Code 14): – किसी Packet को एक Host से दूसरे Host तक Travel करने में लगने वाले Time को Time Stamp Request & Reply Messages द्वारा पता किया जाता है।

c. Address Mask Request (Code 17) & Address Mask Reply (Code 18): – किसी Host को खुद के IP Address की जानकारी हो सकती है लेकिन ये जरुरी नहीं की उसे खुद के Subnet Mask की जानकारी हो। अपना Subnet Mask पता

करने के लिए Host Router को Address Mask Request भेजता है और Router इस Host का Subnet Mask Address Mask Reply Message के रूप में भेजता है। यदि Host को Router के Address की जानकारी होती है तो वह सीधा ही Router को Request भेजता है नहीं तो यह Request Broadcast की जाती है।

**06. <u>NETBEUI PROTOCOL: -</u>**

- NetBIOS Extended User Interface, प्रोटोकॉल एक नेटवर्किंग प्रोटोकॉल है। जिसे IBM और Microsoft ने में Develop किया था। यह प्रोटोकॉल लोकल एरिया नेटवर्क की साइज को तक एक्सटेंड करने की क्षमता प्रदान करता है।
- NetBEUI प्रोटोकॉल LAN मैनेजर और Windows के मध्य वर्कग्रूप स्थापित करने के लिए प्रमुख प्रोटोकॉल है।यह काफी अधिक तेजी से तथा कुशलता से कार्य करने वाला प्रोटोकॉल है।
- यह कनेक्शन ओरिएन्टेड कम्युनिकेशन जैसे मैपिंग ड्राइवर्स का उपयोग करने के लिए Net Use Command तथा किसी Service को स्टार्ट करने के लिए Net Start Command का कार्य का निष्पादन करता है।
- यह कनेक्शन लेस्स कम्युनिकेशन में जैसे Datagrams Packet को सेंड करना, NetBIOS को रजिस्टर करना, NetBIOS Name Resolution का कार्य का भी निष्पादन करता है।

**07. <u>UDP (USER DATAGRAM PROTOCOL) (यूजर डाटाग्राम प्रोटोकॉल): -</u>**

UDP (User Datagram Protocol) एक Transport Layer Connection Less Protocol है। इस Protocol को RFC 768 में Define किया गया है। UDP एक Unreliable Protocol है यानि की ये Data के पहुँचने की Guarantee नहीं देता है। UDP सिर्फ Datagram को Forward करता है इसके बाद उस Datagram का क्या होता है इससे UDP को कोई मतलब नहीं होता है। UDP में Three Way Handshake, Flow Control, Sequencing और Data का Acknowledgment भी नहीं होता है।

UDP के Connectionless होने से मतलब है की जब Data का Transfer होता है तो Sender और Receiver के बीच में कोई Connection Establish नहीं किया जाता है। TCP के Comparison में UDP एक बहुत ही Fast Service है क्योंकि इसमें Extra काम जैसे की Acknowledgment, Sequencing आदि कुछ भी नहीं होता है। जहाँ पर आपको Reliability की जगह Speed की आवश्यकता हो वहाँ पर UDP को यूज़ कर सकते है।

UDP भी Checksum के द्वारा Basic Error Checking Provide करता है। एक ही Host पर चलने वाली बहुत सी Applications को UDP Port Numbers के द्वारा Differentiate करता है।

<u>Characteristics of UDP (UDP की विशेषताएं): -</u>

i. UDP एक Unreliable Service है, इसमें Data Delivery की कोई Guarantee नहीं होती है।
ii. UDP Basic Error Checking Provide करता है।
iii. UDP Data Sequencing Perform नहीं करता है।
iv. UDP दूसरे Protocols के Comparison में बहुत ही Fast है।

<u>UDP Header Format (UDP हैडर फॉर्मेट): -</u>

UDP data के साथ एक बहुत ही Simple 64 bits की Header Attach करता है। इसमें सिर्फ 4 Fields होते है।

| | |
|---|---|
| SOURCE PORT (16 bits) | DESTINATION PORT (16 bits) |
| LENGTH (16 bits) | CHECKSUM (16 bits) |

- <u>Source Port (16 bits): –</u> इस Field की Size 16 bit होती है। ये Source के Port Number को Carry करता है।
- <u>Destination Port (16 bits): –</u> 16 bits के इस Field में Destination Port Number Carry किया जाता है।

- Length (16 bits): – इस Field में Header और Data की Length Stored होती है।
- Checksum (16 bits): – ये Field Basic Error Checking के लिए यूज़ किया जाता है।

Applications of UDP (UDP के उपयोग): -

- UDP को Domain Name Server के द्वारा Simple Request/Response Process के लिए यूज़ किया जाता है।
- Bootstrap Protocol और Dynamic Host Control Protocol भी UDP को Short Messages Send और Receive करने के लिए यूज़ करते है।
- Trivial File Transfer Protocol UDP को बड़ी बड़ी Files को Send करने के लिए यूज़ करता है।
- Simple Network Management Protocol Messages Send करने के लिए UDP का यूज़ करता है।
- Routing Information Protocol (RIP) Routing Information भेजने के लिए UDP को यूज़ करता है।

**TCP (TRANSMISSION CONTROL PROTOCOL) (ट्रांसमिशन कण्ट्रोल प्रोटोकॉल): -**

TCP (Transmission Control Protocol) एक Transport Layer Connection Oriented Protocol है। ये Protocol Reliable Delivery Provide करता है। TCP और Internet Protocol मिलकर Internet Protocol Suit बनाते है।

TCP Connection Oriented Protocol है। TCP में दो Devices के बीच में Connection Establish, Three Way Handshake के द्वारा Perform किया जाता है। Three Way Handshake Sender और Receiver के बीच में Messages की Sequence होती है जिससे Connection Establish किया जाता है।

सबसे पहले Sender, Receiver को Message भेजता है की वो Connection Establish करके कुछ Data भेजना चाहता है। जब Receiver को ये Message मिलता है तो Receiver वापस Sender को Message भेजता है की वो Data के लिए Ready है। इसके बाद Sender वापस एक Message भेजता है जो की Receiver को Data की Sequence बताता है। इसके बाद Sender और Receiver के बीच में Data Transfer शुरू हो जाता है। Sender और Receiver के बीच में भेजे जाने वाले ये Messages 3 तरह के होते है।

- SYN – Connection Request
- SYN + ACK – Sequence Number Request cum Acceptance of Connection Request
- ACK – Acceptance of Connection Request and Data Sequence Number

**TCP Header Format (TCP हैडर फॉर्मेट): -**

Data को Transfer करने के दौरान Data के साथ TCP Header Attach की जाती है। इस Header में कई प्रकार की Information होती है जो आपके Segment की Characteristics बताती है। जैसे की Source, Destination और Sequence number आदि। TCP Header 12 Fields से मिलकर बनी होती है और इसकी Minimum Size 20 Byte होती है।

<table>
<tr><td colspan="5">SOURCE PORT (16 bit)</td><td colspan="4">DESTINATION PORT (16 bit)</td></tr>
<tr><td colspan="9">SEQUENCE NUMBER (32 bit)</td></tr>
<tr><td colspan="9">ACKNOWLEDGEMENT NUMBER (32 bit)</td></tr>
<tr><td>DATA OFFSET</td><td>RESERVE BITS</td><td>URG</td><td>ACK</td><td>PSH</td><td>RST</td><td>SYN</td><td>FIN</td><td>WINDOW SIZE ( 16 bit )</td></tr>
<tr><td colspan="5">CHECKSUM ( 16 bit )</td><td colspan="4">URGENT POINTER ( 16 bit )</td></tr>
<tr><td colspan="9">OPTIONS ( 0 – 40 BYTES)</td></tr>
<tr><td colspan="9">DATA ( OPTIONAL )</td></tr>
</table>

DIG: TCP HEDER FORMAT

- Source Port: - इस Field की Size 16 bits होती है। ये Field Sender के Port Number को Carry करता है।
- Destination Port: - इस Field की Size भी 16 bits ही होती है और ये Receiver के Port Number को Carry करता है।
- Sequence Number: - ये Field 32 bits का होता है और इसमें Segment का Sequence Number होता है।
- Acknowledgement Number: - ये Field भी 32 bits का होता है और इसमें Acknowledgment Number Carry होता है।
- Data Offset: - Data Offset ये बताता है की TCP Segment में Data कहाँ से शुरू होता है। इस Field की Size 4 bits होती है।
- Reserved Field: - इस Field की Size 6 bits होती है। इसे Future Use के लिए रख जाता है। ये हमेशा Zero पर Set रहता है।
- Control Bits: - ये Field 6 bits का होता है। इसमें एक एक bit के 6 Flags होते है। इन Flags को Set करके आप बता सकते है की ये Segment किस तरह का है।
  i. URG (Urgent) – ये Flag Set (1) करने से Segment को Traffic में Priority मिलती है।
  ii. ACK (Acknowledgment) – ये Flag किसी भी Message को Acknowledge करने के लिए Set (1) किया जाता है।
  iii. PSH (Push) – ये Flag Segment को Forcefully Send करता हैं चाहे Window Full हुई हो या नहीं।
  iv. RST (Reset) – ये Flag Connection को Forcefully Terminate कर देता है।
  v. SYN (Synchronize) – ये Flag Connection Establish करने के काम आता है।
  vi. FIN (Finish) – ये Flag Connection को Terminate करने के लिए Set किया जाता है।
- Window Field: - ये एक 16 bit Field होता है। ये Identify करता है की Receiver कितनी Bytes Receive करने में Capable है।
- Checksum Field: - ये Field Error Checking के लिए यूज़ किया जाता है। इसे TCP Segment और IP Header के Select Field से Compute किया जाता है। यदि Receivers Side पर Calculate किया हुआ Checksum Same ना हो तो Segment Discard कर दिया जाता है। इस Field की Size 16 bit होती है।
- Urgent Pointer Field: - ये एक 16 bit का Field होता है। जब Urgent Flag Set किया जाता है तो ये Field Traffic की Last Byte को Identify करता है।
- Options Field: - ये Field Variable Size का होता है। ये Field TCP Segment के लिए Optional Parameters Set करने के लिए यूज़ किया जाता है।
- Data Field: - ये Field भी Variable Size का होता है। ये Field निश्चित करता है की TCP Header 32 bit Boundery के भीतर ही समाप्त हो जाये। ये Field हमेशा Zero पर set रहता है।

**Difference Between TCP and UDP Protocol (TCP और UDP में अंतर): -**

| TRANSMISSION CONTROL PROTOCOL (TCP) | UDER DATAGRAM PROTOCOL (UDP) |
|---|---|
| TCP Connection Oriented Protocol होता है। | UDP एक Connection Less Protocol होता है। |
| TCP Data Delivery की Guarantee देता है। | UDP Data के पहुँचने की कोई Guarantee नहीं देता है। |
| TCP Data की Receipt के तौर पर Acknowledgment भेजता है। | UDP के द्वारा कोई Acknowledgment नहीं भेजा जाता है। |
| TCP एक बहुत ही Slow Service है। | UDP बहुत Fast Service है। |

| | |
|---|---|
| TCP Data की Sequencing करता है। | UDP के द्वारा Data की Sequencing नहीं की जाती है। |
| यदि कोई Segment Fransfer के दौरान Drop हो जाये तो TCP उस Segment को दोबारा भेज देता है। | Drop होने वाले Segments को UDP वापस नहीं भेजता है। |
| TCP Sliding Window Protocol के द्वारा Flow Control Provide करता है। | UDP में Flow Control नहीं होता है। |
| इसमें Congestion को नियंत्रित किया जाता है। | इसमें Congestion Control नहीं होता। |
| यह एक Reliable Protocol है। | यह एक Unreliable Protocol है। |
| TCP एक Heavy Weight Protocol है। | जबकि UDP एक Light Weigh Protocol है। |
| इसके Header का साइज़ 20 Bytes है। | इसके Header का साइज़ 08 Bytes है। |
| यह 3 - Way Handshake का प्रयोग Connection को स्थापित करने के लिए करता है। | यह किसी भी Handshake का प्रयोग नहीं करता। |
| TCP की जरुरत निम्न Protocols को होती है: - HTTP, HTTPS, FTP, SMTP, Telnet आदि। | इसकी आवश्यकता इन Protocols को होती है: - DNS, DHCP, SNMP, VOIP, RIP आदि। |
| इसका उदाहरण- Phone Call करना। | इसका उदाहरण: - Online Video Game खेलना। |

**08. <u>DNS DOMAIN NAME SYSTEM (डोमेन नेम सिस्टम): -</u>**

DNS का Full Form Domain Name System है। "DNS एक ऐसा सिस्टम है जो की डोमेन नेम को IP Address यानि नंबर के फॉर्म में Translate करता है ताकि वेब ब्राउज़र यह समझ सके की आप इन्टरनेट पर कौनसा वेब पेज Access करना चाहते हैं। DNS को कई नामों से जाना जाता है, जिसमें Name Server, Domain Name System Server शामिल हैं।

हर डोमेन नेम (जैसे webinhindi.com) और Internet से Connected Device एक Unique IP Address (जैसे: 198.15.42.15) होता है जिससे पता चलता है की वेबसाइट का Content कौन से सर्वर पर स्टोर है।

इस सिस्टम के अंदर में एक Domain Name Server स्थापित होता है इसे आप एक फ़ोन बुक या टेलीफ़ोन डायरेक्टरी या अपने मोबाइल के कांटेक्ट लिस्ट से तुलना कर सकते है जहाँ एक तरफ नाम और उसके मोबाइल नंबर लिखे होते हैं, ठीक इसी तरह डोमेन नाम सर्वर में भी Domain Name और उसके IP Address की जानकारी Stored रहती है।

<u>Working of DNS (DNS का कार्यपद्धति): -</u>

a. जब हम ब्राउज़र के एड्रेस बार में किसी वेबसाइट की एड्रेस यानि डोमेन नाम जैसे google.com इंटर करते हैं तो सबसे पहला काम उस डोमेन का IP Address ढूँढना होता है इसके लिए यह पहले Browser के Cache Memory को चेक किया जाता है यदि आप इससे पहले गूगल की वेबसाइट को Visit कर चुके हैं तो इसका IP एड्रेस आपके ब्राउज़र के कैश में स्टोर हो सकता है।
b. यदि Cache में IP मिल जाये तो इससे वेबसाइट ओपन हो जाता है।
c. यदि ब्राउज़र Cache में IP की जानकारी Stored नही है तो यह आपके सिस्टम के Operating System जैसे Windows, Android या Mac को Request Transfer करेगा।
d. आपका Operating System इस Request को Resolver यानि आपके Internet Service Provider (ISP) को भेज देता है जिसके पास भी Cache होता है जिसमे IP Address का Record हो सकता है।

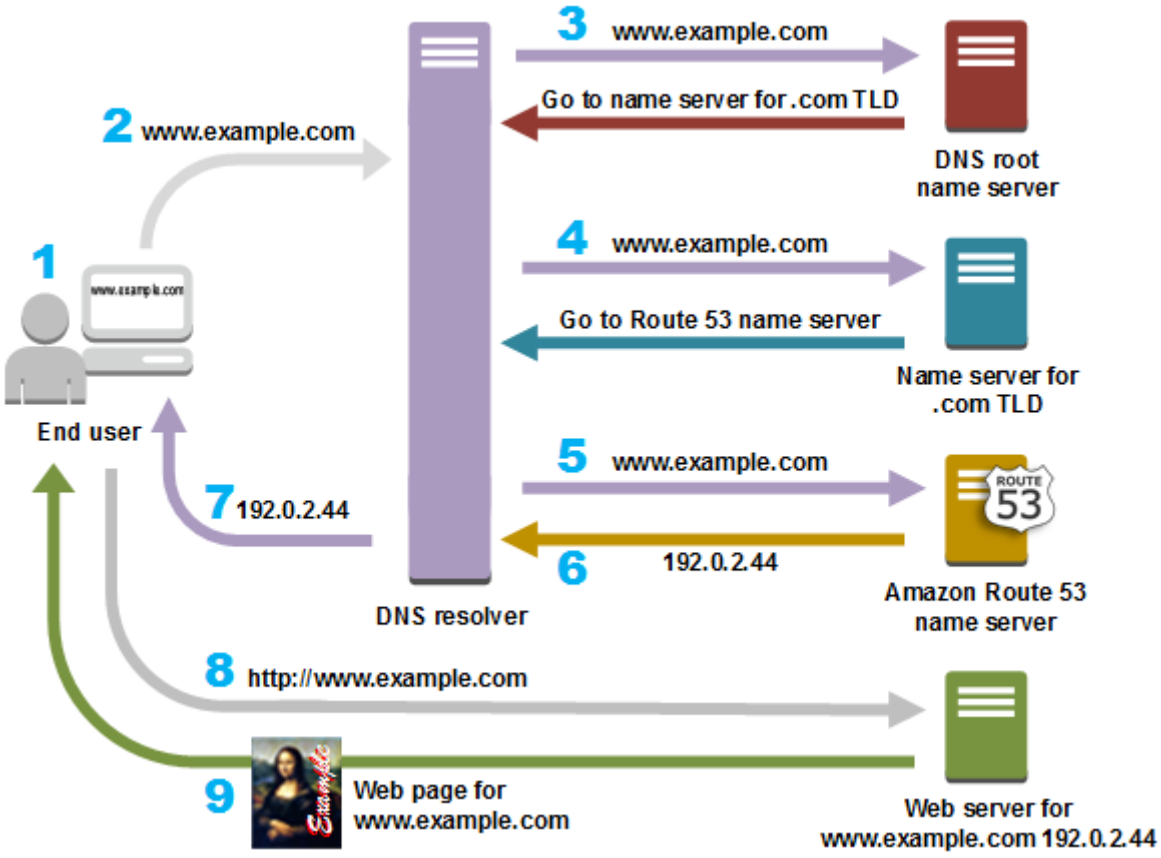
e. यदि यहाँ IP मिल जाता है तो यह प्रोसेस यही खत्म हो जाता है और Client को IP की जानकारी दे दी जाती है और वेबसाइट एक्सेस हो जाता है।

f. यदि यहाँ भी आईपी न मिले तो Resolver से रिक्वेस्ट ट्रान्सफर हो कर Root Server को चला जाता है।

g. Root Server आगे Top Level Domain Server को रिक्वेस्ट करता है जिसे Top Level Domain जैसे .com, .org, .edu, .gov, .in के सर्वर की जानकारी होती है। यहाँ वेबसाइट के डोमेन के अनुसार उपयुक्त टॉप लेवल डोमेन सर्वर से संपर्क किया जाता है।

h. टॉप लेवल डोमेन सर्वर से जानकारी मिलने के बाद अब आखिर में Authoritative Name Server से Actual Name Server की जानकारी ली जाती है और यहाँ से डोमेन की IP पता चल जाती है।

i. जब IP Address ढूंढ लिया जाता है तब इसे Client यानि आपके Computer को भेज दिया जाता है ताकि इसके जरिये वेबसाइट को एक्सेस किया जा सके और IP को Cache में स्टोर भी कर लिया जाता है।




**09. <u>EMAIL (ई-मेल): -</u>**

इलैक्ट्रानिक मेल या संक्षेप मे ई-मेल इंटरनेट की सबसे अधिक उपयोग की जाने वाली सेवा है। इलैक्ट्रानिक मेल एक ऐसा इलैक्ट्रानिक संदेश होता है, जो किसी नेटर्वक से जुडे विभिन्न कम्प्यूटरो के बीच भेजा व प्राप्त किया जाता है। ई-मेल का उपयोग व्यक्तियो या व्यक्तियो के समूहो के बीच जो भौगोलिक रूप से हजारो मील दूर भी हो सकता है। ई-मेल को मेल सर्वर के माध्यम से भेजा जाता और प्राप्त किया जाता है। कोई मेल सर्वर ऐसा कम्प्यूटर होता है। जिसका कार्य ई-मेलो को प्रोसेस करना और उचित क्लाइंट कम्प्यूटरो को भेजना होता है।

<u>Sending Process of E-mail (Mail भेजने की प्रक्रिया): -</u> किसी E-Mail को भेजने के लिये निम्नलिखित Steps होते है: -

01. अपने सिस्टम को इंटरनेट से कनेक्ट करने के पश्चात् इंटरनेट एक्सप्लोलर को खोलते है। इसमे एड्रेस बार मे उस वेब साइट को Type करते है जिसमे हमारी E-Mail Id है, जैसे www.gmail.com को Type करके Enter Key Press करते है।

02. इसके पश्चात् हम User Name Box मे अपनी Email Id तथा Password Box मे Password लिखते है तथा Enter Key Press करते है। इसके पश्चात् स्क्रीन पर हमारा Home Page खुलता है।
03. इसमे हम Write Mail / Compose मेल ऑप्शन पर क्लिक करते है तो स्क्रीन पर एक नयी Window खुलती है, इसमे प्रथम Box मे वह Mail Id लिखते है जिसे व्यक्ति को हम मेल करना चाहते है। उसके बाद यदि कोई फाइल अटैच करना है तब Attachment बटन पर क्लिक करते है तो स्क्रीन पर Attachment Box खुलता है।
04. इस Box मे Browse Button के माध्यम से उस फाइल को Browse करके Attach हो जाती है।
05. इसके पश्चात् Send Button पर क्लिक करते है। इस तरह संलग्न की गयी फाइल उस ID पर पहुँच जाती है जो हमने Mention की है।

Reciving of E-mail (E-Mail प्राप्त करने की प्रक्रिया): - E-Mail को प्राप्त करने के लिये निम्नलिखित Steps होते है: -
01. अपने सिस्टम को इंटरनेट से कनेक्ट करने के पश्चात् इंटरनेट एक्सप्लोलर को खोलते है। इसमे एड्रेस बार मे उस वेब साइट को Type करते है जिसमे हमारी E-Mail Id है, जैसे www.gmail.com को Type करके Enter Key Press करते है।
02. इसके पश्चात् हम User Name Box मे अपनी Email Id तथा Password Box मे Password लिखते है तथा Enter key Press करते है। इसके पश्चात् स्क्रीन पर हमारा Home Page खुलता है।
03. इसके पश्चात् हमे जो भी Mail किसी के द्वारा भेजे गये है उसे हम अपने Inbox मे जाकर प्राप्त कर सकते है।

Validation Condition of Email: -
a. एक E-mail में एक Username होना जरुरी है जिसके बाद @(at sign) होना चाहिए और उसके पश्चात Domain Name।
b. इसमें Username 64 Characters Long से और Domain Name 254 Characters से लम्बा नहीं होना चाहिए।
c. एक @ sign होना चाहिए E-mail Address में।
d. Email में Space और Special Characters: ( ) , : ; < > \ [ ] को allow किया जाता है। कभी कभी Space, Backslash, और Quotation Mark भी काम कर जाता है लेकिन इसके पहले एक Forward Slash जरुर से होना चाहिए।

Advantages of Email (ईमेल के लाभ): -
i. Email की Delivery Speed बहुत ही Fast होती है, इससे लोगों को Information तुरंत प्राप्त हो जाता है।
ii. Email Quick Communication के लिए बहुत ही ज्यादा Convenient Method हैं।
iii. Email में Attachment का Feature होने के कारण आप ईमेल के साथ कुछ भी File Attach कर सकते हैं।
iv. Email आपके सभी Conversation को Record करती हैं, इसलिए आप उन Conversation को एक Record के तरह कभी भी देख सकते हैं।
v. Email को आपके ईमेल प्रोग्राम में आसानी से स्टोर किया जा सकता है। आप अपने ईमेल को कहीं भी - कभी भी एक्सेस कर सकते हैं।
vi. कुछ लिखने के लिए Texting के विपरीत एक Email में Unlimited Space मिलता है।

Disadvantage of Email (ईमेल से हानि): -
i. Email Send या Receive करने के लिए Internet Connection की जरुरत होती है।
ii. Email में हम ज्यादा बड़ी Size की Files को नहीं भेज सकते हैं, उसकी एक Limit (25 MB) होती है।
iii. Email में हम सभी प्रकार के Files Formats जैसे की ".exe" को भेज नहीं सकते हैं।
iv. Email की एक प्रकार हैं Spam, जिससे हमारे Inbox में इन Spam Mail के ज्यादा होने से हमें सही Email को खोज पाना मुश्किल हो जाता है।

**10. SMTP 9SIMPLE MAIL TRANSFER PROTOCOL) (सिंपल मेल ट्रांसफर प्रोटोकॉल): -**

SMTP एक TCP/IP आधारित Application Layer Protocol है, जो Mail Transmission के लिए उपयोग होता है। यानि जब एक E-Mail Id से मेल भेजी जाती है तो उस E-Mail को Client Computer से Mail Server तक पहुँचाने का कार्य SMTP द्वारा होता है। SMTP को एक Push Protocol भी बोला जाता है, और यह Port 25 का प्रयोग करता है। इसी तरह से एक Mail Server से दूसरे Mail Server को Mail Transfer करने में भी SMTP की ही भूमिका होती है।

SMTP प्रोटोकॉल के साथ हमेशा दो और प्रोटोकॉल कार्य करते हैं। POP और IMAP इन दोनों प्रोटोकॉल का काम Mail Server से मेल डाउनलोड कर Client Computer तक पहुँचाना होता है।

Working Process of SMTP (SMTP की कार्य विधि): -

SMTP एक बहुत ही सरल कार्यप्रणाली द्वारा कार्य करता है,जो की End To End मेल डिलीवरी पर आधारित होता है। SMTP Process के दो Working Points होते हैं, पहला SMTP Client जो की Mail Sender होता है, और दूसरा है SMTP MAIL Server जो Mail Receiver होता है। SMTP Client कंप्यूटर में SMTP से जुडी Mail Settings Save रहती हैं। जैसे Gmail का ही उदाहरण लें, तो Smtp@Gmail.Com और साथ ही Port No 25 Configure होगा। इसी तरह से यदि Microsoft Outlook का उपयोग करेंगे तो उसमे में भी Mail Server से जुड़ी Settings डलेंगी और SMTP Port 25 Configure होगा।

तो सबसे पहले जब एक SMTP Client द्वारा मेल Send की जाती है,जैसे Gmail या Microsoft Outlook द्वारा तो वह मेल सीधे SMTP Server पर पहुँचती है। जहाँ पर SMTP Server द्वारा मेल को Process किया जाता है। जिसमे यदि Internal Network की मेल है, तो वह Server पर ही Save रहती है, जिसे SMTP Client Sync कर लेता है और फिर IMAP या POP द्वारा वह मेल कंप्यूटर पर डाउनलोड हो जाती है और यदि कोई बाहरी एड्रेस है, तो ऐसे में SMTP Server उस Mail को दूसरे उस सम्बंधित Mail Server पर Transfer कर देता है।

SMTP Commands (SMTP के कमांड): -

a. HELLO: - इस कमांड द्वारा एक Mail Server दूसरे Mail Server से संवाद स्थापित करता है। यह SMTP Session के शुरुवात होने की प्रक्रिया है।
b. MAIL FROM: - यह कमांड Sender के मेल एड्रेस को दर्शाती है जिसमे Sender का E-Mail एड्रेस From फील्ड में डाल दिया जाता है।
c. RCPT TO: - यह मेल के Recipient यानि प्राप्त करने वाले को दर्शाता है,जिसमे यदि एक से अधिक Recipient हैं तो यह कमांड हर एड्रेस पर दोहराई जाती है।
d. Size: - इस SMTP कमांड द्वारा सर्वर को Attached ईमेल के अंदाजन Size के बारे में Inform करा दिया जाता है।
e. Data: - इस कमांड के साथ ही ईमेल ट्रांसफर होना शुरू हो जाती है, जिसे स्टार्ट करने के लिए Server द्वारा 354 रिप्लाई कोड दिया जाता है, जो प्रोसेस को शुरू करने की हरी झंडी है।

**11. FTP FILE TRANSFER PROTOCOL (फाइल ट्रांसफर प्रोटोकॉल): -**

FTP File Transfer Protocol है का उपयोग एक कंप्यूटर से दूसरे कंप्यूटर के बीच फाइल ट्रान्सफर करने के लिए किया जाता है। एफटीपी दो Systems के बीच फाइलों के आदान-प्रदान के लिए Set of Rules यानी की कुछ नियमों को निर्धारित करता है। जब कोई Web Developer वेबसाइट बनाता है तो उस वेबसाइट के Files को सर्वर पर Upload करना होता है और इस काम के लिए FTP का उपयोग किया जाता है जो की बड़े-बड़े फाइलों को सर्वर पर अपलोड, डाउनलोड, रीनेम, डिलीट, कॉपी और मूव करने में मदद करता है।

एफटीपी के द्वारा Web Server पर फाइल अपलोड करने के लिए आप नीचे दिए गये तीन तरीके का उपयोग कर सकते हैं: -

a. Command Line का उपयोग करके: - हर Operating Systems चाहे वह Windows हो, Linux हो या Mac OS हो सभी में FTP के लिए कुछ Built in Command दिए होते हैं जिनका उपयोग करके FTP Site से Connect हो सकते हैं।
b. Web Browser का उपयोग करके: - सीधे Web Browser का भी Use कर सकते हैं इसके लिए आपको Address Bar में http:// की जगह ftp:// लिखना होगा और साथ में आपको Username और Password को भी URL में Type करना होगा। ब्राउज़र पर एड्रेस कुछ इस तरह होगा: ftp://username:password@ftp.website.org/
c. Graphical FTP Client का उपयोग करके: - Graphical FTP Client का भी Use कर सकते हैं जो की एक प्रकार का Application होता है और जिसका Interface बहुत ही User Friendly और आसान होता है। यदि आप विंडोज Use कर रहें हैं तो FileZilla नाम का Application आप इन्टरनेट से मुफ्त में डाउनलोड कर सकते हैं।

File Transfer करने के लिए FTP दो प्रकार के Connection का उपयोग करता है: -

i. Control Connection: - इसका उपयोग Connection को Open या Close करने और Server को Command भेजने के लिया किया जाता है।
ii. Data Connection: - Connection स्थापित होने बाद Data Connection के माध्यम से Client Server के बीच फाइल ट्रान्सफर किया जाता है।

Advantage of FTP (FTP से लाभ): -

- FTP Client के जरिये आप एक से अधिक Files के अलावा Multiple Directories को एक साथ Transfer कर सकते हैं।
- फाइलों को तेज़ गति से ट्रान्सफर करना एफटीपी का सबसे बड़ा Advantage है।
- यदि ट्रान्सफर के समय Connection Loss हो जाए तो परेशान होने की जरुरत नही है आप बाद में उसे Continue कर सकते हैं। आप चाहें तो बीच में Transfer को Pause भी कर सकते हैं और बाद में Resume भी कर सकते हैं।
- आप File या Directory Transfer को Schedule भी कर सकते हैं यानी बताये गये समय पर यह Automatic अपना काम कर सकता है।
- FTP पर Auto Backup की सुविधा भी जो की बड़े काम की चीज है।

Disadvantages of FTP (FTP से हानि): -

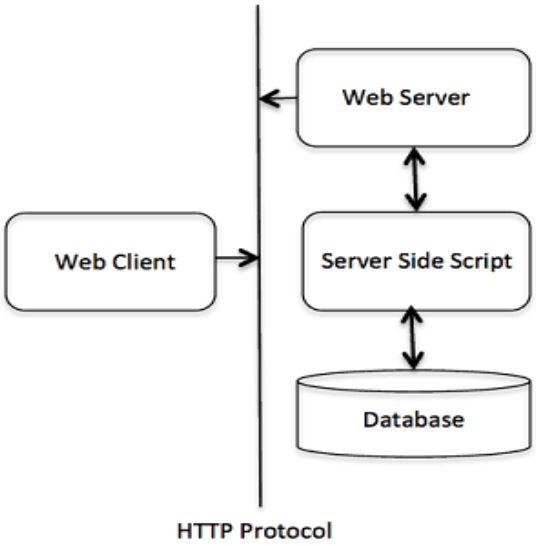
- सारे FTP Servers Encryption की सुविधा नही देते हैं और बिना Encryption के Data Transfer करना सुरक्षित नही है।
- अगर आपका पासवर्ड कमजोर है तो Brute Force Attack के जरिये अलग-अलग Password Combination बना कर Hackers आपके Password को Guess कर सकते हैं।

## 12. HTTP (HYPTE TEXT TRANSFER PROTOCOL) (हाइपर टेक्स्ट ट्रांसफर प्रोटोकॉल): -

HTTP का पूरा नाम हाइपरटेक्स्ट ट्रांसफर प्रोटोकॉल है जिसका उपयोग वेब पर डेटा ट्रांसफर करने के लिए किया जाता है। यह इंटरनेट प्रोटोकॉल सूट का हिस्सा है और वेबपेज डेटा ट्रांसमिट करने के लिए इस्तेमाल की जाने वाली कमांड और सेवाओं को परिभाषित करता है। एड्रेस के सामने http: // इंटर करने वाले किसी भी वेब पेज तक पहुंचने पर ब्राउज़र को HTTP पर कम्यूनिकेट करने के लिए कहता है। उदाहरण के लिए, http://google.com है। आज के ब्राउज़र्स को अब URL के सामने HTTP की आवश्यकता नहीं है क्योंकि यह संचार का डिफ़ॉल्ट तरीका है।

Basic Architecture of HTTP (HTTP का बेसिक आर्किटेक्चर): -

HTTP प्रोटोकॉल क्लाइंट / सर्वर आधारित आर्किटेक्चर पर आधारित एक रिक्वेस्ट / रिस्पॉन्स प्रोटोकॉल है जहां वेब ब्राउजर, रोबोट और सर्च इंजन आदि HTTP क्लाइंट की तरह काम करते हैं और वेब सर्वर एक सर्वर की तरह काम करता है।




Client: - HTTP क्लाइंट एक रिक्वेस्ट मेथड, URI, और प्रोटोकॉल वर्जन के रूप में सर्वर को MIME के द्वारा एक रिक्वेस्ट भेजता है।

Server: - HTTP सर्वर एक Status Line के साथ Responds देता है, जिसमें मैसेज प्रोटोकॉल वर्जन और एक सफलता या त्रुटि कोड शामिल होता है, जिसे MIME के द्वारा पूरा किया जाता हैं जैसे सर्वर जानकारी, एंटिटी मेटा जानकारी और Possible Entity Body Content शामिल होता है।

HTTP Error Codes (एरर कोड्स) HTTP से जुड़े कुछ Common Error Codes इस प्रकार हैं: -

a. 400 Bad File Request: - यह Error Code तब दिखाई देता है जब हमारा URL गलत हो जैसे की Small की जगह Capital Letter Use करना, चिन्हों को Type करने में गलती करना आदि।
b. 401 Unauthorized: - गलत Password Enter करने की वजह से यह एरर आ सकता है।
c. 403 Forbidden / Access Denied: - जब आप किसी ऐसे Page को Open कर रहें हों जिसकी Permission आपको नही है तो ऐसी स्थिति में यह Response Code दिखाई दे सकता है।
d. 404 File Not Found: - यह सबसे Common Error है। जब किसी ऐसे File या Document के लिए Request कर रहें हो जो कि Server पर उपलब्ध नही है, Delete कर दिया गया है या किसी दुसरे Location पर Move कर दिया गया है तब ऐसी स्थिति में 404 Error आता है।
e. 503 Service Unavailable: - Internet Connection में Problem हो, Server Busy हो, या Site किसी अन्य Address पर Move हो गया हो तब इस प्रकार का Error आ सकता है।

HTTP Protocol Secured नही होता, इसे आसानी से Hack किया जा सकता है। HTTP में Data Unencrypted Form में होता है, HTTP Request को बीच में किसी Hacker द्वारा Read किया जा सकता है और Server की तरफ से Response भी कर सकता है। इसलिए HTTP के जरिये Sensitive Information जैसे की Password, Credit Card Details आदि Transfer नही किये जाते।

**HTTPS: -** HTTPS का Full Form "HyperText Transfer Protocol Secured" है। यह HTTP का Secured Version है इसमें SSL (Secured Socket Layer) का Use होता है जो की Browser और Server के बीच Encrypted Form में Data Transfer करता है। HTTPS के तीन Main Goals होते हैं: -

a. Privacy: Data को Encrypt करना जिससे की Client और Server के बीच कोई भी Middleman Data को Read न कर सके।
b. Integrity: यह Ensure करना की Data दोनों End के बीच में कहीं Change न हुआ हो।
c. Authentication: इस System में Client Server दोनों को एक दुसरे को अपनी-अपनी Identity Prove करनी पड़ती है ताकि Communication की सत्यता की जाँच किया जाता है।