डाटा कम्युनिकेशन एंड कंप्यूटर नेटवर्क

ई.हरीश दाधीच

ई.विकास माथुर

बी.टेक ,पोलोटेक्निक एवं आईटीआई पाठ्यक्रम अनुसार

प्रस्तावना

प्रस्तुत पुस्तक “डाटा कम्युनिकेशन(संचार) एंड कंप्यूटर नेटवर्क” डिप्लोमा पाठ्यक्रम के कंप्यूटर इंजीनियरिंग के छात्रों के लिए लिखी गई है। इस पुस्तक में डाटा कम्युनिकेशन व कंप्यूटर नेटवर्क के संपूर्ण पाठ्यक्रम को बहुत ही सरल भाषा में प्रस्तुत किया गया हैं। पुस्तक के हर एक पाठ में प्रत्येक विषय को सरल सैद्धांतिक रूप से विस्तार पूर्वक समझाया गया हैं जिससे छात्र आसानी से डाटा कम्युनिकेशन व कंप्यूटर नेटवर्क विषय का ज्ञान ले सके। इस पुस्तक में डाटा संचार तथा कंप्यूटर नेटवर्क के विभिन्न सैद्धांतिक तथा प्रायोगिक विषयो को संकलित किया गया है और आशा हैं कि यह पुस्तक छात्रों के ज्ञान में वृद्धि करेगी। इस पुस्तक द्वारा छात्र यह सिखने में सक्षम होंगे कि किस तरह दो या दो से ज्यादा कंप्यूटर के समूह को बनाया जाता हैं तथा डाटा का आदान प्रदान किया जाता हैं और किस तरह कंप्यूटर से बड़े समूह आपस में जुड़ के इंटरनेट की सुविधा को प्रदान करते हैं जो कि आज के कंप्यूटर आधुनिक युग में एक महत्वपूर्ण विषय हैं।

इस पुस्तक का मुख्य उद्देश्य आज के कंप्यूटर युग में छात्रों का डाटा कम्युनिकेशन , कंप्यूटर नेटवर्किंग , कंप्यूटर नेटवर्क सुरक्षा(सिक्योरिटी) , वेबसाइट डेवलोपमेन्ट(निर्माण) जैसे क्षेत्रों में छात्र ज्ञान की वृद्धि कर के अपने सुनहरे भविष्य की नीव रख सके।

डाटा कम्युनिकेशन(संचार) पुस्तक में डाटा संचार परिचय, ओएसआई/टी सी पी मॉडल, फिजिकल लेयर, डाटा लिंक लेयर , नेटवर्क लेयर, ट्रांसपोर्ट लेयर तथा एप्लीकेशन लेयर एवं नेटवर्क सिक्योरिटी आदि अध्यायों को समाहित किया गया हैं।

अध्याय 1 में डाटा संचार के प्रकार , डाटा संचार के घटक, कम्युनिकेशन चैनल , कंप्यूटर नेटवर्क व नेटवर्क टोपोलॉजी को विस्तार पूर्वक समझाया गया है।

अध्याय 2 में कंप्यूटर नेटवर्क का सबसे महत्वपूर्ण भाग ओएसआई/टी सी पी मॉडल की विस्तार पूर्वक कार्यप्रणाली को समझाया गया है तथा इंटरनेट प्रोटोकॉल के वर्गीकरण तथा उपयोग के सिद्धांतो को समझाया गया हैं।

अध्याय 3 में फिजिकल लेयर परिचय के साथ मल्टीप्लेक्सिंग , मल्टीप्लेक्सिंग के प्रकार , तकनीक , एन्कोडिंग तकनीक , स्विचिंग आदि विषयो को विस्तार पूर्वक समझाया गया हैं।

अध्याय 4 में डाटा लिंक लेयर की माध्यम से संचार त्रुटि , फ्लो कण्ट्रोल , व त्रुटि(एरर) के साथ सभी संचार(कम्युनिकेशन) अल्गोरिथम को उदहारण के साथ प्रस्तुत किया गया हैं तथा तकनीक को विस्तार पूर्वक समझाया गया हैं। ।

अध्याय 5 में कंप्यूटर संचार की सबसे मुख्य लेयर नेटवर्क लेयर को नेटवर्क लेयर प्रोटोकॉल व रूटिंग के प्रकार के माध्यम से समझाया गया हैं। अंत में इस लेयर में काम आने वाले सभी प्रोटोकॉल को प्रस्तुत किया गया है।

अध्याय 6 में ट्रांसपोर्ट लेयर टी सी पी तथा यू डी पी प्रोटोकॉल को थ्री वे हैंडशेकिंग के साथ प्रोटोकॉल की तकनीक तथा संचार के समय मैसेज(सन्देश) हेडर की कार्यप्रणाली को विस्तार पूर्वक समझाया गया हैं।

अध्याय 7 में एप्लीकेशन लेयर में कंप्यूटर नेटवर्क व संचार की तकनीक, एप्लीकेशन लेयर के निर्माण की विधि जैसे क्लाइंट सर्वर मॉडल, वेबसाइट डोमेन , एप्लीकेशन प्रोटोकॉल, एच टी टी पी व वर्ल्ड वाइड वेब आदि प्रोटोकॉल की तकनीक को समझाया गया हैं तथा अंत में नेटवर्क में डाटा तथा संचार को सुरक्षित कैसे रखा जाए उसके लिए सिक्योरिटी तकनीक तथा नीतियों को प्रस्तुत किया गया हैं।

इस पुस्तक में पाठ्यक्रमानुसार अध्याय सरल भाषा में लिखित तथा उपयुक्त रेखा चित्रों द्वारा वर्णित हैं जो डाटा कम्युनिकेशन(संचार) तथा कंप्यूटर नेटवर्क विषयो से सम्बंधित प्रतियोगी परीक्षाओं हेतु भी छात्रों का ज्ञान सुद्रढ़ करेगा।

हमें पूरी उम्मीद हैं कि पुस्तक छात्रों के लिए उपयोगी सिद्ध होगी।

- हरीश दाधीच

विकास माथुर

सूची

अध्याय संख्या		विषय	पृष्ठ संख्या
1.	**डेटा संचार एक परिचय**		5-36
	1.1	प्रस्तावना	5
	1.2	संचार (कम्युनिकेशन)	8
	1.3	डाटा कम्युनिकेशन	9
	1.3.1	डाटा कम्युनिकेशन के प्रकार	9
	1.3.2	डाटा संचार के घटक	11
	1.3.3	डाटा संचार के माध्यम	12
	1.4	कम्युनिकेशन चैनल	15
	1.5	कंप्यूटर नेटवर्क	16
	1.5.1	कंप्यूटर नेटवर्क के प्रकार	16
	1.6	नेटवर्क टोपोलॉजी	18
	1.6.1	नेटवर्क टोपोलॉजी परिचय	18
	1.6.2	नेटवर्क टोपोलॉजी के प्रकार	19
	1.7	ट्रांसमिशन	23
	1.7.1	ट्रांसमिशन कम्युनिकेशन चैनल	26
	1.7.2	ट्रांसमिशन मोड	28
	1.7.3	ट्रांसमिशन के प्रकार	30
	1.8	डाटा प्रस्तुतीकरण	34
2.	**ओएसआई-टीसीपी / आईपी मॉडल**		37-61
	2.1	ओएसआई मॉडल एक परिचय	37
	2.1.1	ओएसआई मॉडल की परतें	38
	2.2	टीसीपी / आईपी मॉडल	45
	2.2.1	टीसीपी / आईपी मॉडल रेफ़्रेन्स मॉडल	46
	2.3	ओएसआई-टीसीपी / आईपी मॉडल के प्रमुख प्रोटोकॉल	48
	2.3.1	एड्रेस रेसोलुशन प्रोटोकॉल	48
	2.3.2	इंटरनेट मैसेज प्रोटोकॉल	49
	2.3.3	रूटिंग इनफार्मेशन प्रोटोकॉल	50
	2.3.4	ओपन शॉर्टेस्ट पाथ फर्स्ट प्रोटोकॉल	53
	2.3.5	ट्रांसमिशन कण्ट्रोल प्रोटोकॉल	55

	2.3.6	यूज़र डाटा ग्राम प्रोटोकॉल	56
	2.3.7	डोमेन नाम सिस्टम	57
3.	**फिजिकल लेयर**		62-95
	3.1	फिजिकल लेयर एक परिचय	62
	3.2	मल्टीप्लेक्सिंग	64
	3.2.1	मल्टीप्लेक्सिंग प्रस्तावना	64
	3.2.2	मल्टीप्लेक्सिंग के प्रकार	65
	3.3	सिग्नल एंड एन्कोडिंग तकनीक	71
	3.3.1	प्रस्तावना	71
	3.3.2	डिजिटल डाटा और एनालॉग सिग्नल(एन्कोडिंग तकनीक)	73
	3.3.3	मल्टीलेवल डिजिटल ट्रांसमिशन	76
	3.3.4	लाइन कोडन के प्रकार	79
	3.4	स्वीचिंग नेटवर्क एंड उपयोग	85
	3.4.1	प्रस्तावना	85
	3.4.2	सर्किट स्वीचिंग	86
	3.4.3	मैसेज स्वीचिंग	90
	3.4.4	पैकेट स्वीचिंग नेटवर्क	90
	3.5	X .21 प्रोटोकॉल	93
4.	**डाटा लिंक लेयर**		95
	4.1	डाटा लिंक लेयर एक परिचय	95
	4.1.1	ट्रांसमिशन एरर	96
	4.2	फ्लो कण्ट्रोल एंड एरर कण्ट्रोल	100
	4.2.1	स्टॉप एंड वेट ARQ (Stop & Wait ARQ)	101
	4.2.2	गो -बैक- एन ARQ (Go-Back-N ARQ)	105
	4.2.3	सेलेक्टिव रिपीट ARQ (Selective Repeat ARQ)	109
	4.3	एरर डिटेक्शन एंड करेक्शन	112
	4.3.1	एरर डिटेक्शन	112
	4.3.2	एरर करेक्शन	114
	4.4	मीडियम एक्सेस कण्ट्रोल सबलेयर	115

5.	**नेटवर्क लेयर**		122
	5.1	नेटवर्क लेयर एक परिचय	122
	5.1.1	कनेक्शन डिवाइस इन नेटवर्क लेयर	130
	5.2	नेटवर्क लेयर प्रोटोकॉल	140
	5.2.1	रूटिंग के प्रकार	140
	5.2.2	इंटरनेट प्रोटोकॉल	148
6.	**ट्रांसपोर्ट लेयर**		155
	6.1	ट्रांसमिशन कण्ट्रोल प्रोटोकॉल TCP लेयर एक परिचय	155
	6.2	ट्रांसमिशन कण्ट्रोल प्रोटोकॉल TCP परिचय	157
	6.2.1	ट्रांसमिशन कण्ट्रोल प्रोटोकॉल TCP खंड	159
	6.2.2	थ्री वे हैंडशेकिंग	161
	6.3	यूज़र डाटा ग्राम प्रोटोकॉल UDP परिचय	163
	6.3.1	यूज़र डाटा ग्राम प्रोटोकॉल UDP खंड	166
	6.3.2	यूज़र डाटा ग्राम प्रोटोकॉल UDP ऑपरेशन	168
7.	**एप्लीकेशन लेयर एवं नेटवर्क सिक्योरिटी**		170
	7.1	एप्लीकेशन लेयर एक परिचय	170
	7.2	क्लाइंट - सर्वर मॉडल	171
	7.3	डोमेन सर्वर नेम (DNS)	175
	7.4	ईमेल एवं एप्लीकेशन प्रोटोकॉल	182
	7.5	एचटीटीपी(HTTP) एवं वर्ल्ड वाइड वेब(WWW)	199
	7.6	नेटवर्क सिक्योरिटी एक परिचय	209
	7.6.1	सिक्योरिटी मुद्दे	210
	7.6.2	सिक्योरिटी नीतियां	211
	7.6.3	सिक्योरिटी टूल	211
	7.7	क्रप्टोग्राफी	213
	7.8	क्रप्टोग्राफी अल्गोरिथम	214

वैज्ञानिक तथा तकनीकी शब्दावली आयोग के अंतर्गत डाटा कम्युनिकेशन की मूलभूत शब्दावली 220-250

अध्याय – 1 डेटा संचार एक परिचय

1.1 प्रस्तावना :–

1970 और 1980 के दशको में हमने कम्प्यूटर साईंस और डाटा कम्युनिकेशन के क्षेत्र का विलय होते देखा था, जिसके चलते टेक्नोलॉजी, प्रॉडक्ट्स और वर्तमान की ग्रुप्ड कम्प्यूटर कम्युनिकेशन इंडस्ट्री से जुड़ी कंपनियों में आमतौर पर बदलाव हुए।

कम्प्यूटर कम्युनिकेशन क्रांति ने अनेक महत्वपूर्ण तथ्यों को जन्म दिया–

1. डाटा प्रोसेसिंग(कम्प्यूटर्स) और डाटा कम्युनिकेशन (ट्रांसमिशन और स्विचिंग उपकरण) के मध्य कोई बुनियादी अंतर नहीं रह गया है।
2. डाटा, वॉईस और वीडियो कम्युनिकेशन के मध्य भी कोई बुनियादी अंतर नहीं रह गया है।
3. सिंगल–प्रोसेसर कम्प्यूटर, मल्टीप्रोसेसर कम्प्यूटर, लोकल नेटवर्क, मेट्रोपोलिटन नेटवर्क और लांग–हॉल नेटवर्क के मध्य जो अंतर था वह काफी कम हो चुका है।

किसी संदेश को आदान–प्रदान करने के कई तरीके हो सकते है। यदि संदेश देने वाला और प्राप्त करने वाला आसपास ही हो, तो जोर से बोलकर संदेश दिया जा सकता है। यदि वह कुछ ही दूरी पर है, तो संदेश को कागज पर लिखकर चपरासी के द्वारा भिजवाया जा सकता है। अगर दूरी अधिक है, तो डाक के माध्यम से संदेश भिजवाया जा सकता है। यदि संदेश बहुत लंबा न हो और भेजने तथा पाने वाले दोनों के पास टेलीफोन हों, तो इसके माध्यम से भी संदेश दिया जा सकता है। किन्तु इन सभी तरीकों में एक तत्व छिपा हुआ है और वह है – संदेश के आदान–प्रदान की गति अर्थात् संदेश कितनी देर में पहुॅंच रहा है और इस पर कितना खर्च आ रहा है। सस्ता और तत्कालिक होने की वजह से टेलीफोनिक कम्युनिकेशन लोकप्रिय है। हम किसी व्यक्ति से टेलोफोन पर बात कर सकते हैं ओर उसे अनेक संदेश भी दे सकते है। परंतु टेलोफोन पर चित्र नहीं भेजे जा सकते है।

डाटा अथवा संदेश अधिक मात्रा में हों तो उन्हें टेलीफोन पर भेजने के लिए याद भी नहीं रखा जा सकता है। इसी संदर्भ में संदेश, पिक्चर्स और आवाज से युक्त छाटा कम्युनिकेशन का महत्व उभरकर सामने आया है। डाटा कम्युनिकेशन के मामले में जिन मूलभूत तत्वों पर ध्यान दिया जाना आवश्यक है, वे हैं–

1. लंबी दूरी के लिए संदेश, पिक्चर अथवा वॉईस प्रेषित करने की लागत कम होनी चाहिए।
2. प्राप्त करने वाले (रिसीवर) के मन में रत्ती भर भी संदेह या गलतफहमी के बिना प्रेषण कार्य पूरा होना चाहिए। इसका अर्थ यह है कि शोर–शराबा आदि किसी तरह का व्यवधान नहीं होना चाहिए।

3. इससे पहले कि संदेश पुराना या अनुपयोगी हो जाए, इसे यथोचित समय में पहुँचना चाहिए।
4. संदेश सुरक्षित और संरक्षित रहना चाहिए। इसे केवल उसी व्यक्ति के पास पहुँचना चाहिए जिसके लिए भेजा जा रहा है। पोस्ट के माध्यम से संदेश भेजने का तरीका बिल्कुल भी सुरक्षित नहीं होता है। यदि कोई अन्य व्यक्ति टेलीफोन लाईन को टेप कर लें तो वह भी बातचीत सुन सकता है।

कम्युनिकेशन सिस्टम में प्रयुक्त होने वाली मूलभूत शब्दावली :

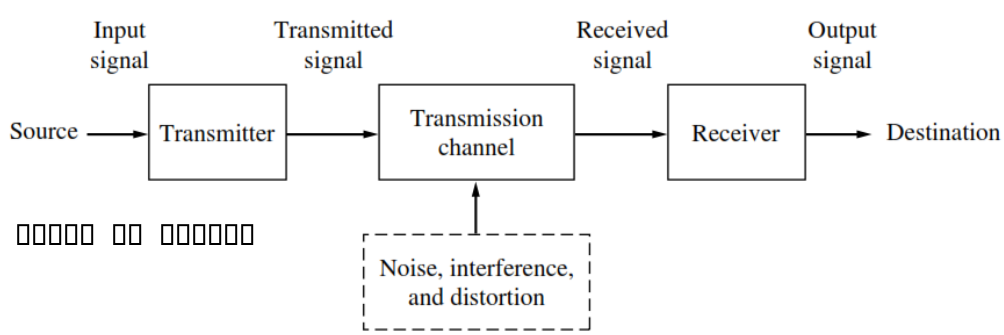
कम्युनिकेशन सिस्टम की व्याख्या करने के लिए मूल रूप से तीन शब्दों का उपयोग किया जाता है, (1) डाटा, (2) सूचना या इंफॉर्मेशन और (3) संकेत या सिग्नल।

(1) **डाटा** : डाटा वह सामग्री है, जिसके माध्यम से इंफॉर्मेशन को ट्रांसफर किया जाता है। डाटा का संबंध आकार, रूप या फॉर्म से है, जैसे क्रमबद्व संख्याएँ, वीडियो फ्रेम्स, शब्दों या टेक्स्ट की पंक्तियाँ या चित्र/इमेजेस।

(2) **इंफॉर्मेशन** : इंफॉर्मेशन शब्द का अर्थ है, डाटा की वेल्यू अथवा अभिप्राय या डाटा को किस तरह से समझा जा रहा है। जिस तरह से डाटा और इंफॉर्मेशन शब्दों की अपनी–अपनी परिभाषाएँ हैं, उसी प्रकार से संदेश शब्द के साथ इन्हीं शब्दों का साहित्य में भी आमतौर पर इसी अर्थ

(3) **सिग्नल्स** : इलेक्ट्रिकल अथवा ऑप्टिकल फॉर्मेट में इलेक्ट्रोमेग्नेटिक वेब्ज को सिग्नल्स कहते हैं। जिनका प्रयोग किसी भौतिक माध्यम द्वारा डाटा प्रेषित करने के लिए किया जाता है।

चित्र 1.1 में कम्युनिकेशन लिंक का उदाहरण ब्लॉक डायग्राम के माध्यम से दर्शाया गया है। इस तरह की लिंक का उद्देश्य किसी स-।छ यूजर, जिसे सोर्स अर्थात स्त्रोत कहा जाता है, से अन्य स-।छ यूजर जिसे डेस्टीनेशन अर्थात् गंतव्य कहा जाता है, के पास संदेश ट्रांसफर करना होता है। सोर्स का आउटपुट डाटा ट्रांसमिट करने वाल ट्रांसमीटर के लिए संदेश इनपुट की तरह से काम करता है।



चित्र1.1 :कम्युनिकेशन प्रणाली

डाटा कम्यूनिकेशन्स :

जब हम डाटा/ इंफॉर्मेशन को कम्यूनिकेट करते हैं, तब हम इंफॉर्मेशन या सूचना की शेयरिंग कर रहे होते है। अर्थात् इसे आपस में बॉट रहे होते है। यह शेयरिंग स्थानीय अथवा सुदूरर्ती (रिमोट) हो सकती है। व्यक्तियों के मध्य स्थानीय कम्यूनिकेशन प्रायः आमने सामने होता है, जबकि रिमोट कम्यूनिकेशन दूरी वाले स्थानों के मध्य होता है। टेलीकम्यूनिकेशन शब्द का अर्थ है, ऐसा कम्यूनिकेशन जो दूरी पर स्थित स्थान पर हो । इसमें टेलीफोन, टेलीग्राफी और टेलीविजन सम्मिलित है।

डाटा शब्द से आश्य किसी भी रूप में उपलब्ध या भेजी गई ऐसी इंफॉर्मेशन से होता है, जिस पर डाटा की रचना करने वाले और उपयोग करने वाले दोनों ही पक्ष सहमत होते हैं।

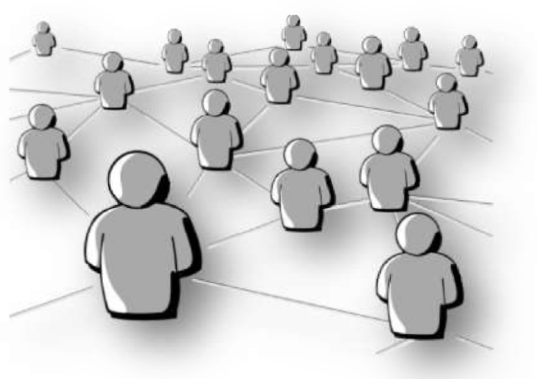
डाटा कम्यूनिकेशन ट्रांसमिशन मीडियम के किसी रूप जैसे वॉयर केबल के माध्यम से दो उपकरणों या डिवाईसेस के मध्य डाटा के आदान–प्रदान को कहते हैं। डाटा कम्यूनिकेशन्स की प्रक्रिया संपन्न होने के लिए यह जरूरी है कि कम्यूनिकेटिंग उपकरण– हार्डवेयर (भौतिक उपकरण) और साफ्टवेयर (प्रोग्राम्स) से मिलकर बने एक कम्यूनिकेशन सिस्टम का हिस्सा हो। किसी डाटा कम्यूनिकेशन सिस्टम का आउटपुट या प्रभावशीलता तीन मूलभूत विशेषताओं – (1) डिलेवरी, (2) एक्यूरेसी या शुद्वता और (3) समयबद्वता पर निर्भर करती है।

1. **डिलेवरी** : सही गंतव्य पर डाटा की डिलेवरी और इसे केवल उसी डिवाईस या यूजर तक पहुॅचना चाहिए जिसके लिए भेजा जा रहा हो।
2. **एक्यूरेसी** : डाटा शुद्वता तथा पूर्णता के साथ डिलेवर होना चाहिए। ट्रांसमिशन के दौरान परिवर्तित हुआ अथवा अशुद्व हुआ डाटा किसी काम का नहीं रहता है।
3. **समयबद्वता** : डाटा की डिलेवरी समयबद्व तरीके से हो जानी चाहिए। विलंब से डिलेवर होने वाले डाटा का कोई उपयोग नहीं रहता है। वीडियो और ऑडियो की स्थिति में, टाईमली डिलेवरी का अर्थ है, डाटा के तैयार होते ही इसे बिना किसी विलंब के उसी क्रम में डिलेवर हो जाना, जिस क्रम में वह जनरेट हुआ है। इस तरह की डिलेवरी को रीयल टाईम ट्रांसमिशन भी कहते है।

1.2 संचार (कम्यूनिकेशन)

जैसा की हम जानते है की आजकल की आधुनिक दुनिया में कंप्यूटर स्टैंड-अलोन सिस्टम के रूप में काम नहीं करता है बल्कि संचार प्रणाली के हिस्से के रूप में काम करता है। कंप्यूटर के अलावा जहाज, विमान, रॉकेट, उपग्रहों और कई अन्य जटिल प्रणालियाँ अपने नेविगेशन सिस्टम के लिए **संचार प्रणाली** (Communication System) पर भरोसा करती हैं। सरल शब्दों में, डाटा कम्युनिकेशन (Data Communication) ट्रांसमिशन मीडियम (Transmission Medium) के माध्यम से दो उपकरणों के बीच डेटा का आदान-प्रदान होता है। डेटा किसी भी संचार माध्यम पर **डिजिटल या एनालॉग सिगनल** (Digital or Analog Signal) के रूप में प्रसारित किया जाता है। कंप्यूटर नेटवर्किंग (Computer Networking) में नेटवर्किंग उपकरणों के बीच भौतिक कनेक्शन केबल मीडिया या वायरलेस मीडिया के माध्यम से स्थापित किया जाता है। डाटा कम्युनिकेशन का सबसे अच्छा उदाहरण **इंटरनेट (Internet)**है अर्थात डेटा संचार दो या दो से अधिक कंप्यूटर केंद्रों के बीच डिजिटल या एनालॉग डेटा सिगनल्स का आदान-प्रदान होता है, जो संचार चैनल से जुड़े हुये होते हैं।

कम्युनिकेशन की विभिन्न कटैगरीज हैं और वे किसी भी समय एक से अधिक हो सकती हैं। क्योंकि जहां विभिन्न प्रकार के कम्युनिकेशन और अलग-अलग संदर्भ और सेटिंग्स होती है, वहां इस शब्द की कई परिभाषाये हैं। लेकिन, चूंकि यह किताब आईटी और कंप्यूटर से संबंधित है, यहां हम डेटा कम्युनिकेशन के बारे में ही बात करेंगे।



चित्र 1.2 : **कम्युनिकेशन चैनल**

1.3 **डेटा संचार** (डेटा कम्युनिकेशन) क्या है?

डेटा कम्युनिकेशन, ट्रांसमिशन मेडियम के माध्यम से दो डिवाइसेस के बीच डेटा का एक्सचेंज (O और 1 कि फॉर्म में) हैं। नेटवर्किंग में कंप्यूटिंग डिवाइसेस के बीच (भोतिक) फिजिकल कनेक्शन केबल मीडिया या वायरलेस मीडिया के माध्यम से स्थापित किया जाता है।

कंप्यूटर नेटवर्क का सबसे अच्छा उदाहरण इंटरनेट है।

कंप्यूटर का उपयोग, इनफॉर्मेशन को उत्पन्न करने के लिए किया जाता है। यह उत्पन्न कि गई इनफॉर्मेशन अपने आप में उपयोगी नहीं है। यह इनफॉर्मेशन सही समय पर सही व्यक्ति को दी जानी चाहिए। अक्सर इनफॉर्मेशन को एक स्थान से दूसरे स्थान पर ट्रांसमिट किया जाना चाहिए। इस प्रोसेस को डाटा कम्युनिकेशन कहा जाता है।

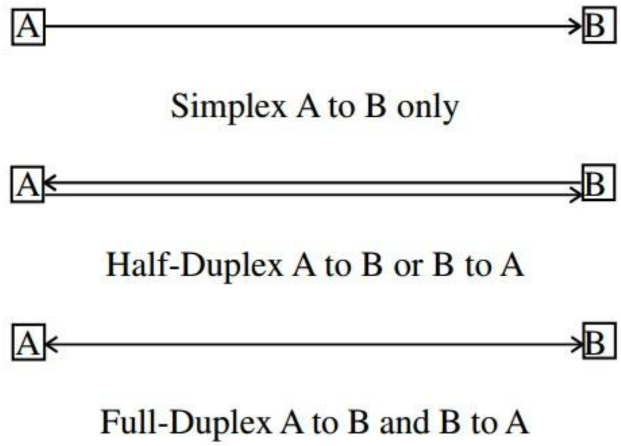
यहां, हम डेटा कम्युनिकेशन में उपयोग किए गए हार्डवेयर, सॉफ़्टवेयर और प्रोसेस कि बात करेंगे। डाटा कम्युनिकेशन एक पॉइंट से दूसरे पॉइंट पर डेटा ट्रांसपोर्टिंग की एक्टिव प्रोसेस है। नेटवर्क एक कम्युनिकेशन सिस्टम हैं, जिन्हे इनफॉर्मेशन को एक ओरिजिन पॉइंट से डेस्टिनेशन पॉइंट तक इनफॉर्मेशन भेजने के लिए डिज़ाइन किया गया है। ध्यान दें कि वे कम्युनिकेशन सिस्टम हैं, कंप्यूटर सिस्टम नहीं।

1.3.1 डाटा कम्युनिकेशन के प्रकार (Types of Data Communication)

1. **सिम्पलेक्स (Simplex)**: सिम्पलेक्स मोड में, कम्युनिकेशन यूनिडायरेक्शनल होता है। केवल एक डिवाइस डेटा संचारित कर सकता है जबकि अन्य डिवाइस केवल डेटा प्राप्त कर सकता है। उदाहरण के लिए, **कीबोर्ड** (Keyboard) और **सीपीयू** (CPU) के बीच संचार एक सिम्पलेक्स ट्रांसमिशन मोड (Simplex Transmission Mode) का पालन करता है। इस मोड में, कीबोर्ड केवल डेटा भेज सकता है और सीपीयू केवल डेटा प्राप्त कर सकता है।

2. **अर्द्ध ड्यूप्लेक्स (Half Duplex)**: अर्द्ध ड्यूप्लेक्स ट्रांसमिशन में, दोनों डिवाइस डेटा संचारित और प्राप्त कर सकते हैं लेकिन एक साथ नहीं। जब एक डिवाइस संचारित होता है, तो अन्य डिवाइस केवल प्राप्त कर सकता है। उदाहरण **वॉकी-टॉकी** (walkie-talkie)।

3. **पूर्ण ड्यूप्लेक्स (Full Duplex)**: पूर्ण डुप्लेक्स मोड में, दोनों कनेक्टेड डिवाइस एक ही समय में डेटा भेज सकते हैं और साथ ही डेटा प्राप्त कर सकते हैं। उदाहरण **टेलीफोन** (Telephone)।



चित्र 1.3 : **कम्युनिकेशन** (**सिम्पलेक्स** , **हाफ डुप्लेक्स** , **फुल डुप्लेक्स**)

डेटा कम्युनिकेशन के पीछे मूलभूत उद्देश्य क्या है?

- डेटा कम्युनिकेशन का उद्देश्य दो पॉइंट के बीच इनफॉर्मेशन का आदान-प्रदान करना है।
- डेटा कम्युनिकेशन के प्रकार
- आम तौर पर डेटा कम्युनिकेशन के दो टाइप माने जाता है-

1) लोकल (Local) – लोकल एरिया नेटवर्क के रूप में,जो एक छोटे एरिया को कवर करता हैं और इसमें सीमित, कम युजर्स कि संख्या होती हैं।
2) ग्लोबल(Global) - यह लंबी दूरी को कवर करता है और इसमें अनलिमिटेड यूजर्स संख्या होती है।

डेटा कम्युनिकेशन प्रणाली का इफेक्टिवनेस तीन विशेषताओं(कैरेक्टरिस्टिक) पर निर्भर करती है

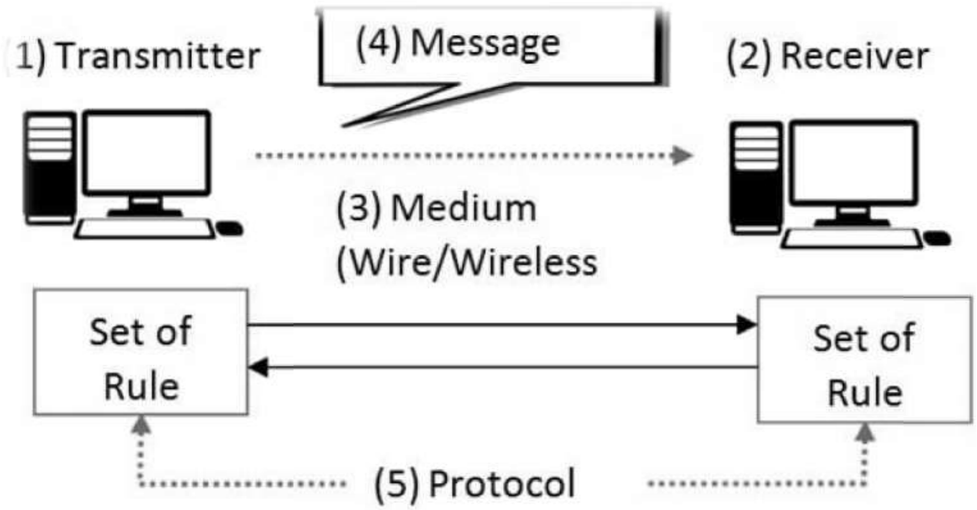
1) डिलीवरी (Delivery): सिस्टम को सही डेस्टिनेशन पर डेटा को डिस्ट्रीब्यूट करना चाहिए। यह डेटा अभिप्रेत डिवाइस या यूजर को ही प्राप्त होना चाहिए।

2) एक्यूरेसी (Accuracy): सिस्टम को सही ढंग से डेटा डिलीवर करना चाहिए। यदि डेटा को ट्रांसमिशन में बदल दिया गया तो वह अनुपयोगी है।

3) टाइम लाइन (Timeliness): सिस्टम को समय पर डेटा डिलीवर करना चाहिए। देर से डिलीवर किया गया डेटा बेकार है। वीडियो, ऑडियो और वॉयस डेटा के मामले में, समय पर डिलीवर करने का मतलब है डेटा जैसे डेटा प्रोडयुस किया जाता हैं वही ऑर्डर में डिस्ट्रीब्यूट, और बिना देरी के।

1.3.2 डेटा संचार के घटक

जब डेटा एक जगह से दूसरी जगह तक ट्रांसमिट होता हैं, तो उसके मुख्य पांच कंपोनेंट्स होते हैं



चित्र 1.4 :डेटा संचार के घटक

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

2) **रिसीवर**(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) **संदेश**(Message):
मैसेज एक ट्रांसमिशन (डेटा) है जिसे कम्युनिकेट किया जाना है। इसमें टेक्स्ट, नंबर्स, इमेज, साउंड, या वीडियो या कुछ भी हो सकते हैं।

4) **माध्यम** (Medium):
ट्रांसमिशन मेडियम एक फिजिकल पाथ है जिसके द्वारा मैसेज सेंडर से रिसीवर तक जाता है। इसमें ट्विस्टेड पेयर वायर, कोएक्सिअल केबल, फाइबर ऑप्टिक केबल, लेजर या रेडियो वेव (स्थलीय या सैटेलाइट माइक्रोवेव) हो सकता हैं।

5) **प्रोटोकॉल** (Protocol):

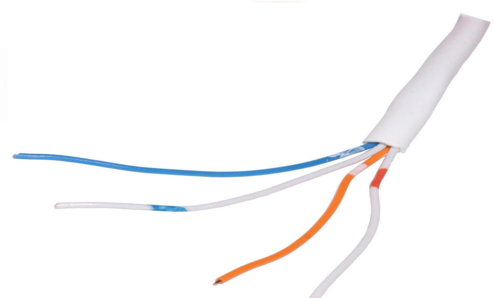
प्रोटोकॉल नियमों का एक ग्रुप है जो डेटा कम्युनिकेशन को कंट्रोल करता है। यह कम्युनिकेशन डिवाइसेस के बीच एक एग्रीमेंट को रिप्रेसेंट है। प्रोटोकॉल के बिना, दो डिवाइस कनेक्ट किए जा सकते हैं, लेकिन कम्युनिकेशन नहीं कर सकते, जैसे जापानी समझने वाले व्यक्ति को हिंदी भाषा समझ में नहीं आएगी।

1.3.3 डेटा संचार के माध्यम (Medium of Data Communication)

1) **वायर्ड मीडिया** (Wired Media):

- *वायर पेयर्स (Wire Pairs):*

वायर पेयर्स सामान्यतः लोकल टेलीफोन कम्युनिकेशन में और कम दूरी के डिजिटल डाटा कम्युनिकेशन के लिए उपयोग कीए जाते हैं। वे आम तौर पर कॉपर से बने होते हैं। इन वायर पेयर्स से डेटा ट्रांसमिशन स्पीड सामान्यतः 100 मीटर की दूरी पर 9600 बिट प्रति सेकंड है।

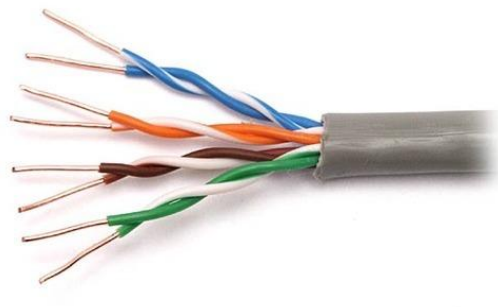


चित्र 1.5 :वायर पेयर्स

- *ट्विस्टेड पेयर्स (Twisted pair):*

ट्विस्टेड पेयर्स वायर टेलीकम्यूनिकेशन के लिए सबसे व्यापक रूप से प्रयोग किया जाने वाला मेडियम है। ट्विस्टेड पेयर्स केबलिंग में कॉपर के तार होते हैं जो पेयर्स में ट्विस्टेड होते हैं। साधारण टेलीफोन वायर में दो ट्विस्टेड पेयर इंसुलेटेड कॉपर वायर शामिल होते हैं।कंप्यूटर नेटवर्किंग केबलिंग (IEEE 802.3 द्वारा डिफाइन वायर्ड ईथरनेट) में कॉपर केबलिंग के 4 पेयर्स होते हैं, जिन्हे साउंड और डाटा ट्रांसमिशन दोनों के लिए उपयोग किया जा सकता है। दो वायर को ट्विस्टेड करने से क्रॉसटॉक और इलेक्ट्रोमैग्नेटिक इंडक्शन को कम करने में मदद मिलती है।

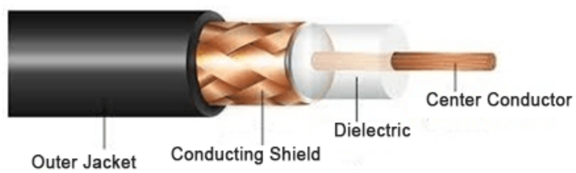
ट्रांसमिशन स्पीड कि रेंज 2 मिलियन बिट प्रति सेकंड से 10 अरब बिट प्रति सेकंड होती है।



चित्र 1.6 :ट्विस्टेड पेयर्स केबल

- *समाक्षीय केबल* (कोएक्सिअल केबल -*Coaxial cable*):

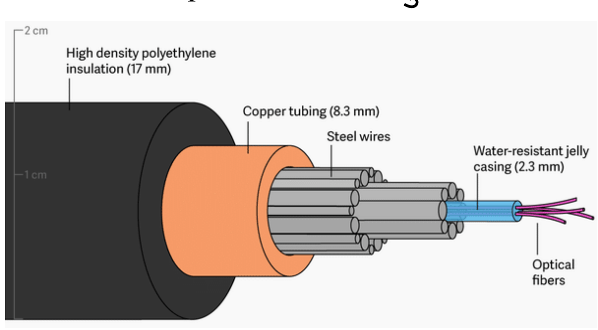
कोएक्सिअल केबल को केबल टेलिविजन सिस्टम, आफिस बिल्डींग और अन्य लोकेल एरिया नेटवर्क साइट के लिए व्यापक रूप से उपयोग किया जाता है।इस केबल में इंसुलेटिंग लेयर में तांबे या एल्यूमीनियम तार शामिल होते हैं। इन्सुलेशन का यह लेयर इंटरफेयरेंस और डिस्टॉर्शन को कम करने में मदद करता हैं।ट्रांसमिशन की स्पीड 200 मिलियन से लेकर 500 मिलियन बिट प्रति सेकंड तक होती है।



चित्र 1.7 :कोएक्सिअल केबल

- *ऑप्टिकल फाइबर* (*Optical fiber*):

ऑप्टिकल फाइबर केबल में एक या अधिक ग्लास फाइबर फिलामेंट हाते हैं, जो प्रोटेक्टिव लेयर से लिपटे होते हैं। वे डेटा को लाइट के पल्स के माध्यम से ट्रांसमिट करते हैं। वे लाइट ट्रांसमिट करते हैं, जो लंबी दूरी तक ट्रैवल कर सकते हैं।फाइबर ऑप्टिक केबल इलेक्ट्रोमैग्नेटिक रेडिएशन से प्रभावित नहीं हाते। इनका ट्रांसमिशन स्पीड बिलियन प्रति बिट की हो सकता है। फाइबर ऑप्टिक्स की ट्रांसमिशन स्पीड twisted-pair केबल्स की तुलना में सैकड़ों गुना तेज है।



चित्र 1.8 :ऑप्टिकल फाइबर

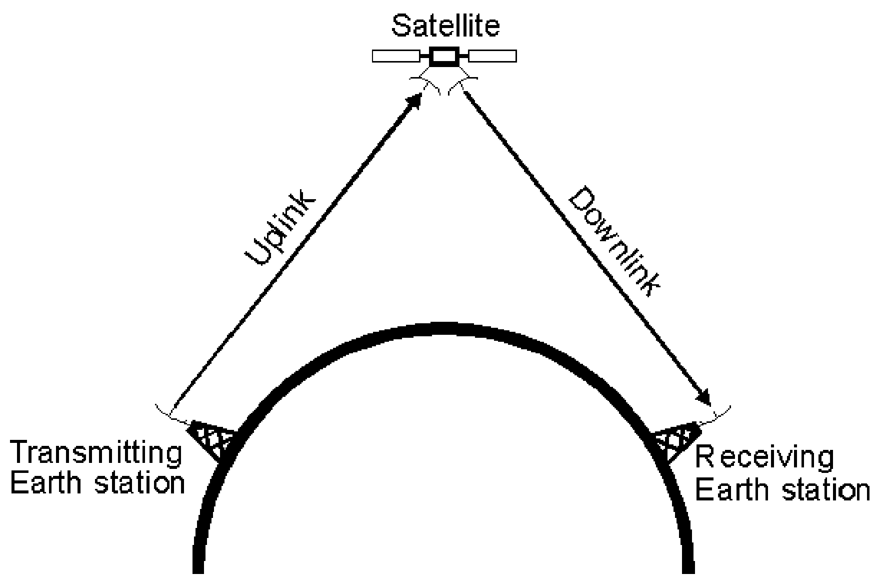
2. वायरलेस मीडिया (Wireless Media) :

i) टेरेस्ट्रियल माइक्रोवेव (Terrestrial microwave):

टेरेस्ट्रियल माइक्रोवेव पृथ्वी के ट्रांसमीटर और रिसीवर का उपयोग करते हैं। यह उपकरण उपग्रह डिश के समान दिखता है। टेरेस्ट्रियल माइक्रोवेव कम गिगाहर्ट्ज़ रेंज का उपयोग करते हैं।रिले स्टेशनों के बीच का डिस्टेंस लगभग 48 किमी (30 मील) हो सकता हैं।माइक्रोवेव एंटेना आमतौर पर इमारतों, टॉवर, पहाड़ियों, और पर्वत चोटियों के पर होते हैं।

ii) *कम्युनिकेशन सैटेलाइट्स* (Communications satellites):

सैटैलाइट माइक्रोवेव रेडियो सिग्नल का उपयोग उनके टेलिकम्यूनिकेशन माध्यम के रूप में करते हैं।उपग्रहों अंतरिक्ष में होते हैं, आमतौर पर 35,400 किमी (22,000 मील) भूमध्य रेखा से ऊपर। ये साउंड, डेटा, और टीवी सिग्नल को प्राप्त करने और रिले करने में सक्षम होते हैं।



चित्र 1.9 :वायरलेस माध्यम

1.4 कम्युनिकेशन्स चैनल (Types Of Communication channel):

Bandwidth एक टर्म हैं जिसे कम्युनिकेशन सिस्टम कि डेटा-हैंडलिंग कैपेसिटी को डिस्क्राइब करने के लिए इस्तेमाल किया जाता हैं।बैंडविड्थ फ्रिक्वेंसी की रेंज है जो डेटा ट्रांसमिशन के लिए उपलब्ध है।

i) नैरोबैंड (Narrowband):

नैरोबैंड बैंड कम डेटा वॉल्यूम को हैंडल करता है। डाटा ट्रांसमिशन रेट 45 से लेकर 300 बॉड तक होता हैं। Narrowband कम्युनिकेशन के लिए कम स्पीड वाले डिवाइस का उपयोग किया जाता हैं।

ii) वौइस्बैंड (Voiceband):

वॉयसबैंड 300 और 9600 बॉड के बीच मध्यम डेटा ट्रांसमिशन वॉल्यूम को हैंडल करता है। इनका मुख्य उपयोग टेलीफोन वॉइस कम्युनिकेशन के लिए किया जाता हैं, इसलिए इसे वॉयसबैंड कहते हैं।

iii) ब्रॉडबैंड (Broadband):

ब्रॉडबैंड बहुत बड़े डेटा वॉल्यम को हैंडल करता है। इनका डेटा ट्रांसमिशन रेट 1 मिलियन बॉड या इससे अधिक होता हैं। हाई स्पीड डेटा एनेलिसिस और सैटैलाइट कम्युनिकेशन, ब्रॉडबैंड कम्युनिकेशन के उदाहरण हैं।

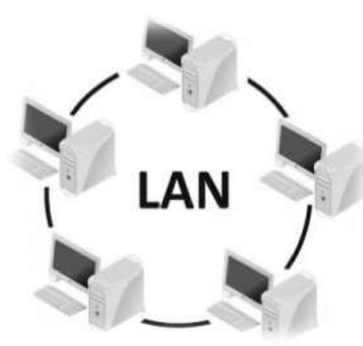
1.5 कंप्यूटर नेटवर्क

नेटवर्क नेटवर्किंग उपकरणों की मदद से एक दूसरे से जुड़े कंप्यूटरों का एक संग्रह होता है। एक नेटवर्क को उसके आकार, स्वामित्व, दूरी और भौतिक संरचना के आधार पर वर्गीकृत किया गया है। विभिन्न प्रकार के नेटवर्क जैसे **लोकल एरिया नेटवर्क** (LAN), **मेट्रोपॉलिटन एरिया नेटवर्क** (MAN) और **वाइड एरिया नेटवर्क** (WAN) हैं, जैसा की नेटवर्क दो या अधिक कंप्यूटर का एक संग्रह है, जो जानकारी और संसाधनों को शेयर करने के लिए एक साथ जुड़े हुए होते हैं। कंप्यूटर नेटवर्क हार्डवेयर और सॉफ्टवेयर का एक संयोजन है जो नेटवर्क पर कंप्यूटर के बीच संचार की अनुमति देता है।

चित्र 1.10 :कंप्यूटर नेटवर्क

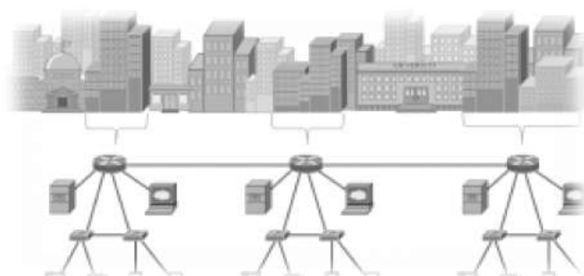
1.5.1 कंप्यूटर नेटवर्क के प्रकार

- **लोकल एरिया नेटवर्क Local Area Network (LAN)** :- एक लोकल एरिया नेटवर्क एक छोटे से क्षेत्र में फैला हुआ होता है। किसी संगठन में कंप्यूटर कनेक्ट करने के लिए LAN का उपयोग किया जा सकता है। लैन पर प्रत्येक कंप्यूटर का अपना सेंट्रल प्रोसेसिंग यूनिट (CPU) होता है, लेकिन वे महंगे डिवाइस जैसे प्रिंटर और मॉडेम को शेयर कर सकते हैं। एक LAN पर कंप्यूटर भी स्वयं के बीच डेटा साझा कर सकते हैं, लैन (LAN) पर डेटा स्थानांतरित करने की दर बहुत तेज है लगभग **10 MBPS** और गीगाबाइट ईथरनेट पर करीब **1 GBPS** तक होती है तथा इसमें 100 से 1000 कंप्यूटर को जोड़ा जा सकता है।



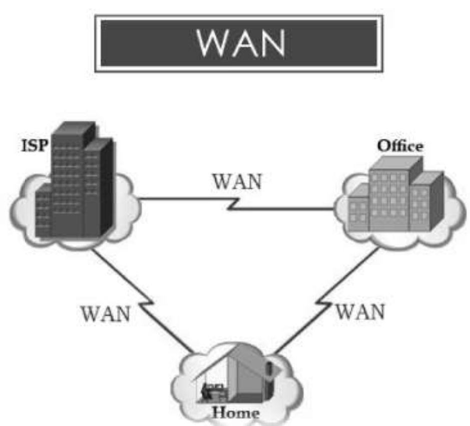
चित्र 1.11 :लोकल एरिया नेटवर्क

- **महानगर एरिया नेटवर्क Metropolitan Area Network (MAN)** :- एक मेट्रोपॉलिटन एरिया नेटवर्क लैन की तुलना में एक बड़ा भौगोलिक क्षेत्र में फैला हुआ होता है। किसी शहर में कंप्यूटरों को कनेक्ट करने के लिए MAN का उपयोग किया जाता है, मैन नेटवर्क जो कई स्विचेस या राउटर से बना होता है जो **फाइबर ऑप्टिक केबल** (Fiber Optic Cable) का उपयोग करके उच्च गति कनेक्शन प्रदान करता है।



चित्र 1.12 : महानगर एरिया नेटवर्क

- **वाइड एरिया नेटवर्क Wide Area Network (WAN)** :- वाइड एरिया नेटवर्क डेटा, आवाज, छवि और वीडियो के लंबे प्रसारण की अनुमति देता है। एक WAN एक MAN नेटवर्क से बड़ा होता है। वैन (WAN) का उपयोग बड़े भौगोलिक क्षेत्रों, जैसे देश, महाद्वीप या संपूर्ण विश्व के डेटा को स्थानांतरित करने के लिए किया जाता है। उदाहरण के लिए, इंटरनेट सबसे बड़ा वैन (WAN) है, कंप्यूटर एक पब्लिक नेटवर्क का उपयोग करते हुए वैन से जुड़े होते हैं, जैसे टेलीफोन लाइन, उपग्रह और लीज्ड लाइन।



चित्र 1.13 : वाइड एरिया नेटवर्क

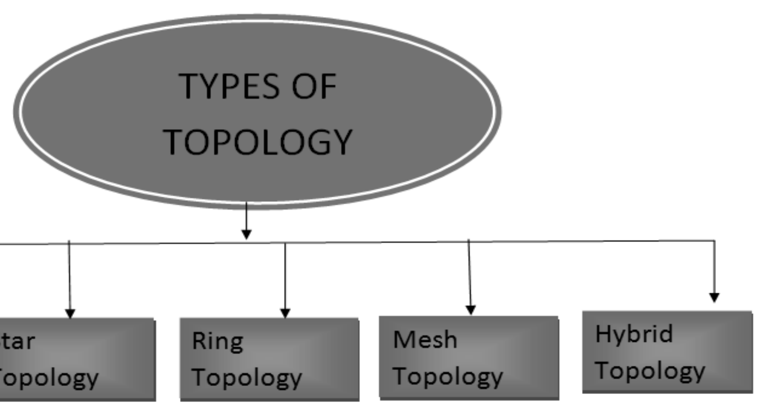
1.6 नेटवर्क टोपोलॉजी

नेटवक टोपोलॉजी कंप्यूटर नेटवर्क बनाने की एक विधि है जो विभिन्न कॉन्फ़िगरेशन को प्रदान करता है जिनका उपयोग नेटवर्क बनाने के लिए किया जाता है। एक नेटवर्क बनाने के लिए कंप्यूटर और अन्य नेटवर्किंग उपकरणों को एक साथ जोड़ने के दौरान, उपयोगकर्ता को संरचना, लेआउट और केबल बिछाने की आवश्यकताओं पर विचार करना होता है। पॉइंट टू पॉइंट कनेक्शन या मल्टीपॉइंट कनेक्शन का उपयोग करके एक नेटवर्क बनाया जा सकता है। एक पॉइंट टू पॉइंट कनेक्शन में, केवल दो डिवाइस एक-दूसरे से जुड़े होते हैं। उपयोगकर्ता एक डेडिकेटेड लाइन से लोकल नेटवर्क से एक रिमोट नेटवर्क पर डेटा स्थानांतरित कर सकते हैं। पॉइंट टू पॉइंट कनेक्शन के उदाहरण हैं माइक्रोवेव, सैटेलाइट, और टेलीविज़न नेटवर्क। मल्टीपॉइंट कनेक्शन में, कई डिवाइस कनेक्शन शेयर करती हैं और इसे मल्टीपॉइंट कनेक्शन के रूप में कहा जाता है।

1.6.1 नेटवर्क टोपोलॉजी परिभाषा

टोपोलॉजी नेटवर्क उपकरणों का एक पैटर्न होता है और जिस तरह से ये डिवाइस कनेक्ट हैं, टोपोलॉजी फिजिकल या लॉजिकल हो सकते हैं। फिजिकल टोपोलॉजी नेटवर्क की वास्तविक भौतिक संरचना को संदर्भित करता है, जबकि एक लॉजिकल टोपोलॉजी उस तरीके को निर्धारित करती है जिसमें डेटा वास्तव में नेटवर्क के माध्यम से एक डिवाइस से अन्य तक पहुंच जाता है विभिन्न प्रकार के टोपोलॉजी इस प्रकार हैं:

नेटवर्क टोपोलॉजी के प्रकार



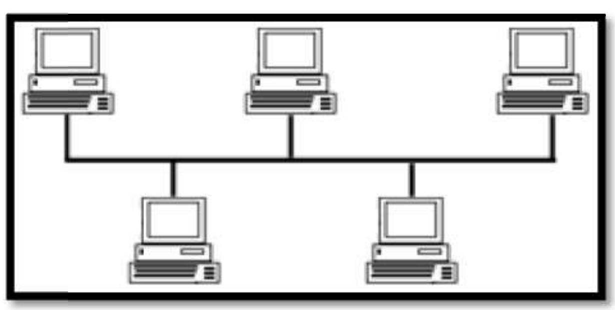
चित्र 1.14 : नेटवर्क टोपोलॉजी के प्रकार

1. **फिजिकल टोपोलॉजी** (Physical Topology) : फिजिकल टोपोलॉजी से हमारा तात्पर्य यह है की यह उपकरणों के भौतिक लेआउट का प्रतिनिधित्व करता है। जैसे की इस नेटवर्क टोपोलॉजी में जुड़े उपकरणों, कनेक्टेड कंप्यूटर और केबल आदि। यह नेटवर्क पर उपकरणों की व्यवस्था और एक दूसरे के साथ संवाद करने के तरीके को भी संदर्भित करता है। पांच मूल भौतिक टोपोलॉजी **बस** (Bus), **स्टार** (Star), **ट्री** (Tree) और **मेश** (Mesh) हैं।

2. **लॉजिकल टोपोलॉजी** (Logical Topology) : लॉजिकल टोपोलॉजी के सहायता से नेटवर्क में डेटा को एक डिवाइस से दूसरे स्थान पर स्थानांतरित किया जाता है, भले ही डिवाइस के बीच भौतिक रूप से कोई संबंध न हो। उदाहरण के लिए, आईबीएम (IBM) के टोकन रिंग एक लॉजिकल **रिंग टोपोलॉजी** (Ring Topology) है।

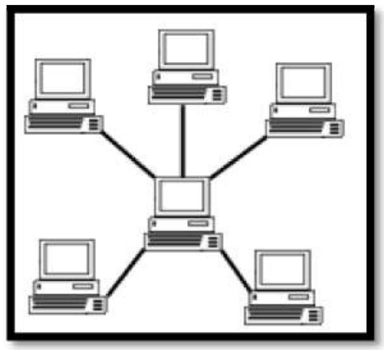
1.6.2 नेटवर्क टोपोलॉजी मुख्य रूप से 6 प्रकार की होती है:

- **बस टोपोलॉजी** (Bus Topology) : बस टोपोलॉजी में, डिवाइस डेटा भेजने और प्राप्त करने के लिए एक सामान्य बैकबोन केबल शेयर करती है। एक **Thick C0-axial** केबल का उपयोग सभी उपकरणों को जोड़ने के लिए किया जाता है। बस टोपोलॉजी एक नेटवर्क में अधिक डिवाइस जोड़ने के लिए **डेज़ी चैन स्कीम** (Daisy Chain Scheme) का उपयोग करती है। डेज़ी चेन स्कीम में, डिवाइस 1 डिवाइस 2 से जुड़ा होता है, डिवाइस 2 डिवाइस 3 से जुड़ा है, डिवाइस 3 डिवाइस 4 से और डिवाइस 4 डिवाइस 5 से जुड़ा है। पहले और अंतिम डिवाइस टर्मिनेटर (50-ओम रेसिस्टर) से जुड़े होते हैं।



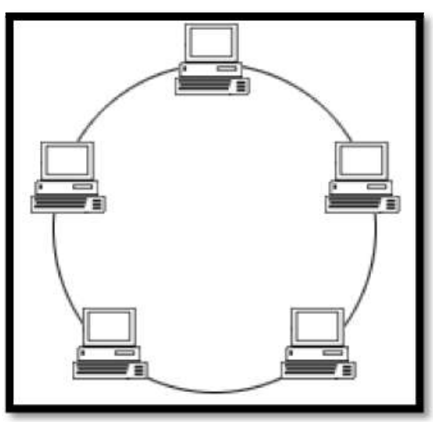
चित्र 1.15 : बस टोपोलॉजी

- **स्टार टोपोलॉजी** (Star Topology) : स्टार टोपोलॉजी में, कई डिवाइस एक केंद्रीय कनेक्शन बिंदु से जुड़े होते हैं जिन्हें हब (Hub) या स्विच (Switch) कहा जाता है। उपकरणों को तांबे केबल या फाइबर ऑप्टिक केबल्स का उपयोग करके स्विच से जोड़ा जाता है। स्टार नेटवर्क विभिन्न उपयोगकर्ताओं के बीच जानकारी शेयर करने के लिए एक लागत प्रभावी (Cost Effective) तरीका प्रदान करता हैं।स्टार टोपोलॉजी का उपयोग एयरलाइन आरक्षण काउंटर और छोटे व्यवसाय कार्यालयों में किया जा सकता है, जहां कर्मचारी सामान्य अनुप्रयोगों और फ़ाइलों तक एक्सेस के लिए इसका उपयोग करते हैं।



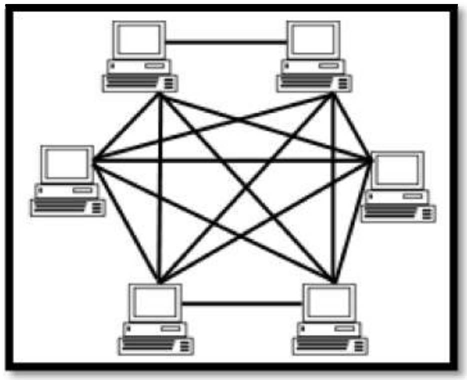
चित्र 1.16 : स्टार टोपोलॉजी

- **रिंग टोपोलॉजी** (Ring Topology) : रिंग टोपोलॉजी में, प्रत्येक डिवाइस एक सर्कुलर स्ट्रक्चर बनाकर अन्य डिवाइस से जुड़े होते है। डेटा का प्रवाह केवल एक दिशा, क्लॉक वाइज या एंटी क्लॉक वाइज में होता है, रिंग टोपोलॉजी में प्रत्येक डिवाइस एक रिपीटर (Repeater) के रूप में कार्य करता है यह सिगनल को बढ़ाता है और इसे अगले डिवाइस पर प्रसारित करता है।



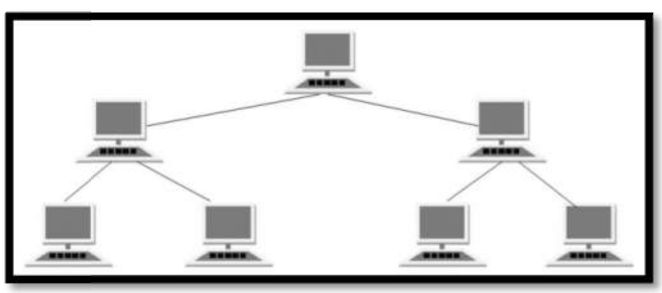
चित्र 1.17 : रिंग टोपोलॉजी

- **मेश टोपोलॉजी** (Mesh Topology) : मेश टोपोलॉजी में, प्रत्येक उपकरण हर दूसरे डिवाइस से जुड़ा होता है। एक डिवाइस नेटवर्क में सभी उपकरणों को डेटा भेज सकता है। डिवाइस द्वारा भेजे गए डेटा डेस्टिनेशन तक पहुंचने के लिए किसी भी संभावित पथ (Possible Paths) ले सकता है।



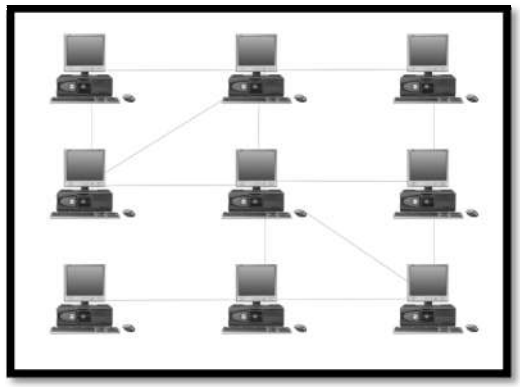
चित्र 1.18 : मेश टोपोलॉजी

- **ट्री टोपोलॉजी** (Tree Topology) : एक ट्री टोपोलॉजी लीनियर बस और स्टार टोपोलॉजी की विशेषताओं को जोड़ती है। ट्री टोपोलॉजी में, स्टार नेटवर्क का एक समूह लीनियर बस बैकबोन से जुड़ा हुआ होता है। ट्री टोपोलॉजी उपयोगकर्ता को आवश्यकताओं के आधार पर मौजूदा नेटवर्क को विस्तारित और कॉन्फ़िगर करने में सक्षम बनाता है। **Twisted Pair Cable** आमतौर पर ट्री टोपोलॉजी द्वारा उपयोग किया जाता है, ट्री टोपोलॉजी को **Hierarchical Structure** भी कहा जाता है।



चित्र 1.19 : ट्री टोपोलॉजी

- **हाइब्रिड टोपोलॉजी** (Hybrid Topology) : हाइब्रिड टोपोलॉजी विभिन्न नेटवर्क टोपोलॉजी का एक संयोजन होता है। यह एक विशेष टोपोलॉजी के रूप में भी जाना जाता है। यह टोपोलॉजी कॉर्पोरेट कार्यालयों के लिए अपने आंतरिक LANs को एक साथ जोड़ने के लिए उपयोगी है, जबकि **वाइड एरिया नेटवर्क** (WAN) के माध्यम से बाहरी नेटवर्क को जोड़ते हैं।



चित्र 1.20 : हाइब्रिड टोपोलॉजी

1.7 ट्रांसमिशन :

डाटा को एनालॉग या डिजिटल रूप में ट्रांसमिट किया जा सकता है। एनालॉग और डिजिटल, दोनो ही प्रकार के सिग्नल्स यथोचित **ट्रांसमिशन** माध्यम पर ट्रांसमिट किए जा सकते है। इन सिग्नल्स को किस रूप में विश्लेि ात किया जाना है, यह **ट्रांसमिशन** सिस्टम का कार्य होता है। तालिका 2.1 में डाटा **ट्रांसमिशन** की विधियों का सारांश प्रस्तुत किया गया है।

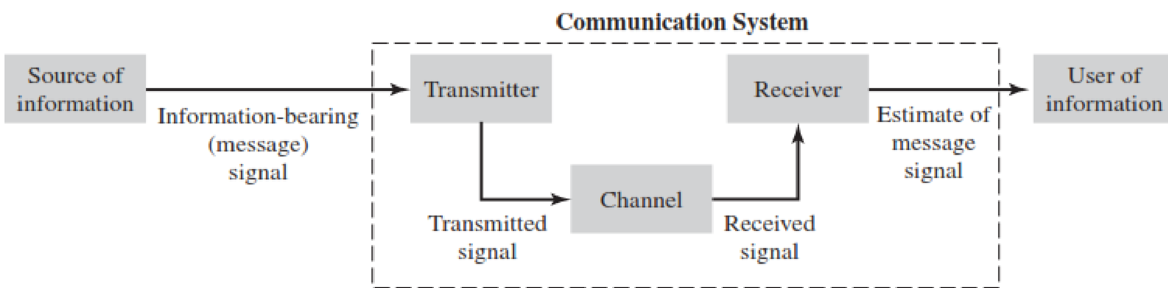
	एनालॉग सिग्नल	**डिजिटल सिग्नल**
माध्यम	सूचना विद्युत स्पंदनों के ज़रिए आती है।	सूचना बाइनरी फॉर्मेट(0 और 1) में बदली जाती है।
गुणवत्ता	डेटा के अनुवाद या पुनः उपयोग पर क्वालिटी डैमेज का खतरा रहता है।	डिजिटल में यह खतरा नहीं होता।
डेटा का आकार	डेटा के आकार की एक लिमिट होती है या निर्धारित समय तक ही ट्रांसमीट किया जा सकता है।	आसानी से फेरबदल किया जा सकता है व इसमे ज्यादा विकल्प होते हैं।
उपकरण	एनालॉग तकनीक सस्ती मानी जाती है।	डिजिटल उपकरण एनालॉग की तुलना में महँगे होते हैं।
त्रुटियां(errors)	एनालॉग संचार में गड़बड़ी संचार में त्रुटियां उत्पन्न करती है।	त्रुटियों को व्यक्त करने के लिए हम प्रतीकों को प्रतिस्थापित, डालने या हटाने में सक्षम होते हैं।
बैंडविड्थ(bandwidth)	एनालॉग सिग्नल प्रोसेसिंग कम बैंडविड्थ का उपभोग करती है।	डिजिटल सिग्नल प्रोसेसिंग ज्यादा बैंडविड्थ का उपभोग करती है।
क्षमता	एनालॉग ऑडियो कैसेट की क्षमता 700-1.1 एमबी होती है।	नियमित सीडी की क्षमता 700एमबी तक होती है।
सुरक्षा	एनालॉग बाहर के प्रभाव से खुदको नही बचा पाता।	संदेश के एन्क्रिप्टेड होने से यह एक सुरक्षित माध्यम है
इस्तेमाल	केवल एनालॉग डिवाइस में ही इसका इस्तेमाल किया जा सकता है।	डिजिटल सिंगनल्स का उपयोग कंप्यूटिंग और डिजिटल इलेक्ट्रॉनिक्स के लिए सबसे ज्यादा उपयुक्त है।

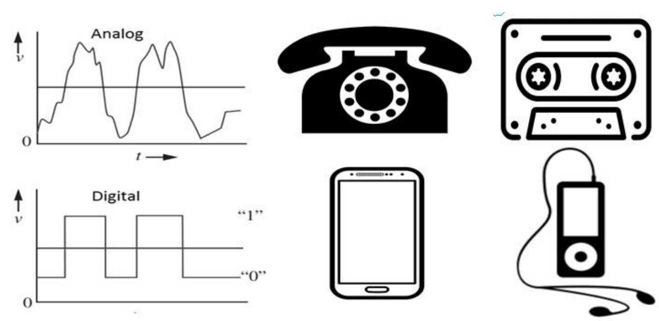
टेबल: एनालॉग और डिजिटल ट्रांसमिशन

एनालॉग **ट्रांसमिशन**, एनालॉग सिग्नल्स को ट्रांसमिट करने का एक ऐसा तरीका है, जिसमें उसकी सामग्री या वेल्यू पर विचार नहीं किया जाता है, अर्थात् सिग्नल्स एनालॉग डाटा (उदाहरणार्थ – ध्वनि) या डिजिटल डाटा (उदाहरणार्थ, मॉडेम के माध्यम से जाने वाला बायनरी डाटा) प्रदर्शित कर सकते हैं। दोनों ही परिस्थितियों में, एनालॉग सिग्नल कुछ दूरी तय करने के उपरांत कमजोर (क्षीण) हो जाएँगे। अधिक लंबी दूरी तय करने के लिए एनालॉग सिस्टम में एम्प्लीफायर शोरगुल (नॉईस) के तत्वों को भी बढ़ा देता है। लंबी दूरियॉ प्राप्त करने के लिए निचले स्तरों पर एम्प्लीफायर्स लगाने के साथ ही सिग्नल में उत्तरोत्तर विकृति बढ़ति जाती है। ध्वनि जैसे एनालॉग डाटा में बहुत–सी

विकृतियों को सहन किया जा सकता है और डाटा बोधगम्य बना रहता है। डिजिटल डाटा के लिए ये निचले स्तर के एम्प्लीफायर्स ऍरर उत्पन्न करते हैं।

डिजिटल **ट्रांसमिशन** का संबंध सिग्नल की वेन्यू से होता है। किसी डिजिटल सिग्नल को कमजोर पड़ने तथा डाटा की अखण्डता को बिगाड़ने वाले नॉईस और अन्य हानिकारक तत्वों द्वारा प्रभावित किए जाने के पूर्व सीमित दूरी तक ही ट्रांसमिट किया जा सकता है। अधिक दूरियों तक सिग्नल भेजने के लिए रिपीटर्स प्रयुक्त किए जाते हैं। रिपीटर डिजिटल सिग्नल को प्राप्त करता है, 1s और 0s के पैटर्न को रिकवर करता है। तथा नए सिग्नल का पुनः प्रसारण करता है। इस प्रकार सिग्नल के कमजोर पड़ने (एटेन्यूएशन) पर नियंत्रण पाया जाता है।





चित्र 1.21 : एनालॉग एवं डिजिटल सिगनेलिंग

इस विधि को एनालॉग सिग्नल के साथ भी प्रयुक्त किया ला सकता है, यदि यह मान लिया जाए कि सिग्नल डिजिटल डाटा को ला रहा है। **ट्रांसमिशन** सिस्टम में यथोचित दूरियों पर एम्प्लीफायर्स के स्थान पर रिपीटर्स होते हैं। रिपीटर एनालॉग सिग्नल से डिजिटल डाटा रिकवर करता है और एक नया, स्वच्छ एनालॉग सिग्नल निर्मित करता है। इस प्रकार नॉईस एकत्र नहीं हो पाता है।

सामान्यतः यह प्रश्न उठता है कि **ट्रांसमिशन** की उपयुक्त विधि कौन–सी है। इसका उत्तर टेलीकम्यूनिकेशन उद्योग द्वारा समझा जा सकता है, जिसके ग्राहक डिजिटल हैं। लंबी दूरियों की टेलीकम्यूनिकेशन सुविधाओं और भवन की भीतरी सेवा, दोनों ही में डिजिटल **ट्रांसमिशन** का प्रवेश हो

गया है तथा जहाँ कहीं भी संभव है, डिजिटल सिग्नलिंग तकनीकें पहुँचती जा रही हैं। इसके सर्वाधिक महत्वपूर्ण कारण निम्नानुसार हैं –

1. **डिजिटल टेक्नोलॉजी** : लार्ज स्केल इंटीग्रेशन (LSI) और वेरीलार्ज स्केल इंटीग्रेशन (VLSI) टेक्नोलॉजी के प्रवेश के परिणामस्वरूप, डिजिटल सर्किटरी की लागत और आकार में निरंतर कमी आती जा रही है। एनालॉग उपकरण ऐसी गिरावट नहीं दर्शा रहे हैं।
2. **डाटा इंटीग्रिटी** : एम्प्लीफायर्स के स्थान पर रिपीटर्स के उपयोग के माध्यम से नॉईस और सिग्नल संबंधी इन्य क्षतियों का प्रभाव एकत्रित नहीं हो पाता है। इस प्रकार डिजिटल माधयमों द्वारा कम गुणवत्ता वाली लाईंस पर भी डाटा की इंटीग्रिटी बनाए रखते हुए उसे लंबी दूरियों तक भेजा जाना संभव हो पाया है।
3. **क्षमता का पूर्ण उपयोग** : सैटेलाईट चैपल्स और ऑप्टिकल फाईबर से बनने वाले अत्यंत उच्च बैंडविड्थ के **ट्रांसमिशन** लिंक्स का निर्माण करना कम खर्चीला होता जा रहा है। क्षमता के ऐसे प्रभावी उपयोग के लिए उच्च स्तरीय मल्टीप्लेक्सिंग की आवश्यकता होती है तथा इसे एनालॉग (फ्रीक्वेंसी विभाजन) विधियों के स्थान पर डिजिटल (टाईम विभाजन) तकनीक द्वारा सरलतापूर्वक व कम लागत में प्राप्त किया जा सकता है।
4. **सुरक्षा और नीजता** : एनक्रिप्शन विधि को डिजिटल डाटा और डिजीटाईज्ड किए गए एनालॉग डाटा में तत्काल ही प्रयुक्त किया जा सकता है।
5. **इंटीग्रेशन** : एनालॉग और डिजिटल दोनों ही डाटा को डिजिटल रूप में विष्लेषित किए जाने पर सभी सिग्नल्स एक समान स्वरूप में हो जाते हैं और इनके साथ एक समान रूप से व्यवहार किया जा सकता है। इस प्रकार ध्वनि, विडियो और डिजिटल डाटा को एकीकृत करते हुए बड़े स्तर की मितव्ययिता और सुविधाएँ प्राप्त की जा सकती है।

एनालॉग **ट्रांसमिशन** की तुलना में डिजिटल **ट्रांसमिशन** के लाभ :

1. सर्किट्स और उपकरण का अधिक कार्यकुशल उपयोग करने के लिए डाटा (ध्वनि, संगीत और इमेजेस) को डिजिटल **ट्रांसमिशन** में शामिल किया जा सकता है।
2. डिजिटल **ट्रांसमिशन** में वर्तमान टेलीफोन लाइंस का उपयोग करते हुए उच्च डाटा रेट्स प्राप्त करना संभव होता है।
3. एनालॉग **ट्रांसमिशन** भी तुलना में डिजिटल **ट्रांसमिशन** बहुत सस्ता पड़ता है।
4. एनालॉग की तुलना में डिजिटल **ट्रांसमिशन** का रखरखाव सरल होता है। ट्रांसमिट की गई बिट या तो अचूकता से मिलती है या प्राप्त ही नहीं होती है। इससे समस्याओं का पता लगाना सरल हो जाता है।

1.7.1 कम्यूनिकेशन चैनल :

जब हमें एक PC से दूसरे PC तक मैसेज/डाटा ट्रांसमिट किए जाने की जरूरत होती है, तो हम सर्वप्रथम डाटा को विद्युत/विद्युत–चुंबकिय ऊर्जा में बदल लेते हैं। इसके लिए हम कुछ रूपांतरण तकनीकों की सहायता लेते हैं। इसके बाद इसे किसी कम्यूनिकेशन चैनल से होकर गुजारा जाता है। यह चैनल, इलेक्ट्रिक वायर्स के स्वरूप में अथवा उच्च ऊर्जा वाली विद्युत–चुंबकीय ऊर्जा को रिसीवर एण्ड पर ट्रांसमिट करता है, जो इसे मैसेज देने के लिए फिर से रूपांतरित कर देता है। कम्यूनिकेशन चैनल, विद्युत चुंबकिय ऊर्जा को एक स्त्रोत से एक या अधिक गंतव्य बिंदुओं तक पहुँचाने का मार्ग उपलब्ध कराता है। यह एक ऐसा मार्ग होता है, जिस पर डाटा को दूरवर्ती उपकरणों के मध्य हस्तांतरित किया जाता है।

एक आदर्श कम्यूनिकेशन चैनल की विशे ामाएँ :

एक आदर्श कम्यूनिकेशन चैनल में निम्नलिखित विशे ाताएँ होनी चाहिए –

1. इसमें न्यूनतम लागत पर ट्रांसमीटर से रिसीवर तक विद्युत–चुंबकीय ऊर्जा की अधिकतम मात्रा भेजने की क्षमता होना चाहिए।
2. इसे मार्ग में अधिक मात्रा में नॉईस ाामिल नहीं करना चाहिए। जिससे कि रिसीवर, मैसेज को समझने अथवा सही फॉर्मेट में रिसीव करने में सक्षम हो सके।
3. ट्रांसमीटर, जहाँ सेंडर स्थित है और रिसीवर, जहाँ सिग्नल प्राप्त किया जाना है, के मध्य दूरी संबंधी कोई सीमा नहीं होनी चाहिए।

कम्यूनिकेशन चैनल को दो मुख्य रूपों में विश्ले ाित किया जा सकता हैं –

1 फ्रीक्वेंसी डोमेन।
2 टाईम डोमेन।

1. **फ्रीक्वेंसी डोमेन का विश्ले ाण :** चित्र फ्रीक्वेंसी डोमेन में चैनल के चारित्रिक निरूपण में प्रयुक्त की जाने वाली विधि दर्शाता है। चैनल के लिए f साईकल्स प्रति सेकंड (हट्र्ज) की फ्रीक्वेंसी से दौलन करने वाला साइनुसॉइडल सिग्नल $x(t)=\cos(2\pi f t)$ लागू किया जाला है। चैनल का आऊटपुट $y(t)$सामान्यतः समान फ्रीक्वेंसी परंतु भिन्न एम्प्लीट्यूड और फेज वाल साइनुसॉइडल (तरंग वाला) सिग्नल से बना होता है।

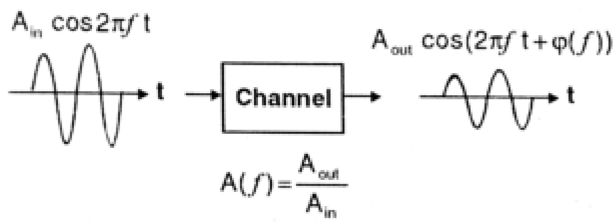
$$y(t) = A(f)\cos(2\pi f t + \varphi(f)) = A(f)\cos(2\pi f(t - \tau(f)))$$

चैनल का विश्ले ाण इनपुट साइनुसॉइडल सिग्नल पर इसके प्रभाव द्वारा तय किया जाता है। इसका पहला प्रभाव तो साइनुसॉइडल सिग्नल का एटेन्यूएशन (कमजोर पड़ना) होता है। यह प्रभाव एम्प्लीट्यूड–रिस्पांस फंक्शन $A(f)$ से स्प ट होता है, जो फ्रीक्वेंसी f पर साइनुसॉइडस के इनपुट एम्प्लीट्यूड हेतु आऊटपुट एम्प्लीट्यूड के अनुपात के रूप में दर्शाया जाता है।

इनपुट साइनुसॉइड की तुलना में आऊटपुट साइनुसॉइड में फेज शिफ्ट $\varphi(f)$ दूसरा प्रभाव होता है। आमतौर पर एम्प्लीट्यूड रिस्पांस और फेज शिफ्ट दोनों ही साइनुसॉइड की फ्रीक्वेंसी f पर निर्भर होते है।

किसी सिग्नल के एटेन्यूएशन को सिस्टम से भेजे जाने के दौरान, सिग्नल की ाक्ति में आने वाली कमी या उसमें हुई क्षति के रूप में परिभाि ात किया जाता है। एटेन्यूएशन को सामान्यतः dB में व्यक्त किया जाता है –

एम्प्लीट्यूड के साइनुसॉइडल सिग्नल का पावर है $A^2/2$ है। इस प्रकार चैनल में एटेन्यूएशन चित्र म $P_{in}/P_{out} = A^2_{in}/A^2_{out} = 1/A^2(f)$ दिया जाता है।



एम्प्लीट्यूड रिस्पांस फंक्शन $A(f)$ को फ्रीक्वेंसीज की उप विंडों के दर्शाए जाने के रूप में देखा जा सकता है, जिनसे चैनल गुजरने वाला है। चैनल की बैंडविड्थ W] फ्रीक्वेंसीज की उस विंडो की विड्थ का पैमाना होती है, जो चैनल से होकर ट्रांसमिट होती है। एम्प्लीट्यूड रिस्पांस फंक्शन का एक अन्य आदर्श रूप "बैंड पास" चैनल है, जो निचले स्तर की फ्रीक्वेंसीज के स्थान पर $f1$ से $f2$ रेंज में फ्रीक्वेंसीज को भेजला है। ऐसे चैनल की बैंडविड्थ $W= f2- f1$ होती है।

कम्यूनिकेशन सिस्टम, इनपुट सिग्नल के फ्रीक्वेंसी कम्पोनेंट्स को मॉडिफाय अथवा एम्प्लीफय करने के लिए इलेक्ट्रॉनिक सर्किट्स का उपयोग करते हैं। जब सर्किट्स इस रूप में प्रयुक्त किए जाते हैं, तो फिल्टर्स कहलाते हैं।

2. **टाईम डोमेन का विश्ले ाण** : चित्र , कम्यूनिकेशन चैनल के टाईम डोमेंन का विश्ले ाण दर्शाता है। चैनल को टाईम **जत्र0** पर एक अत्यंत ही संकुचित पल्स दी जाती है। कुछ प्रसार समय के उपरांत, पल्स से जुड़ी ऊर्जा चैनल आऊटपुट पर सिग्नल **h(t)** के रूप में दृि टगोचर होती है। किसी दिए हुए माध्यम में प्रसार की गति, प्रकाश की गति से अधिक नहीं हो सकती है। सिग्नल **h(t)**चैनल कर इम्पल्स रिस्पांस कहलाता है। अपरिवर्तनशील आऊटपुट पल्स **h(t)** समय में फैलता है। पल्स की विड्थ बताती है कि आऊटपुट कितनी तेजी से इनपुट का अनुसरण करता है और इसी से यह स्प ट होता है कि चैनल पर पल्स को कितनी तेजी से ट्रांसमिट किया जा सकता है।

चैनल की क्षमता : किन्हीं दी हुई परिस्थितियों का अनुपालन करते हुए, एक प्रदत्त कम्यूनिकेशन मार्ग अथवा चैनल पर डाटा को ट्रांसमिट किए जा सकने की अधिकतम दर, चैनल केपेसिटी या चैनल क्षमता के रूप में जानी जाती है।

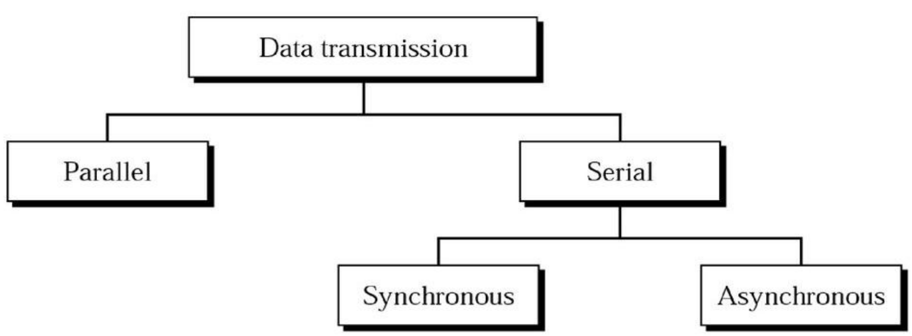
यहाँ चार ऐसी अवधारणाएँ होती हैं, जिन्हें हम एक–दूसरे से संबद्ध करने का प्रयास करते हैं।

1. **डाटा रेट :** बिट्स प्रति सेकंड में वह दर, जिस पर डाटा को कम्यूनिकेट किया जा सके।
2. **बैंडविड्थ :** यह ट्रांसमिट किए गए सिग्नल की बैंडविड्थ होती है, जो ट्रांसमीटर और **ट्रांसमिशन** माध्यम की प्रकृति द्वारा निर्धारित की जाती है तथा सायकल्स प्रति सेकंड अथवा हर्ट्ज में दर्शायी जाती है।
3. **नॉईस :** यह कम्यूनिकेशनस मार्ग पर नॉईस का औसत स्तर होता है।
4. **ऍरर रेट :** यह ऍरर की वह दर होती है, जहाँ 0 ट्रांसमिट किया जाए और 1 प्राप्त हो अथवा 1 ट्रांसमिट करने पर 0 मिले तो वहाँ ऍरर उत्पन्न होता है।

1.7.2 ट्रांसमिशन मोड़ :

किसी लिंक के आरपार बायनरी डाटा का **ट्रांसमिशन**, समानांतर या श्रृंखलाबद्ध मोड में सम्पन्न किया जा सकता है। समानांतर मोड में, प्रत्येक क्लॉक टिक के साथ मल्टीपल बिट्स भेजी जाती हैं। श्रृंखलाबद्ध मोड में, प्रत्येक क्लॉक के साथ 1 बिट भेजी जाती है। जहाँ समानांतर डाटा भेजने का एक ही तरीका है, वहीं श्रृंखलाबद्ध **ट्रांसमिशन** की दो उप श्रेणियाँ हैं :

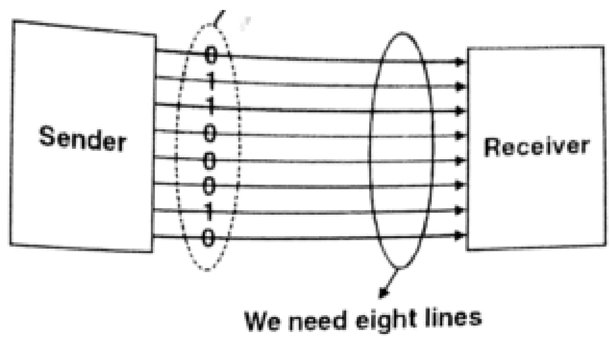
(1) सिंक्रोनस और (2) एसिंक्रोनस।



चित्र 1.22 : डाटा ट्रांसमिशन

बायनरी डाटा का **ट्रांसमिशन** में डाटा **ट्रांसमिशन** हार्डवेअर में प्रयुक्त की जाने वाली सर्किट डिजाइन के अनुसार भी सम्पन्न किया जा सकता है। इस आधार पर इसकी तीन उपश्रेणियॉ हैं – सिम्प्लेक्स, हाफ डुप्लेक्स और फुल डुप्लेक्स ।

1. **समानांतर (पेरेलल) ट्रांसमिशन** : 1 और 0 से बने बायनरी डाटा को प्रत्येक बिट्स के समूहों में व्यवस्थित किया जा सकता है। कम्प्यूटर्स डाटा को बिट्स के समूहों में उत्पन्न और उपभोग करते हैं। समूहबद्ध या ग्रुपिंग करते हुए, हम एक बार में 1 के स्थान पर विट्स डाटा भेज सकते हैं। यह समानांतर या पेरेलल **ट्रांसमिशन** कहलाता है।



चित्र 1.23 : पैरेलल ट्रांसमिशन (8 बिट एक साथ भेजी गई)

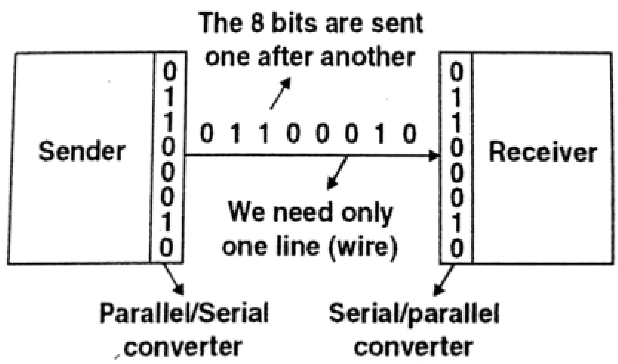
लाभ :

ट्रांसफर की उच्च गति : गति ही समानांतर **ट्रांसमिशन** का लाभ है। श्रृंखलाबद्ध **ट्रांसमिशन** की अपेक्षा समानांतर **ट्रांसमिशन** में ट्रांसफर की गति को n फेक्टर द्वारा बढ़ा सकते है।

हानियॉ :

1. **अत्यंत महंगा :** समानांतर **ट्रांसमिशन** को केवल डाटा स्ट्रीम ट्रांसमिट करने भर के लिए ही द कम्यूनिकेशन लाइन्स की आवश्यकता होती है और यह बहुत ही महंगा पड़ता है।
2. **सीमित दूरियॉ :** महंगा होने की वजह से, आम तौर पर समानांतर **ट्रांसमिशन**, अल्प दूरियों के लिए ही सीमित हो जाता है।

2. **श्रृंखलाबद्ध (सिरीयल) ट्रांसमिशन :** श्रृंखलाबद्ध **ट्रांसमिशन** में एक बिट दूसरी का अनुसरण करती है, इसलिए कम्यूनिकेट कर रही दो डिवाइसेज के मध्य डाटा ट्रांसमिट करने के लिए हमें द के स्थान पर केवल एक ही कम्यूनिकेशन चैनल की आवश्यकता होती है (चित्र 1.24)



चित्र 1.24: सीरियल ट्रांसमिशन

लाभ :

ट्रांसमिशन की लागत में कमी होना : समानांतर **ट्रांसमिशन** की तुलना में श्रृंखलाबद्ध **ट्रांसमिशन** का लाभ यह है कि केवल एक ही कम्यूनिकेशन चैनल होने की वजह से श्रृंखलाबद्ध **ट्रांसमिशन** की लागत समानांतर की तुलना में n फेक्टर द्वारा कम हो जाती है।

हानियॉ :

1. **धीमी ट्रांसफर गति** : चूंकि डिवाइसेज के अन्तर्गत कम्यूनिकेशन समानांतर होता है, इसलिए सेंडर व लाइन (समानांतर से श्रृंखलाबद्ध) के मध्य और लाइन व रिसीवर (श्रृंखलाबद्ध से समानांतर) के मध्य, इंटरफेस पर कन्वर्शन डिवाइसेज की आवश्यकता होती है।

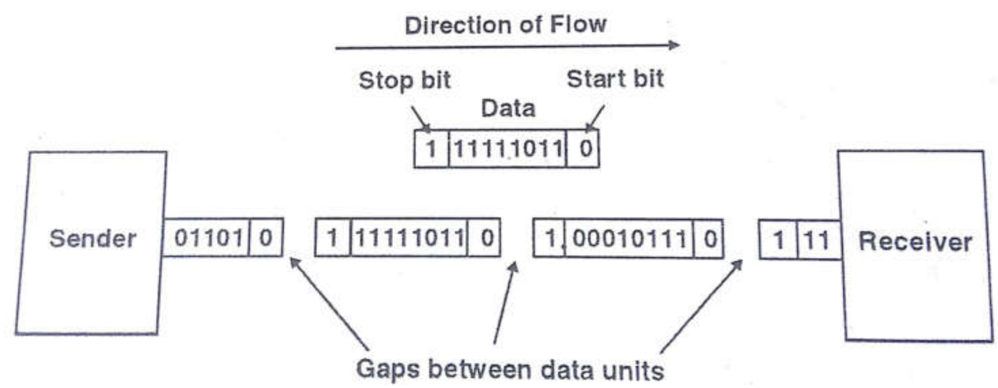
1.7.3 श्रृंखलाबद्ध ट्रांसमिशन के प्रकार :

यह दो में से एक प्रकार से सम्पन्न होता है – एसिंक्रनस अथवा सिंक्रोनस

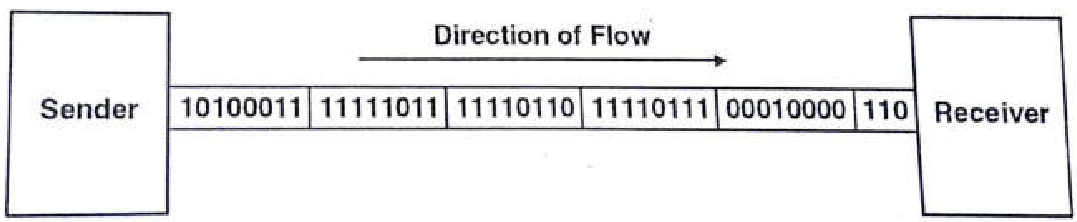
1. **एसिंक्रोनस ट्रांसमिशन** : इसे एसिंक्रोनस **ट्रांसमिशन** इससिलिए कहा जाता है, क्योंकि इसमें सिग्नल की टाइमिंग महत्वपूर्ण नहीं होती है। अत : इन्फॉर्मेशन को पैटर्न्स के तरीकों से प्राप्त और ट्रांसलेटेड किया जाता है। जब तक इन पैटर्न्स को प्रयुक्त किया जाता है, रिसीविंग डिवाइस जिस क्रम में उसे भेजा जा रहा है उस क्रम के बारे में चिंता किए बिना ही इन्फॉर्मेशन को पुनः प्राप्त (रिट्राइव) कर सकता है।

2. **सिंक्रोनस ट्रांसमिशन** : यहॉ बिट स्ट्रीम को ऐसी लंबी फ्रेम्स में समूहबद्ध किया जाता है, जिनमें मल्टीपल बाइट्स हो सकती हैं। प्रत्येक बाइट को **ट्रांसमिशन** लिंक में इसके व अगली बाइट के मध्य, अंतराल के बिना समाहित किया जाता है। डिकोडिंग कार्य के लिए बिट स्ट्रीम को बाइट्स में पृथक–पृथक किया जाना रिसीवर पर छोड़ दिया जाता है।

दूसरे   ाब्दों में, डाटा को 1s और 0s की अटूट स्ट्रिंग के रूप में ट्रांसमिट किया जाता है और रिसीवर उस स्ट्रिंग को बाइट्स या कैरेक्टर्स में अलग करता है, उसे इन्फॉर्मेशन के पुनः निर्माण की आवश्यकता होती है।



चित्र : असिंक्रोनोस ट्रांसमिशन



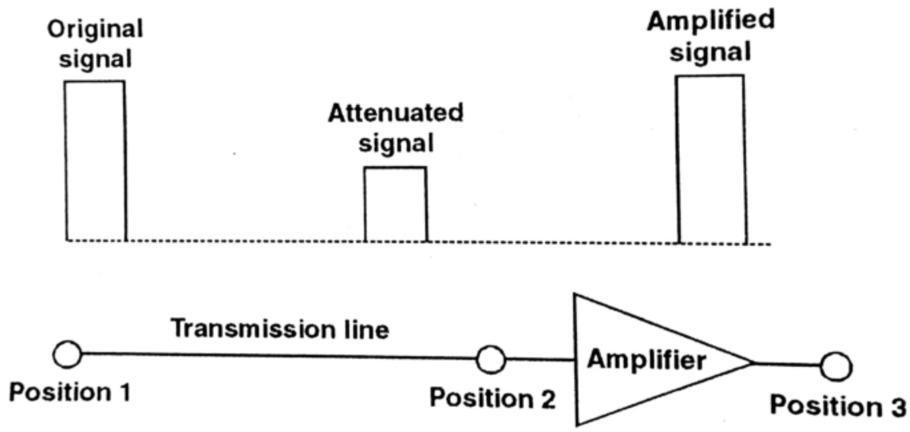
चित्र 1.25 : सिंक्रोनस ट्रांसमिशन

ट्रांसमिशन संबंधी गड़बड़ियॉ :

किसी भी कम्युनिकेशन सिस्टम में प्राप्त किया गया सिग्नल, **ट्रांसमिशन** संबंधी अनेक गड़बड़ियों की वजह से ट्रांसमिट किए गए सिग्नल से भिन्न हो सकता है। एनालॉग सिग्नल्स में ये गड़बड़ियॉ सिग्नल की गुणवत्ता को घटा सकती हैं। डिजीटल सिग्नल्स में बिट एरर्स प्रवि ठ हो सकते हैं : बायनरी 1 बायनरी 0 में या इसके उलट परिवर्तित हो सकती है। यहॉ हम विभिन्न गड़बड़ियॉ का अध्ययन करेंगे और देखेंगे कि ये कम्युनिकेशन लिंक की इन्फॉर्मेशन ले जाने की क्षमता को कैसे प्रभावित कर सकते हैं।

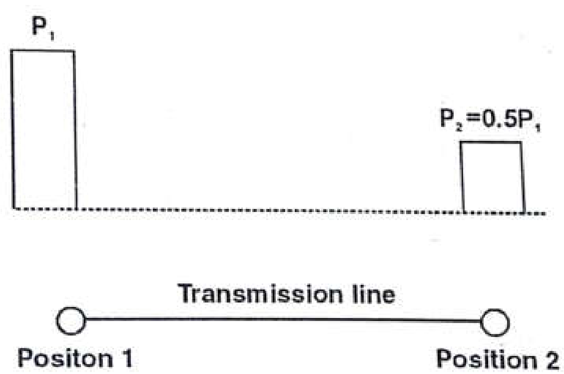
अत्यंत महत्वपूर्ण गड़बड़ियॉं निम्नलिखित है –

1 सिग्नल का कमजोर होना (अटेन्यूएशन) और विकृति आना।
2 विलम्ब संबंधी विकृति।
3 नॉइस



चित्र 1.26: एम्प्लिफिएर्स पेरिऑडियकाली

1. **अटेन्यूएशन** : सिग्नल की ताकत **ट्रांसमिशन** माध्यम की कई विधियों के कारण कम होती जाती है। उदाहरण के लिए किसी वायर में विद्युत सिग्नल के प्रवाह के दौरान उत्पन्न होने वाली ऊ मा से विद्युत ाक्ति कम हो जाती है। ऊर्जा के इस क्षय की पूर्ति के लिए निश्चित अंतराल पर चैनल पर एम्पिलफायर्स प्रयुक्त किए जाते हैं,

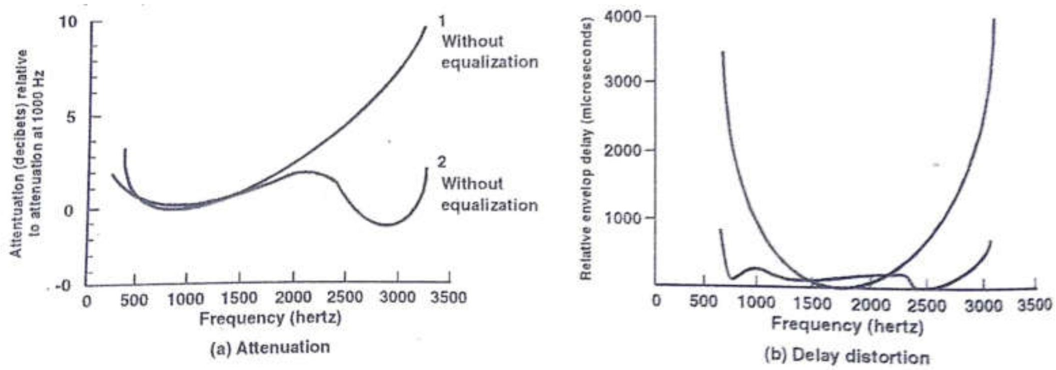


चित्र 1.27 : सिग्नल पोजीशन

2. **डिले डिसटार्शन या विलम्ब संबंधी विकृति** : डिले डिसटार्शन एक ऐसा विशि ट प्रभाव है, जो निर्देशित माध्यमों में ही पाया जाता है। यह विकृति इस तथ्य से उत्पन्न होती है कि निर्देशित माध्यम में से सिग्नल के प्रसार की गति, फ्रीक्वेंसी के साथ बदलती है। बैंड से सीमित सिग्नल के लिए, गमि का रूझान केंद्रीय फ्रीक्वेंसी के समीप अधिकतम रहता है और बैंड के दो सिरों की ओर कम होता जाता है। इस प्रकार सिग्नल के विभिन्न फ्रीक्वेंसी कंपोनेंट्स, रिसीवर पर

विभिन्न समयों में आते हैं। इसका परिणाम विभिन्न फ्रीक्वेंसीज के मध्य फेज शिफ्ट्स के रूप में उत्पन्न होता है।

इस प्रभाव को डिले डिसटार्शन के रूप में इसलिए जाता है, क्योंकि प्राप्त होने वाला सिग्नल, उसकी संघटक फ्रीक्वेंसीज पर अनुभव किए जाने वाले विभिन्न डिलेज की वजह से विकृत हो जाता है।



चित्र 1.28: डिले डिसऑर्डर कर्व

3. **नॉइस** : डिले डिसटार्शन के अतिरिक्त सिग्नल **ट्रांसमिशन** और डिटेक्शन विधियों के साथ जुड़े विभिन्न नॉइसेज और व्यवधान, प्राप्त किए गए सिग्नल को समझने में एरर्स की वजह बन सकते हैं। नॉइस ाब्द का अर्थ सिग्नल के ऐसे अवांछित घटकों से होता है, जो सिग्नल पर उसके स्त्रोत से रिसीवर तक की यात्रा के दौरान सम्मिलित हो जाते हैं अथवा ये स्वयं रिसीवर पर ही उत्पन्न हो सकते हैं। नॉइस के संभव स्त्रोतों में निम्नलिखित ाामिल हैं –

1. **थर्मल नॉइस** : यह इलेक्ट्रॉन्स की रेण्डम गति से उत्पन्न होता है। यह सभी इलेक्ट्रॉनिक उपकरणों में विद्यामान रहता है और तापमान का एक फंक्शन है। चूंकि यह फ्रीक्वेंसी स्पेक्ट्रम पर एक समान रूप से वितरित रहता है, इसलिए थर्मल नॉइस को सामान्यतः व्हाइट नॉइस के रूप में जाना जाता है। व्हाइट नॉइस की वजह से हाने वाले **ट्रांसमिशन** एरर्स को रेण्डम एरर्स के रूप मे जाना जाता है।
2. **इंटरमॉड्यूलेशन डिसटार्शन** : यह डिसटार्शन विभिन्न फ्रीक्वेंसीज पर सिग्नल्स के मिश्रण से किसी अन्य फ्रीक्वेंसी पर ऊर्जा उत्पन्न होने से घटित होता है। उदाहरण के लिए **f1** और **f2** फ्रीक्वेंसीज पर सिग्नल्स **f1+ f2 ,** 2**f1- f2** अथवा 2**f2- f1** जैसी अन्य फ्रीक्वेंसीज पर ऊर्जा उत्पन्न कर सकते हैं।

3. **क्रॉसटॉक** : यह एक सिग्नल चैनल के सिग्नल से अन्य चैनल के सिग्नल का अवांछित संयोजन होता है। उदाहरण के लिए टेलीफोन का उपयोग करते समय कभी–कभी पृ ठभूमि में किसी बातचीत के धीमे स्वर सुनाई दे सकते हैं, जो केबल में समीपवर्ती वायर्स के मध्य इलेक्ट्रोमेग्नेटिक संयोजन से उत्पन्न हो सकते हैं।

4. **इम्पल्स नॉइस** : यह ऐसे लम्बे, ांत अंतरालों द्वारा पहचाने जाते हैं, जो नॉइस बस्ट्र्स द्वारा बाधित होते हैं। ये बस्ट्र्स अनियमित अव्यवस्थित प्लसेज से निर्मित होते है।

1.8 डाटा प्रस्तुतिकरण के प्रकार :

आजकल इन्फॉर्मेशन टेक्सट, संख्याओ, छवियों, ध्वनि और वीडियो जैसे विभिन्न स्वरूपों में उपलब्ध हैं।

टेक्सट : टेक्सट को बिट पेटर्न अर्थात बिट्स (0s या 1s)की सीक्वेंस के रूप में दर्शाया जाता है। किसी पेटर्न में बिट्स की संख्या, भा ा में उपस्थित सिम्बल्स की संख्या पर निर्भर होती है। ब्लैंक, न्यूलाइन और टैब जैसे अन्य सिंबल्स को, टेक्स्ट के अलाइनमेंट तथा पठनीयता के लिए प्रयुक्त किया जाता है।

ASCII : अमेरिकन नेशनल स्टैण्डर्ड्स इंस्टीट्यूट (ANCI) ने एक कोड निर्मित किया है, जिसे अमेरिकन स्टैण्डर्ड कोड फॉर इन्फॉर्मेशन इंटरचेंज (ASCII) कहते हैं। यह कोड प्रत्येक सिंबल के लिए 7 बिट्स का उपयोग करता है इसका अर्थ है कि इस कोड के द्वारा 128 (2^7) विभिन्न सिंबल्स परिभा ित किए जा सकते हैं।

एक्सटेंडेड ASCII : प्रत्येक पैटर्न की साइज 1 बाइट (8 बिट्स) की बनाने के लिए ASCII बिट पैटर्न्स में, बाईं ओर एक अतिरिक्त 0 की वृद्धि की जाती है। अब प्रत्येक पैटर्न ठीक 1 बाइट मेमोरी का है। दूसरे ब्दों में, एक्सटेंडेड ASCII में प्रथम पैटर्न 00000000 है और अंतिम 01111111 है।

यूनिकोड : अब तक बताए कोई भी कोड्स अंग्रेजी के अलावा अन्य किसी भा ा के सिंबल्स को नहीं दर्शाते हैं। इसके लिए कहीं अधिक क्षमता वाले कोड की आवश्यकता होती है। हार्डवेअर और सॉफ्टवेअर निर्माताओं के एक गठबंधन ने यूनिकोड नामक एक ऐसा कोड निर्मित किया है, जो 16 बिट्स का उपयोग करता है और 65,536 (2^{16}) तक सिंबल्स दर्शा सकता है।

ISO : इंटरनेशनल ऑर्गेनाइजेशन फॉर स्टैंडर्डाइजेशन, जिसे ISD कहते हैं, ने 32-बिट पैटर्न का उपयोग करते हुए एक कोड निर्मित किया है। यह कोड 4,294,967,296 (2^{32}) तक सिंबल्स दर्शा सकता है। ये निश्चित रूप से दुनिया में आज किसी भी सिग्नल को दर्शाने के लिए पर्याप्त होते हैं।

नंबर्स : संख्याओं को भी बिट पैटर्न्स का उपयोग करते हुए दर्शाया जाता है ASCII जैसे किसी कोड को संख्याएँ दर्शाने के लिए प्रयूक्त नहीं किया जाता है। संख्या को सीधे ही किसी बायनरी नंबर में बदल लिया जाता है। इसका कारण, संख्याओं पर गणितीय क्रियाओं का सरलीकरण है।

इमेजेस या छवियॉ : आजकल छवियों को भी बिट पैटर्न्स द्वारा दर्शाया जा रहा है। किंतु इसकी विधि भिन्न है। इसके सरलतम स्वरूप में, किसी छवि को पिक्सेल्स के मेट्रिक्स (पिक्चर एलिमेंट्स) में विभाजित किया जाता है, जहॉ प्रत्येक पिक्सेल एक छोटा बिंदु (डॉट) होता है पिक्सेल का आकार, रिजाल्यूशन कितना है, इस पर निर्भर करता है।

ऑडियो : ऑडियो, ध्वनि का प्रस्तुतिकरण है। प्रकृति से यह टेक्स्ट, संख्याओं या छवियों से भिन्न होता है। यह असंगत की अपेक्षा सतत् प्रवाह होता है। जब हम आवाज अथवा संगीत को विद्युत संकेतों में बदलने के लिए माइक्रोफोन का उपयोग कर रहे होते हैं, तब भी हम एक सतत सिग्नल निर्मित करते हैं।

वीडियो : वीडियो एक सतत प्रवाह की तरह (जैसे टीवी कैमरे से) उत्पन्न हो सकता है अथवा यह छवियों का ऐसा मिलाजुला स्वरूप हो सकता है, जिसमें प्रत्येक छवि एक ऐसी असंगत इकाई होती है, जिन्हें इस तरह से व्यवस्थित किया जाता है कि गति का अहसास होता है। हम वीडियो को पुनः डिजीटल या एनालॉग सिग्नल में बदल सकते हैं।

संदर्भ ग्रंथो की सूची

a. Goleniewski, L. (2006) *Telecommunications Essentials*, Addison Wesley Professional.

b. Kurose, J.F. and K.W. Ross (2003) *Computer Networking: A Top Down Approach Featuring the Internet*, Addison Wesley.

c. Mir, N.F. (2006) *Computer and Communication Networks*, Prentice Hall.

d. Ogletree, T.W. and M.E. Soper (2006) *Upgrading and Repairing Networks*, Que.

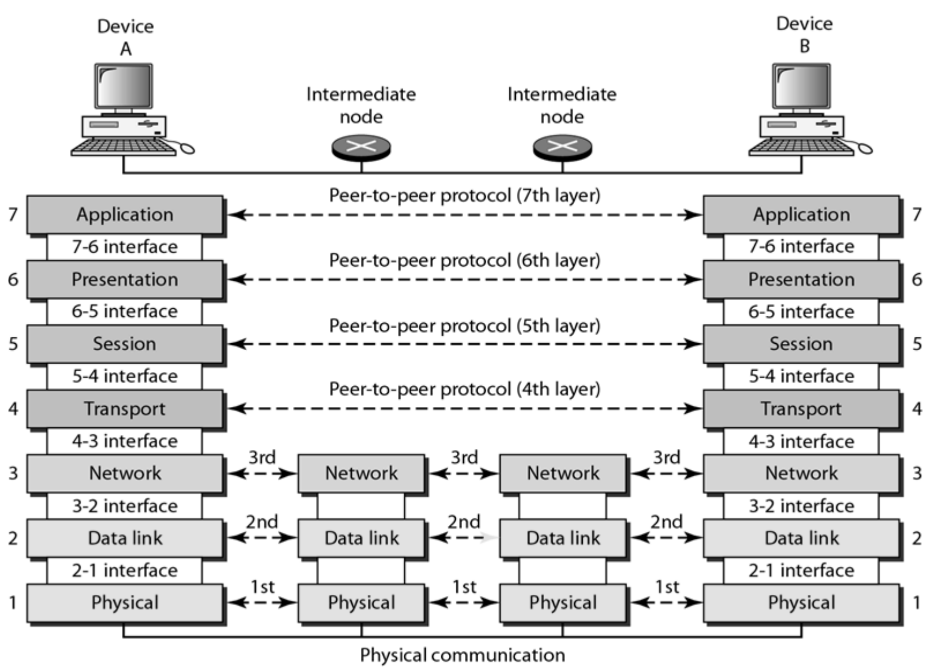
e. L. L. Peterson and B. S. Davie, Computer Networks, 2nd Edition, Morgan-Kaufmann, 2000.

f. वैज्ञानिक तथा तकनीकी शब्दावली आयोग द्वारा प्रकाशित मूलभूत शब्दावली

2.1 **ओ. एस. आई. मॉडल (एक परिचय)**

ओ. एस. आई. मॉडल दर्शाता है कि डेटा कम्युनिकेशन्स कैसे होना चाहिए। यह फंक्शन्स या प्रोसेस को सात ग्रुप में विभाजित करता है जिन्हें लेयर के रूप में डिस्क्राइब किया जाता है।

ओपन सिस्टम्स इंटरकनेक्शन Open Systems Interconnection (ओ. एस. आई.) मॉडल लेयर में प्रोटोकॉल को इम्प्लीमेंट करने के लिए एक नेटवर्किंग फ्रेमवर्क को डिफाइन करता है, जिसमें एक लेयर से लेकर अगले तक कंट्रोल को पास किया जाता है। यह कंप्यूटर नेटवर्क आर्किटेक्चर को लॉजिकल प्रोग्रेस में 7 लेयर में विभाजित करता है। निचली लेयर इलेक्ट्रिकल सिग्नल, बाइनरी डेटा के सेगमेंट, और नेटवर्क में इस डेटा का राउटिंग से डिल करता हैं। नेटवर्क रिक्वेस्ट और रिस्पॉड, डेटा का रिप्रेजेंटेशन, और नेटवर्क प्रोटोकॉल जैसे कि यूजर्स के दृष्टिकोण से देखा जाता है उसे हाइर लेयर कवर करता हैं। ओ. एस. आई. (रिफरेन्स मॉडल , इंटरनेशनल स्टैंडर्ड्स आर्गेनाइजेशन)(ISO) द्वारा डेवलप प्रपोजल पर आधारित है। ओ. एस. आई. मॉडल का मूल उद्देश्य इक्विपमेंट मैनुफक्चरर्स के लिए डिजाइन स्टैंडर्ड का एक सेट प्रदान करना था ताकि वे एक दूसरे के साथ कम्यूनिकेट कर सकें।



चित्र 2.1:ओ. एस. आई. मॉडल की लेयर्स

ओ. एस. आई. रिफरेन्स मॉडल का उद्देश्य:

हर कोई जानता है कि इनफॉर्मेशन को टुकड़ों में बाटने से समझने और समझाने में आसानी होती हैं। यही बात नेटवर्किंग के लिए भी लागू होती हैं। ओ. एस. आई. मॉडल सात लेयर के एक स्ट्रक्चर्ड सेट को रिप्रेजेंट करता हैं, जो एक दूसरे के साथ कनेक्ट होते है। इस मॉडल में प्रत्येक लेयर को डिवाइसेस, कंप्यूटर और नेटवर्क सेग्मेंट्स को कनेक्ट करने की क्षमता बनाए रखने के लिए डेवलप किया गया था।

निम्नलिखित उद्देश्यों के लिए ओ. एस. आई. मॉडल बनाया गया था: -

सॉफ्टवेयर डेवलपर्स और हार्डवेयर के लिए एक कॉमन प्लेटफ़ॉर्म बनाना, ताकि ऐसे नेटवर्किंग प्रॉडक्ट के निर्माण को प्रोत्साहित किया जा सके जो नेटवर्क पर एक दूसरे के साथ कम्यूनिकेट कर सकते हैं। छोटे सेग्मेंट्स में बड़ी डेटा एक्सचेंज प्रोसेस को विभाजित करके नेटवर्क एडमिनिस्ट्रेटर्स को सहायता करने के लिए यह लेयर बनाए गए हैं। छोटे सेग्मेंट्स समझने, मैनेज करने और ट्रबलशूट के लिए आसान है। लेयर्स में डिवाइड होने से केवल वही डिवाइसेस को ट्रबलशूट करना होगा जो फॉल्टी लेयर में काम कर रहे हैं।

ओ. एस. आई. रेफरेंस मॉडल का उद्देश्य वेंडर्स और डेवलपर्स को मार्गदर्शन करना है ताकि डिजिटल कम्युनिकेशन प्रॉडक्ट और सॉफ्टवेयर प्रोग्राम तैयार किए जा सकें, और कम्युनिकेशन टूल्स के बीच स्पष्ट तुलना की सुविधा प्रदान कि जा सकें। टेलीकम्युनिकशन्स में शामिल अधिकांश विक्रेता, ओ. एस. आई. मॉडल के संबंध में अपने प्रॉटक्ट और सर्विसेस का वर्णन करने का प्रयास करते हैं। यद्यपि डिस्कशन और मूल्यांकन मार्गदर्शन के लिए ओ. एस. आई. मॉडल उपयोगी है, लेकिन ओ. एस. आई. शायद ही कभी लागू किया जाता है, क्योंकि कुछ नेटवर्क प्रॉडक्ट या स्टैंडर्ड टूल्स सभी रिलेटेड फंक्शन को मॉडल से संबंधित सभी डिफाइन लेयर में एक साथ रखते हैं।

2.1.1 ओ. एस. आई. मॉडल की सात परतें

ओ. एस. आई. का मुख्य कांसेप्ट यह है कि टेलीकम्युनिकशन्स नेटवर्क में दो एंडपॉइंट के बीच कम्युनिकेशन की प्रोसेस को संबंधित फंक्शन के सात अलग-अलग लेयर में डिवाइड किया जा सके। प्रत्येक कम्युनिकेटिंग यूजर या प्रोग्राम उस कंप्यूटर पर है जो फ़ंक्शन के उन सात लेयर

प्रदान कर सकता है। इसलिए यूज़र्स के बीच किसी दिए गए मैसेजेस में, सोर्स कंप्यूटर में लेयर्स के माध्यम से डेटा फ्लो नीचे कि और होता हैं और फिर रिसिविंग कंप्यूटर में लेयर्स के माध्यम से ऊपर कि और होता हैं।

फ़ंक्शन के सात लेयर ऐप्लीकेशन, ऑपरेटिंग सिस्टम, नेटवर्क कार्ड डिवाइस ड्राइवरों और नेटवर्किंग हार्डवेयर के कॉम्बिनेशन द्वारा प्रोवाइड किए जाते हैं जो एक नेटवर्क केबल या वाई-फाई या अन्य वायरलेस प्रोटोकॉल पर सिग्नल भेजने के लिए सक्षम होते हैं।

ओ. एस. आई. मॉडल में, कंट्रोल एक लेवल से दूसरे तक, एक स्टेशन पर ऐप्लीकेशन लेयर (लेयर 7) से शुरू होता है, और नीचे की तरफ जाता है, चैनल पर अगले स्टेशन पर जाता है और हाइरार्की का बैकअप लिया जाता है। ओ. एस. आई. मॉडल इंटर-नेटवर्किंग के टास्क को लेता है और इसे उस हिस्से में विभाजित करता है जिसे वर्टीकल स्टैक के रूप में रेफर किया जाता है जिसमें निम्नलिखित 7 लेयर शामिल हैं-

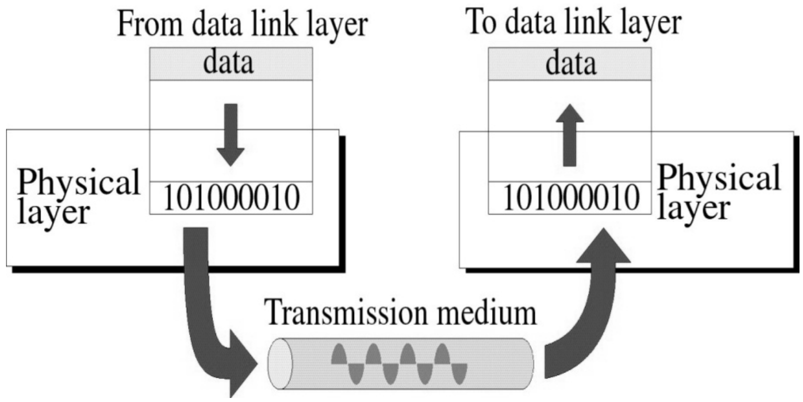
1. **फिजिकल लेयर (Physical Layer) :** भौतिक परत ओएसआई मॉडल की पहली परत है। भौतिक परत डेटा लिंक नामक ऊपरी परत से डेटा प्राप्त करता है तथा यह प्राप्त डेटा को बिट स्ट्रीम (Bit Stream) में परिवर्तित करता है। बिट में '0' या '1' मान होता है।यह डिवाइसेस के बीच वास्तविक फिजिकल कनेक्शन के लिए ज़िम्मेदार है। फिजिकल लेयर में बिट्स के रूप में इनफॉर्मेशन होती है। यह डिवाइसेस के बीच वास्तविक फिजिकल कनेक्शन के लिए ज़िम्मेदार है। डेटा प्राप्त करते समय, इस लेयर को सिग्नल प्राप्त होते हैं। इसके बाद यह लेयर इसे 0 और 1 में कनवर्ट करता हैं और उन्हें डाटा लिंक लेयर (Data Link layer) पर भेज देता हैं। फिजिकल लेयर के उदाहरणों में ईथरनेट केबल्स और टोकन रिंग नेटवर्क शामिल हैं इसके अतिरिक्त, हब और अन्य रिपिटर्स स्टैंडर्ड नेटवर्क डिवाइस होते हैं जो कि फिजिकल लेयर पर कार्य करते हैं, जैसे केबल कनेक्टर हैं।

   फिजिकल लेयर पर, फिजिकल मेडियम द्वारा सपोर्टेड सिग्नल के टाइप का उपयोग करके डेटा ट्रांसमिट किया जाता है: इलेक्ट्रिक वोल्टेज, रेडियो फ्रीक्वेंसी, या इंफ्रारेड या आर्डिनरी लाइट के पल्स।

   मुख्य बिंदु

   - यह फिजिकल कनेक्शन को एक्टिवेट करता है, मेंटेन रखता है और डिएक्टिवेट करता है।
   - यह नेटवर्क पर अनस्ट्रक्चर्ड रॉ डेटा के ट्रांसमिशन और रिसेप्शन के लिए जिम्मेदार है।

- ट्रांसमिशन के लिए आवश्यक वोल्टेज और डाटा रेट फिजिकल लेयर में डिफाइन किए जाते है।
- यह डिजिटल सिग्नल या ऑप्टिकल सिग्नल में डिजिटल / एनालॉग बिट्स को कन्वर्ट करता है।
- डाटा एन्कोडिंग भी इस लेयर में किया जाता है।

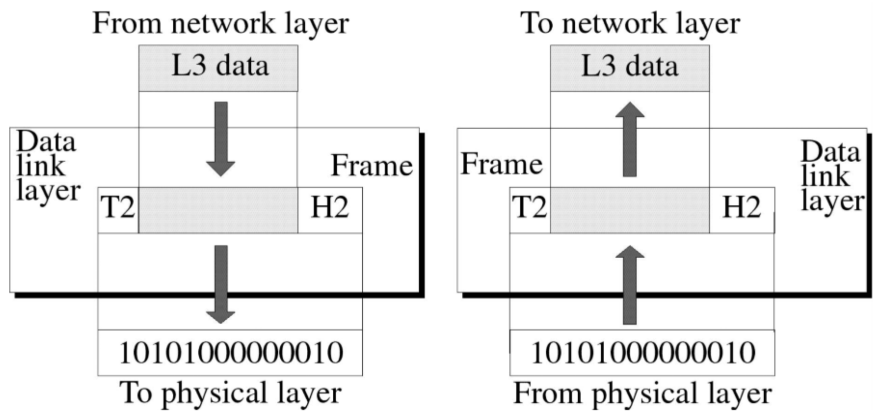


चित्र 2.2 : फिजिकल लेयर

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

मुख्य बिंदु

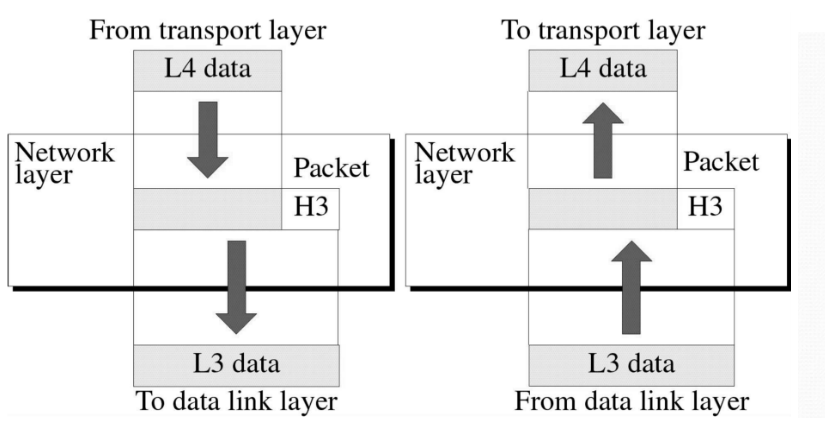
- डाटा लिंक लेयर उस इनफॉर्मेशन को सिंक्रनाइज़ करता है जो फिजिकल लेयर पर ट्रांसमिट होती है।
- इस लेयर का मुख्य कार्य यह सुनिश्चित करना है कि फिजिकल लेयर पर एक नोड से दूसरे में डेटा ट्रांसफर एरर फ्री हो।
- अनुक्रमिक रूप से प्राप्त ट्रांसमिशन और डेटा फ्रेम्स इस लेयर द्वारा मैनेज किया जाता है।



चित्र 2.3 : डाटा लिंक लेयर

3. नेटवर्क लेयर (Network layer): नेटवर्क लेयर डेटा लिंक लेयर के ऊपर राउटिंग की कांसेप्ट को एड करता है। जब डेटा नेटवर्क लेयर पर आता है, तो प्रत्येक फ्रेम 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 पूश 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।

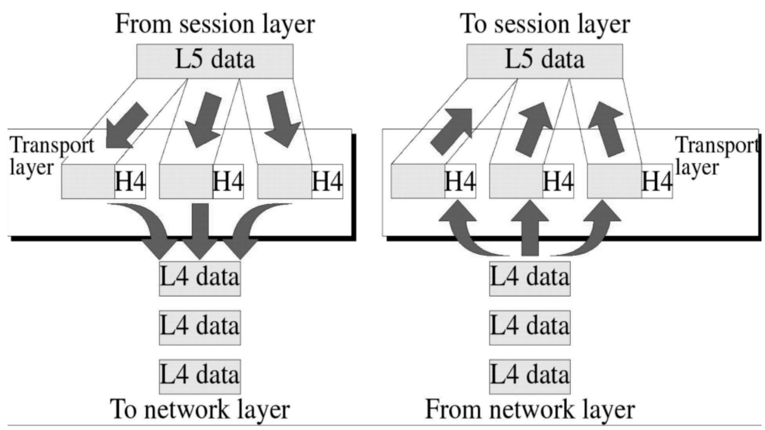


चित्र 2.4 : नेटवर्क लेयर

मुख्य बिंदु

- यह एक नोड से अन्य नोड तक विभिन्न चैनलों के माध्यम से सिग्नल को राउट करता है।
- यह एक नेटवर्क कंट्रोलर के रूप में कार्य करता है। यह सबनेट ट्रैफिक मैनेज करता है।
- यह तय करता है कि डेटा को किस रूट को लेना चाहिए।
- यह आउटगोइंग मैसेजेस को पैकेट में बांटता है और इनकमिंग पैकेट को हाइर लेवर के लिए मैसेजेस को अस्सेम्बल करता है।

4. **ट्रांसपोर्ट लेयर (Transport Layer) :** 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।

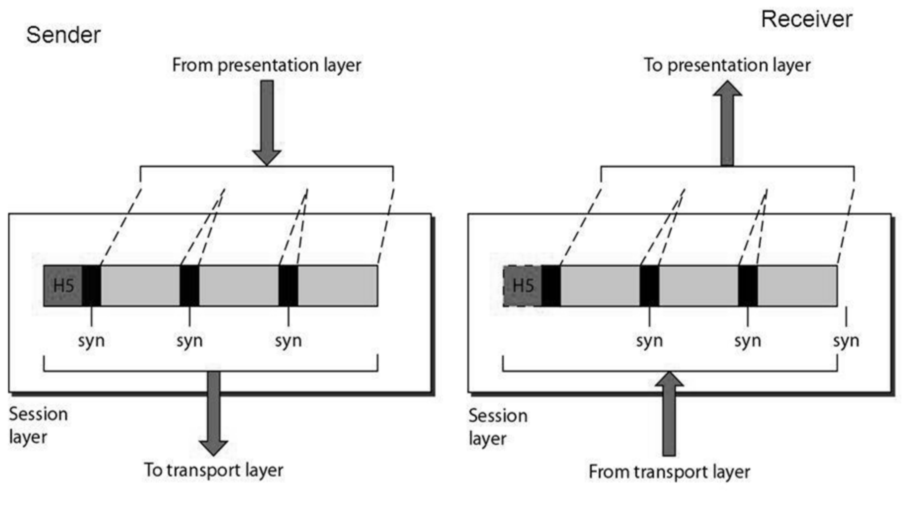


चित्र 2.5 : T लेयर

मुख्य बिंदु

- एंड सिस्टम के बीच डेटा के ट्रांसपरेंट ट्रांसफर के लिए जिम्मेदार।
- एंड-टू-एंड एरर रिवकरी और फ्लो कंट्रोल के लिए जिम्मेदार।
- संपूर्ण डेटा ट्रांसफर के लिए जिम्मेदार।
- यहां SPX, TCP, UDP जैसे प्रोटोकॉल काम करते हैं।

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



चित्र 2.6 : सेशन लेयर

मुख्य बिंदु

- ऐप्लीकेशन के बीच एस्टैब्लिशमेंन्ट, मैनेजमेंट और कनेक्शन के टर्मिनेशन के लिए जिम्मेदार।
- Session layer प्रत्येक एंड पर एप्लिकेशन के बीच कोऑर्डिनेशन, एक्सचेंज और डाइलॉग सेटअप करता है।
- यह सेशन और कनेक्शन कोऑर्डिनेशन के साथ काम करता है।
- इस लेयर पर NFS, NetBios names, RPC, SQL जैसे प्रोटोकॉल काम करते हैं।

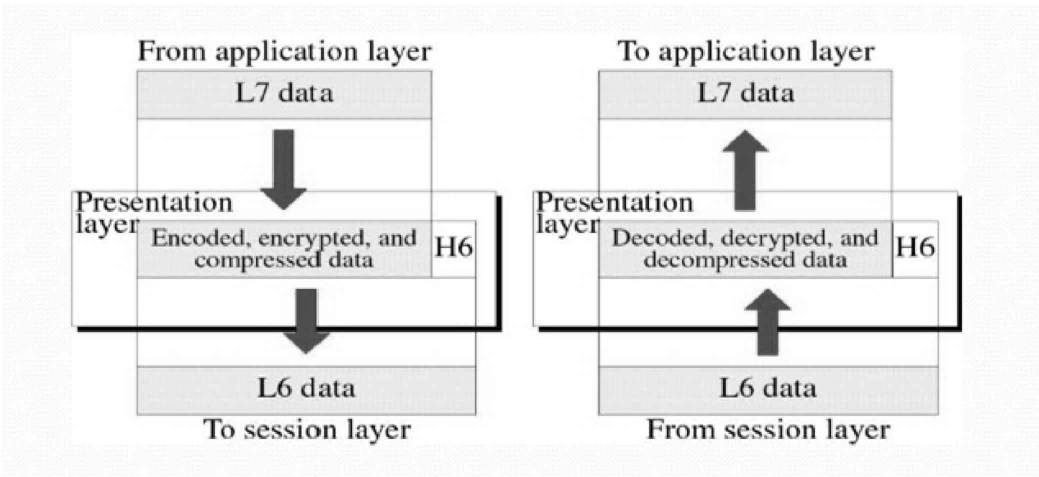
6. **प्रेजेंटेशन लेयर** (Presentation Layer) : प्रेजेंटेशन लेयर को ट्रॅनस्लेशन लेयर भी कहा जाता है। एप्लिकेशन लेयर से डेटा यहां एक्सट्रैक्ट किया जाता है और नेटवर्क पर ट्रांसमिट करने के लिए आवश्यक फॉर्मेट के अनुसार मैनिप्युलेट किया जाता है।

प्रेजेंटेशन लेयर के फंक्शन इस प्रकार हैं:

ट्रॅनस्लेशन (Translation) : उदाहरण के लिए, ASCII से EBCDIC

एन्क्रिप्शन / डेक्रिप्शन(Encryption/ Decryption) : डेटा एन्क्रिप्शन डेटा को किसी अन्य रूप या कोड में ट्रांसलेट करता है। एन्क्रिप्टेड डेटा को सिफर टेक्स्ट के रूप में जाना जाता है और डिक्रिप्टेड डेटा को प्लेन(Plain) टेक्स्ट के रूप में जाना जाता है। डेटा को एन्क्रिप्ट करने और डिक्रिप्टिंग करने के लिए एक key वैल्यू का उपयोग किया जाता है।

कम्प्रेशन(Compression): नेटवर्क पर ट्रांसमिट किए जाने वाले बिट की संख्या को कम कर देता है।



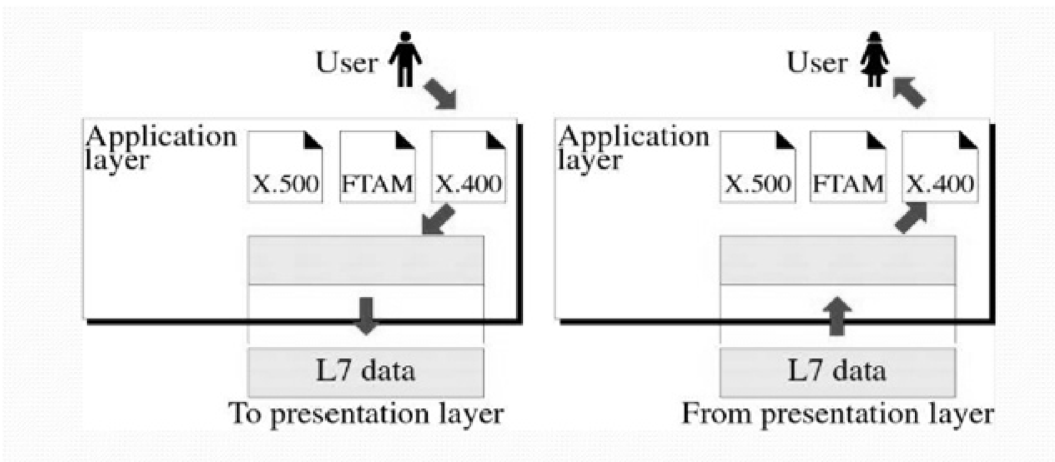
चित्र 2.7 : प्रेजेंटेशन लेयर

मुख्य बिंदु

- प्रेजेंटेशन लेयर 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।
- डेटा प्राप्त करते समय, प्रेजेंटेशन लेयर ऐपलीकेशन लेयर के लिए डेटा ट्रांसफॉर्म कर रेडी करता हैं।
- दो कम्युनिकेशन सिस्टम में लैग्वेज (सिंटैक्स) भिन्न हो सकती हैं। इस स्थिति के अंतर्गत प्रेजेंटेशन लेयर ट्रांसलेटर की भूमिका निभाता है।
- यह डाटा कंप्रेशन, डाटा एन्क्रिप्शन, डेटा कन्वर्शन इत्यादि परफॉर्म करता है।

7. **एप्लीकेशन लेयर** (Application Layer) : 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।



चित्र 2.8 : एप्लिकेशन लेयर

मुख्य बिंदु

- एप्लिकेशन लेयर ऐप्लीकेशन, ऐप्स और एंड यूजर्स प्रोसेसेस को सपोर्ट करता है।
- सर्विस कि क्वालिटी।
- यह लेयर फ़ाइल ट्रांसफर, ई-मेल और अन्य नेटवर्क सॉफ़्टवेयर सर्विसेस के लिए एप्लिकेशन सर्विसेस के लिए ज़िम्मेदार है।
- इस लेयर पर Telnet, FTP, HTTP जैसे प्रोटोकॉल काम करते हैं।

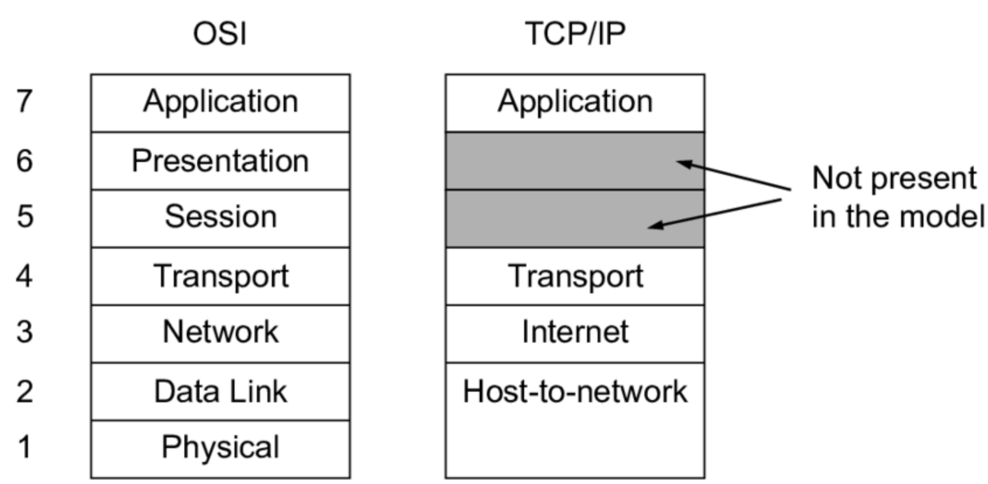
2..2 टी.सी.पी/ आई.पी. मॉडल

टीसीपी/आईपी दो तरह के प्रोटोकॉल होते हैं, जिनका प्रयोग इन्टरनेट की संरचना में होता है। प्रोटोकॉल एक प्रकार के नियम होते हैं, जिनका पालन करना किसी भी कार्य के लिए जरूरी होता है। टीसीपी की फुल फॉर्म होती है, ट्रांसमिशन कण्ट्रोल प्रोटोकॉल। इसका मतलब है, इन्टरनेट पर

किसी भी प्रकार के आदान-प्रदान पर लगने वाले नियम। इन्टरनेट प्रोटोकॉल इन्टरनेट पर किसी भी प्रकार के हलचल की निगरानी करता है और हर कंप्यूटर सिस्टम पर लागू होता है। आईपी को आईपी एड्रेस के तौर पर जाना जाता है। टी.सी.पी/ आई.पी. को "लैंग्वेज ऑफ़ इंटरनेट." के नाम से भी जाना जाता हैं। टी.सी.पी/ आई.पी. WWW का एक प्रोटोकॉल है, जिसके द्वारा हम किसी भी कंप्यूटर में आसानी से इंटरनेट एक्सेस करने के लिए उपयोग में लेते है। अगर किसी नेटवर्क में दो डिवाइस है तो उन्हें आपस में कम्यूनिकेट करने के लिए कॉमन प्रोटोकॉल की जरुरत होगी। टी.सी.पी/ आई.पी. मॉडल (प्रोटोकॉल) एन्ड-to-एन्ड कम्युनिकेशन उपलब्ध कराता है। सभी प्रोटोकॉल और नेटवर्क टी.सी.पी/ आई.पी. मॉडल पर काम करते हैं।

2.2.1 टी.सी.पी/ आई.पी. रिफरेन्स मॉडल :

टी.सी.पी/ आई.पी. दो कम्प्यूटर्स के बीच इनफार्मेशन ट्रांसफर और कम्युनिकेशन को पॉसिबल करता है । इसका प्रयोग डाटा को सुरक्षित ढंग से भेजने के लिए किया जाता है । TCP की भूमिका डाटा को छोटे-छोटे भागों (Packets) में बाँटने की होती है और IP इन पैकेट्स का एड्रेस मुहैया कराता है । टी.सी.पी/ आई.पी. नेट्वर्क प्रोटोकॉल इंटरनेट पर एक साथ भिन्न आकार और विभिन्न प्रकार के सिस्टम्स नेटवर्क से कनेक्ट करने की इसकी क्षमता के कारण सफल है। टी.सी.पी/ आई.पी. का इम्प्लीमेंटेशन लगभग सभी प्रकार के हार्डवेयर व ऑपरेटिंग सिस्टम के लिए समान रूप से काम करता है इसलिए सभी प्रकार के नेटवर्क्स टी.सी.पी/ आई.पी. के प्रयोग द्वारा आपस में कनेक्ट हो सकते हैं।



चित्र 2.9 : टी.सी.पी/ आई.पी. रिफरेन्स मॉडल

टी.सी.पी/ आई.पी. प्रोटोकॉल में 4 लेयर्स होती है जो निम्न है:-

01). नेटवर्क एक्सेस लेयर **(Network Interface Layer):-**

यह टी.सी.पी/ आई.पी. मॉडल की सबसे निम्नतम लेयर है। टी.सी.पी/ आई.पी. का Network Layer, OSI रेफरेन्स मॉडल्स के पहले तीन निचले लेयर्स (i.e ... नेटवर्क, डाटा लिंक और फिजिकल) के सभी फंक्शन को पूरा करता है। नेटवर्क एक्सेस लेयर यह डेस्क्रिबे करती है कि किस प्रकार से किसी भी IP डाटा ग्राम को नेटवर्क में भेजना है। नेटवर्क लेयर में जो डाटा होता है वह पैकेट (डाटा के समूह) के रूप में होता है और इन पैकेटों को सोर्स से डेस्टिनेशन तक पहूँचाने का काम नेटवर्क लेयर का होता है। नेटवर्क लेयर जैसे ही किसी नई हार्डवेयर को डिटेक्ट करती हैं, नए नेटवर्क एक्सेस प्रोटोकॉल को विकसित करती है ताकि टीसीपी / आईपी नेटवर्क नए हार्डवेयर का इस्तेमाल आसानी से कर सकें।

02). इंटरनेट लेयर **(Network Layer) :-**

टी.सी.पी/ आई.पी. मॉडल में इंटरनेट लेयर का काम OSI रेफ्रेन्स मॉडल के लेयर 3 की तरह ही काम करता हैं, यह लेयर ट्रांसपोर्ट लेयर तथा एप्लीकेशन लेयर के मध्य स्थित होती है। यह लेयर नेटवर्क में कनेक्शनलेस कमयुनिकेशन उपलब्ध कराती है। इसमें डेटा को IP डाटाग्राम के रूप में पैकेज किया जाता है यह डाटाग्राम सोर्स तथा डेस्टिनेशन IP एड्रेस को कॉन्टैन किये रहते है जिससे कि डेटा को आसानी से सेन्ट तथा रिसीव किया जा सकें। टी.सी.पी/ आई.पी. इंटरनेट लेयर के अंतर्गत आने वाले मेजर प्रोटोकॉल्स है :- इंटरनेट प्रोटोकॉल (IP), इंटरनेट कण्ट्रोल मैसेज प्रोटोकॉल (ICMP), एड्रेस रेसोलुशन प्रोटोकॉल (ARP), रिवर्स एड्रेस रेसोलुशन प्रोटोकॉल (RARP) और इंटरनेट ग्रुप मैनेजमेंट प्रोटोकॉल (IGMP).

03). ट्रांसपोर्ट लेयर(**Transport Layer):-**

टी.सी.पी/ आई.पी. मॉडल का ट्रांसपोर्ट लेयर डाटा के Transmission के लिए जिम्मेदार होती है यह लेयर एप्लीकेशन लेयर तथा इंटरनेट लेयर के मध्य स्थित होती है। ट्रांसपोर्ट लेयर में एरर चेकिंग , फ्लो कण्ट्रोल भी होता हैं ताकि दो कम्युनिक्शन के बीच कोई भी डाटा अपने सही रिसीवर और सेन्डर तक पहूँच सके, अगर में आसान शब्दों में कहें, तो ये मल्टीप्लेक्सिंग और दी-मल्टीप्लेक्सिंग के प्रोसेस के लिए जिम्मेवार होता हैं। इस लेयर में दो मुख्य प्रोटोकॉल कार्य करते है:-

ट्रांसमिशन कण्ट्रोल प्रोटोकॉल(TCP), यूजर डाटाग्राम प्रोटोकॉल(UDP)

04). एप्लीकेशन लेयर(**Application Layer):-**

TCP/IP प्रोटोकॉल की सबसे उच्चतम लेयर को एप्लीकेशन लेयर कहते है। यह लेयर ऍप्लिकेशन्स को नेटवर्क सर्विसेज उपलब्ध करने से सम्बंधित होती है। इस लेयर का सम्बन्ध किसी भी डाटा के फार्मेशन, एन्काप्सुलेशन और ट्रांसमिशन से होता हैं। ये लेयर ह्यूमन इंटरेक्शन का काम करती हैं जैसे: वेब -ब्राउज़र , ईमेल तथा अन्य एप्लीकेशन के लिए विंडो उपलब्ध कराना. इस लेयर का काम ट्रांसपोर्ट लेयर को डाटा भेजना और उससे डाटा को रिसीव करना । एप्लीकेशन लेयर में होने वाले कुछ प्रोटोकॉल्स निम्न प्रकार से है:-

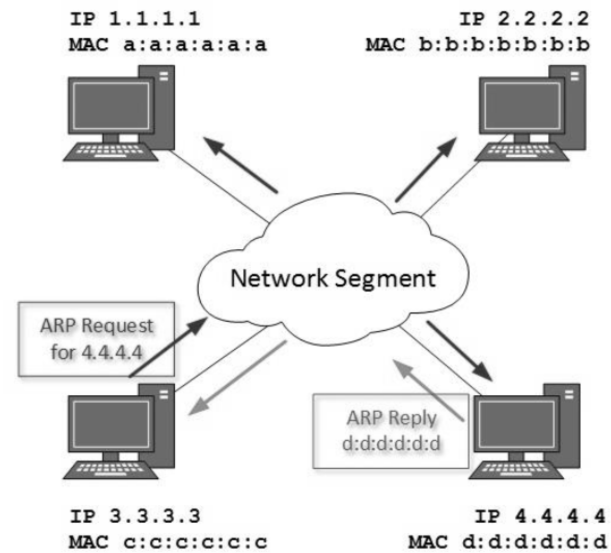
हाइपरटेक्स्ट ट्रांसफर प्रोटोकॉल (HTTP)
सिंपल मेल ट्रांसफर प्रोटोकॉल (SMTP)
डायनामिक होस्ट कॉन्फ़िगरेशन प्रोटोकॉल (DHCP)
डोमेन नाम सिस्टम (DNS)
सिंपल नेटवर्क मैनेजमेंट प्रोटोकॉल (SNMP)
फाइल ट्रांसफर प्रोटोकॉल (FTP)

2..3 ओ. एस. आई. - टी.सी.पी/ आई.पी. मॉडल के प्रमुख प्रोटोकॉल

2.3.1 एड्रेस रेसोलुशन प्रोटोकॉल- एआरपी (ARP)

इंटरनेट पर प्रत्येक मशीन में एक या अधिक आईपी एड्रेस हैं, लेकिन ये एड्रेस पैकेट(डाटा) भेजने के लिए पर्याप्त नहीं हैं। डेटा लिंक लेयर एनआईसी (नेटवर्क इंटरफेस कार्ड्स) जैसे ईथरनेट कार्ड इंटरनेट पते को नहीं समझते हैं। ईथरनेट के मामले में, निर्मित हर एनआईसी एक अद्वितीय 48-बिट ईथरनेट एड्रेस से लैस होता है। संचार करते समय, होस्ट को गंतव्य मशीन के लेयर -2 (मैक) एड्रेस की आवश्यकता होती है जो एक ही प्रसारण डोमेन या नेटवर्क से संबंधित होती है। मैक एक एड्रेस है जो एक मशीन के नेटवर्क इंटरफेस कार्ड (एनआईसी) में फिजिकली(जो देखा जा सकता है) दिए जाता है दिया और यह कभी नहीं बदलता है।

दूसरी तरफ, सार्वजनिक डोमेन पर आईपी पता शायद ही कभी बदला जाता है। अगर कुछ मामले में एनआईसी बदल जाता है, तो मैक एड्रेस भी बदल जाता है। इस तरह, लेयर -2 संचार के लिए, दोनों के बीच एक मैपिंग आवश्यक है।

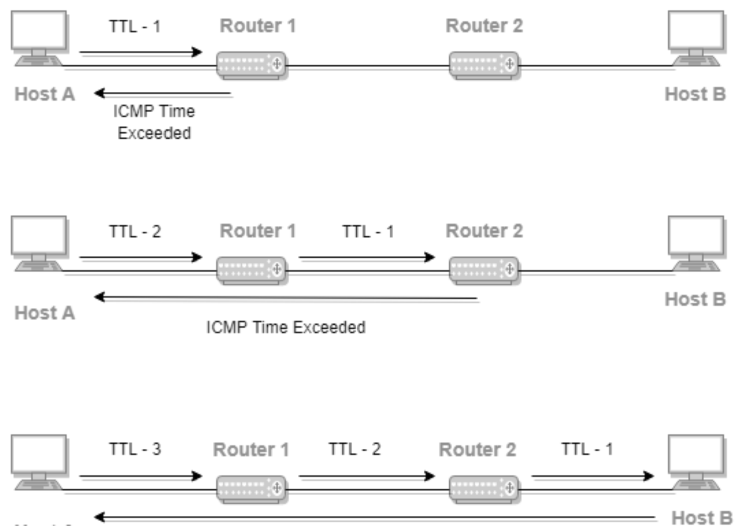


चित्र 2.10 :एड्रेस रेसोलुशन प्रोटोकॉल कार्यप्रणाली

2.3.2 इंटरनेट कण्ट्रोल मैसेज प्रोटोकॉल (ICMP)

आईसीएमपी नेटवर्क नैदानिक और त्रुटि रिपोर्टिंग प्रोटोकॉल है। आईसीएमपी आईपी प्रोटोकॉल सूट से संबंधित है और आईपी का उपयोग वाहक प्रोटोकॉल के रूप में करता है। आईसीएमपी पैकेट बनाने के बाद, यह आईपी पैकेट में एनकेप्सुलेटेड है। चूंकि आईपी स्वयं एक सर्वोत्तम प्रयास गैर-भरोसेमंद प्रोटोकॉल है, इसलिए आईसीएमपी उपयोगी है।

नेटवर्क के बारे में कोई प्रतिक्रिया मूल सेन्डर को वापस भेज दी जाती है। यदि नेटवर्क में कुछ त्रुटि होती है, तो यह आईसीएमपी के माध्यम से रिपोर्ट की जाती है। आईसीएमपी में दर्जनों निदान और त्रुटि रिपोर्टिंग संदेश शामिल रहते हैं।
इंटरनेट के संचालन राउटर द्वारा बारीकी से निगरानी की जाती है। जब राउटर में पैकेट प्रोसेसिंग के दौरान कुछ अप्रत्याशित होता है, तो आईसीएमपी (इंटरनेट कंट्रोल मैसेज प्रोटोकॉल) द्वारा प्रेषक को घटना की सूचना दी जाती है। आईसीएमपी का उपयोग इंटरनेट का परीक्षण करने के लिए भी किया जाता है। लगभग दर्जन प्रकार के आईसीएमपी संदेशों को परिभाषित किया जाता है। प्रत्येक आईसीएमपी संदेश प्रकार को आईपी पैकेट में एनकेप्सुलेटेड किया जाता है।



चित्र 2.11 :इंटरनेट कण्ट्रोल मैसेज प्रोटोकॉल कार्यप्रणाली

2.3.3 रूटिंग इनफार्मेशन प्रोटोकॉल (RIP)

RIP जो है वह एक ओपन स्टैण्डर्ड प्रोटोकॉल है अर्थात् यह किसी भी कंपनी के राऊटर के साथ काम कर सकता है. इसे कभी कभी IP RIP भी कहते है. RIP एक क्लास्सफुल राऊटिंग प्रोटोकॉल है इस कारण यह VLSM (वेरिएबल लेंथ सबनेट मास्क) को सपोर्ट नहीं करता.

RIP एक डिस्टेंस वेक्टर राऊटिंग प्रोटोकॉल है. इसमें हॉप काउंट का प्रयोग मैट्रिक्स के रूप में सबसे उपयुक्त पथ (मार्ग) को निर्धारित करने के लिए किया जाता है. जिससे कि उस पथ से डेटा पैकेट्स डेस्टिनेशन तक पहुँच सकें.

RIP में हॉप्स की अधिकतम संख्या केवल 15 तक हो सकती है तथा इसमें हॉप काउंट 16 को अनंत (इनफिनिट) माना जाता है. हॉप काउंट 16 का प्रयोग ऐसे नेटवर्क को इंगित करने के लिए किया जाता है जिन्हें एक्सेस नहीं किया जा सकता है.इसका प्रयोग छोटे नेटवर्कों में किया जाता है.

RIP की कार्यप्रणाली

रूटिंग इनफार्मेशन प्रोटोकॉल या RIP एक डायनामिक रूटिंग प्रोटोकॉल है जो कि हॉप काउंट को एक रूटिंग के माप के तौर पर प्रयोग करता है और इसीके द्वारा वो सोर्स और डेस्टिनेशन के बीच में सबसे छोटे रास्ते कि गणना कर लेता है। ये एक डिस्टेंस वेक्टर रूटिंग प्रोटोकॉल है

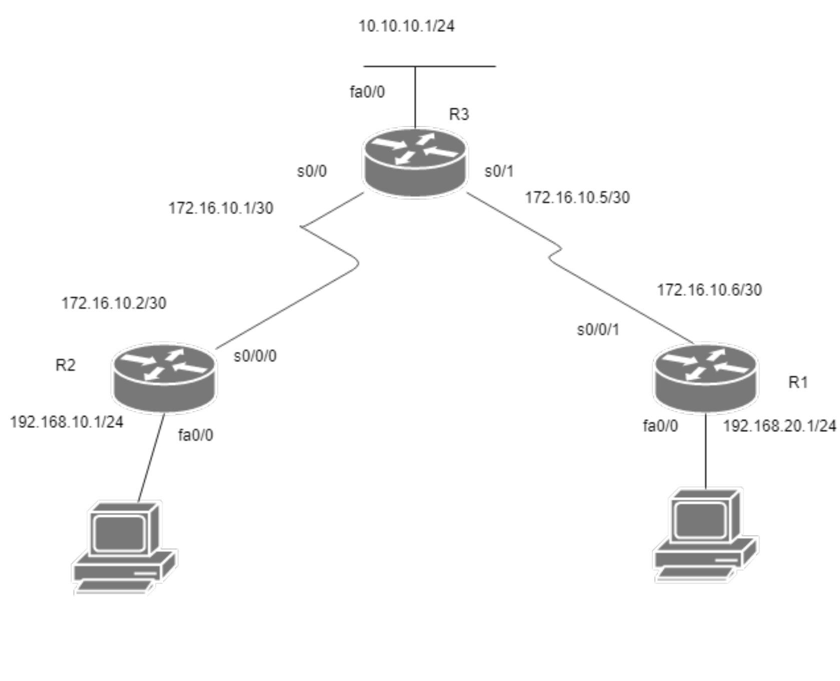
जिसका AD मान 120 होता है और ये ओपन सिस्टम इंटरकनेक्शन मॉडल (OSI) के आप्लिकतिओन लेयर पर काम करता है। ये पोर्ट संख्या 520 पर काम करता है।

हॉप काउंट

सीधे शब्दों में कहें तो हो काउंट का अर्थ हुआ डेस्टिनेशन और सोर्स के बीच कितने रॉयटर्स आ रहे हैं इस सब की संख्या। ऐसा रास्ता जिसमे हॉप काउंट सबसे कम हो उसे नेटवर्क तक पहुँचने का सबसे अच्छा रास्ता माना जाता है और फिर उसे रूटिंग टेबल में भी डाल दिया जाता है। RIP रूटिंग लूप से भी बचाता है और वो ऐसा डेस्टिनेशन और सोर्स के बीच के रास्ते में हॉप्स की संख्या को कम कर के करता है। सबसे ज्यादा हॉप काउंट जो RIP में हो सकते हैं वो हैं 15 और वो 16 होते ही वो नेटवर्क के पहुँच के B आहर हो जाता है।

RIP का कॉन्फ़िगरेशन

नीचे दिए गये टोपोलॉजी पर ध्यान दीजिये जहां पर कुल तीन राऊटर हैं- R1, R2, और R3. R1 का IP एड्रेस है- 172.16.10.6/30 on s0/0/1, 192.168.20.1/24 on fa0/0. R2 का IP एड्रेस है- 172.16.10.2/30 on s0/0/0, 192.168.10.1/24 on fa0/0. R3 का IP एड्रेस है- 172.16.10.5/30 on s0/1, 172.16.10.1/30 on s0/0, 10.10.10.1/24 on fa0/0.



चित्र 2.12 :रूटिंग इनफार्मेशन प्रोटोकॉल (IP एड्रेस कॉन्फ़िगरेशन)

अब हम **RIP** को **R1** के लिए ऐसे कॉन्फ़िगर करेंगे**:**

R1(config)# router rip

R1(config-router)# network 192.168.20.0

R1(config-router)# network 172.16.10.4

R1(config-router)# version 2

R1(config-router)# no auto-summary

no auto-summary कमांड ऑटो-summerization को डिसएबल कर देता है। अगर हम ऑटो-समरी को नहीं सेलेक्ट करेंगे तो सबनेट मास्क वर्जन 1 में क्लासफुल हो जाएगा।

अब R2 के लिए कॉन्फ़िगरेशन:

R2(config)# router rip

R2(config-router)# network 192.168.10.0

R2(config-router)# network 172.16.10.0

R2(config-router)# version 2

R2(config-router)# no auto-summary

इसी तरह R3 के लिए भी करेंगे:

R3(config)# router rip

R3(config-router)# network 10.10.10.0

R3(config-router)# network 172.16.10.4

R3(config-router)# network 172.16.10.0

R3(config-router)# version 2

R3(config-router)# no auto-summary

RIP के टाइमर्स

अपडेट टाइमर्स : ये रॉयटर्स द्वारा आदान-प्रदान हो रहे रूटिंग सम्बन्धी सूचनाओं के लिए एक डिफ़ॉल्ट टाइमर होता है जिसका ऑपरेटिंग RIP 30 सेकंड्स होता है। इस अपडेट टाइमर की मदद से सभी राऊटर पीरियड्स के आधार पर अपने-अपने रूटिंग टेबल को एक्सचेंज करते हैं।

इनवैलिड टाइमर्स : अगर 180 सेकंड्स तक कोई भी अपडेट नहीं आया तो डेस्टिनेशन राऊटर इसे इनवैलिड करार देता है। इस स्थिति में, डेस्टिनेशन राऊटर एक 16 हॉप काउंट उस राऊटर के लिए मार्क कर देता है।

होल्ड डाउन टाइमर : ये वो टाइमर है जिसमे कोई भी राऊटर अपने पड़ोस के राऊटर के जवाब का इन्तजार करता है। अगर दिए गये समय में पड़ोस का राऊटर रेस्पोंद करने में नाकाम साबित होता है तो इसे मरा हुआ घोषित कर दिया जाता है। ये डिफ़ॉल्ट के राउर पर 180 सेकंड्स होता है।

फ्लश टाइम : ये वो टाइमर है जिसके बाद रूट की एंट्री हटा दी जाएगी अगर वो सही समय में जवाब नहीं देता है तो। ये 60 सेकंड्स का डिफ़ॉल्ट होता है। ये टाइमर तब शुरू होता है जब रूट को इनवैलिड घोषित कर दिया गया हो।

2.3.4 ओपन शॉर्टेस्ट पाथ फर्स्ट प्रोटोकॉल (OSPF)

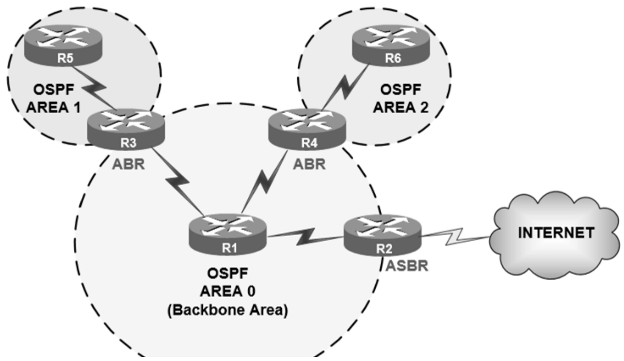
ओपन शॉर्टेस्ट पाथ फर्स्ट यानी कि OSPF को RIP के कुछ कमियों कि वजह से बनाया गया था। ये कमियां निम्नलिखित हैं:

- t15 हॉप काउंट की बंदिश
- रूटिंग हायरार्की के अंदर नेटवर्क को ऑर्गेनिसे करने में अक्षमता। ये बड़े क्षेत्र के नेटवर्क पर प्रबन्धन और परफॉरमेंस के लिए काफी जरूरी होता है।
- नेटवर्क ट्रैफिक में बहुत ही ज्यादा चढ़ाव जो कि बार-बार कुछ ही अंतराल पर routing टेब्स को बार-बार भेजने के कारण होता है।

जैसा कि इसके नाम से पता चलता है, OSPF एक ऐसा ओपन पब्लिक स्टैण्डर्ड है जिसे काफी बड़े तौर पर इंडस्ट्री में स्वीकार किया गया है। OSPF इनेबल किये हुए राउटर्स एक आइडेंटिफिकेशन मैसेज को भेजकर नेटवर्क की खोज करते हैं और उसके बाद एक ऐसा मैसेज

भेजते हैं जो कुछ रॉउटिंग के आइटम्स रखे होते हैं (बजाय रॉउटिंग टेबल्स के)। ये इस केटेगरी में लिस्ट किया गया एकमात्र स्टेट रॉउटिंग प्रोटोकॉल है।

OSPF की कार्यप्रणाली



चित्र 2.13 :ओपन शॉर्टेस्ट पाथ फर्स्ट प्रोटोकॉल

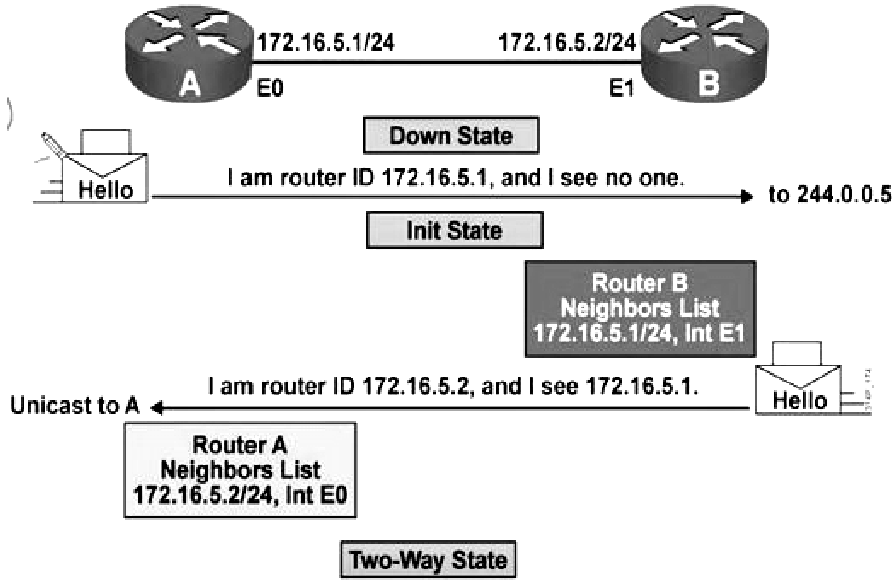
ये एक लिंक स्टेट प्रोटोकॉल है जिसे इंटीरियर गेटवे प्रोटोकॉल्स परिवार के बीच सबसे ज्यादा प्रसिद्ध माना गया है। इसे 80s के बीच में IETF जो कि एक वोर्किंग समूह है उसके द्वारा विकसित किया गया था। जब OSPF को कॉन्फ़िगर किया जाता है तब वो पड़ोसियों को सुनता है और सभी लिंक स्टेट डाटा को जमा करता है जिसके द्वारा नेटवर्क के अंदर उपलब्ध सभी के सभी रास्तों का एक टोपोलॉजी नक्शा बनाकर उस सूचना को अपने टोपोलॉजी डेटाबेस में सुरक्षित कर लेता है। इस डेटाबेस को लिंक स्टेट डेटाबेस (LSDB) कहते हैं।

अपने टोपोलॉजी डेटाबेस में जमा की हुई सूचनाओं के बल पर यह सारे उपलब्ध सबनेट या नेटवर्क तक बेस्ट शॉर्टेस्ट रास्ता चुनता है और उसके लिए जिस अल्गोरिथम का प्रयोग करता है उसे shortest पाथ फर्स्ट अल्गोरिथम (SFP) बोलते हैं। इसे कंप्यूटर वैज्ञानिक Edsger W. Dijkstra द्वारा 1956 में विकसित किया गया था। इसके बाद OSPF तीन टेबल बनाता है जिसमे निम्नलिखित सूचनाएँ रहती है:

नेबर(Neighbor टेबल): इसमें उन सारे OSPF पड़ोसियों की सोचना रहती है जिनसे डाटा का आदान-प्रदान किया जाता है।

टोपोलॉजी टेबल: इसमें नेटवर्क का पूरा का पूरा रोडमैप होता है जिसमे सारे OSPF routers की सूचनाएँ होती है और गणना किये गये सारे बेस्ट रास्ते और वैकल्पिक रास्तों की सूचनाएँ भी होती है।

रॉउटिंग टेबल: इसमें अभी के काम कर रहे बेस्ट वोर्किंग पाथ की सूचना रहती है जिसके द्वारा डाटा को ट्रांसमिट किया जा रहा होता है।



चित्र 2.14 :ओपन शॉर्टेस्ट पाथ फर्स्ट प्रोटोकॉल (रूटिंग कम्युनिकेशन)

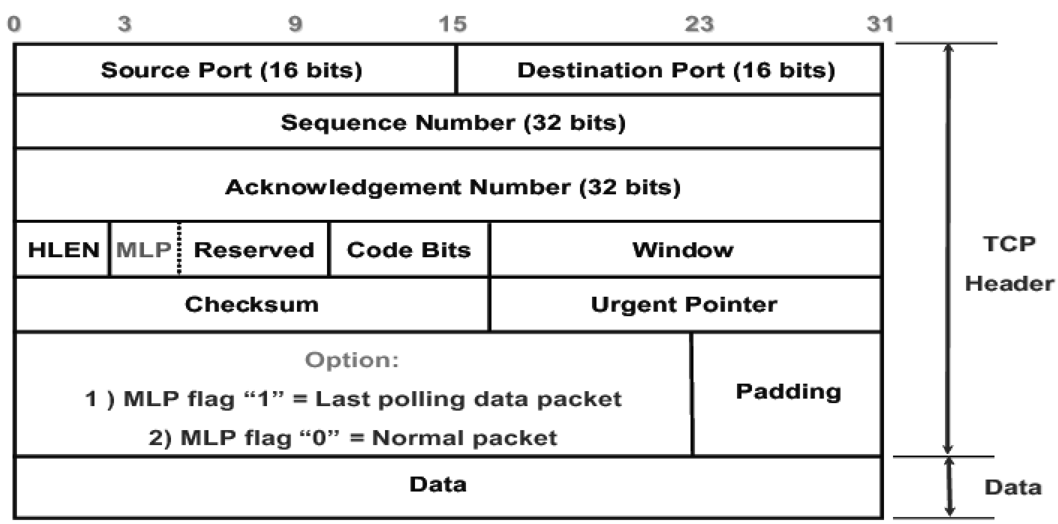
2.3.5 ट्रांसमिशन कंट्रोल प्रोटोकॉल (टी. सी. पी.)

ट्रांसमिशन कंट्रोल प्रोटोकॉल अर्थात Transmission Control Protocol (TCP) इंटरनेट कई नेटवर्क का जाल होता है। इस नेटवर्क से कई प्रकार के कम्पयुटर जुडे होते है। इन सभी को जोड़ने के लिय कुछ नियम से बने कंट्रोल प्रोटोकॉल होते है, जिसके माधय्म से सारे कम्पयुटर एक दुसरे के भाषा को समझ सके। उधारण के तौर पर किसी मेल को भेजने के लिये इसका फोर्मेट क्या हो, इसके लिये भी एक कंट्रोल प्रोटोकॉल होता है। सभी इंटरनेट मेल प्रोग्राम इस ट्रांसमिशन कंट्रोल प्रोटोकॉल को मानने के लिए बाध्य होते है। वर्तमान समय मे सैकडो़ प्रोटोकॉल को सामुहिक रूप से ट्रांसमिशन कंट्रोल प्रोटोकॉल (TCP) या इंटरनेट प्रोटोकॉल (IP) का नाम दिया गया है।

TCP प्रोटोकॉल एक कनेक्शन ओरिएंटेड प्रोटोकॉल है | कनेक्शन ओरिएंटेड से आशय डाटा को ट्रांसफर करने से पूर्व यह प्रोटोकॉल कनेक्शन को पूरी तरह से वेरीफाई करता है की रिसीवर डिवाइस से कनेक्शन शुरू हुवा है या नहीं इस प्रोसेस में क्लाइंट सर्वर को एक रिक्वेस्ट करता है जिसको सीन (SYN) कहा जाता है| रिस्पांस के तोर पर सर्वर क्लाइंट को एक रेकुएस करता

है जिसको सीन प्राप्ति (Syn acknowledgement) कहा जाता है ! TCP प्रोटोकॉल में इस कार्यप्रणाली को हैंड शॉकिंग(Hand शाकिंग) भी कहा जाता है |

TCP प्रोटोकॉल एक रिलाएबल प्रोटोकॉल (भरोसेबंद) है , यानि यह डाटा ट्रांसफर करते समय हैंड शाकिंग के आलावा भी ऐसी अनेक मैकेनिज्म (कार्य प्रणाली तंत्र) का इस्तमाल करता है | जिससे डाटा डेस्टिनेशन तक रिलाएबल तरिके से पहुचता है , TCP प्रोटोकॉल में डाटा डिलीवरी की पूरी तरह से गारंटी होती है | TCP प्रोटोकॉल में डाटा उसी सीक्वेंस(क्रम) में रिसीव होता है जिस सीक्वेंस में डाटा को सेंड किया जाता है ! यानि क्लाइंट और सर्वर में डाटा ट्रांसफर के समय डाटा का आर्डर चेंज नहीं होता है , यह फ्लो कण्ट्रोल के ऊपर भी वर्क करता है|! इस तरह के फंक्शनिंग और मैकेनिज्म के प्रयोग होने से तकप(ट्रांस्मिशन कण्ट्रोल प्रोटोकॉल), UDP(यूजर डाटाग्राम प्रोटोकॉल) की तुलना में एक धीरे कार्य करने वाला करने वाला प्रोटोकॉल है | TCP प्रोटोकॉल का इस्तमाल हम हमारे दैनिक जीवन में कहि प्रकार की सर्विस में करते है जैसे HTTP ,HTTPS ,Telnet ,FTP ,SMTP आदि इसका डाटा पैकेट निम्न प्रकार से होता है तथा हैडर की पूरी कार्यप्रणाली विस्तार से हम आगे के भाग में पड़ेंगे |

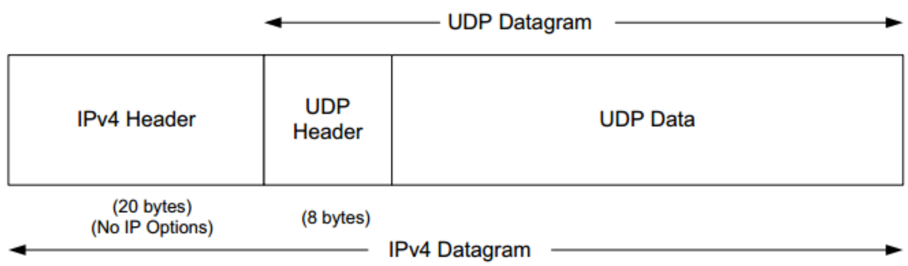


चित्र 2.15 : टी सी पी हैडर

2.3.6 यूजर डाटा ग्राम प्रोटोकॉल (यू.डी.पी.)

UDP एक कनेक्शन लेस प्रोटोकॉल है | इसमें डाटा को ट्रांसफर करने से पहले या कनेक्शन एस्टब्लिश करने से पहले किसी भी प्रकार की प्राप्ति सन्देश (acknowledgement) से रिलेटेड फंक्शनिंग नहीं होती है | यानि इसमें जो भी डिवाइस सर्वर या क्लाइंट यह कभी वेरीफाई नहीं

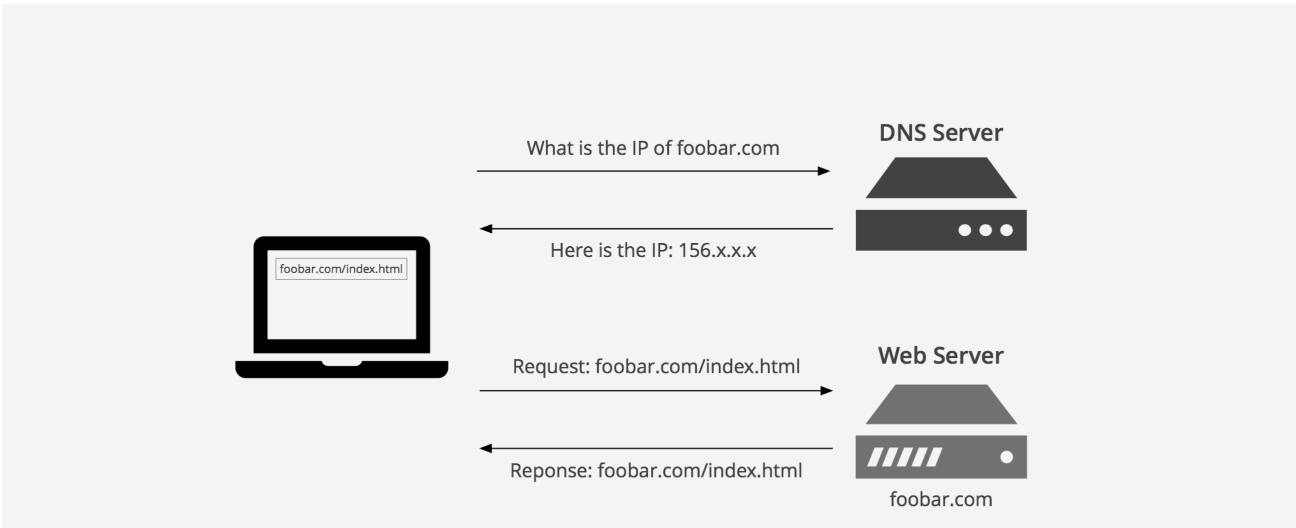
करता है, की रिसीवर से कनेक्शन है या नहीं, डाटा उसको मिला है या नहीं, इसके इसी कार्य प्रणाली की वजह से इसको कनेक्शन लेस प्रोटोकॉल कहा जाता है | इस के इस प्रकार के मैकेनिज्म (कार्य प्रणाली तंत्र) की वजह से इसमें डाटा डिलीवरी की कोई गारंटी नहीं होती है | इसमें अधिक काम्प्लेक्स फंक्शनिंग और मैकेनिज्म नहीं होने की वजह से इस प्रोटोकॉल की डाटा ट्रांसफर करने की स्पीड काफी अछि होती है | UDP में SNMTP ,TFTP जैसे सर्विसेज काम में ली जाती हे UDP को काम में लेनी वाली सर्विस का सबसे अच्छा उदारहण आज के वक्त में व्हाट्सअप और फेसबुक जैसे मैसेंजर है| हैडर की पूरी कार्यप्रणाली विस्तार से हम आगे के भाग में पड़ेंगे |



चित्र 2.16 : **यू डी पी हैडर**

2.3.7 डोमेन नाम सिस्टम (डी. एन. ए.)

डोमेन नाम सिस्टम को संक्षिप्त मे DNS भी कहा जाता है | DNS इंटरनेट डोमेन और होस्ट नाम को IP एड्रेस मे तथा IP एड्रेस को होस्ट नाम मे ट्रांसलेट करने का काम करता है | जब भी हम कंप्यूटर के ब्राउज़र मे किसी वेबसाइट का नाम टाइप करते है तो वो वेबसाइट उसके IP एड्रेस मे कन्वर्ट हो जाता है | डोमेन नाम IP एड्रेस मे ट्रांसलेट हो जाता है लेकिन क्या आपने कभी सोचा है की ये क्यों होता है | ऐसा इसलिए होता है क्योकि कोई भी कंप्यूटर जब भी नेटवर्क मे होता है तो वो IP एड्रेस को समझता है न की किसी होस्ट नाम को | किसी भी वेबसाइट का नाम अल्फाबेट्स(abcd आदि) मे इसलिए रखा जाता है क्योकि वो हमारे लिए आसान होता है और हम नेम्स को आसानी से याद रख सकते है | सोच कर दिखेये की अगर होस्ट नाम न हो और केवल IP एड्रेस याद रखने हो या फिर अगर IP एड्रेस से website को ओपन करना हो तो क्या हमारे लिए IP एड्रेस याद रखना संभव हो पायेगा – नहीं | तो DNS एक सर्विस होती है जो की डोमेन नेम्स (वेबसाइट का नाम) को IP एड्रेस मे तथा IP एड्रेस को डोमेन नाम (वेबसाइट नाम) मे परिवर्तित करती है |



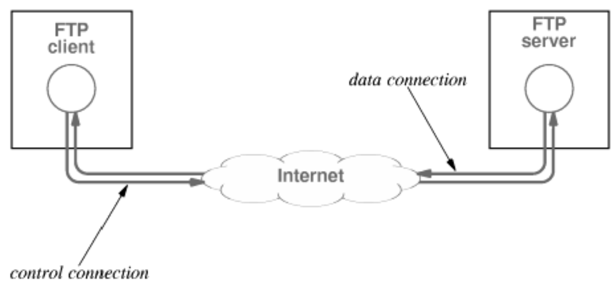
चित्र 2.17 : डोमेन नाम सिस्टम की कार्यप्रणाली

2.3.8 फाइल ट्रान्सफर प्रोटोकॉल (ऍफ़.टी.पी)

ऍफ़ टी पी (FTP) का पूरा नाम फाइल ट्रांसफर प्रोटोकॉल है। जैसा की नाम से पता चल रहा है की इसका उपयोग एक कंप्यूटर से दूसरे कंप्यूटर के बीच फाइल ट्रान्सफर करने के लिए किया जाता है। एफटीपी एक प्रकार का प्रोटोकॉल है जो की दो सिस्टम्स के बीच फाइलों के आदान-प्रदान के लिए सेट ऑफ़ रूल्स यानी की कुछ नियमों को निर्धारित करता है।

FTP प्रोटोकॉल बहुत ही पुराना प्रोटोकॉल है और आज भी इसका उपयोग हो रहा है इसके बावजूद कई सारे इंटरनेट उसेर्स ऐसे भी होंगे जिन्हें अभी तक FTP के बारे में पता नही होगा, लेकिन यदि आप कोई वेबसाइट बनाने जा रहें हैं तो आपके लिए यह बहुत ही उपयोगी टूल साबित हो सकता है। जब कोई वेब डेवलपर वेबसाइट बनाता है तो उस वेबसाइट के फाइल्स को सर्वर पर अपलोड 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। जब कोई भी डेवलपर वेबसाइट बनाता है तो उस वेबसाइट के फाइल्स को सर्वर पर

अपलोड 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।



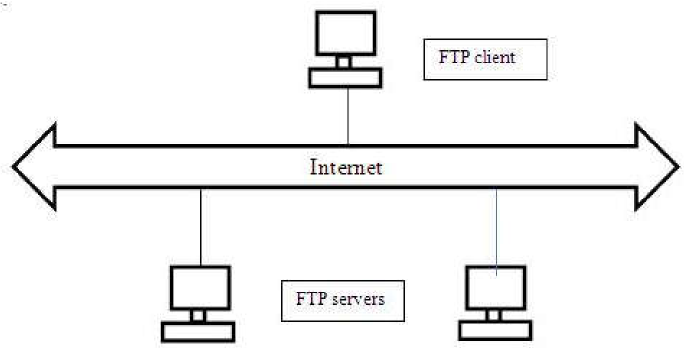
चित्र 2.18: फाइल ट्रान्सफर प्रोटोकॉल

फाइल ट्रान्सफर प्रोटोकॉल की कार्यप्रणाली

एफटीपी प्रोटोकॉल काम कैसे करता है। इसके लिए सबसे पहले यूजर के सिस्टम में FTP क्लाइंट इनस्टॉल होना चाहिए इसके अलावा सर्वर से कनेक्शन स्थापित करने के लिए आपके पास यूज़रनाम और पासवर्ड होनी चाहिए।

फाइल रोल कनेक्शन: इसका उपयोग कनेक्शन को ओपन या क्लोज करने और सर्वर को कमांड भेजने के लिया किया जाता है।

डाटा कनेक्शन: कनेक्शन स्थापित होने बाद डाटा कनेक्शन के माध्यम से क्लाइंट-सर्वर के बीच फाइल ट्रान्सफर किया जाता है। क्लाइंट द्वारा पोर्ट नंबर 21 पर कण्ट्रोल कनेक्शन शुरू किया जाता है कनेक्शन स्थापित होने पर क्लाइंट द्वारा कमांड्स भेजे जाते हैं और कमांड के अनुसार सर्वर पोर्ट नंबर 20 पर डाटा कनेक्शन शुरू करता है और इसी डाटा कनेक्शन के जरिये फाइलों को ट्रान्सफर किया जाता है।



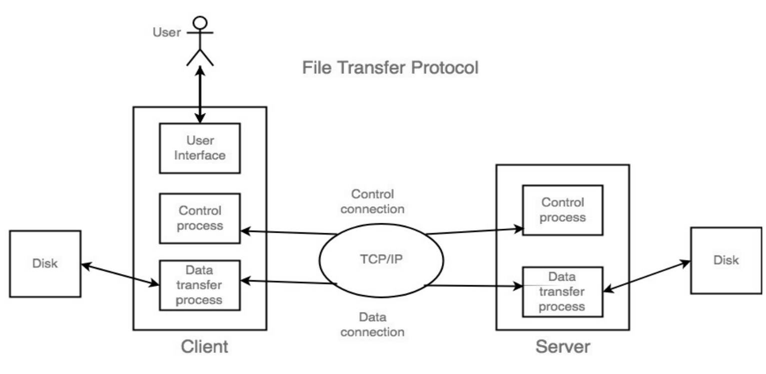
चित्र 2.19: फाइल ट्रान्सफर प्रोटोकॉल (क्लाइंट सर्वर)

FTP दो अलग-अलग मोड्स पर काम कर सकता है:

एक्टिव मोड तथा पैसिव मोड

एक्टिव मोड: एक्टिव मोड में क्लाइंट किसी भी पोर्ट नंबर (1023 से ज़्यादा) का उपयोग करके FTP सर्वर के पोर्ट 21 पर कनेक्ट हो जाता है यानी कण्ट्रोल कनेक्शन को ओपन कर देता है। इसके बाद क्लाइंट अपना पोर्ट नंबर सर्वर की बताता है जिसपर डाटा कनेक्शन एस्टब्लिश करना है। क्लाइंट का पोर्ट नंबर मिलने के बाद सर्वर अपने पोर्ट 20 से क्लाइंट के पोर्ट नंबर पर डाटा कनेक्शन को ओपन कर देता है।

पैसिव मोड: पैसिव मोड में क्लाइंट किसी भी पोर्ट नंबर (1023 से ज़्यादा) से FTP सर्वर के पोर्ट 21 पर कमांड कनेक्शन को ओपन करता है। FTP क्लाइंट उस कमांड कनेक्शन के माध्यम से सर्वर को PASV कमांड भेजता है। FTP सर्वर उसी कमांड कनेक्शन से अपना पोर्ट नंबर FTP क्लाइंट को बताता है। FTP क्लाइंट की तरफ से क्लाइंट के पोर्ट नंबर और सर्वर द्वारा बतायगये पोर्ट नंबर के बीच डाटा कनेक्शन ओपन कर दिया जाता है।



चित्र 2.20 : ऍफ़ टी पी कनेक्शन

संदर्भ ग्रंथो की सूची

a) Spurgeon, Charles E. (2000) *Ethernet: The Definitive Guide*, O'Reilly Media

b) Tanenbaum, A.S. (2002) Computer Networks, Prentice Hall.

c) Douglas E. Comer, Computer Networks and Internets

d) D. Bertsekas & R. Gallager, *Data Networks*.

e) S. Keshav, An Engineering Approach to Computer Networking.

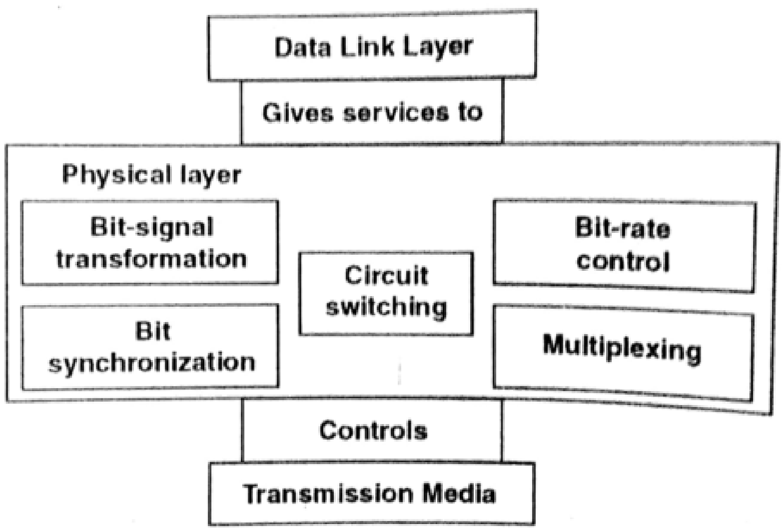
f) J. Walrand & P. Varaiya, *High-Performance Communication Networks*.

g) A. Bakre and B. R. Badrinath, "I-TCP: Indirect TCP for Mobile Hosts," Proc. 15th Int'l. Conf. Distributed Computing Systems (IDCS)

h) वैज्ञानिक तथा तकनीकी शब्दावली आयोग द्वारा प्रकाशित मूलभूत शब्दावली

3.1 फिजिकल लेयरः–

फिजिकल लेयर वह लेयर है, जो मुख्य रूप से ट्रांसमिशन मीडिया से कम्यूनिकेट करती है। इसमें नेटवर्क का वह फिजिकल पार्ट शामिल होता है, जो नेटवर्क के कॉम्पोनेंट्स को एक–दूसरे से जोड़ता है। यह लेयर नेटवर्क के एक नोड से अगले नोड तक इंफॉर्मेशन को भौतिक रूप से भेजने में सहभागी होती है। 5–लेयर इंटरनेट मॉडल में फिजिकल लेयर की पोजीशन को में समझाया गया है।



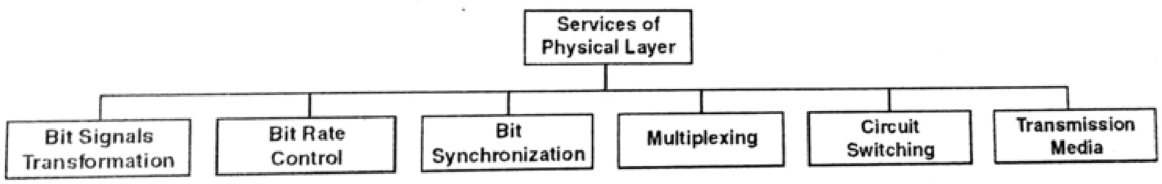
चित्र 3.1 : ओ एस आई मॉडल में फिजिकल लेयर की स्थिति

फिजिकल लेयर को कई जटिल कार्य सम्पन्न करने होते है। इनमें से एक प्रमुख कार्य डाटा लिंग लेयर को सेवा प्रदान करना है। डाटा लिंग लेयर में डाटा 0s और 1s से बने होते है। इन्हें फ्रेम्स में व्यवस्थित किया जाता है, जो ट्रांसमिशन मीडियम के आर–पार भेजे जाने के लिए तैयार रहती है। 0s और 1s की इस स्ट्रीम को सर्वप्रथम अन्य एंटीटी सिग्नल्स में बदलना पड़ता है। फिजिकल लेयर द्वारा प्रदान की जाने वाली सेवाओं में एक ऐसा सिग्नल निर्मित करना भी शामिल होता है, जो बिट्स की इस स्ट्रीम को दर्शाता हो।

फिजिकल लेयर द्वारा दी जाने वाली सेवाएँः—

फिजिकल लेयर सेंडर से रिसीवर तक बिट्स की स्ट्रीम प्रेषित करती है। ट्रांसफर नोड—टू—नोड, एक नोड से अगले नोड तक होता है। समीपवर्ती दो नोड्स की फिजिकल लेयर्स एक ऐसा लॉजिकल पाईप उपलब्ध कराती हैं, जिसमें से बिट्स यात्रा कर सकती है।

चित्र 3.2 में फिजिकल लेयर द्वारा उपलब्ध कराई जाने वाली सामान्य सेवाओं को दर्शाया गया है।



चित्र 3.2 : फिजिकल लेयर की सेवाएं

1. **बिट से सिग्नल में रूपांतरणः** फिजिकल लेयर के अंतर्गत लॉजिकल पाईप ट्रांसमिशन माध्यम बिट्स को ट्रांसफर नहीं कर सकता है, अस्तु हमें बिट्स को एक ऐसे सिग्नल अर्थात् इलेक्ट्रोमेग्नेटिक ऊर्जा द्वारा दर्शाया जाने की आवश्यकता होती है, जो माध्यम के द्वारा ट्रांसफर किया जा सके।
2. **बिट रेट कंट्रोल** : चूँकि ट्रांसमिशन माध्यम ही डाटा रेट की ऊपरी सीमा का पता लगाता है, अस्तु फिजिकल लेयर कंट्रोलर होती है। फिजिकल लेयर की हार्डवेयर और सॉफ्टवेयर की डिजाईन डाटा रेट का निर्धारण करती है।
3. **बिट सिंक्रोनाईजेशन** : डाटा कम्यूनिकेशन्स में बिट ट्रांसफर की टाईमिंग महत्वपूर्ण है। फिजिकल लेयर ऐसी क्लॉकिंग विधि उपलब्ध कराते हुए बिट्स के सिंक्रोनाईजेशन को निष्पादित करती है, जो सेंडर और रिसीवर दोनों को नियंत्रित करें।
4. **मल्टीप्लेक्सिंग** : मल्टीप्लेक्सिंग किसी लिंक अर्थात् भौतिक माध्यम को बेहतर कार्य कुशलता के लिए लॉजिकल चैनल्स में विभाजित कर दिए जाने की प्रक्रिया है। फिजिकल लेयर विविध विधियों का उपयोग करते हुए इसे सम्पन्न करती है।
5. **स्विचिंग** :—डाटा कम्यूनिकेशन्स में स्विचिंग को विभिन्न लेयर्स में निष्पादित किया जा सकता है। हमारे पास सर्किट स्विचिंग, पैकेट स्विचिंग और मैसेज स्विचिंग होती हैं। दो नोड्स को एक समर्पित (डेडिकेड) लिंक रखने की अनुमति प्रदान करने वाली सर्किट स्विचिंग विधि

अधिकतर फिजिकल लेयर का कार्य है। पैकेट स्विचिंग डाटा लिंक लेयर और नेटवर्क लेयर का मामला है।

6. **ट्रांसमिशन मीडिया** : फिजिकल लेयर अपनी बिट्स के ट्रांसफर हेतु ट्रांसमिशन मीडिया (माध्यम) पर निर्भर होती है। हालांकि ट्रांसमिशन माध्यम वस्तुतः फिजिकल लेयर का अंश नहीं होते हैं, फिर भी ये माध्यम इस लेयर द्वारा नियंत्रित होते है। माध्यम निर्देशित और अनिर्देशित हो सकते हैं। ट्विस्टेड पेयर केबल, कोएक्सियल केबल तथा फाईबर ऑप्टिक केबल्स निर्देशित माध्यम के खण्ड में आते हैं। रेडियो तथा माईक्रोवेव कम्यूनिकेशन अनिर्देशित खण्ड में आते हैं।

3.2 मल्टीप्लेक्सिंग

3.2.1 प्रस्तावनाः—जब दो उपकरण पॉईंट—टू—पॉईंट लिंक द्वारा जुड़ते हैं, तो सामान्यतः मल्टीपल फ्रेम्स का अतिरिक्त रूप से होना वांछनीय हो जाता है। इससे स्टेशन्स के मध्य डाटा लिंक में रूकावट नहीं आती है। अब इसके विपरीत स्थिति पर गौर करें। जब कम्यूनिकेट करने वाले दो स्टेशन्स डाटा लिंक की पूरी क्षमता का उपयोग न करें। कार्यक्षमता बढ़ाने के लिए उस क्षमता में साझेदारी करना संभव हो सकता है। ऐसी साझेदारी को ही मल्टीप्लेसिंग का नाम दिया गया है।

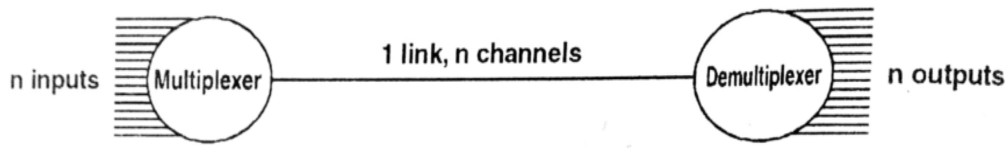
मल्टीप्लेक्सर :

भौतिक चैनल को विभिन्न लॉजिकल चैनल्स में विभाजित करने की वह तकनीक जिससे अनेक स्वतंत्र सिग्नल्स को एक साथ इस पर ट्रांसमिट किया जा सके, मल्टीप्लेक्सिंग के रूप में जानी जाती है। वह इलेक्ट्रॉनिक उपकरण जो यह कार्य करता है, मल्टीप्लेक्सर के रूप में जाना जाता है। मल्टीप्लेक्सर कम गति की विभिन्न संचार लाईनों को एक साथ लाता है, उन्हें एक उच्च गति वाले चैनल में बदलता है और दूसरे छोर पर ऑपरेशन को पलट देता है। आज कल प्रोग्राम किए जा सकने वाले मल्टीप्लेक्सर भी उपलब्ध हो गए हैं।

मल्टीप्लेक्सिंग का एक सर्वसामान्य उपयोग, लंबी दूरी के संचार में होता है।

मल्टीप्लेक्सिंग फंक्शन को उसके सरलतम स्वरूप में दर्शाया गया है। मल्टीप्लेक्सर में यहाँ n इनपुट्स हैं। मल्टील्पेक्सर सिंगल डाटा लिंक द्वारा एक डिमल्टीप्लेक्सर से जुड़ा हुआ है। लिंक डाटा

के n भिन्न चैनल्स को ले जाने में सक्षम है। मल्टील्पेक्सर n इनपुट लाईंस से डाटा को जोड़ता (मल्टीप्लेक्स करता) है। डिमल्टीप्लेक्सर मल्टीप्लेक्स की गई डाटा स्ट्रीम को ग्रहण करता है, चैनल्स के अनुसार डाटा को पृथक (डिमल्टीप्लेक्स) करता है और उन्हें यथोचित आऊटपुट लाईंस पर डिलीवर करता है।



चित्र 3.3 : मल्टीप्लेक्सिंग

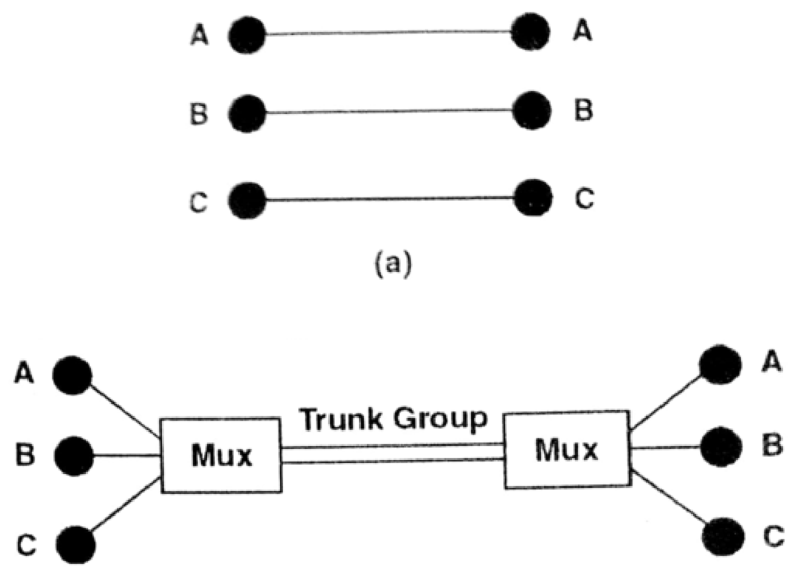
डाटा कम्यूनिकेशसन्स में मल्टीप्लेक्सिंग के बड़े पैमाने पर किए जा रहे उपयोग को निम्न प्रकार से समझाया जा सकता है–

- डाटा रेट जितनी उच्च होगी, ट्रांसमिशन सुविधा उतनी ही किफायती होगी। अर्थात् किसी दी गई एप्लीकेशन में विशेष दूरी के लिए प्रति kbps लागत, ट्रांसमिशन सुविधा की डाटा रेट में वृद्धि के साथ कम होती जाती है।
- अधिकांश व्यक्तिगत डाटा संचार उपकरणों को तुलनात्मक रूप से मध्यम श्रेणी की डाटा रेट की सहायता की आवश्यकता होती है।

3.2.2 मल्टीप्लेक्सिंग के प्रकार :

यहाँ हम तीन प्रकार की मल्टीप्लेक्सिंग तकनीकों पर ध्यान केंद्रित कर रहे है। प्रथम, फ्रीक्वेंसी डिविजन मल्टीप्लेक्सिंग (FDM) सर्वाधिक प्रयुक्त की जाती है और रेडियो तथा टेलिवीजन सेट में सामान्य है। दूसरी टाईम डिविजन मल्टीप्लेक्सिंग (TDM) का विशिष्ट प्रकरण है, जो सिंक्रोनस TDM के रूप में जानी जाती है। इसे डिजिटाईज्ड वॉइस स्ट्रीम्स और डाटा स्ट्रीम्स के मल्टीप्लेक्सिंग हेतु सामान्य तौर पर प्रयुक्त किया जाता है। हम सिंक्रोनस TDM में मल्टीप्लेक्सर की जटिलता को जोडते हुए उसकी कार्य कुशलता में वृद्धि करते हैं। इसे स्टेटिस्टिकल TDM एसिंक्रोनस TDM और इंटेलीमेंट TDM जैसे विभिन्न नामों से जाना जाता है। तीसरा प्रकार वेवलैंथ

डिविजन मल्टीप्लेक्सिंग (WDM) का एक विशिष्ट प्रकरण है, जो FDM का ऑप्टिकल डोमेन संस्करण है।

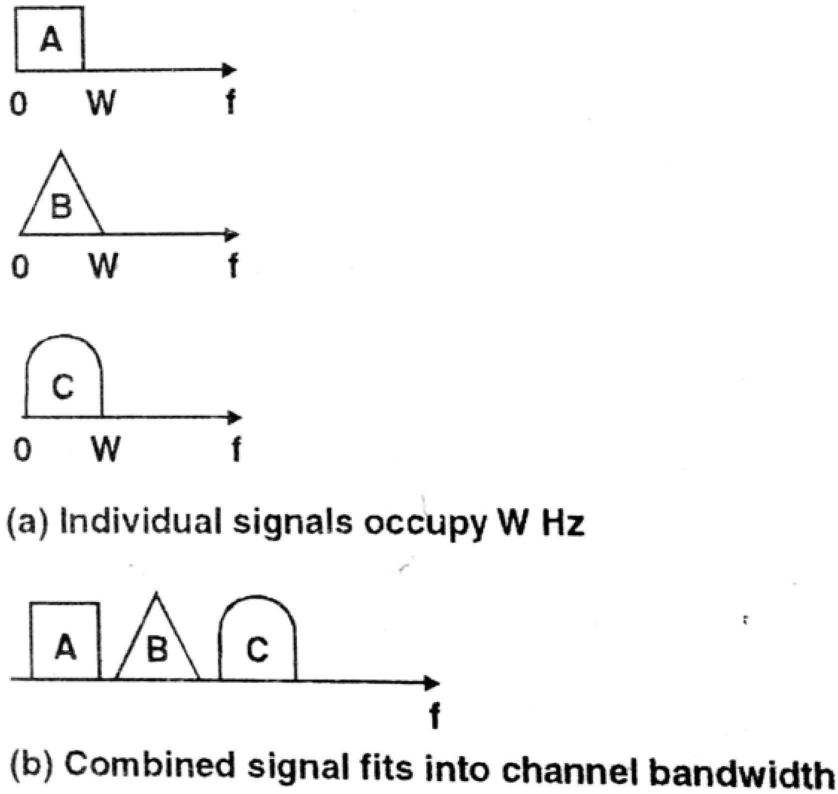


चित्र 3.4 : मल्टीप्लेक्सिंग प्रक्रिया

1. फ्रीक्वेंसी डिविजन मल्टीप्लेक्सिंग :

FDM तब संभव होता है, जब ट्रासमिशन माध्यम की उपयोगी बैंडविड्थ ट्रांसमिट किए जाने वाले सिग्नलों की आवश्यक बैंडविड्थ से अधिक हो जाती है। अनेक सिग्नल्स तब एक साथ ले जाए जा सकते हैं, जबकि प्रत्येक सिग्नल को एक भिन्न केरियर फ्रीक्वेंसी में मॉड्यूलेट कर दिया जाए और केरियर फ्रीक्वेंसीज को इस प्रकार पर्याप्त रूप से पृथक कर दिया जाए जिससे कि सिग्नल्स की बैंडविड्थ्स में कोई महत्वपूर्ण ओवर लेपिंग न आ जाए।

इस प्रकार फ्रीक्वेंसी डिविजन मल्टीप्लेक्सिंग (FDM) में बैंडविड्थ को अनेक विभिन्न फ्रीक्वेंसी स्लॉट्स में विभाजित कर दिया जाता है, जिनमें से प्रत्येक किसी व्यक्तिगत कनेक्शन के सिग्नल की प्रतिपूर्ति कर सकता है। मल्टीप्लेक्सर प्रत्येक कनेक्शन को एक फ्रीक्वेंसी स्लॉट प्रदान करता है और कनेक्शन के सिग्नल को स्लॉट विशेष में रखने के लिए मॉड्यूलेशन का उपयोग करता है।



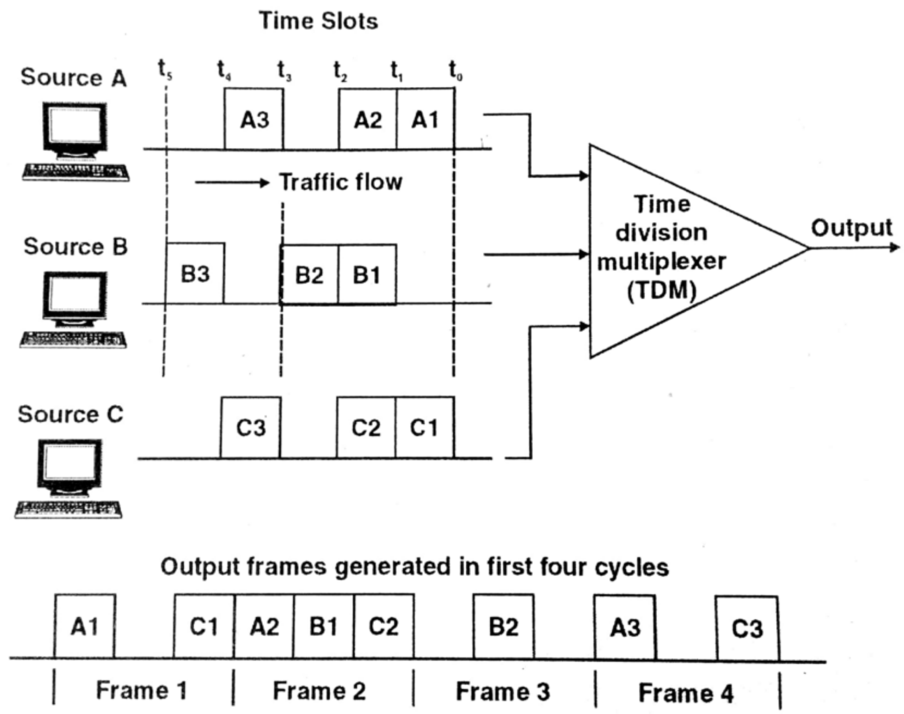
चित्र 3.5 : मल्टीप्लेक्सिंग (व्यक्तिगत संयुक्त)

ब्रॉड कॉस्ट रेडियो और ब्रॉडकॉस्ट केबल टेलीविजन FDM के उदाहरण हैं। इनमें प्रत्येक स्टेशन को एक विशेष फ्रीक्वेंसी बैंड प्रदान किया जाता है। FDM को सेल्यूलर टेलीफोन में भी प्रयुक्त किया जाता है, जहाँ एक भौगोलिक इकाई के अंतर्गत यूजर्स के द्वारा प्रादर्श रूप से 25 से 30 kHz प्रत्येक के फ्रीक्वेंसी स्लॉट्स के सेट में साझेदारी की जाती है। प्रत्येक यूजर को प्रत्येक दिशा के लिए एक फ्रीक्वेंसी स्लॉट प्रदान किया जाता है।

2. टाईम डिविजन मल्टीप्लेक्सिंग :

FDM प्रकरण के फ्रीक्वेंसी स्लॉट्स के विपरीत टाईम डिविजन मल्टीप्लेक्सिंग (TDM) में ट्रांसमिशन टाईम स्लॉट्स का उपयोग किया जाता है। (TDM) में ट्रांसमिशन टाईम स्लॉट्स का उपयोग किया जाता है। TDM विधि को तब प्रयुक्त किया जा सकता है, जब भेजने और ग्रहण करने वाली प्रत्येक डिवाईसेस की डाटा रेट, ट्रांसमिशन लिंक की डाटा रेट क्षमता से बहुत कम हो।

ऐसी परिस्थिति में एक लाईन पर एकाधिक (मल्टीपल) स्वतंत्र सिग्नलों का एक साथ ट्रांसमिशन प्रत्येक डाटा स्त्रोतों से प्राप्त होने वाली बिट्स को उनके टाईम स्लॉट्स के बीच में क्रमानुसार (सीक्वेंशियली) लगाते हुए प्राप्त किया जा सकता है।



चित्र 3.6 : सिंक्रोनस टाइम डिवीज़न मल्टीप्लेक्सिंग

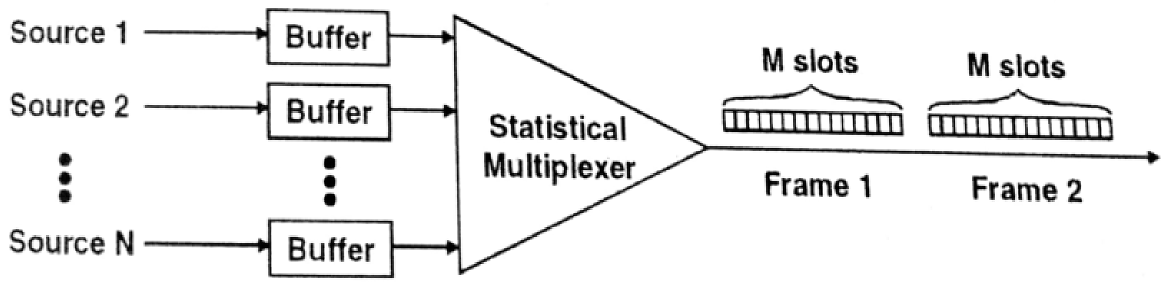
(i) सिंक्रोनस टाईम डिविजन मल्टीप्लेक्सिंग : यदि लोअर स्पीड लाईंस में से प्रत्येक में हॉयर स्पीड लाईन की ओर तुलनात्मक रूप से ट्रेफिक का स्थिर प्रवाह दिखाई देता है, तो ऐसी स्थिति में सामान्यतः सिंक्रोनस टाईम डिविजन मल्टीप्लेक्सिंग का उपयोग किया जाता है।

सिंक्रोनस TDM में सामान्यतः TDMके रूप में ही जाना जाता है। इस विधि में ट्रांसमिशन टाईम को N समान आकार वाले स्लॉट्स के ब्लॉक्स अथवा फ्रेम्स में विभाजित कर दिया जाता है, जैसा कि चित्र 3.6 में दर्शाया गया है। यदि N इनपुट लिंक्स हों और वह प्रत्येक k बिट्

स प्रति सेकंड की दर पर कार्यरत हो तो ज्क्ड उनकी इंफॉर्मेशन स्ट्रीम्स को $(Nk + \Delta)bps$ ही हॉयर रेट बिट स्ट्रीम में जोड़ देगा। फेक्टर Δ कम्पोजिट डाटा स्ट्रीम में अतिरिक्त सिंक्रोनाईजेशन बिट्स को सम्मिलित किए जाने की संभावना दर्शाता है। TDM विधि में प्रत्येक इनपुट लाईन को

उसका डाटा भौतिक लिंक पर भेजने का अवसर चक्रीय आधार (रांउड रोबिन) पर प्रदान किया जाता है।

(ii) स्टेटिस्टीकल टाईम डिविजन मल्टीप्लेक्सिंग : सिंक्रोनस TDM विधि तब उपयोगी नहीं होती है, जबकि लाईन में 'बर्स्टी' ट्रेफिक ट्रांसमिट हो रहा हो। ऐसा तब हो सकता है, जब यूजर लंबे निष्क्रीय अंतराल के बाद इंफॉर्मेशन की एकाएक बौछार (बर्स्ट) कर दें। ऐसा आधुनिक नेटवर्क की स्थिति में विशेष रूप में LANs में होता है। इस स्थिति में स्टेटिस्टीकल TDM अथवा एसिंक्रोनस TDM लाईन के उपयोग की एक प्रभावी विधि होती है। स्टेटिस्टीकल TDM इस तथ्य का लाभ लेती है कि सभी नेटवर्क ट्रेफिक स्त्रोत एक ही समय पर ट्रांसमिशन नहीं करते हैं।



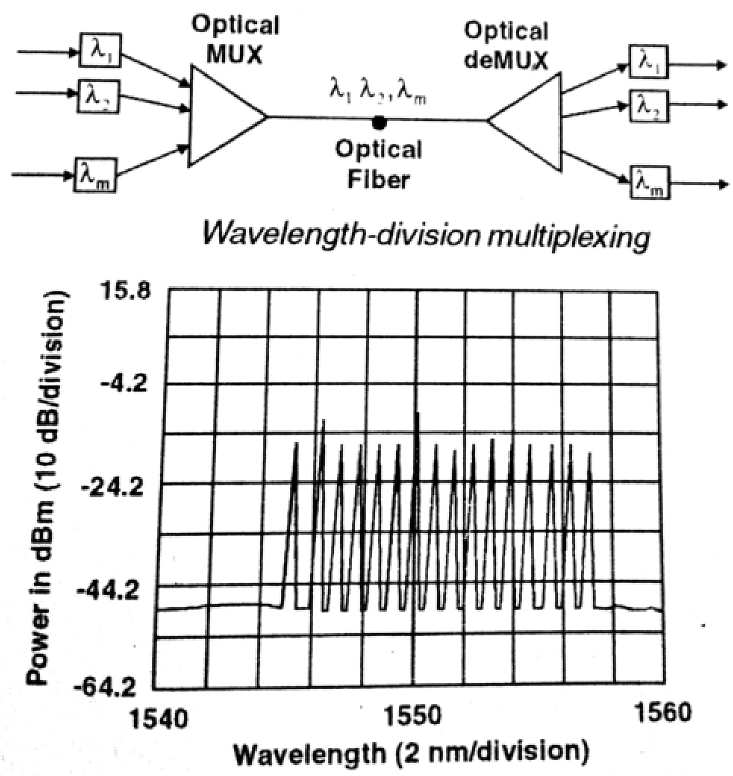
चित्र 3.7 : स्टैटिकल डिवीज़न मल्टीप्लेक्सिंग (M < N टाइम स्लॉट)

चित्र स्टेटिस्टीकल TDM की अवधारणा को दर्शाता है। यहाँ N इनपुट लाईंस से पैकेट्स उपलब्ध M टाईम स्लॉट्स में मल्टीप्लेक्स्ड किए जाने की प्रतीक्षा कर रहे है। किसी एसिंक्रोनस TDM फ्रेम में टाईम स्लॉट्स M की संख्या इनपुट लाईंस N की संख्या से कम होती है। यह किसी दिए गए समय पर प्रेषित की जा सकने वाली इनपुट लाईंस की संख्या के स्टेटिस्टीकल परिकलपन पर आधारित होती है।

सामान्यतः पैकेट्स को सभी की एक समान प्राथमिकता होने पर फर्स्ट–इन–फर्स्ट–आऊट (FIFO) अर्थात् पहले आने वाले को पहले भेजने की रीति में ट्रांसमिट किया जाता है। स्टेटिस्टीकल मल्टीप्लेक्सर्स के कुछ प्रकार पैकेट्स को उनकी प्राथमिकता के अनुसार ट्रांसमिट कर सकते हैं। यह प्राथमिकता पैकेट हेडर में पहले से आवंटित की गई एक कंट्रोल बिट द्वारा निर्दिष्ट की जाती है।

3. वेवलैंथ डिविजन मल्टीप्लेक्सिंग :

एकल ऑप्टिकल फाईबर द्वारा ट्रांसमिट की जाने वाली इंफॉर्मेशन के वेवलैंथ डिविजन मल्टीप्लेक्सिंग (WDM) का उपयोग करते हुए बढ़ाया जा सकता है। WDM को FDM के ऐसे ऑप्टिकल डोमेन संस्करण के रूप में देखा जा सकता है, जिसमें एकाधिक इंफॉर्मेशन सिग्नल्स द्वारा ऑप्टिकल सिग्नल्स को विभिन्न ऑप्टिकल वेवलैंथ अर्थात् रंगों पर मॉड्यूलेट किया जाता है। आऊटपुट (परिणामी) सिग्नल्स को जोड़ा जाता है तथा चित्र 3.8 में दर्शाए अनुसार एक साथ उसी ऑप्टिकल फाईबर पर प्रेषित कर दिया जाता है। रंगों के सिग्नल्स को मिलाने और पृथक करने के लिए प्रिज्म और अपवर्तकों को प्रयुक्त किया जा सकता है। चित्र में ऐसे ही एक सिस्टम में ट्रांसमिट किया गया सिग्नल दर्शाया गया है। OC-192 पर 32 वेवलैंथ वाले WDM सिस्टम्स भी उपलब्ध हैं, जिसमें 320 gbps की कुल बिट रेट होती है। WDM का एक लाभ यह है कि अतिरिक्त ऑप्टिकल फाईबर उपयोग में लाने के विपुल निवेश के बिना ही बैंडविड्थ में अत्याधिक वृद्धि प्राप्त की जा सकती है।



चित्र 3.8 : वेवलेंथ (2 nm / डिवीज़न)

3.3 सिंग्नल एंड एन्कोडिंग तकनीक

3.3.1 प्रस्तावना : कम्प्यूनिकेशन लिंक निर्मित करते समय, ट्रांसमिट किए गए डिजिटल सिग्नल के फॉर्मेट को ध्यान में रखना चाहिए। यह इसलिए महत्वपूर्ण है, क्योंकि रिसीवर को प्राप्त होने वाले सिग्नल से ठीक–ठीक टाईमिंग इंफॉर्मेशन प्राप्त करने में सक्षम होना चाहिए। टाईमिंग के तीन मुख्य उद्देश्य निम्न हैं–

1. SNR के अधिकतम होने पर रिसीवर द्वारा सिग्नल का नमूना लेने की अनुमति देने के लिए।
2. पल्स के मध्य उचित अंतर रखने के लिए।
3. प्रत्येक टाईमिंग इंटरवेल के प्रारंभ और अंत को निर्दिष्ट करेन के लिए।

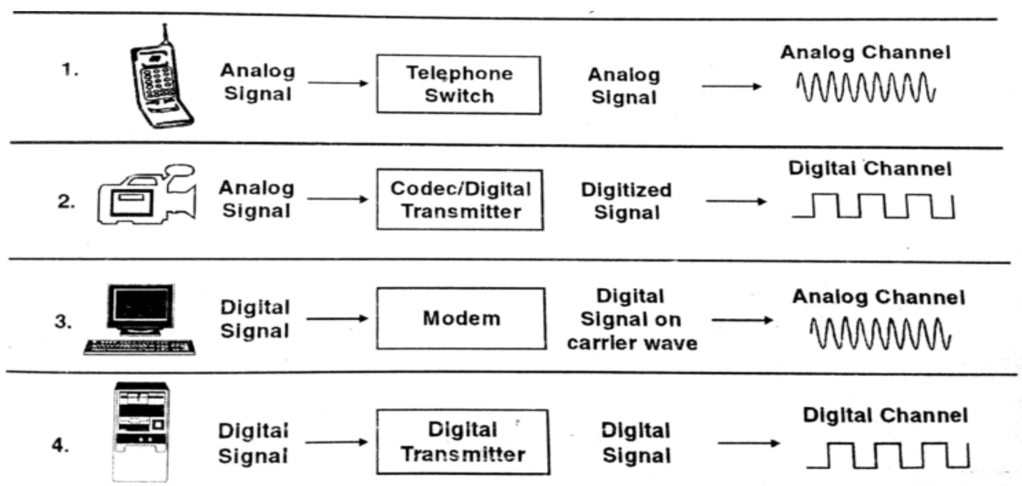
यहाँ हम एनालॉग अथवा डिजिटल चैनल्स पर ट्रांसमिशन के लिए डिजिटल बिट स्ट्रीम्स के एनकोडिंग पर ध्यान केंद्रित करेंगे। किसी एनालॉग चैनल पर डिजिटल डाटा को ट्रांसमिट करने के लिए डिजिटल बिट स्ट्रीम को साइन्यूसॉइडल (ऐसा हो सके) तरीके से उस परिवर्तनशील वेब फॉर्म पर सुपरइम्पोज किया जाता है, जो ट्रांसमिशन माध्यम की ट्रांसफर प्रॉपर्टीज के साथ पूरी तरह से मेल खाता हो। यह साईन वेब केरियर वेब कहलाती है।

किसी डिजिटल चैनल पर मैसेज बिट्स को ट्रांसमिट करते समय एनकोडिंग प्रक्रिया में ऐसी विधियाँ सम्मिलित हो सकती है, जो बिट स्ट्रीम को एक ऐसे स्वरूप में बदल दें, जिसमें टाईमिंग सक्षमताएँ अतिनिर्हित हों, ऍरर कंट्रोल के लिए रीडन्डेंट बिट्स को जोड़ा जा सके अथवा बिट स्ट्रीम से टाईमिंग एक्सट्रेक्शन को सुधारने के क्रम में 1 अथवा 0 की लंबी स्ट्रींग्स को टालने के लिए रेंडम रूप में सिम्बल्स को व्यवस्थित किया जा सके।

चित्र में दर्शाए अनुसार एनालॉग और डिजिटल दोनों ही सिग्नल्स या तो एनालॉग अथवा डिजिटल ट्रांसमिशन सिस्टम्स द्वारा ट्रांसमिट किए जा सकते हैं। यह दर्शाता है कि हमारे पास निम्नलिखित चार उपयुक्त कॉम्बीनेशल्स होते हैं–

1. एनालॉग लाईन पर ट्रांसमिट किया गया एनालॉग सिग्नल। उदाहरण के लिए एक एनालॉग टेलीफोन लाईन पर वॉईस सिग्नल को उसके मौलिक स्वरूप में सीधे ही ट्रांसमिट किया जा सकता है।

2. एक एनालॉग सिग्नल को डिजिटल बिट स्ट्रीम द्वारा अधिक स्पष्टता के साथ गतिशील किया जा सकता है और डिजिटल चैनल पर ट्रांसमिट किया जा सकता है।
3. एक मॉडेम (मॉड्यूलेटर/डिमॉड्यूलेटर) एक डिजिटल सिग्नल (अथवा डिजिटाईज किए गए एनालॉग सिग्नल) को सुपरइम्पोज करता है, जिसे तदुपरांत एक एनालॉग चैनल पर ट्रांसमिट किया जाता है।
4. डिजिटल लाईन पर डिजिटल सिग्नल को सीधे ही ट्रांसमिट किया जा सकता है।



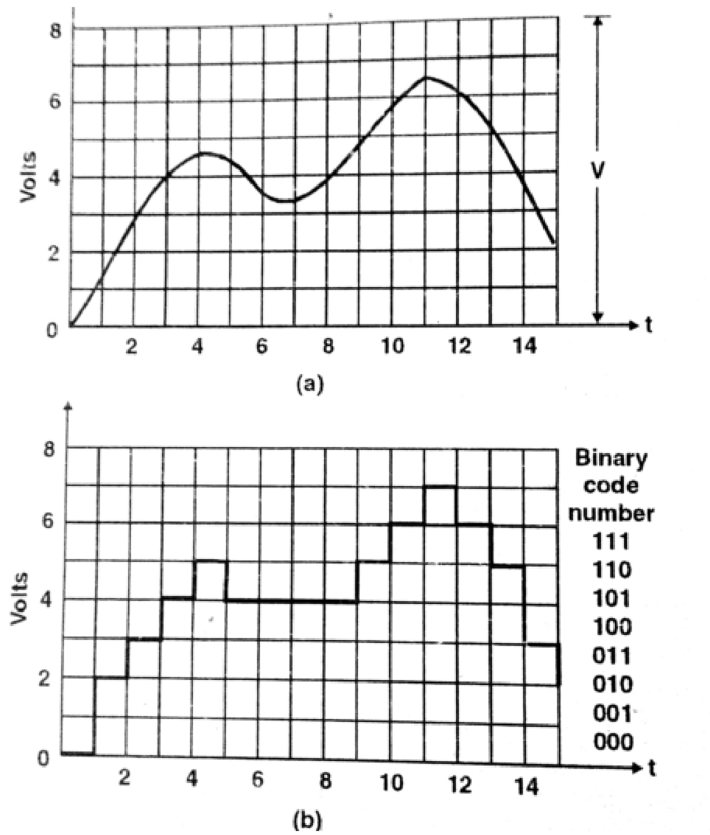
चित्र 3.9 : एनालॉग एंड डिजिटल सिग्नल (एनालॉग एंड डिजिटल ट्रामसनीशन द्वारा

एनालॉग सिग्नल्स का डिजिटल स्वरूप में रूपांतरण :

हम जानते हैं कि एनालॉग इंफॉर्मेशन संभाषण (स्पीच), ऑडियो सिग्नल्स और वीडियो से निर्मित होती है। ये सभी मानवीय संचार में आवश्यक है और विभिन्न मल्टीमिडिया एप्लीकेशन्स में प्रयुक्त किए जाते हैं। एनालॉग सिग्नल को डिजिटल फॉर्मेट में परिवर्तित करने की प्रक्रिया डिजिटाईजेशन के रूप में जानी जाती है। इस प्रक्रिया को सम्पन्न करने और डिजिटाईज्ड फॉर्मेट से एनालॉग सिग्नल को प्राप्त किए जाने को कोडेक के रूप में जाना जाता है, जो कि कोडर–डिकोडर के लिए संक्षिप्त रूप में प्रयुक्त किया जाता है।

एक एनालॉग सिग्नल को डिजिटल स्वरूप में परिवर्तित करने के लिए नियमित अंतरालों पर सिग्नल वेब की ऊँचाई की तत्कालिक माप लेते हुए शुरूआत की जाती है। इसे सिग्नल की सेम्पलिंग कहा जाता है। इन एनालॉग सेम्पल्स को डिजिटल फॉर्मेट में परिवर्तित करने की एक विधि

एनालॉग सिग्नल के एम्प्लीट्यूड भ्रमण को बराबर स्पेस वाले उन N लेवल्स में विभाजित कर दिए जाने की होती है, जिन्हें इंटीजर्स वेल्यूज को एक पृथक बायनरी वर्ड प्रदान किया जाता है।



चित्र 3.10 : एनालॉग वेवफॉर्म का डिजिटिज़ेशन (a. वास्तविक सिग्नल 0 एंड V वाल्टस b. क्वांटीजेड एंड संपलेड डिजिटल वर्शन)

3.3.2 डिजिटल डाटा और एनालॉग सिग्नल्स :

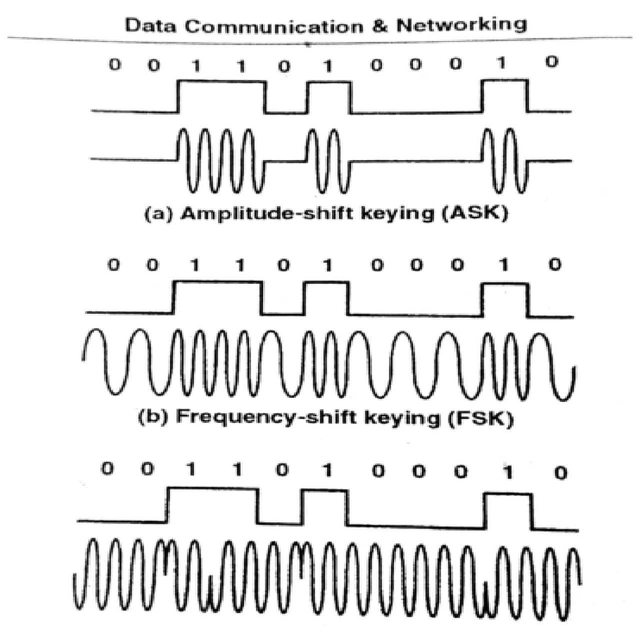
अब हम एनालॉग सिग्नल्स का उपयोग करते हुए डिजिटल डाटा को ट्रांसमिट किए जाने की स्थिति पर विचार करेंगे। सार्वजनिक टेलीफोन नेटवर्क के माध्यम से डिजिटल डाटा को प्रेषित किया जाना, इस रूपांतरा का सर्वाधिक प्रचलित उपयोग है। टेलीफोन नेटवर्क का निर्माण लगभग 300 से 3400 Hz की वॉईस फ्रीक्वेंसी रेंज में एनालॉग सिग्नल्स की प्राप्ति, स्विच और प्रेषित करने के लिए किया गया था। वर्तमन में यह उपभोक्ताओं की ओर से मिलने वाले डिजिटल सिग्नल्स को संभालने हेतु उपयुक्त नहीं है। इसलिए डिजिटल डिवाईसेस को एक मॉडेम (मॉड्यूलेटर–डिमॉड्यूलेटर) के

माध्यम से नेटवर्क से जोड़ा जाता है। यह डिजिटल डाटा को एनालॉग सिग्नल्स में और एनालॉग सिग्नल्स को डिजिटल डाटा में परिवर्तित करता है।

एनकोडिंग तकनीकें :

हम जानते है कि मॉड्यूलेशन में केरियर सिग्नल के तीन लक्षणों–एम्प्लीट्यूड, फ्रीक्वेंसी और फेज में से एक अथवा अधिक पर ऑपरेशन किया जाना सम्मिलित रहता है। इसके अनुसार तीन आधारभूत एनकोडिंग अथवा मॉड्यूलेशन स्कीम्स होती हैं, जो डिजिटल डाटा को एनालॉग सिग्नल्स में परिवर्तन करती हैं। जैसा कि चित्र 3.11 में दर्शाया गया है–

1. एम्प्लीट्यूड–शिफ्ट कीइंग (ASK)
2. फ्रीक्वेंसी–शिफ्ट कीइंग (FSK)
3. फेज–शिफ्ट कीइंग (PSK)



चित्र 3.11: डिजिटल डाटा के लिए एनालॉग सिग्मल का मॉडुलेशन

1. ASk : ASK में केरियर फ्रीक्वेंसी के दो पृथक–पृथक एम्प्लीट्यूड्स द्वारा दो बायनरी वेल्यूज दर्शाए जाते है। आमतौर पर एम्प्लीटयूड्स में से एक शून्य होता है अर्थात् एक बायनरी डिजिट को स्थिर एम्प्लीट्यूड पर केरियर की उपस्थिति द्वारा और अन्य को केरियर की अनुपस्थिति द्वारा दर्शाया जाता है। रीजल्टिंग सिग्नल होता है–

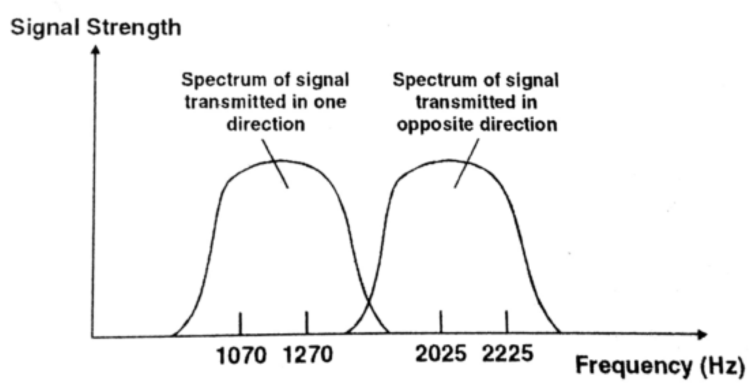
ASK स्कीम ऑप्टिकल फाईबर पर डिजिटल डाटा को प्रेषित करने के लिए प्रयुक्त की जाती है। LED ट्रांसमीटर्स के लिए ऊपर दर्शाया गया समीकरण मान्य है। अर्थात् एक सिग्नल एलीमेंट एक लाईट पल्स द्वारा दर्शाया जाता है, जबकि दूसरा सिग्नल एलीमेंट लाईट की अनुपस्थिति द्वारा दर्शाया जाता है। लेजर ट्रांसमीटर्स में सामान्यतः एक निश्चित बायस करंग होता है।

2. FSK: FSK में दो बायनरी वेल्यूज को केरियर फ्रीक्वेंसी के निकटतम दो पृथक–पृथक फ्रीक्वेंसीज द्वारा दर्शारूा जाता है। रिजल्टिंग सिग्नल होता है–

$$\text{FSK} \qquad s(t)=\begin{cases} A\cos(2\pi f1t) binary\ 1 \\ A\cos(2\pi f2t) binary\ 0 \end{cases}$$

जहाँ f_1 और f_2 सामान्यतः केरियर फ्रीक्वेंसी f_0 से बराबर परंतु विपरीत मात्राओं में ऑफसेट रहते है।

जैसा हम जानते है कि वॉईस ग्रेड लाईन लगभग 300 से 3400 Hz की रेंज में फ्रीक्वेंसीज को पास करेगी और फुल डुप्लेक्स का अभिप्राय है कि सिग्नल्स दोनों ही दिशाओं में एक ही समय में ट्रांसमिट किए जाते हैं। फुल डुप्लेक्स ट्रांसमिशन प्राप्त करने के लिए इस बैंडविड्थ को विभाजित किया जाता है।



चित्र 3.12: फुल डुप्लेक्स FSK ट्रांसमिशन

3. PSK : PKS में केरियर सिग्नल का फेज डाटा दर्शाने के लिए शिफ्ट कर दिया जाता है। चित्र **डिजिटल डाटा** का निचला भाग टू–फेज सिस्टम का एक उदाहरण है। इस सिस्टम में बायनरी 0 को प्रेषित किए गए पूर्ववर्ती सिग्नल बर्स्ट की तरह से ही ट्रांसमिट किए जा रहे, उसी फेज के सिग्नल बर्स्ट द्वारा दर्शाया जाता है। बायनरी 1 को पहले वाले के विपरीत फेज का सिग्नल बर्स्ट में जाना जाता हैं,

$$\text{PSK} \qquad s(t)=\begin{cases} A\cos(2\pi fct+\pi)\, binary\ 1 \\ A\cos(2\pi fct+\pi)\, binary\ 0 \end{cases}$$

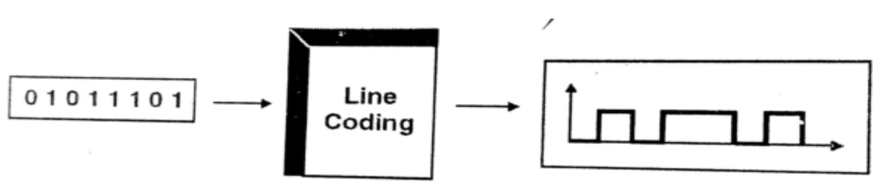
3.3.3 मल्टीलेवल डिजिटल ट्रांसमिशनः

किसी डिजिटल सिस्टम में बिट रेट बढ़ाने का एक ओर तरीका पल्सेस को दो से अधिक लेवल्स पर ट्रांसमिट किया जाना है। उदाहरण के लिए, पल्सेस सेट [-A, -A/3m, + A/3, +A] से एम्प्लीट्यूड ले सकती हैं। QPSK की ही भांति इन पल्सेस के उपयोग से बिट्स की जोड़ी (00, 01, 10, 11) प्रेषित की जा सकती है। इस परिस्थिति में चूँकि प्रत्येक पल्स इंफॉर्मेशन की 2 बिट्स प्रेषित करती है, तो नॉयक्विस्ट थ्योरम से हम 4B इचे की बिट रेट को ट्रांसमिट कर सकते हैं। इसकी तुलना में बायनरी सिग्नलिंग से 2B bps को ही ट्रांसमिट किया जा सकता है।

डिजिटल स्वरूप में डिजिटल डाटा प्रेषित करनाः

यहाँ हम ऐसी दो तकनीकों का अध्ययन करेंगे जिनका उपयोग हम डाटा को डिजिटल स्वरूप में ही ट्रांसमिट करने हेतु कर सकते हैं।

1. लाईन कोडिंग : लाईन कोडिंग बायनरी डाटा और बिट्स की सिक्वेंस को डिजिटल सिग्नल में परिवर्तित किए जाने की प्रक्रिया है। लाईन कोडिंग बिट्स की सिक्वेंस को डिजिटल सिग्नल में परिवर्तित कर देती है। चित्र में लाईन कोडिंग की अवधारणा को दर्शाया गया है।

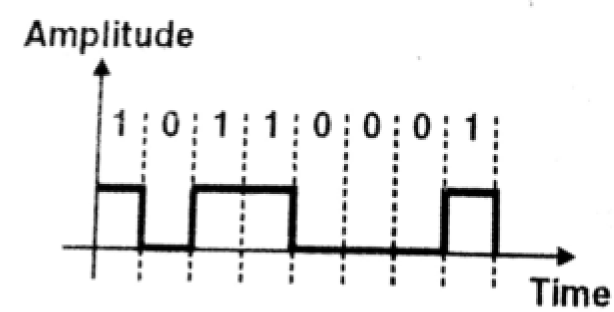


चित्र 3.13: लाइन कोडिंग

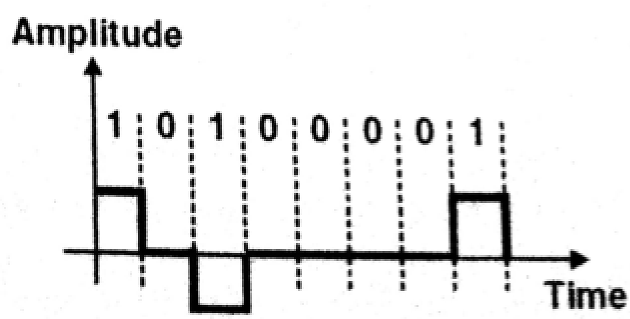
लाईन कोडिंग की विशेषताएँ :

लाईन कोडिंग की विशेषताएँ निम्नलिखित है–

1. **सिग्नल लेवल बनाम डाटा लेवल :** जैसा हम जानते है कि डिजिटल सिग्नल की एक सीमित संख्या में वेल्यूज हो सकती है। इनमें से कुछ ही वेल्यूज को डाटा प्रदर्शित करने के लिए प्रयुक्त किया जा सकता है और शेष को अन्य कार्य हेतु प्रयुक्त किया जाता है। किसी सिग्नल विशेष में मान्य वेल्यूज की संख्या को हम सिग्नल लेवल्स की संख्या के रूप में दर्शाते हैं। जबकि डाटा दर्शाने हेतु प्रयुक्त वेल्यूज की संख्या को डाटा लेवल्स की संख्या के रूप में लिया जाता है।



(a) Two signal levels, two data levels



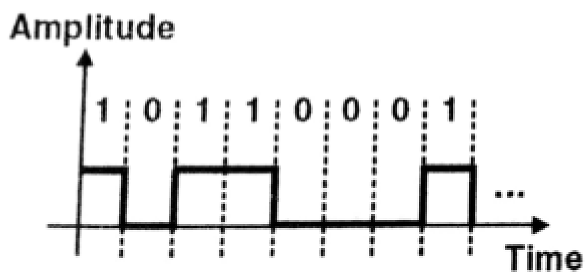
चित्र 3.14 : सिग्नल लेवल एवं डाटा लेवल

2. **पल्स रेट बनाम बिट रेट :** पल्स रेट प्रति सेकण्ड पल्सेज की संख्या बताती है। पल्स समय की वह न्यूनतम मात्रा होती हैं, जो किसी सिम्बल को प्रेषित किए जाने हेतु आवश्यक है। बिट रेट प्रति सेकण्ड बिट्स की संख्या को परिभाषित करती है। यदि कोई पल्स केवल 1 बिट ही ट्रांसमिट करती है, तो पल्स रेट और बिट रेट एक समान

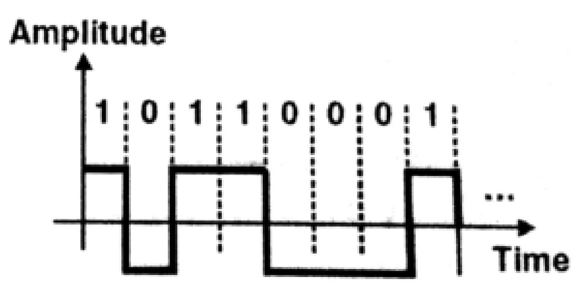
होती है। यदि पल्स 1 से अधिक बिट ट्रांसमिट करती है, तो पल्स रेट की तुलना में बिट रेट अधिक होगी। आमतौर पर हमारे पास निम्नलिखित फॉर्मूला होता है, जिसमें L सिग्नल के डाटा लेवल्स की संख्या है–

$$BitRate=PulseRate \times \log_2 L$$

3. **DC कम्पोनेंट्स** : कुछ ही लाईन कोडिंग विधियाँ ऐसी होती हैं, जो रेसिड्यूअल डॉयरेक्ट करंट (do) कम्पोनेंट (शून्य फ्रीक्वेंसी) छोड़ती हैं। दो कारणों से इस कम्पोनेंट की आवश्यकता नहीं रह जाती है। प्रथम, सिग्नल यदि ऐसे सिस्टम से होकर गुजरता है, जो उसे कब कम्पोनेंट को गुजरने की अनुमति नहीं देता है, तो सिग्नल विकृत हो जाता है और इससे आऊटपुट में ऍरर्स उत्पन्न हो सकते हैं। द्वितीय, इस कम्पोनेंट के होने से लाईन पर अतिरिक्त ऊर्जा आ जाती है, जो अनुपयोगी होती है।



(a) A signal with dc component

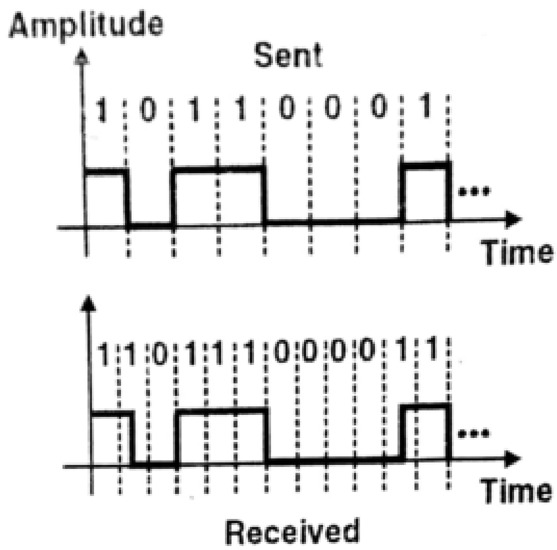


(b) A signal without dc component

चित्र 3.15 : DC कॉम्पोनेन्ट

4. **सेल्फ सिंक्रोनाईजेशनः** सेंडर से भेजे गए सिग्नलों को अचूक रूप से जानने के लिए रिसीवर के बिट इंटरवल्स को सेंडर के बिट इंटरवल्स के एकदम अनुरूप होना चाहिए। यदि रिसीवर क्लॉक तेज अथवा धीमी है, तो बिट इंटरवल्स का मेल नहीं होगा ओर हो सकता है

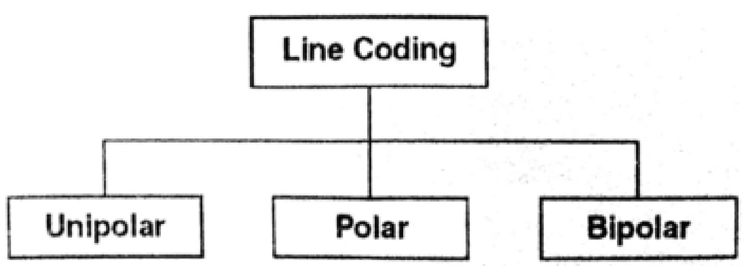
कि रिसीवर की व्याख्या उस तरह से न करें, जैसा कि सेंडर अपेक्षा रखता है। चित्र 3.16 में एक ऐसी स्थिति दशाई गई है, जिसमें रिसीवर की बिट अवधि छोटी है। सेंडश्र 10110001 भेजता है, जबकि रिसीवर 110111000011 ग्रहण कर रहा है।



चित्र 3.16: सेल्फ सिंक्रोनाइजेशन

3.3.4 लाईन कोडिंग स्कीम्स के प्रकारः

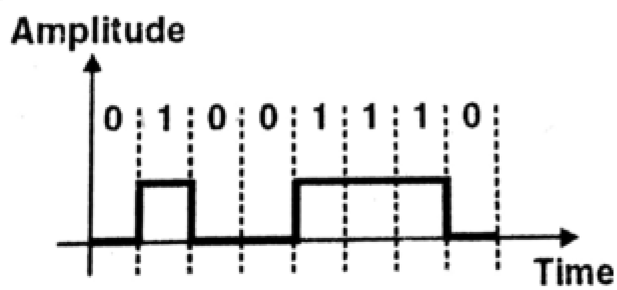
लाईन कोडिंग स्कीम्स को तीन मुख्य श्रेणियों में विभाजित किया जाता है– **(1) यूनिपोलर, (2) पोलर तथा (3) बायपोलर,** जैसा कि चित्र में दर्शाया गया है।



चित्र 3.17: लाइन कोडिंग स्कीम

1. यूनिपोलर : यूनिपोलर एनकोडिंग अत्यंत ही सरल और बहुत महत्वपूर्ण है। यह हमें अधिक जटिल एनकोडिंग सिस्टम से निर्मित योजनाओं से सरलतापूर्वक परिचित करता है और ऐसी समस्याओं के प्रकारों का पता लगाने की अनुमति प्रदान करता है, जिनका किसी डिजिटल ट्रांसमिशन में समाधान होना चाहिए।

डिजिटल ट्रांसमिशन सिस्टम्स वॉल्टेज पल्सेस को एक मीडियम लिंक, जो आमतौर पर एक वॉयर अथवा केबल होता है, से प्रेषित करते हुए ऑपरेट होता है। विभिन्न प्रकार की एनकोडिंग में एक वॉल्टेज लेवल बायनरी 0 के लिए तथा दूसरा लेवल बायनरी 1 के लिए होता है। पल्स की पालेरिटी यह दर्शाती है कि यह पॉजिटिव है या नेगेटिव है। इसे यूनिपोलर एनकोडिंग इसलिए कहते हैं, क्योंकि यह केवल एक ही पोलेरिटी का उपयोग करता है। दो में से एक बायनरी दशाओं को यह यह पोलेरिटी प्रदान की जाती है, जो कि सामान्यतः 1 होती है। दूसरी दशा जो सामान्यतः 0 है, को शून्य वॉल्टेज द्वारा दर्शाया जाता है।



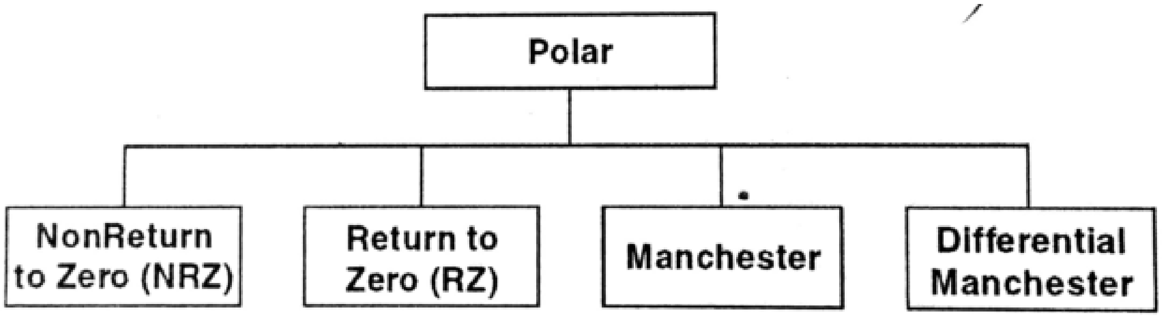
चित्र 3.18: यूनिपोलर एन्कोडिंग

2. पोलरः पोलर एनकोडिंग दो वॉल्टेज लेवल्स का उपयोग करती है– एक पॉजिटिव और एक नेगेटिव। इन दो लेवल्स का उपयोग करते हुए अधिकांश पोलर एनकोडिंग विधियों में लाईन पर औसत वॉल्टेज लेवल न्यूनतम कर लिया जाता है और इस प्रकार यूनिपोलर एनकोडिंग में दर्शित होने वाली कब कम्पोनेंट समस्या दूर हो जाती है।

पोलर एनकोडिंग की मौजूदा विभिन्न विधियों में से हम चार सर्वाधिक लोकप्रिय प्रकारों पर चर्चा करेंगे–

(i) नॉन–रिटर्न टू जीरों (NRZ)

(ii) रिटर्न टू जीरो (RZ)
(iii) मैनचेस्टर
(iv) डिफरेंशिल मैनचेस्टर



चित्र 3.19: पोलर एन्कोडिंग के प्रकार

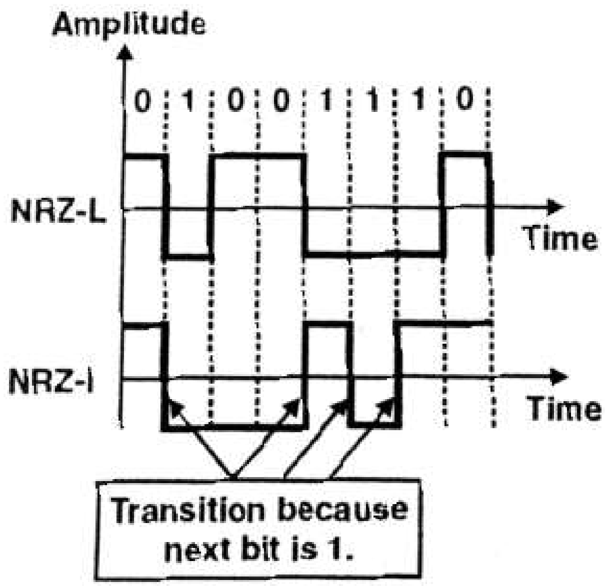
(i)नॉनरिटर्न टू जीरो (NRZ) : यहाँ सिग्नल की वेल्यू हमेशा या तो पॉजिटिव अथवा नेगेटिव होती है। NRZ के दो मुख्य रूप हैं।

(a) **NRZ-L (NRZ-Level)** एनकोडिंग में सिग्नल का लेवल इसके द्वारा प्रदर्शित बिट के प्रकार पर निर्भर करता है। पॉजिटिव वॉल्टेज का सामान्यतः अभिप्राय यह होता है कि बिट एक 0 है, जबकि नेगेटिव वॉल्टेज का अभिप्राय है कि बिट एक 1 है। इस प्रकार सिग्नल का लेवल बिट की अवस्था पर निर्भर करता है। समस्या तब उत्पन्न हो सकती है, जबकि डाटा अथवा 1 की लंबी श्रृंखला से निर्मित हुआ हो।

(b) **NRZ-I (NRZ-Invert)** में वॉल्टेज लेवल का प्रतिलोम 1 बिट दर्शाता है। यह पॉजिटिव और नेगेटिव वॉल्टेज के मध्य की स्थिति है, जो 1 बिट दर्शाती है। 0 बिट को परिवर्तनहीनता या बदलाव के अभाव द्वारा दर्शाया जाता है। NRZ-L की तुलना में NRZ-I श्रेष्ठतर है, क्योंकि प्रत्येक बार जब 1 बिट का सामना होता है, तो सिग्नल परिवर्तन द्वारा सिंक्रोनाईजेशन दिया जाता है।

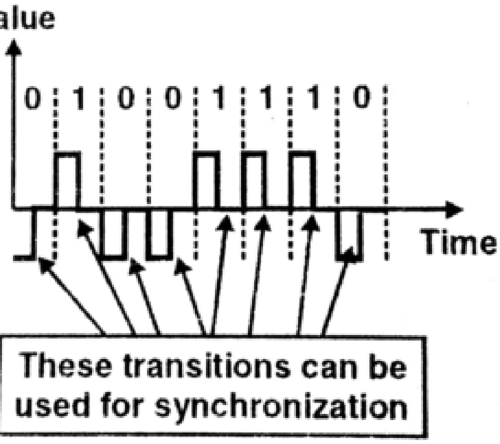
डाटा स्ट्रीम में 1s की उपस्थिति रिसीवर को उसका टाईमर ट्रांशमिशन के वास्तविक रूप से पहुँचने के कारण सिंक्रोनाईज करने की अनुमति प्रदान करती है। 0 की श्रृंखला उसी प्रकार समस्याएँ उत्पन्न कर सकती है, किंतु 0 की संभावना के चलते ऐसा नहीं होता है। यह एक कम महत्वपूर्ण समस्या है।

चित्र NRZ-L और NRZ-I सिक्वेंस में पॉजिटिव और नेगेटिव वॉल्टेज का अपना विशिश्ट अभिप्राय होता है – पॉजिटिव 0 को नेगेटिव 1 को दर्शाता है। NRZ-I सिक्वेंस में केवल वॉल्टेज भर का अपने आप में कोई अर्थ नहीं होता है। इसके स्थान पर रिसीवर को 1 की पहचान किए जाने के आधार के रूप में एक लेवल से दूसरे में होने वाले परिवर्तन की आवश्यकता होती है।



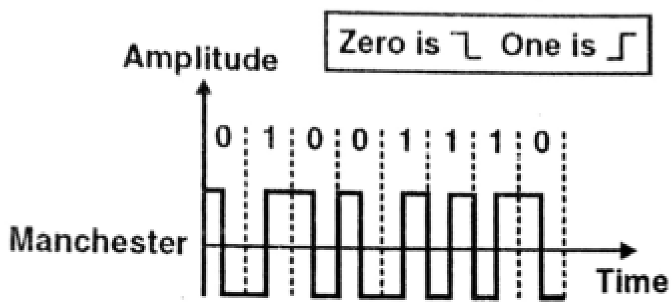
चित्र 3.20 : NRZ -L एंड NRZ -I एन्कोडिंग

(ii) रिटर्न टू जीरो (RZ) : जब कभी भी मूल डाटा लगातार 1s अथवा 0s की श्रृंखलाओं से निर्मित होता है, तो रिसीवर उसका स्थान खो सकता है। इसका समाधान एनकोडेड सिग्नल में किसी तरह से सिंक्रोनाईजेशन को सम्मिलित कर दिया जाना है। ठीक वैसा ही समाधान जो NRZ-I प्रदान करता है, परंतु उसमें 0s के साथ ही साथ 1s की श्रृंखलाओं को संभालने की क्षमता भी होनी चाहिए।



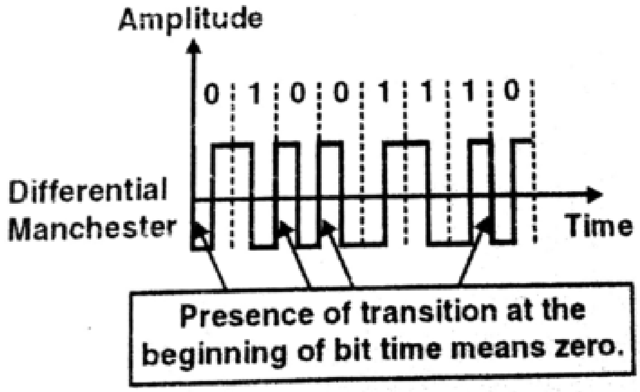
चित्र 3.21 : RZ एन्कोडिंग

(iii) मैनचेस्टर : मैनचेस्टर एनकोडिंग में सिंक्रोनाईजेशन और बिट प्रस्तुतीकरण के लिए प्रत्येक बिट इंटरवल्स के मध्य में ट्रांजिशन का उपयोग किया जाता है। नेगेटिव–टू–पॉजिटिव ट्रांजिशन बायनरी 1 को दर्शाता है और पॉजिटिव–टू–नेगेटिव ट्रांजिशन बायनरी 0 को दर्शाता है। दोहरे कार्य के लिए एकल ट्रांजिशन का उपयोग करते हुए मैनचेस्टर एनकोडिंग RZ जैसे स्वर का ही सिंक्रोनाईजेशन प्राप्त करता हैं,



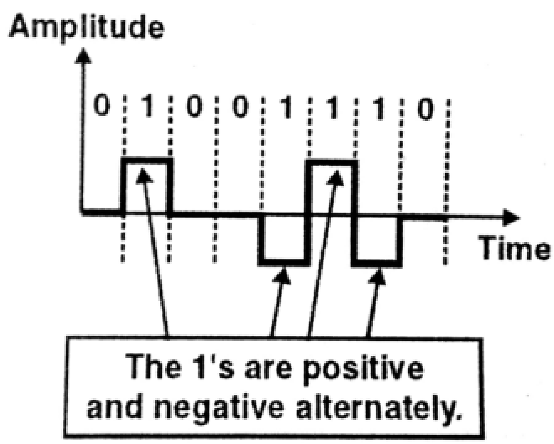
चित्रः मेनचेस्टर एन्कोडिंग

(iv) डिफरेंशियल मैनचेस्टर : इसमें बिट इंटरवल के मध्य में इन्वर्शन को सिंक्रोनाईजेशन के लिए प्रयुक्त किया जाता है, किंतु इंटरवल के प्रारंभ में अतिरिक्त ट्रांजिशन की उपस्थिति अथवा अनुपस्थिति का उपयोग बिट को पहचानने के लिए किया जाता है। ट्रांजिशन का अर्थ होता है, बायनरी 0 और ट्रांजिशन न होने का अर्थ बायनरी 1 होता है।



चित्र 3.22 : डिफरेंशियल मेनचेस्टर एन्कोडिंग

3. बॉयपोलर : RZ की तरह बॉयपोलर एनकोडिंग भी तीन वॉल्टेज लेवल्स – पॉजिटिव, नेगेटिव और जीरो का उपयोग करती है। परंतु RZ के विपरीत बॉयपोलर एनकोडिंग में जीरो लेवल बायनरी 0 को दर्शाने के लिए प्रयुक्त किया जाता है। 1s को अदल–बदलकर पॉजिटिव और नेगेटिव वॉल्टेज द्वारा दर्शाया जाता है। यदि पहली 1 बिट पॉजिटिव एम्प्लीट्यूड से दर्शाई जाती है, तो दूसरी नेगेटिव एम्प्लीट्यूड से दर्शाई जाती है।



चित्र 3.23 : बाइपोलर एन्कोडिंग

3.4 स्विचिंग नेटवर्क एंड उपयोग

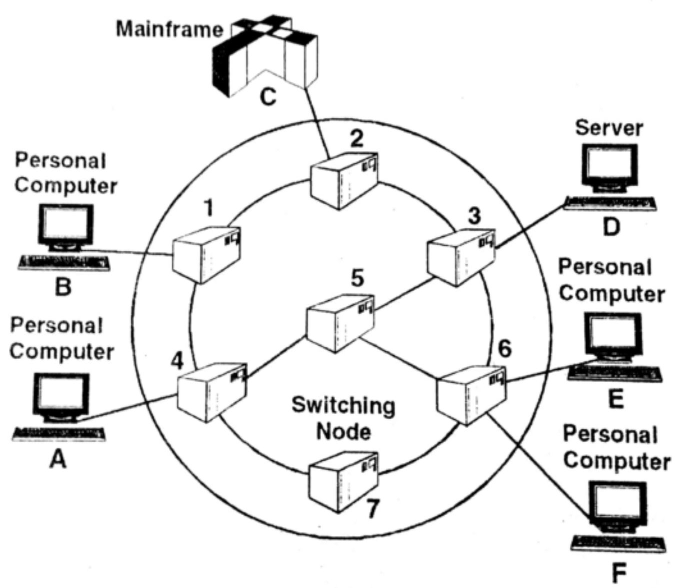
3.4.1 प्रस्तावना : हम लंबी दूरी पर स्त्रोत से गंतव्य तक ट्रांसमिट किए जाने वाले डाटा को मध्यवर्ती स्विचिंग नोड्स के नेटवर्क की सहायता से ले जाते हैं। स्विचिंग नोड्स का उद्देश्य ऐसी स्विचिंग सुविधा प्रदान करना है, जो डाटा को नोड से नोड तब तक गतिशील करती रहे, जब तक कि वह अपने गंतव्य तक नहीं पहुँच जाए।

प्रत्येक स्टेशन एक नोड से जुड़ा हुआ होता है और नोड्स का सेट कम्यूनिकेशन्स नेटवर्क के रूप में अथवा स्विच्ड कम्यूनिकेशन नेटवर्क्स के रूप में जाना जाता है। किसी स्टेशन से नेटवर्क में प्रवेश करने वाले डाटा को नोड से नोड तक स्विच करते हुए गंतव्य तक ले जाया जाता है।

वाईड एरिया स्विच्ड नेटवर्क्स में तीन बिल्कुल ही भिन्न तकनीकें प्रयुक्त की जाती हैं–

1. सर्किट स्विचिंग नेटवर्क्स
2. मैसेज स्विचिंग नेटवर्क्स
3. पैकेट स्विचिंग नेटवर्क्स

इन तकनीकों में उनके नोड्स द्वारा स्त्रोत से गंतव्य तक इंफॉर्मेशन को एक लिंक से दूसरी तक स्विच किए जाने की विधि का अंतर होता है।



चित्र 3.24 : स्विचिंग नेटवर्क

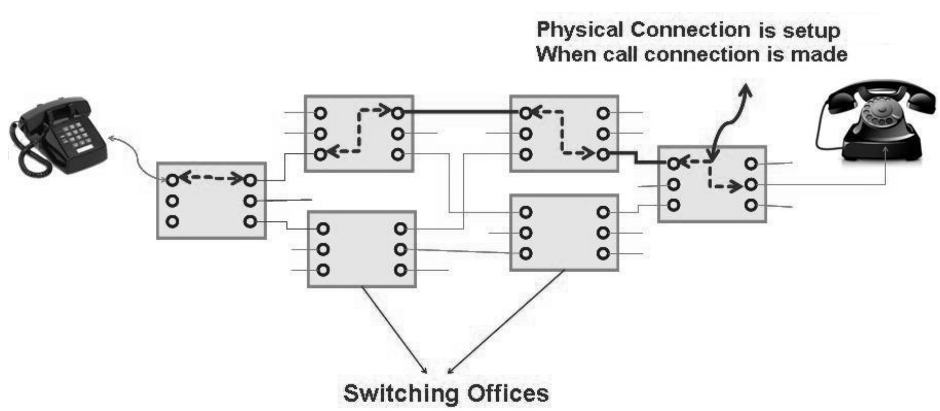
3.4.2 सर्किट स्विचिंग नेटवर्क्स :

सर्किट स्विचिंग के माध्यम से कम्यूनिकेशन का अभिप्राय यह है कि दो स्टेशन्स के मध्य एक समर्पित संचार मार्ग मौजूद है। इस मार्ग में नेटवर्क नोड्स के मध्य लिंक्स का एक जुड़ा हुआ अनुक्रम उपस्थित होता है। सर्किट स्विचिंग के माध्यम से संचार तीन चरणों से निर्मित होता है,

(i)सर्किट एस्टेब्लिशमेंट : इसके पूर्व कि कोई सिग्नल भेजे जाएँ, स्टेशन से स्टेशन (एंड–टू–एंड) तक पूरा सर्किट स्थापित किया जाना आवश्यक होता है।

(ii) डाटा ट्रांसफर : अब इंफॉर्मेशन को A से नेटवर्क के द्वारा E तक भेजा जा सकता है। नेटवर्क की प्रकृति के अनुसार डाटा है–A-4 लिंक, 4 से होते हुए आंतरिक स्विचिंग; 4–5 चैनल, 5 से होते हुए आंतरिक स्विचिंग; 5–6 चैनल, 6 से होते हुए आंतरिक स्विचिंग 6-E लिंक। सामान्यतः कनेक्शन फुल डुप्लेक्स होता है।

(iii) सर्किट डिसकनेक्ट : डाटा ट्रांसफर की कुछ अवधि के उपरांत कनेक्शन को हटा लिया जाता है। सामान्यतः ऐसा दो स्टेशन्स में से एक के एक्शन के द्वारा किया जाता है। समर्पित संसाधनों को डिअलॉकेट करने के लिए 4, 5 और 6 नोड्स पर सिग्नल्स प्रसारित किए जाते हैं।



चित्र 3.25: सर्किट स्विचिंग (टेलीफोन लाइन उदाहरण)

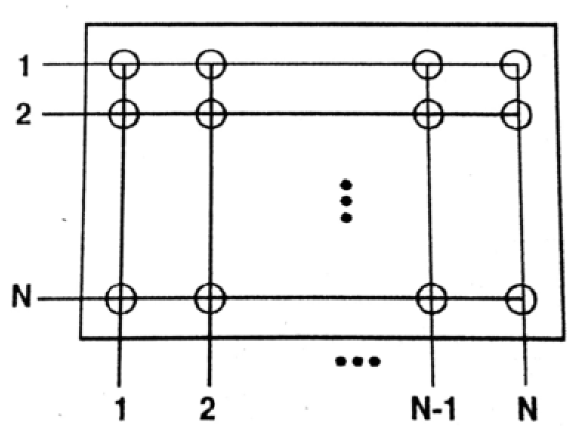
सर्किट स्विचिंग तकनीकें :

इन दिनों सर्किट स्विचिंग में तीनों तकनीकों में से कोई भी तकनीक उपयोग में लाई जा सकती हैं–

1. स्पेस डिवीजन स्विचेज
2. टाईम डिवीजन स्विचेज
3. हायब्रिड (टाईम स्पेस स्विचेज)

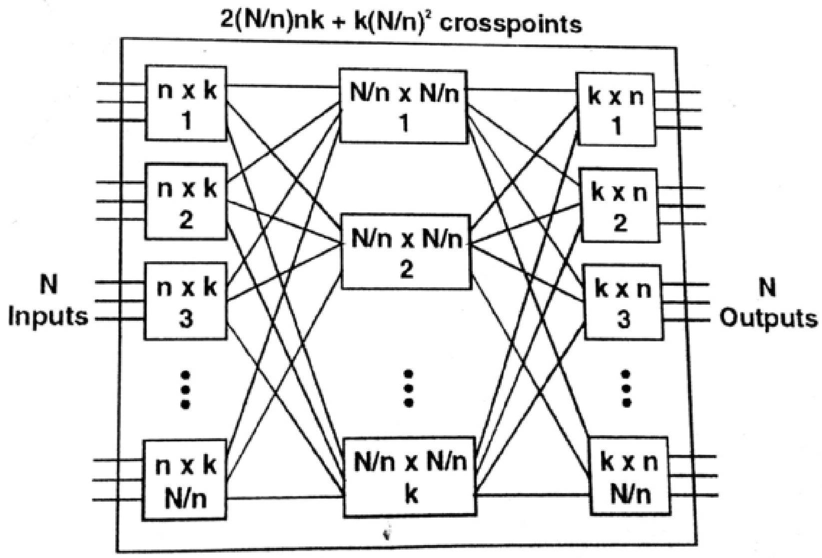
(i) स्पेस डिवीजन स्विचेज : स्पेस डिवीजन स्विचेज इनपुट्स और आउटपुट्स के मध्य हमें एक ऐसा पृथक भौतिक कनेक्शन प्रदान करते हैं, जिससे कि विभिन्न सिग्नल्स को अंतराल (स्पेस) में ही अलग–अलग किया जा सके।

(a) क्रॉसबार स्विचेज : चित्र 3.26 क्रॉसबार स्विच को प्रदर्शित करता है। क्रॉसबार स्विच क्रॉसपाईंट्स के एक N x N ओर से निर्मित होता है, जो किसी इनपुट को किसी भी उपलब्ध आऊटपुट से कनेक्ट कर सकता है। जब किसी इनकर्मिंग लाईन से एक आऊटगोइंग लाईन के लिए कोई रिक्वेस्ट आती है, इंफॉर्मेशन को इनपुट से आऊटपुट में प्रवाहित होने में सहायता प्रदान करने के लिए तत्संबंधित क्रॉसपॉईंट को बंद कर दिया जाता है। क्रॉसबार स्विच को नॉन ब्लॉकिंग कहा जाता है।



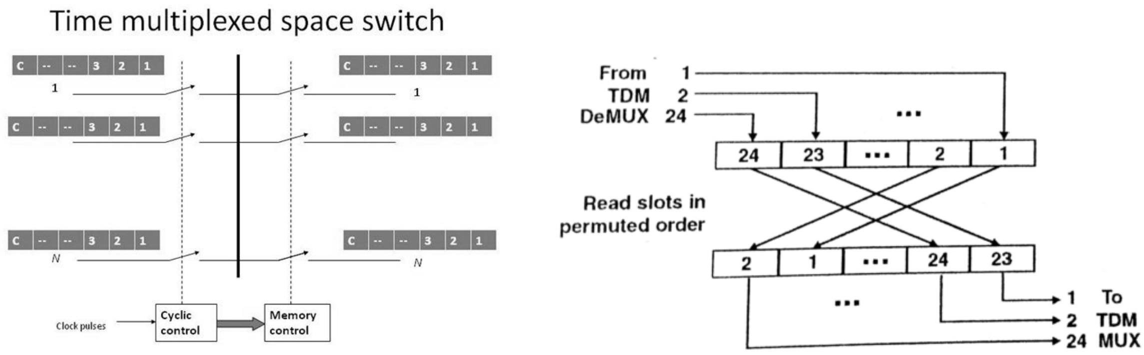
चित्र 3.26: क्रॉस बार स्विचिंग

(b) मल्टीस्टेज स्विचेज : मल्टीस्टेच स्विच तीन चरणों वाले छोटे–छोटे स्पेस डिवीजन स्विचेज से निर्मित होता है (चित्र 3.27)। N इनपुट्स को द इनपुट लाईंस के N/n ग्रुप्स में समूहबद्ध किया जाता है। प्रथम चरण में n इनपुट लाईंस का प्रत्येक ग्रुप एक ऐसे छोटे स्विच में प्रविष्ट होता है, जो क्रॉसपॉईंट्स के एक n x n अरे से निर्मित होता है। प्रत्येक इनपुट स्विच में एक लाईन k मध्यवर्ती चरण के प्रत्येक N/n x N/n स्विचेज से जुड़ी हुई होती है। बदले में प्रत्येक मध्यवर्ती स्विच में तृतीय चरण में एक–एक लाईन प्रत्येक N/n स्विचेज से जोड़ी जाती है। बाद वाले स्विचेज K x N हैं। n इनपुट लाईंस का प्रत्येक सेट इसके प्रभाव से अंतिम चरण में स्विचेज में से किसी एक के लिए k संभव मार्ग को साझा करता है।



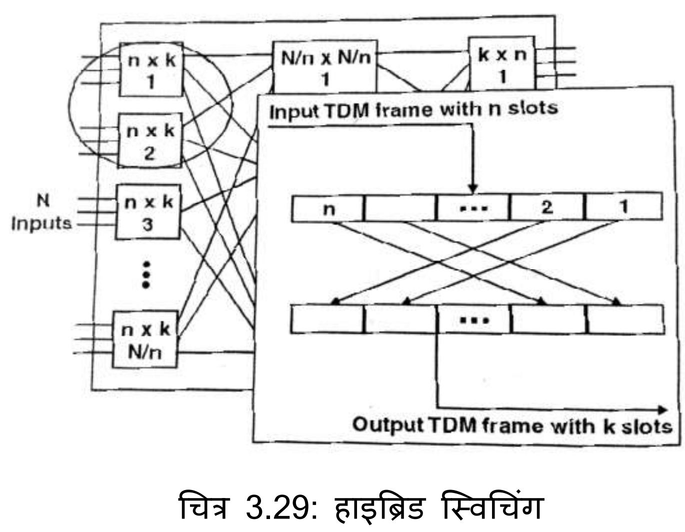
चित्र 3.27 : मल्टी स्टेज स्विचिंग

(ii) टाईम डिवीजन स्विचेज : जैसा हम जानते हैं कि टाईम डिविजन मल्टीप्लेक्सिंग (TDM) किस तरह से एक सिंगल हाई स्पीड लाईन द्वारा एकाधिक भौतिक लाईंस को प्रतिस्थापित कर सकता है। ज्कड में किसी फ्रेम के भीतर एक स्लॉट सिंगल कनेक्शन से संबंधित होता है। टाईम स्लॉट इंटरचेंज (TSI) विधि किसी स्पेस स्विच में क्रॉस पॉइंट्स के स्थान पर मेमोरी में स्लॉट की रीडिंग तथा राईटिंग को प्रतिस्थापित कर देती है।



चित्र 3.28: टाइम डिवीज़न स्विचिंग

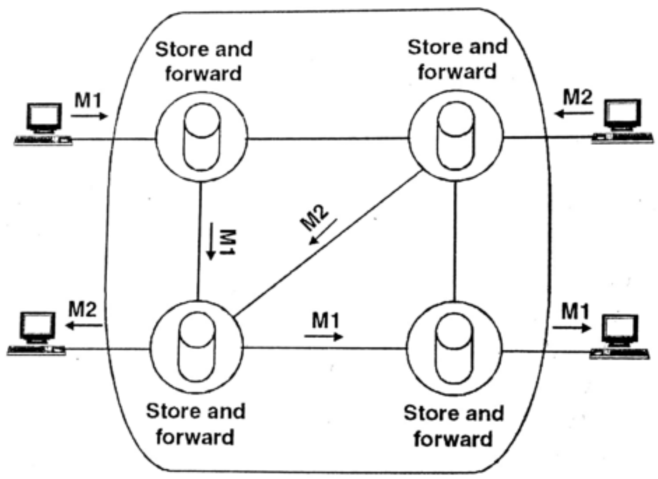
(iii) हॉयब्रिड टाईम– स्पेस/टाईम–स्विचेज : यहाँ हम एक ऐसी हॉयब्रिड स्विच डिजाईन पर विचार कर रहे है, जिसमें इनपुट व आऊटपुट चरणों मे TSI स्विचेज प्रयुक्त किए जाते हैं तथा मध्यवर्ती चरण में क्रॉसबार स्पेस स्विच प्रयुक्त होता है। इन स्विचेज को टाईम–स्पेस–टाईम–स्विचेज कहा जाता है। डिजाईन की विधि के प्रथम चरण में स्पेस डिवीजन स्विच में इनपुट लाईंस और TSI स्विच में टाईम स्लॉट्स के मध्य ठीक–ठीक तालमेल स्थापित करने की आवश्यकता होती है। मानाकि हम मल्टीस्टेज स्पेस स्विच के प्रथम चरण में n x k स्विच को n x k TSI स्विच से प्रतिस्थापित कर देते हैं,



चित्र 3.29: हाइब्रिड स्विचिंग

3.4.3. मैसेज स्विचिंग :

मैसेज स्विचिंग को वर्णनात्मक शब्दावली स्टोर एण्ड फॉरवर्ड द्वारा अधिक जाना जाता है। इस मेकेनिज्म में एक नोड (आमतौर पर अनेक डिस्क्स वाला एक विशेष कम्प्यूटर) मैसेज ग्रहण करता है, यथोचित रूट के फ्री होने तक इसे संग्रहीत रखता है और फिर इसे आगे प्रेषित कर देता है।



चित्र 3.30: मैसेज स्विचिंग

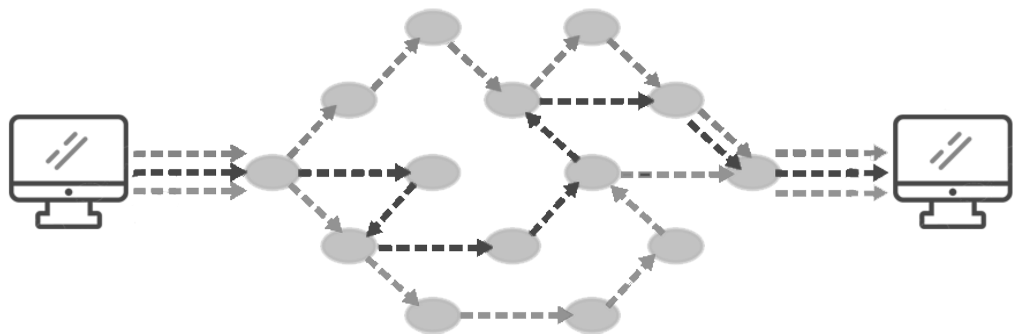
स्टोर एण्ड फॉरवर्ड को एक स्विचिंग तकनीक माना जाता है, क्योंकि किसी ट्रांसमिशन के सेंडर और रिसीवर के मध्य कोई सीधी लिंक नहीं होती है। अकेले एक मार्ग से नोड को मैसेज डिलीवर किया जाता है, फिर उसे दूसरे मार्ग से उसके डेस्टिनेशन के लिए रीरूटेड कर दिया जाता है।

3.4.4 पैकेट स्विचिंग नेटवर्क्सः

1970 के आस–पास लंबी दूरी के डिजिटल डाटा आर्किटेक्चर– पैकेट स्विचिंग के लिए एक नए प्रकार के स्विचिंग की तकनीक ने समय के साथ एक सुविस्तृत की मूलभूत तकनीक सैद्धांतिक रूप से आज भी वैसी ही है, जैसी यह 1970 के आरंभिक समय के नेटवर्क्स में थी तथा लंबी दूरी के डाटा कम्यूनिकेशन्स के लिए पैकेट स्विचिंग कुछ प्रभावशाली तकनीकों में से एक है।

हम देखेगे कि पैकेट स्विचिंग के अनेकानेक लाभ (अनुकूलता, संसाधनों की साझेदारी, संशक्तता, संवेदनशीलता) एक कीमत के साथ आते हैं। पैकेट स्विचिंग नेटवर्क पैकेट स्विचिंग नोड्स

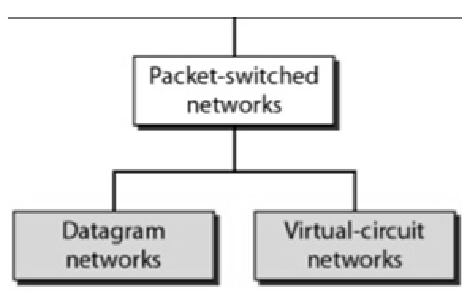
का एक डिस्ट्रिब्यूटेड सेट होता है। आदर्श रूप से सभी पैकेट स्विचिंग नोड्स को संपूर्ण नेटवर्क की अवस्था का सदैव पता रहता है।



चित्र 3.31: पैकेट स्विचिंग

पैकेट स्विचिंग की स्विचिंग तकनीकें:

यदि किसी स्टेशन को एक ऐसा मैसेज पैकेट स्विचिंग नेटवेर्क के माध्यम से प्रेषित करना है, जिसकी लंबाई अधिकतम पैकेट साईज से भी बड़ी है, तो वह मैसेज को पैकेट्स में विभाजित कर देता और इन पैकेट्स को एक बार में एक करके नेटवर्क पर भेजेगा। समकालीन नेटवर्क्स की दो विधियाँ प्रयुक्त की जाती हैं–(i) डाटाग्राम पैकेट स्विचिंग और (ii) वर्चुअल सर्किट पैकेट स्विचिंग।

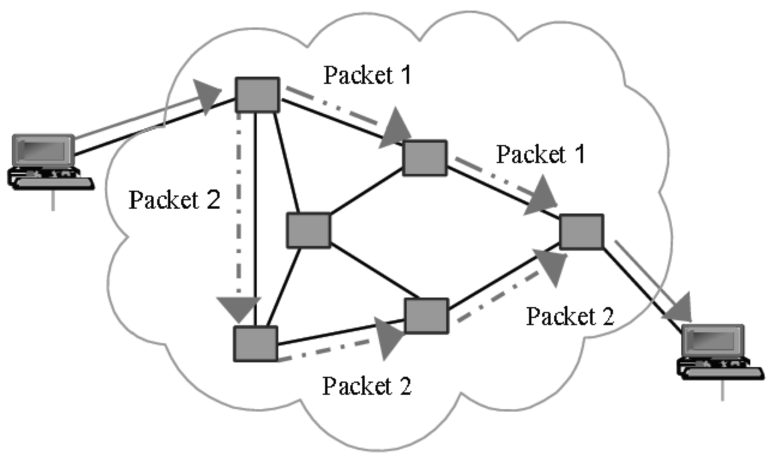


चित्र 3.32 : पैकेट स्विचिंग के प्रकार

(i) डाटाग्राम पैकेट स्विचिंग : इस विधि में, प्रत्येक पैकेट के साथ स्वतंत्र रूप से कार्य किया जाता है। इसमें पूर्व में प्रेषित किए गए पैकेट्स का कोई उल्लेख नहीं होता है।

डाटा ग्राम विधि के लाभः

1. इस विधि में कॉल सेटअप चरण की उपेक्षा की जाती है। इसलिए यदि कोई स्टेशन केवल एक अथवा कुछ ही पैकेट्स प्रेषित करना चाहे तो डाटा ग्राम डिलीवरी त्वरीत होगा।
2. चूँकि यह अधिक पुरातन है, इसलिए यह अधिक लचीला या अनुकूलनीय भी है।
3. डाटाग्राम डिलीवरी अंतर्निहित रूप से अधिक विश्वसनीय है। वर्चुअल सर्किट्स के उपयोग के दौरान यदि कोई नोड फेल होता है, तो उस नोड से होकर गुजरने वाले समस्त वर्चुअल सर्किट्स लुप्त हो जाते हैं। डाटाग्राम डिलीवरी में यदि कोई नोड फेल होता है, तो बाद में आने वाले पैकेट्स उस नोड को बायपस करते हुए एक वैकल्पिक रूट की तलाश कर सकते है।



चित्र 3.33 : डाटा ग्राम पैकेट स्विचिंग

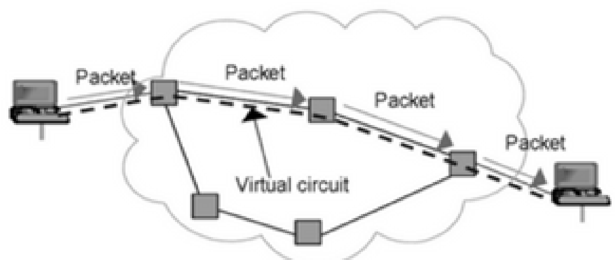
(ii) वर्चुअल सर्किट : इसमें कोई भी पैकेट्स को प्रेषित किए जाने के पहले एक पूर्व नियोजित रूट निर्मित किया जाता है। उदाहरणार्थ मान लीजिए कि E को प्रेषित किए जाने के लिए A के पास एक अथवा अधिक मैसेज है। वह सर्वप्रथम कॉल रिक्वेस्ट पैकेट के रूप में जाना जाने वाला एक विशेष कंट्रोल पैकेट E से लॉजिकल कनेक्शन का अनुरोध करते हुए 4 को प्रेषित करता है। नोड 4 द्वारा रिक्वेस्ट और उसके बाद आने वाले सभी पैकेट्स को 5 के लिए रूट करने का निर्णय लिया

जाता है। यह इस रिक्वेस्ट और समस्त उतरवर्ती पैकेट्स को 6 के लिए रूट करने का निर्णय लेता है।

वर्चुअल सर्किट के लाभ :

यदि दो स्टेशन्स दीर्घ अवधि तक डाटा का आदान–प्रदान करना चाहें, तो वर्चुअल सर्किट्स के निम्नलिखित अपने लाभ हैं–

1. सर्वप्रथम, नेटवर्क वर्चुअल सर्किट के साथ ही साथ सिक्वेंसिंग और ऍरर कंट्रोल से संबंधित सेवाएँ प्रदान कर सकता है। सिक्वेंसिंग का अर्थ इस तथ्य से होता है कि चूँ कि समस्त पैकेट्स एक ही रूट का अनुपालन करते है, अस्तु अपने वास्तविक क्रम में आते हैं। ऍरर कंट्रोल सेवा यह सुनिश्चित करती है कि पैकेट्स यथोचित सिक्वेंस में ही आएँ और वे सभी सर्वशुद्ध रूप में भी आएँ।



चित्र 3.34: वर्चुअल सर्किट पैकेट स्विचिंग

3.5 X.21

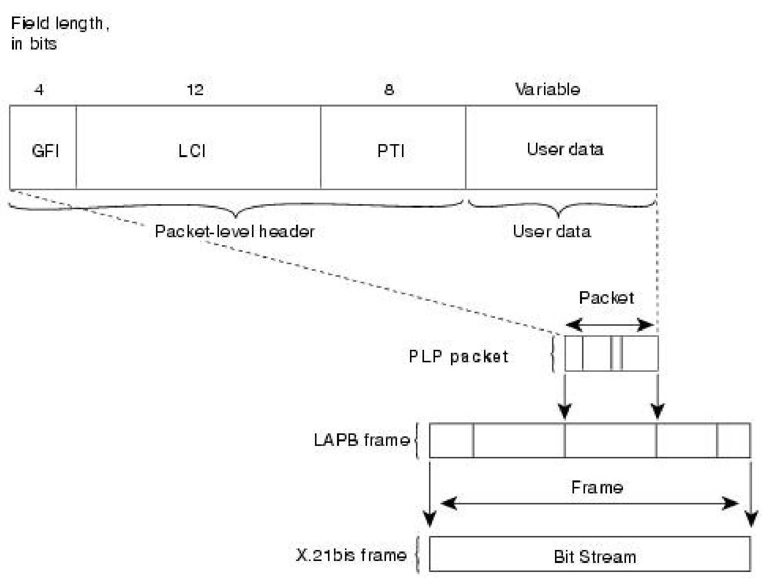
यह सर्वाधिक प्रयुक्त किया जाने वाला प्रोटोकॉल स्टैंडर्ड है। यह स्टैंडर्ड एक होस्ट सिस्टम और एक पैकेट स्विचिंग नेटवर्क के मध्य इंटरफेस दर्शाता है। इस स्टैंडर्ड को पैकेट स्विचिंग नेटवर्क्स हेतु इंटरफेसिंग के लिए तथा ISDN में पैकेट स्विचिंग के लिए प्रयुक्त करने हेतु लगभग पूरी दुनिया में उपयोग किया जाता है। इस स्टैंडर्ड में प्रोटोकॉल्स के तीन लेवल्स होते हैं–

1. फिजिकल लेवल
2. लिंक लेवल
3. पैकेट लेवल

ये तीनों लेवल्स OSI मॉडल की निम्नतम तीन लेयर्स से संबंध्धिा होते है। फिजिकल लेवल जुड़े हुए स्टेशन (कम्प्यूटर, टर्मिनल) और उस स्टेशन को पैकेट स्विचिंग नोड से जोड़ने वाली लिंक के मध्य भौतिक इंटरफेस को संभालता है। स्टैंडर्ड यूजर मशीन्स को डाटा टर्मिनल इक्विपमेंट (DTE) के रूप में और उस पैकेट स्विचिंग जोड़ को जिससे DTE जुड़ा हुआ होता है, डाटा सर्किट टर्मिनेटिंग इक्विपमेंट (DCE) के रूप में उल्लेखित करता है। X.25 फिजिकल लेयर स्पेसिफिकेशन का उपयोग X.21 के रूप में पहचाने जाने वाले स्टैंडर्ड में करता है।

पैकेट फॉर्मेट :

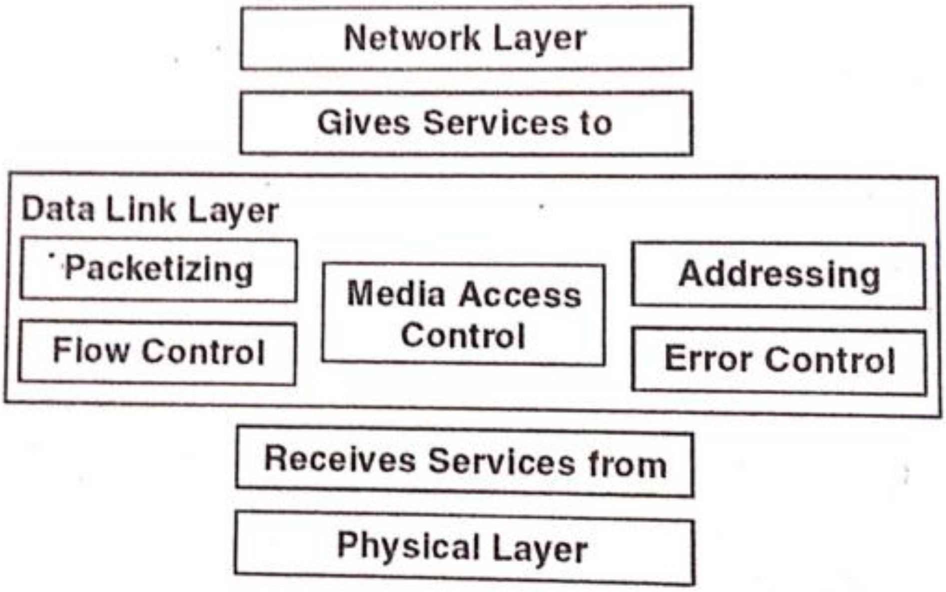
X.25 में प्रयुक्त होने वाले मूलभूत पैकेट फॉर्मेट्स को चित्र 3.35 में प्रदर्शित किया गया है। यूजर डाटा के लिए डाटा को कुछ अधिकतम साईज के ब्लॉकस में विभाजित किया जाता है और डाटा पैकेट बनाने के लिए प्रत्येक ब्लॉक के साथ 24 बिट, 32 बिट अथवा 56 बिट का हेडर जोड़ा जाता है। 15 बिट सिक्वेंस नंबर्स का उपयोग करने वाले वर्चुअल सर्किट्स के लिए हेडर 00110000 वेल्यू वाले प्रोटोकॉल आयडेटिफॉयर ऑक्टेट से प्रारंभ होता है। हेडर 12 बिट वर्चुअल सर्किट नंबर (जिसे 4 बिट ग्रुप नंबर और 8 बिट चैनल नंबर के रूप में व्यक्त किया जाता है) से बना होता है। P (S)औरP (R) फील्ड्स फ्लो कंट्रोल और ऍरर कंट्रोल के कार्य में वर्चुअल सर्किट के आधार पर मदद करती है।



चित्र 3.35 : X.25 पैकेट फॉर्मेट

4.1 डाटा लिंक लेयर एक परिचय :

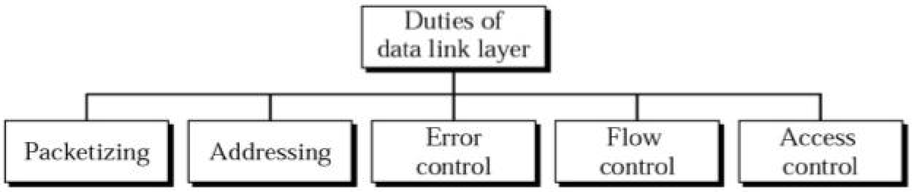
इंटरनेट मॉडल में डाटा लिंक लेयर नेटवर्क लेयर और फिजिकल लेयर के मध्य स्थित होती हैं। यह फिजिकल लेयर से सेवा प्राप्त करती हैं और नेटवर्क लेयर को सेवाएँ प्रदान करती हैं। चित्र 4.1 में इंटरनेट मॉडल में डाटा लिंक लेयर की स्थिति दर्शाई गई है।



चित्र 4.1: ओ. एस. आई. मॉडल में डाटा लिंक लेयर

डाटा लिंक लेयर एक कम्प्यूटर अथवा राउटर से अगले कम्प्यूटर या राउटर तक पैकेट को स्थानांरित किए जाने के लिए जिम्मेदार होती हैं। नेटवर्क लेयर के विपरीत जिस पर वैश्विक जिम्मेदारी होती हैं, डाटा लिंक लेयर स्थानीय स्तर पर जिम्मेदार होती हैं। इसकी जिम्मेदारी दो कम्प्यूटरों के मध्य स्थित होती हैं। दूसरे शब्दो में, चूँकी इंटरनेट में LAN और WAN की सीमाएँ कम्प्यूटर तय करते हैं, हम यह कह सकते हैं कि डाटालिंकलेयर की जिम्मेदारी किसी पैकेट को LAN या WAN के माध्यम से स्थनांतरित करना हैं।

4.1.1 डाटा लिंकलेयर द्वारा उपलब्ध सेवाएँ :



चित्र 4.2: डाटा लिंकलेयर द्वारा उपलब्ध सेवाएँ

डाटालिंक लेयर की सेवाओ में चित्र 4.2 में दर्शाए अनुसार पैकेटाईजिंग, एड्रेसिंग, ऍरर कंट्रोल, फ्लो कंट्रोल और मीडियम एक्सेस कंट्रोल शामिल हैं।

1. पैकेटाईजिंग: डाटा लिंक लेयर डाटा को एक दूसरे कम्प्यूटर तक ले जाने के लिए जिम्मेदार होती हैं।अगले कम्प्यूटर तक जाने के लिए डाटा को एक LAN अथवा एक WAN के माध्यम से जाना होता हैं।इनमें से प्रत्येक के अपने प्रोटोकॉल्स होते हैं। अपरलेयर से आने वाला पैकेट ऐसे यथोचित पैकेट में एनकेप्स्यूलेटेड होना चाहिए, जो वर्तमान LAN अथवा WAN की डाटालिंक लेयर द्वारा परिभाषित हो। डाटा लिंक लेयर में पैकेट के लिए विभिन्न प्रोटोकॉल्स के पास अलग–अलग नाम होते हैं।

2. एड्रेसिंग : डाटा लिंक लेयर पर हमें एक एड्रेसिंग मेथड की आवश्यकता होती हैं। डाटालिंक लेयर एंड्रेसेस को फिजिकल एड्रेसेस (या MAC एड्रेसेस) कहते हैं तथा इन्हें एक कम्प्यूटर से दूसरें कम्प्यूटर में डिलिवरी के समय अगले कम्प्यूटर का एड्रेस खोजने के लिए प्रयुक्त किया जाताहैं। LAN जिस फिजिकल एड्रेस का उपयोग करता है, वह WAN द्वारा प्रयुक्त किए जाने वाले फिजिकल एड्रेस से पूरी तरह से भिन्न होता है। एक LAN वर्चुअल सर्किट एड्रेस का उपयोग करता है।

3. ऍररकंट्रोल : डाटा कम्यूनिकेशन में ऍरर से बचा नहीं जा सकता हैं। बेहतर उपकरण और अधिक विश्वसनीय ट्रंसमिशन माध्यम का उपयोग करते हुए ऍरर्स के उत्पन्न होने की आवृति या उस की गंभीरता को कम किया जा सकता है, परन्तु यह इसे पूरी तरह से डाटा हटा नहीं सकता है। नेटवर्क्स में एक से दुसरी डिवाईस तक डाटा को सम्पूर्ण शुद्धता के साथ स्थानातरिंत किए जाने की सक्षमता होनी चाहिए।

4. फ्लोकंट्रोलः डाटा लिंक लेंयर की एक अन्य जिम्मेदारी फ्लों कंट्रोल हैं। अधिकांश प्रोट्रोकॉल्स में फ्लो कंट्रोल ऐसी प्रक्रियाओं का एक समूह होता है, जो भेजने वाले को यह बताता हैं कि वह प्राप्तकर्ता से एकानॉलेमेंट मिलने की प्रतीक्षा करने के पूर्व कितना डाटा भेज सकता है। डाटा के फ्लो को इतनी अनुमति नहीं दी जा सकती है कि वह ग्रहण करने वाले पर अत्याधिक दबाव बना दें। डाटा प्रवाह एक सीमा तक पहुँचने के पूर्व ही, ग्रहण करने वाली डिवाईस, भेजने वाले को सूचना दे देता है।

5. मीडियम एक्सेस कंट्रोल : जब कम्प्यूटर किसी शेयर्ड मीडियम (केबल अथवा वायु) का उपयोग करता है, तो किसी भी क्षण मीडियम पर एक्सेस कंट्रोल की तकनीक होनी चाहिए। किसी नेटवर्क पर संघर्ष अथवा टकराव को रोकने के लिए मीडियम होनी चाहिए। किसी नेटवर्क पर संघर्ष अथवा टकराव को रोकने के लिए मीडियम एक्सेस कंट्रोल (MAC)विधि की आवश्यकता होती है।

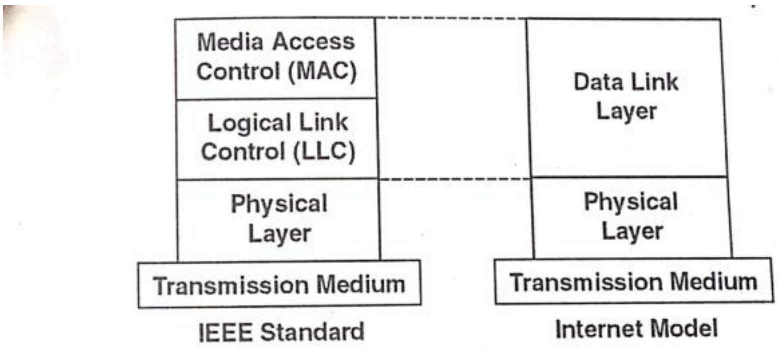
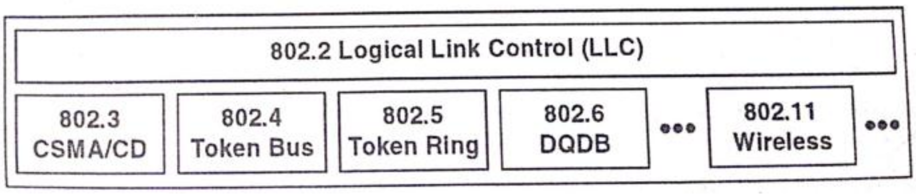


Fig. 10.3 LLC and MAC Sublayers



चित्र 4.3: मीडियम एक्सेस कंट्रोल **लेन स्टैंडर्ड**

डाटा लिंक प्रोटोकॉल्स :

यह महत्वपूर्ण है कि फ्रेम की संरचना दोनों ही डाटा लिंक लेयर्स को पता होनी चाहिए, जिससे कि कंट्रोल बिट्स की पहचान की जा सके। डाटा लिंक लेयर्स को कंट्रोल इंफॉर्मेशन के आदान–प्रदान के लिए अपनाई जाने वाली कंट्रोल फंक्शन के स्थानांतरण के लिए नियमों और प्रक्रियाओं के विशिष्ट सेट को डाटा लिंक कंट्रोल के रूप में जाना जाता है।

एक डाटा लिंक कंट्रोल निम्न को प्रदर्शित करती है –

(i) फ्रेम का फॉर्मेट अर्थात् विभिन्न फील्ड्स की लोकेशन्स और साइजेस।

(ii) इन फील्ड्स की विषय–वस्तु।

(iii) फ्लो कंट्रोल, ऍरर कंट्रोल और लिंक मैनेजमेंट फंक्शन्स को संपन्न करने के लिए विनिमय किए जाने वाले संदेशों का क्रम।

डाटा लिंक प्रोटोकॉल्स के कुद उदाहरण इस प्रकार हैं–

(i) हाई–लेवल डाटा लिंक कंट्रोल;भ्ध्क्स्ब्द्धं

(ii) सिंक्रोनस डाटा लिंक कंट्रोल ॅ;स्क्ब्द्ध।

(iii) एडवांस्ड डाटा कम्यूनिकेशन कंट्रोल प्रोसीजर ; ।क्ब्च्द्ध।

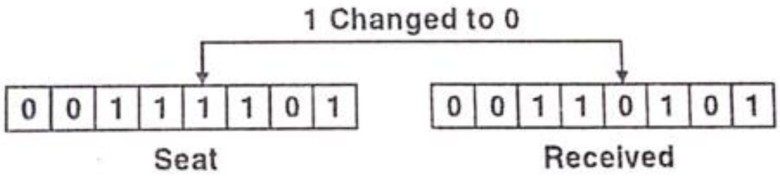
(iv) बायनरी सिंक्रोनस डाटा लिंक कंट्रोल ;ठैप्ल्छब्ए ठैध्ब्0।

डाटा लिंक लेयर में ट्रांसमिशन संबंधी ऍरर्स और उसके प्रकार :

स्त्रोत से गंतव्य तक डाटा को स्थानांतरित करने के लिए नेटवर्क्स होते हैं। ट्रांसमिशन के दौरान मैसेज वेल्यूज–ताप, आर्द्रता, विद्युतीय उतार–चढ़ाव और चुबंकीय हस्तक्षेप जैसे भौतिक कारकों से बाधित हो सकती है। ये व्यवधान मैसेज में ऍरर उत्पन्न कर देते हैं। ग्रहण किए जाने वाले सिरे पर मैसेज की वैद्यता का परीक्षण किए जाने के क्रम में, कुछ डिटेक्शन और करेक्शन कहते हैं। ऍरर डिटेक्शन और करेक्शन को ट्ब् मॉडल की डाटा लिंक लेयर पर या फिर ट्रांसपोर्ट लेयर पनर कार्यान्वित किया जाता है।

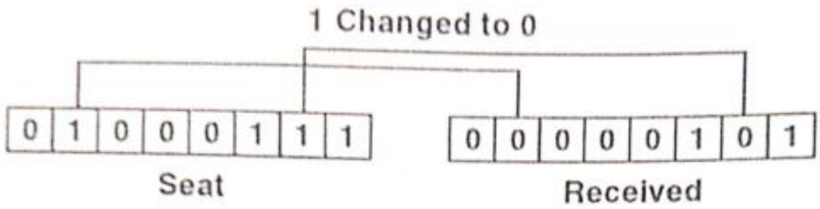
ऍरर्स के तीन प्रकार हैं। ये प्रकार सामान्यतः सिंगल बिट, मल्टीपल बिट और बर्स्ट ऍरर्स होने की सबसे कम संभावना होती है।

(a) सिंगल–बिट ऍरर : इस प्रकार का ऍरर तब होता है, जब भेजा जाने वाला सिंगल बिट डाटा 0 से 1 में अथवा 1 से 0 में बदलता है।



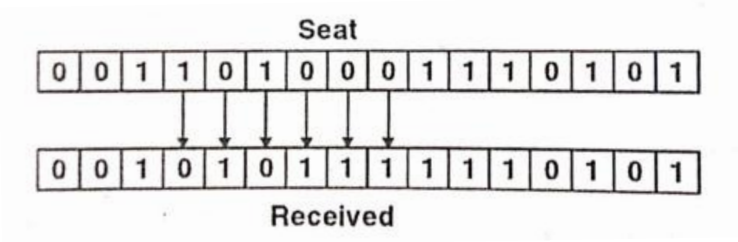
चित्र 4.4 : सिंगल बिट एरर

(b) मल्टीपल–बिट ऍरर : इस प्रकार का ऍरर तब उत्पन्न होता है, जब डाटा में दो अथवा अधिक क्रमबद्ध रूप से न जाने वाली बिट्स 0 से 1 में या फिर 1 से 0 में बदलती है।



चित्र 4.5 : मल्टीबीट बिट एरर

(c) बर्स्ट ऍरर : इस प्रकार का ऍरर तब होता है, जब डाटा में एक के बाद आने वाली दो या अधिक बिट्स 0 से 1 या 1 से 0 में बदल जाती है।



चित्र 4.6 : ब्रस्ट एरर

4.2 फ्लो कंट्रोल :

फ्लो कंट्रोल डाटा की उस मात्रा का रेकॉर्ड रखता है, जिसे एकनॉलेजमेंट प्राप्त होने के पूर्व भेजा जा सकता है। फ्लो कंट्रोल ऐसी प्रक्रियाओं का एक सेट होता है, जो प्रेषक को यह सूचित करता है कि ग्रहण करने वाले (रिसीवर) को ओवरलोड करने करने की अनुमति नहीं दी जानी चाहिए। किसी प्राप्तकर्त्ता डिवाईस के पास आने वाले डाटा को प्रोसेस कर सकने कर सकने की एक सीमित गति होती है और इसी प्रकार से आने वाले डाटा को संग्रहकीत करने के लिए भी उसके पास सीमित मात्रा में मेमोरी होती है। प्राप्तकर्त्ता डिवाईस के पास यह सक्षमता होनी चाहिए कि वह सेंडिंग डिवाईस को उन सीमाओं तक पहुँचने के पूर्व ही सूचित कर सके और ट्रांसमिशन डिवाईस को कम संख्या में फ्रेम्स को भेजे जाने अथवा अस्थायी रूपसे ट्रांसमिशन को रोकने का अनुरोध कर सके। आने वाले डाटा को प्रयुक्त किए जाने के पूर्व जाँचा और प्रोसेस किया जाता है। इस प्रकार के प्रोसेसिंग की दर सामान्यतः ट्रांसमिशन की दर से धीमी होती है। इसी कारण से प्रत्येक रिसीविंग डिवाईस के पास एक मेमारी ब्लॉक होता है, जिसे बफर कहते है। इसमें आने वाले डाटा को प्रोसेसिंग होने तक संग्रहीत किए जाने के लिए रिजर्व रखा जाता है।

ऍरर कंट्रोल :

ऍरर कंट्रोल में ऍरर डिटेक्शन और ऍरर करेक्शन दोनों ही आते हैं। यह रिसीवर को यह बताने की सक्षमता प्रदान करता है कि वह सेंडर को ट्रांसमिशन के दौरान किसी गुम हुए अथवा क्षतिग्रस्त फ्रेम्स की जानकारी दे सके। इसके साथ ही वह सेंउर से उन फ्रेम्स के रीट्रांसमिशन का समन्वय भी कर सके। डाटा लिंक लेयर में ऍरर कंट्रोल शब्द का अर्थ मूल रूप से ऍरर पता लगाने और रीट्रांसमिशन की विधियों से होता है। डाटा लिंक लेयर में ऍरर कंट्रोल सामान्यतः सरलता से कार्यान्वित किया जाता है।

फ्लो और ऍरर कंट्रोल मैकेनिज्म :

फ्लो एंड ऍरर कंट्रोल की सामान्यतः तीन विधियाँ होती है। ये निम्नलिखित है –

1. स्टॉप एंड वेट ARQ
2. गो – बैक NARQ
3. सिलेक्टिव–रिपीट ARQ

4.2.1 स्टॉप–एंड–वेट ARQ:

स्टॉप–एण्ड–वेट ।तफ फ्लो एंड ऍरर कंट्रोल की सबसे सरल विधि है। इसमें निम्न विशिष्टताएँ होती हैं–

(i) सेंडिंग डिवाईस ट्रांसमिट की गई फ्रेम की कॉपी को तब तक रखती है, जब तक कि उसे इस फ्रेम का एकनॉलेजमेंट नहीं मिल जाता है। इससे सेंडर को यह सुविधा मिलती है कि वह फ्रेम्स के पूरी तरह से सही रूप में मिल जाने तक गुम हुए अथवा क्षतिग्रस्त फ्रेमों का रीट्रांसमिशन कर सकता है।

(ii) पहचान के उद्देश्य से डाटा फ्रेम्स और एकनॉलेजमेंट (ACK) फ्रेम्स को अदल–बदल कर 0 और 1 के अंक दिए जाते है। एक डाटा 0 फ्रेम को ACK 1 फ्रेम द्वारा एकनॉलेज किया जाता है, जो यह बताता है कि रिसीवर ने डाटा फ्रेम 0 को रीसीव कर लिया है और उसे अब डाटा फ्रेम 1 की प्रतीक्षा है। इस नंबरिंग के चलते डुप्लीकेट ट्रांसमिशन की स्थिति में डाटा फ्रेम्स की पहचान करने में मदद मिलती है।

(iii) क्षतिग्रस्त अथवा गुम हुई फ्रेम को रीसीवर द्वारा समान रूप से प्रोसेस्ड किया जाता है। रिसीवर द्वारा प्राप्त की गई फ्रेम में यदि किसी ऍरर का पता चलता है, तो वह उस फ्रेम को रद्दकर देता है और एकनॉलेजमेंट नहीं भेजता है।

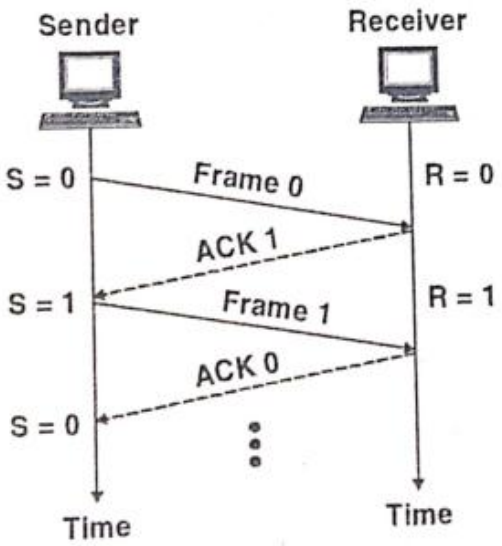
(iv) सेंडर के पास एक कंट्रोल वेरियेबल होता हैं, जिसे हम S कहते हैं। यह हाल ही में भेजी गई फ्रेम (0 या 1) को थामकर रखता है। रिसीवर में एक कंट्रोल वेरियेबल होता है, जिसे हम R कहते हैं। ये आगे आने वाली अपेक्षित फ्रेम (0 या 1) की संख्या को रखता है।

(v) सेंडर जब फ्रेम ट्रांसमिट करता है, तो टाईमर को प्रारंभ कर देता है। यदि एक निर्धारित समय के भीतर कोई एकनॉलेजमेंट नहीं भेजा जाता है, तो सेंडर यह मान लेता है कि फ्रेम या तो गुम हो गई है अथवा क्षतिग्रस्त हो गई है और वह उसे फिर से ट्रांसमिट करता है।

(vi) रिसीवर सुरक्षित और त्रुटिरहित रूप से प्राप्त फ्रेम्स के लिए केवल पॉजिटिव एकनॉलजमेंट भेजता है। जब वह कोई क्षतिग्रस्त या गुम फ्रेम्स प्राप्त करता है, तो मौन ही रहता है। एकनॉलजमेंट नंबर हमेशा अगली अपेक्षित फ्रेम की संख्या को

बताता है। यदि फ्रेम 0 प्राप्त की जाती है, तो ACK 1 भेजा जाएगा और यदि फ्रेम 1 प्राप्त की जाती है, तो ACK व भेजा जाएगा।

कार्यप्रणालीः

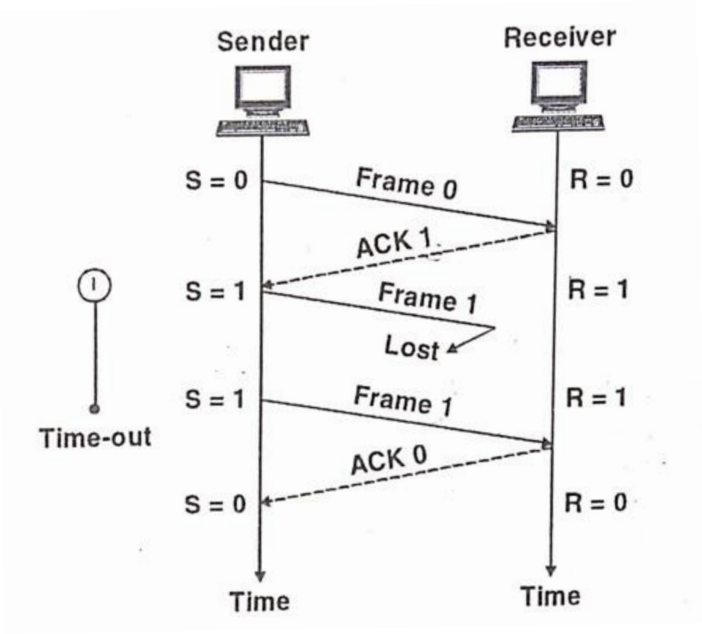


चित्र 4.7 : नार्मल ऑपरेशन

किसी फ्रेम के ट्रांसमिशन में हमारे पास चार स्थितियाँ हो सकती हैं– (1) नॉर्मल, (2) फ्रेम का गुम या क्षतिग्रस्त होना, (3) एकनॉलेजमेंट का गुम होना अथवा (4) एकनॉलजमेंट में विलंब होना।

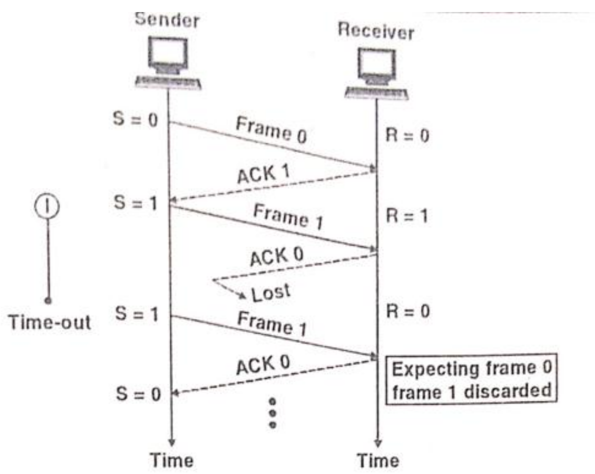
(1) नॉर्मलः नॉर्मल ट्रांसमिशन में सेंडर फ्रेम 0 को ट्रांसमिट करता है और ACK 1 प्राप्त होने की प्रतीक्षा करता है। जब ACK 1 प्राप्त हो जाता है, तब वह फ्रेम 1 को ट्रांसमिट करता है और फिर पुनः ACK 0 प्राप्त होने की प्रतीक्षा करता है

(2) गुम अथवा क्षतिग्रस्त फ्रेमः गुम हो चुकी अथवा क्षतिग्रस्त फ्रेम को रिसीवर द्वारा समान रूप से लिया जाता है। वह इसे रद्द कर देता है, जिसका मुख्यतः यही अर्थ होता है कि फ्रेम गुम हो गई है। गुम हो चुकी फ्रेम के बारे में रिसीवर मौन रहकर इसकी वेल्यू को R ही रहने देता है।



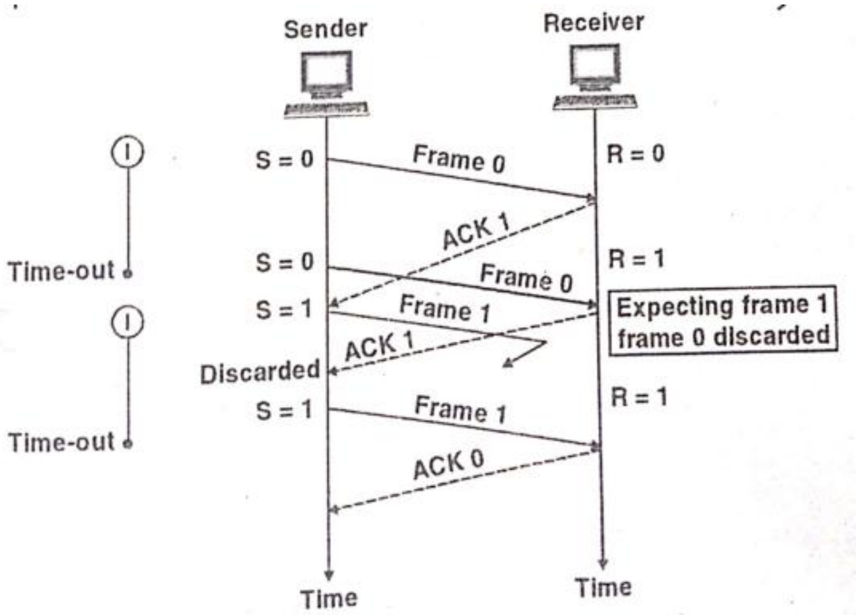
चित्र 4.8 : स्टॉप & वेट ARQ , लॉस्ट फ्रेम

(3) गुम एकनॉलजमेंट : एक गुम हो चुकी अथवा क्षतिग्रस्त हो चुकी एकनॉलजमेंट को सेंडर द्वारा समान रूप में ही लिया जाता है। वह इसे निरस्त कर देता है। चित्र 10.10 में एक गुम हो चुकी ACK0 को दर्शाया गया है। प्रतीक्षारत सेंडर को यह पता नहीं चलता है कि फ्रेम 1 ग्रहण की जा चुकी है अथवा नहीं। जब फ्रेम 1 के लिए टाईमर की समय सीमा समाप्त हो जाती है, तो सेंडर फ्रेम 1 को फिर से ट्रांसमिट करता है। यह मान लें कि रिसीवर को पहले ही फ्रेम 1 प्राप्त हो चुकी है और अब वह फ्रेम 0 (R=0) को प्राप्त होने की अपेक्षा रख रहा है।



चित्र 4.9 : स्टॉप & वेट ARQ , लॉस्ट ACK फ्रेम

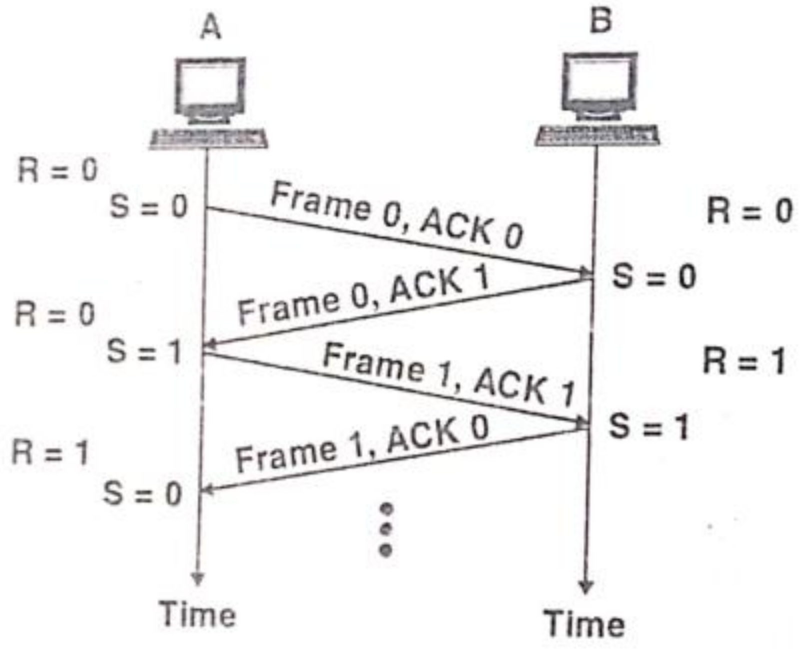
(4) विलंबित एकनॉलजमेंट : अगली समस्या यह हो सकती है कि एकनॉलजमेंट प्राप्त होने में विलंब हो। एकनॉलजमेंट में रिसीवर की ओर से विलंब हो सकता है या फिर लिंक में कोई समस्या आने की वजह से ऐस हो सकता है। चित्र 4.10 में ACK 1 के विलंब को दर्शाया गया है।



चित्र 4.10 : स्टॉप & वेट ARQ , लॉस्ट डिलेड फ्रेम

(a) बॉयडायरेक्शनल ट्रांसमिशनः स्टॉप–एण्ड–वेट विधि में हमने एक ही दिशा में होने वाले (यूनिडायरेक्शनल) ट्रांसमिशन का अध्ययन किया था। यदि दो पक्षों के पास फुल–डुप्लेक्स ट्रांसमिशन के लिए दो स्वतंत्र चैनल्स हो अथवा हॉफ–डुप्लेक्स ट्रांसमिशन के लिए वे एक समान चैनल में भागीदारी कर सकते हों, तो हमें दो तरफा (बॉयडायरेक्शनल) ट्रांसमिशन भी मिल सकता है।

(b) पिगीबैकिंग : पिगीबैकिंग किसी डाटा फ्रेम को एक एकनॉलजमेंट से संयोजित करने की विधि है। उदाहरण के लिए, चित्र 4.11 में स्टेशन A और B दोनों में प्रेषित किए जाने के लिए डाटा है। डाटा और ACK फ्रेम्स को पृथक–पृथक भेजने के अतिरिक्त स्टेशन A एक ऐसी डाटा फ्रेम प्रेषित करता है, जो कि एक ACK से निर्मित होती है। इसी प्रकार का व्यवहार स्टेशन B भी करेंगा।



चित्र 4.11 : पिग्गीबैंकिंग

4.2.2 गो–बैक–N ARQ:

स्टॉप–एण्ड–वेट ARQ में केवल एक ही फ्रेम होती है, जिसे भेजा जाता है और जो एकनॉलेज्ड होने की प्रतीक्षा करती है। यह ट्रांसमिशन माध्यम का कोई बेहतर उपयोग नहीं होता है। कुशलता को बढ़ाने की दृष्टि से जब एकनॉलजमेंट के लिए प्रतीक्षा की जा रही हो उस दौरान एक से अधिक फ्रेम्स ट्रांजिशन में होने चाहिए। दूसरे शब्दों में, हमें एक से अधिक फ्रेम्स को आऊटस्टेंडिंग की अनुमति प्रदान करने की जरूरत होगी। आऊटस्टेंडिंग का अर्थ प्रेषित की गई और एकनॉलेजमंट की प्रतीक्षा कर रही फ्रेम से है। दो प्रोटोकॉल्स गो–बैक–छ ARQ और सिलेक्टिव रिपीट ARQ इस अवधारण का उपयोग करते हैं।

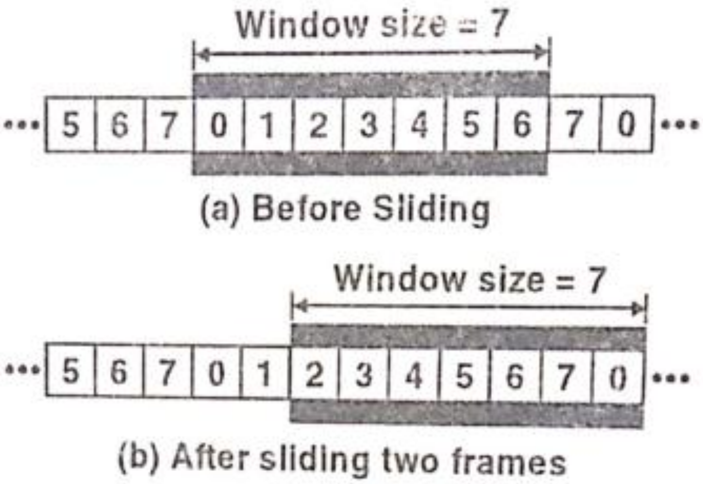
गो–बैक–छ ARQ में हम एकनॉलेजमेंट के बारे में विचार किए जाने के पूर्व ही फ फ्रेम्स तक ट्रांसमिट कर सकते हैं। हम एकनॉलेजमेंट के आने तक इन फ्रेम्स की कॉपी रखते है।

(i) सीक्वेंस नंबर्स : किसी सेंडिंग स्टेशन से प्रेषित की गई फ्रेम्स को क्रमबद्ध रूप से नंबर्स प्रदान किए जाते है। किंतु चूँकि हमें प्रत्येक फ्रेम के सीक्वेंस नंबर को हेडर

में सम्मिलित करने की जरूरत होती है, इसलिए एक सीमा निर्धारित करना आवश्यक है। यदि फ्रेम का हेडर सीक्वेंस नंबर के लिए m बिट्स की अनुमति देता है, तो सीक्वेंस नंबर्स की रेंज 0 से 2^m-1 तक होगी।

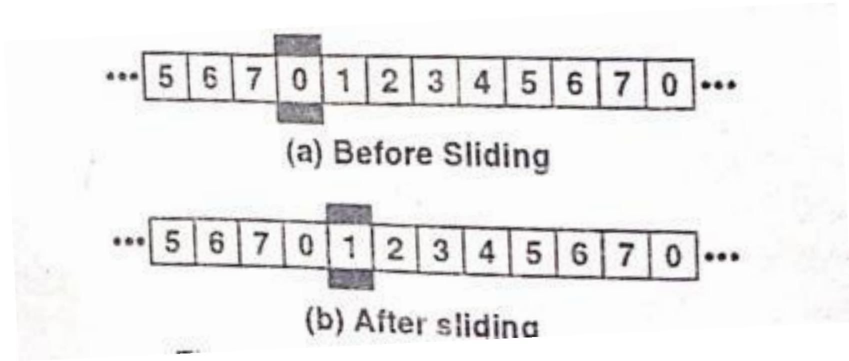
(ii) सेंडर स्लाइडिंग विंडों : सेंडर आऊटस्टेंडिंग फ्रेम्स को तब तक थामकर रख सकता है, जब तक कि वे एकनॉलेज्ड नहीं हो जाती हैं। ऐसी दशा में हम एक विंडो की अवधारणा का उपयोग करते है। हम यह मानकर चलते हैं कि समस्त फ्रेम्स बफर में संग्रहीत होती है। आऊटस्टेंडिंग फ्रेम्स एक विंडो में उपस्थित रहती हैं।

इस प्रोटोकॉल में विंडो की साईज फिक्स्ड होती है, परंतु TCP जैसे अन्य प्रोटोकॉल्स में हम विभिन्न साईज की विंडो ले सकते हैं। जब सही एकनॉलजमेंट प्राप्त हो जाता है, तब विंडो न भेजी गई नई फ्रेम्स पर विचार करने के लिए स्लाईड करती है।



चित्र 4.12 : सेंडिंग स्लाइडिंग विंडो

(iii) रिसीवर स्लाईडिंग विंडो : इस प्रोटोकॉल में रिसीविंग विंडो की साईज हमेशा 1 होती है। रिसीवर हमेशा ही फ्रेम विशेष को विशेष क्रम में ही आने की प्रतीक्षा करता है। क्रम से अलग हटकर आने वाली किसी भी फ्रेम को अनदेखा कर दिया जाता है और इसे फिर से भेजे जाने की आवश्यकता होती है। रिसीवर विंडो भी चित्र 4.13 में दर्शाए अनुसार स्लाईड होती है। भाग a में रिसीवर फ्रेम 0 के लिए प्रतीक्षा कर रहा है।



चित्र 4.13 : रिसीवर स्लाइडिंग विंडो

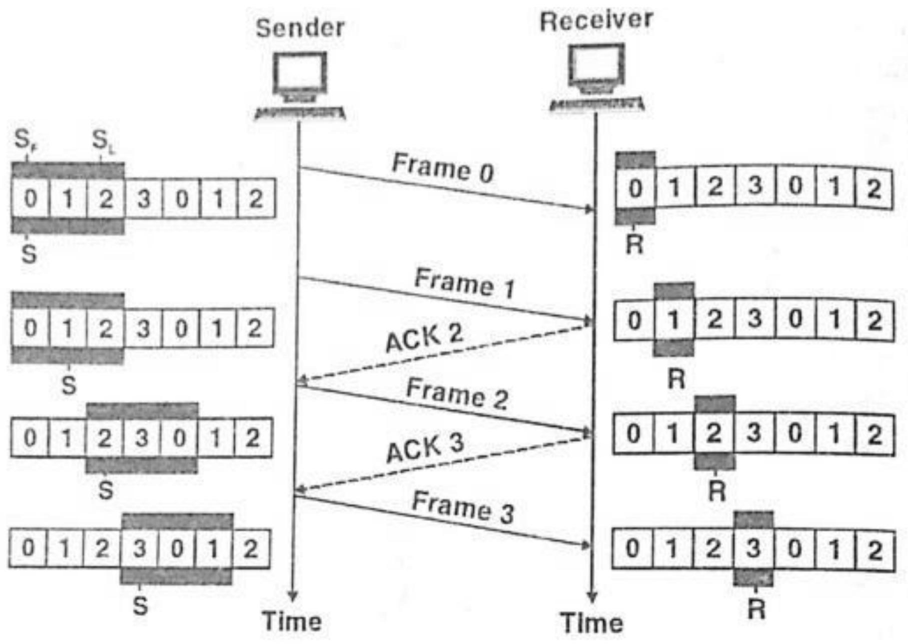
(iv) एकनॉलेजमेंट : यदि कोई फ्रेम सुरक्षित, सही और क्रम में आती हैं, तो रिसीवर पॉजिटिव एकनॉलेजमेंट्स ट्रांसमिट करता है। यदि कोई फ्रेम क्षतिग्रस्त है अथवा वह क्रम से हटकर प्राप्त हुई है, तो रिसीवर मौन हो जाता है और बाद में आने वाली सभी फ्रेम्स को तब अनदेखा करता जाता है, जब तक कि उसे अपेक्षित फ्रेम प्राप्त नहीं हो जाती है। रिसीवर के इस मौन के परिणामस्वरूप एकनॉलेज्ड की गई फ्रेम के टाईमर की अवधि खत्म हो जाती है। इसके फलस्वरूप सेंडर वापस पीछे जाकर सारी फ्रेम्स को फिर से ट्रांसमिट करता है।

कार्यप्रणालीः

किसी फ्रेम के ट्रांसमिशन में हमारे पास निम्न स्थितियाँ हो सकती हैं–

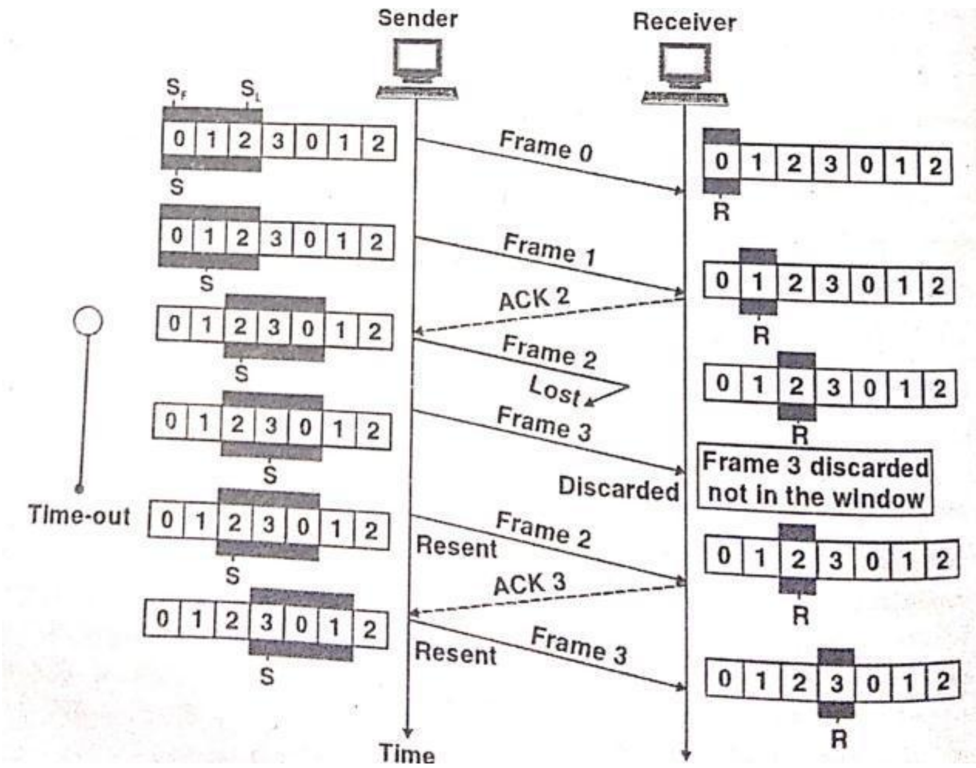
(i) सामान्य : चित्र 4.14 में इस विधि की सामान्य कार्यप्रणाली दर्शाई गई है। सेंडर आऊटस्टेंडिंग फ्रेम्स पर निगरानी बनाएं रखता है और एकनॉलेजमेंट्स के आने के साथ विंडोस को अपडेट्स करता जाता है।

(ii) क्षतिग्रस्त या गुम हो चुकी फ्रेम : चित्र 4.15 दर्शाता है कि फ्रेम 2 गुम हो गई है। यह विचार करें कि रिसीवर जब फ्रेम 3 ग्रहण करता है, तब उदसे उपेक्षित कर दिया जाता है, क्योंकि रिसीवर को फ्रेम 2 की अपेक्षा थी न कि फ्रेम 3 की (उसकी विंडो के अनुसार)। सेंडर साईट पर जब फ्रेम 2 का टाईमर अवधि पूरित हो जाती है, तो सेंडर फ्रेम 2 और 3 (यह वापस 2 पर जाता है) को ट्रांसमिट करेगा।



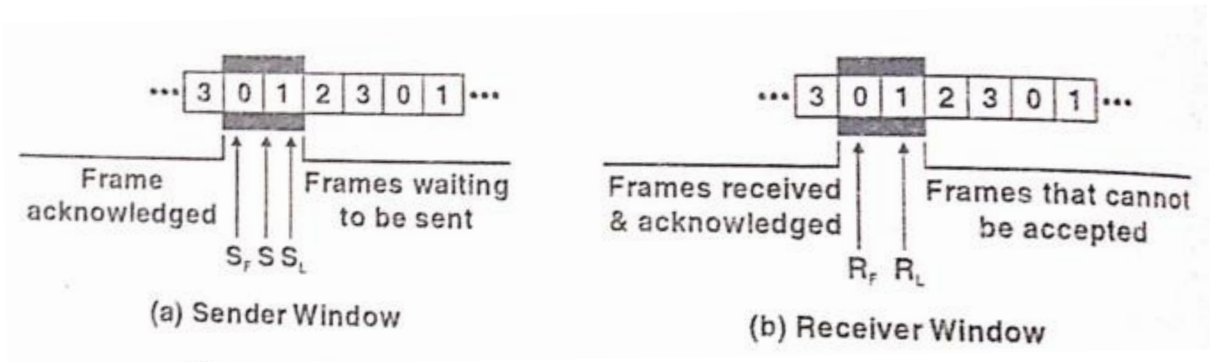
चित्र 4.14 : गो बैक N APQ नार्मल ऑपरेशन

(iii) क्षतिग्रस्त या गुम एकनॉलेजमेंट : यदि कोई एकनॉलजमेंट क्षतिग्रस्त या गुम होता है, तो हमारे सामने दो परिस्थितियाँ होती है। यदि किसी टाईमर के समाप्त होने के पूर्व ही अगला एकनॉलेजमेंट आ जाता है, तो फ्रेम्स के लिए फिर से ट्रांसमिशन की कोई आवश्यकता नहीं होती है, क्योंकि इस प्रोटोकॉलल में एकनॉलेजमेंट्स इकट्ठे होते जाते है। ACK 4 का अर्थ ACK 1 से ACK 4 तक होता है। इसलिए यदि ACK 1, ACK 2 और ACK 3 गुम हो जाते हैं, तो ACK 4 उन सभी को कवर कर लेता है। परंतु यदि अगला ACK टाईम आऊट के उपरांत आता है, तो वह फ्रेम औश्र उसके बाद वाली सभी फ्रेम्स फिर से भेजी जाती हैं। ध्यान दें कि रिसीवर ACK को कभी भी दुबारा नहीं भेजता है।



चित्र 4.15 : गो बैक N APQ लॉस्ट फ्रेम

4.2.3 सिलेक्टिवे रिपीट ARQ



चित्र 4.16 : सेलेक्टिव रिपीट ARQ सेन्डर एंड रिसीवर

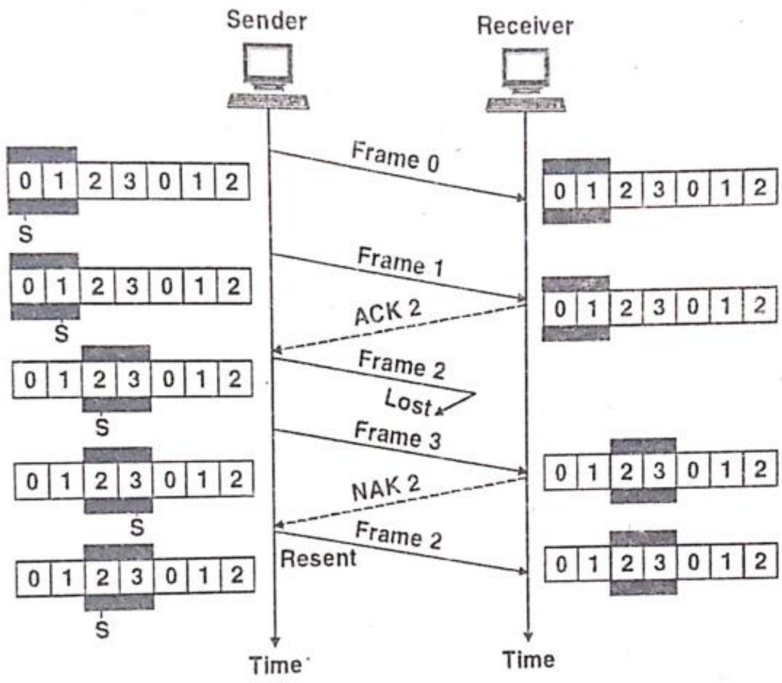
गो–बैक–छ ARQ रिसीवर सिरे पर प्रक्रिया को सरलीकृत करती है। रिसीवर केवल एक ही वेरियेबल का ध्यान रखता है और आऊट–ऑफ–ऑर्डर फ्रेम्स को बफर करने की कोई आवश्यकता नहीं होती है। उन्हें तो केवल उपेक्षित भर कर दिया जाता है। परंतु यह प्रोटोकॉल शोर वाली लिंक के लिए बहुत ही अनावश्यक है। एक नॉईजी लिंक में किसी फ्रेम के क्षतिग्रस्त होने की संभावना बहुत अधिक होती है। इसका अभिप्रायः यह है कि एक से अधिक फ्रेम्स का पुनः ट्रांसमिशन किया जाना।

सिलेक्टिव रिपीट ARQ के लिए सेंडर का कॉनफिग्यूरेशन गो–बैक–छ ARQ के समरूप ही होता है। परंतु इसमें विंडो की साईज 2m वेल्यू के अधिक से अधिक डेढ़ गुना तक हो सकती है। रिसीवर विंडो भी इसी साईज की होनी चाहिए।

गो–बैक–N ARQ में रिसीवर एक विशिष्ट सीक्वेंस नंबर की ही तलाश में रहता है, जबकि सिलेक्टिव रिपीट में, रिसीवर सीक्वेंस नंबर्स की रेंज की तलाश में रहता है। विंडो की सीमाओं को परिभाषित करने के लिए रिसीवर के पास दो कंट्रोल वेरियेबल्स R_Fऔर R_L होते है। चित्र 4.16 सेंडर और रिसीवर विंडोज दर्शाता है।

कार्यप्रणालीः

चित्र 4.17 में ग्रहण करने के बाद फ्रेम्स 0 और 1 स्वीकार कर ली जाती हैं, क्योंकि वे रिसीवर विंडो द्वारा निर्दिष्ट रेंज में है। जब फ्रेम 3 ग्रहण की जाती है, तब उसे भी इसी कारण से स्वीकार कर लिया जाता है। परंतु रिसीवर यह दर्शाने के लिए NAK 2 भेजता है कि फ्रेम 2 को ग्रहण नहीं किया गया है। जब सेंडर NAK 2 ग्रहण करता है, तो यह केवल फ्रेम 2 को ही पुनः ट्रांसमिट करता हैं, जिसे तब स्वीकृत कर लिया जाता है, क्योंकि वह विंडो की रेंज में होता है।



चित्र 4.17 : **सेलेक्टिव रिपीट ARQ लॉस्ट फ्रेम**

सिलेक्टिव रिपीट ARQ : सिलेक्टिव रिपीट ARQ में केवल गुम अथवा क्षतिग्रस्त हो चुकी विशिष्ट फ्रेम ही फिर से भेजी जाती है। लगता ऐसा है कि यह गो–बैक–N ARQ से अधिक कार्यक्षम है, क्योंकि गो–बैक–NARQ में ऍरर के बाद आने वाली सारी अच्छी फ्रेम्स को भी फिर से भेजा जाता है। यद्यपि यह अच्छा प्रदर्शन नहीं करती है।

इसलिए गो–बैक–N ARQ की तुलना में सिलेक्टिव रिपीट ARQ को कम ही प्रयुकत किया जाता है।

प्रस्तावनाः– अधिकांश कम्यूनिकेशन चैनल्स में नॉइस और गतिरोध के कुछ स्तर को टाला नहीं जा सकता है। डिटिजल ट्रांसमिशन सिस्टम की डिजाईन को अनुकूलतम करने के बावजूद भी अत्यल्प लेकिन नॉन जीरो संभावना के साथ, ट्रांसमिशन में बिट ऍरर्स तो होते ही है। बिट ऍरर रेट के स्तर की स्वीकार्यता एप्लीकेशन विशेष पर निर्भर करती है।

4.3 ऍरर–कंट्रोल :

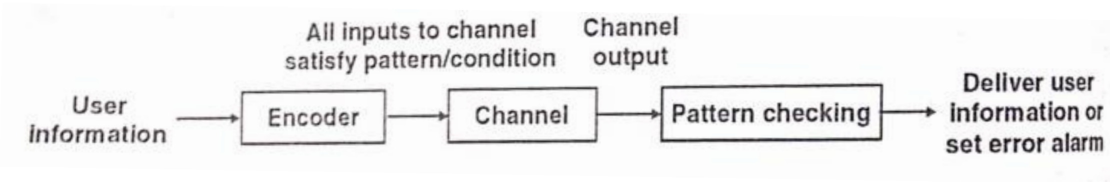
यहाँ ऍरर रेट परफॉर्मेंस को सुधारने के लिए ऍरर कंट्रोल मेथड का परिचय दिया जा रहा है। यह किसी ऐसी स्थिति में एप्लीकेशन के साथ उपलब्ध कराई जाती है, जहाँ डिजिटल ट्रांसमिशन सिस्टम में निहित ऍरर रेट अस्वीकार्य होती है।

ऍरर कंट्रोल के लिए दो मूलभूत मेथड्स होती हैं–

प्रथम मेथड में ऍरर्स का पता लगाना और ऍरर्स का पता लगने पर एक ऑटोमेटिक रीट्रांसमिशन रिक्वेस्ट (ARQ) सम्मिलित होती है। इस विधि में एक रिटर्न चैनल की उपलब्धता को मानकर चला जाता है, जिस पर रीट्रांसमिशन रिक्वेस्ट की जाती है।

दूसरी मेथड, फॉरवर्ड ऍरर करेक्शन (FEC) होती है। इसमें ऍरर्स का पता लगाने के बाद वह प्रोसेसिंग की जाती है, जो एरर्स को सुधारने का प्रयास करती है। FEC तब उपयुक्त होती है, जबकि रिटर्न चैनल उपलब्ध नहीं हो, रीट्रांसमिशन रिक्वेस्ट को सरलता से पूर्ण न किया जा सके।

4.3.1 ऍरर डिटेक्शनः



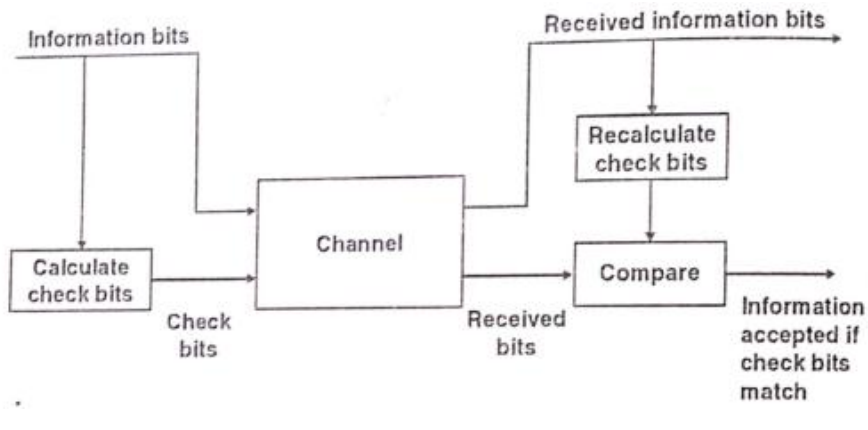
चित्र 4.18 : एरर डिटेक्शन सिस्टम

ऍरर का पता लगाने की मूलभूत अवधारणा बहुत ही सरल है। जैसा चित्र 4.18 में दर्शाया गया है कि किसी एप्लीकेशन द्वारा उत्पन्न इंफॉर्मेशन को एनकोडेड किया जाता है, जिससे कि कम्यूनिकेशन चैनल में इनपुट की जनो वाली स्ट्रीम के पैटर्न या कंडीशन विशेष को तृप्त किया जा सके। कम्यूनिकेशन चैनल के बाहर से आने वाली स्ट्रीम को रिसीवर यह देखने के लिए चेक करता है कि पैटर्न संतृप्त हुआ है या नहीं। यदि नहीं हुआ है, तो रिसीवर यह मान सकता है कि कोई ऍरर उत्पन्न हुआ है और इसके चलते वह यूजर को सतर्क करने के लिए एक अलॉर्म सेट कर देता है। ऍरर का पता लगाने की विधियाँ निम्नलिखित हैं। निम्न ऍरर डिटेक्शन मेथ्ड्स हैं–

(1) पेरिटी मेथड : सर्वाधिक सरलतम कोड सिंगल पेरिटी चेक कोड है, जो k इंफॉर्मेशन बिट्स ग्रहण करता है और एक कोडवर्ड बनाने के लिए एक एकल चेक बिट को जोड़ता है। पेरिटी चेक यह सुनिश्चित करती है कि कोडवर्ड में 1 की कुल संख्या सम हो अर्थातृ कोडवर्ड में इनव पेरिटी (कुछ सिस्टम में चेक बिट को इक्वेशन 1 के बायनरी कॉम्पलीमेंट के रूप में वर्णित करते हुए ऑड पेरिटी का उपयोग किया जाता है) हो। इस परिस्थिति में चेक बिट को पेरिटी बिट कहते है।

यदि किसी कोडवर्ड में ट्रांसमिशन के दौरान एक ही ऍरर होता है, तो चैनल के आऊटपुट पर तत्संबंधित बायनरी ब्लॉक 1 की विषय संख्या से निर्मित होगा और ऍरर का पता चल जाएगा। इसे अधिक सामान्य तौर पर कहें तो यदि कोडवर्ड ऍरर्स की विषम संख्या से उत्पन्न होता है, तो तत्संबंधित आऊटपुट ब्लॉक भी 1 की विषम संख्या से ही निर्मित होगा। इसी प्रकार से सिंगल पेरिटी बिट उन समस्त ऍरर पेटर्न्स का पता लगाने की अनुमति प्रदान करती है, जिनमें ऍरर्स की विषम संख्या मौजूद होती है।

(2) चेकसमः चित्र 4.19 में इस कार्य को किए जाने का एक वैकल्पिक मार्ग दर्शाया गया है। ट्रांसमीटर पर इंफॉर्मेशन को पढ़े जाने के पूर्व इंफॉर्मेशन बिट्स से चेकसम की गणना की जाती है और इंफॉर्मेशन के साथ इसे ट्रांसमिटेड किया जाता है। रिसीवर पर इंफॉर्मेशन के अनुसार पुनः चेकसम को रीकेल्कुलेटेड किया जाता है।



चित्र 4.19 : एरर डिटेक्शन सिस्टम चेक बिट

ऍरर डिटेक्शन से संबंधित दो आधारभूत निष्कर्षों को दर्शाने के लिए इस सरल से उदाहरण को प्रयुक्त किया जा सकता है –

1. ऍरर डिटेक्शन के लिए इंफॉर्मेशन की रीडंडेसी इस मात्रा में आवश्यक होती है कि ट्रांसमिट की गई इंफॉर्मेशन आवश्यक न्यूनतम मात्रा से ऊपर हो। $k+1$ की लम्बाई के एक सिंगल पेरिटी चेक कोड के लिए k बिट्स इंफॉर्मेशन बिट होती है और एक बिट पेरिटी बिट होती है। इस प्रकार ट्रांसमिट की गई बिट्स का एक अंश $1/(k+1)$ रीडंडेंट होता है।
2. प्रत्येक ऍरर डिटेक्शन मेथड कुछ ऍरर्स का पता लगाने में विफल ही रहेगी। विशेष रूप से, कोई ऍरर डिटेक्शन मेथड सदैव ही ऐसे ट्रांसमिशन ऍरर्स का पता लगाने में असफल रहती है, जो एक वैध कोड वर्ड को अन्य वैध कोड वर्ड में परिवर्तित कर देती है। सिंगल पेरिटी चेक कोड के लिए ट्रांसमिशन ऍरर्स की कोई सम संख्या सदैव ही एक वैध कोड वर्ड को अन्य वैध कोड वर्ड से परिवर्तित कर देती है।

4.3.2 पोलीनॉमियल कोड्स :

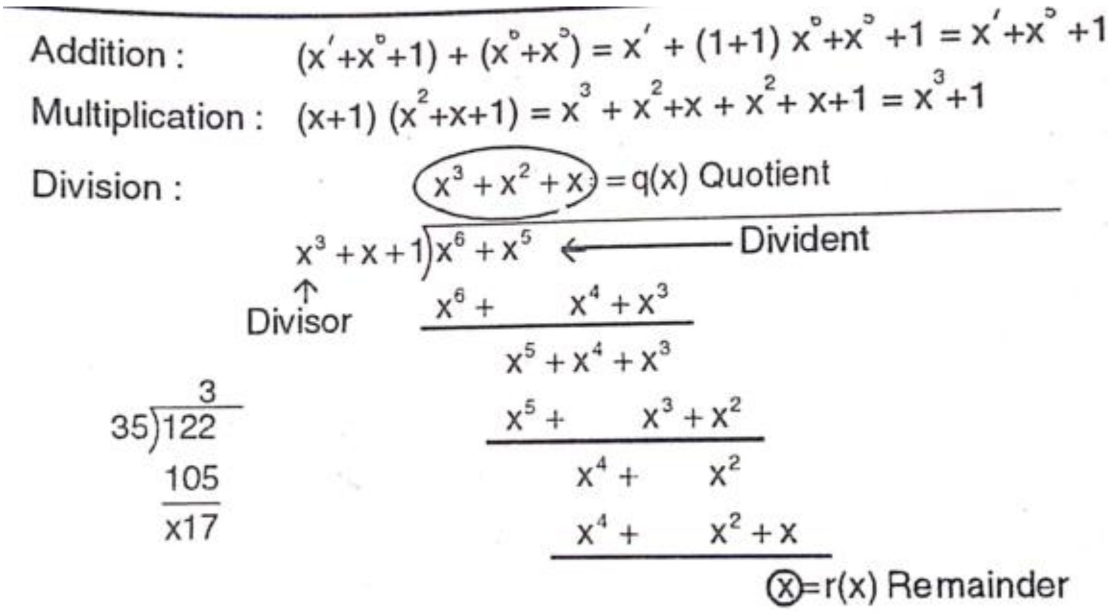
पोलीनॉमियल कोड्स मुख्यतः ऍरर डिटेक्शन तथा करेक्शन में प्रयुक्त होते हैं। पोलीनॉमियल कोड्स को शिफ्ट रजिस्टर में प्रयुक्त होते है। पोलीनॉमियल कोड्स को शिफ्ट रजिस्टर सर्किट्स का उपयोग करते हुए तत्काल कार्यान्वित किया जा सकता है और इसीलिए सर्वाधिक व्यापक रूप में कार्यान्वित किए जाने वाले ऍरर कंट्रोल कोड्स हैं। पोलीनॉमियल कोड्स सायक्लिक रीडंडेंसी चेक (CRC) के रूप में निर्मित की गई चेक बिट्स से बनते हैं। इसी कारण से इन्हें CRC कोड्स के रूप में भी जाना जाता है।

पोलीनॉमियल कोड्स में इंफॉर्मेशन सिम्बल्स कोडवड्स और ऍरर वेक्टर्स द्वारा बायनरी कोडफिशेंट्स वाले पोलीनॉमियल्स से दर्शाया जाता है। डिग्री k-1 की इंफॉर्मेशन को बनाने के लिए k इंफॉर्मेशन बिट्स ($k_{m-1}, k_{k-2}, i_1, i_2$) को प्रयुक्त किया जाता है –

$$I(x)=i_{k-1}X^{k-1} + i_{k-2}X^{k-2}+......i_1X=i_0$$

एनकोडिंग करने की प्रक्रिया $i(x)$ लेती है और $b(x)$ कोडवर्ड पोलीनॉमियल को उत्पन्न करती है, जो इंफोर्मेशन बिट्स तथा अतिरिक्त चेक बिट्स से निर्मित होता है और

जो उसी पैटर्न की परिपूर्ति करता है। ऍरर्स का पता लगाने के लिए रिसीवर यह देखने हेतु जाँच करता है कि पेटर्न परिपूर्ण है या नहीं।



चित्र 4.20 : पोलीनोमिअल अरिथमेटिक

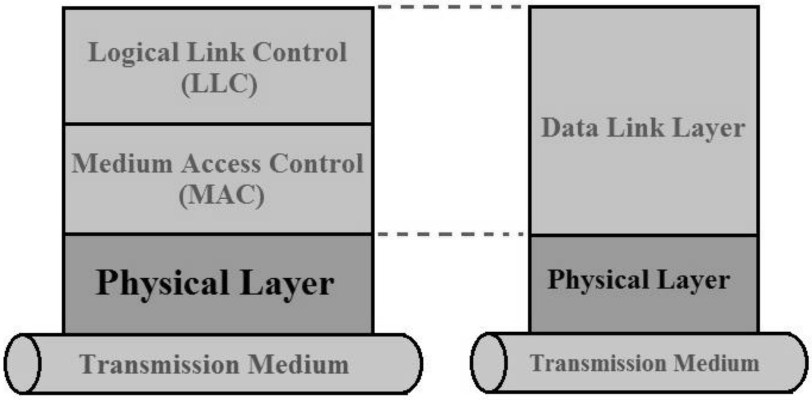
4.4 मीडियम एक्सेस कंट्रोल सबलेयर :

चित्र 4.21 में लेयर्ड मॉडल यह दर्शाता है कि LAN फंक्शन्स को OSI रेफरेंस मॉडल की दो निम्नवर्ती लेयरी के अंतगर्त कैसे रखा जाता है। डाटा लिंक लेयर की दो सबलेयर्स में विभाजित किया जाता है। डाटा लिंक लेयर को दो सबलेयर्स में विभाजित किया जाता है – (1) लॉजिकल लिंक कंट्रोल (LLC) सबलेयर और (2) मीडियम एक्सेस कंट्रोल (MAC) सबलेयर।

1. MAC सबलेयर : MAC सबलेयर शेयर किए जाने वाले फिजिकल मीडियम हेतु एक्सेस के समन्वयन की समस्या से संबन्धित होती है। चित्र 4.21 यह दर्शाता है कि IEEE में IEEE 802.3 (ईथरनेट) तथा IEEE 802.5 (टोकन रिंग) सहित अनेक MAC स्टेंडर्ड्स को डिफाईन किया जाता है। प्रत्येक MAC स्टेंडर्ड में उस फिजिकल लेयर्स से संबद्ध सेट होता है, जिस पर उसे ऑपरेट किया जा सके।

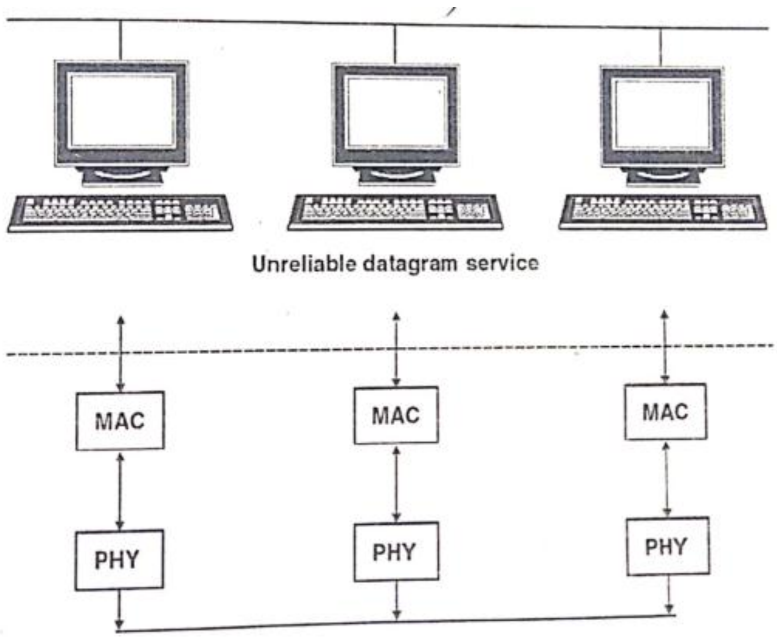
   MAC एंटीटी डाटा के ब्लॉक को LLC सबलेयर से अथवा सीधे ही नेटवर्क लेयर से स्वीकृत करता है।

यह एंटीटी एक ऐसे PDU की रचना करती है, जिसमें सोर्स और डेस्टिनेशन MAC एड्रेस LAN हेतु वर्कस्टेशन्स के भौतिक कनेक्शनों को प्रदर्शित करते है।



चित्र 4.21 : MAC LAN स्टैण्डर्ड

चित्र 4.21 में हमने LAN के माध्यम से परस्पर जुड़े हुए तीन वर्कस्टेशन्स के प्रोटोकॉल स्टेक्स को दर्शाया है। ध्यान दें कि LLC सबलेयर को डाटाग्राम ट्रांसफर सर्विस उपलब्ध कराने के लिए इन तीनों MAC एंटीटीज को किसी को किसी तरह से सहयोग करना पड़ता है। अन्य शब्दों में, MAC एंटीटीज के मध्य इंटरेक्शन एक समान जोड़ियों के मध्य ही नहीं होता है, बल्कि वस्तुतः सभी एंटीटीज को शेयर किए गए मीडियम पर ट्रांसमिट किए जाने वाले समस्त फ्रेम्स को चेक करना पड़ता है।



चित्र 4.21 : MAC अनरेलिएबले डाटाग्राम सर्विस

2. लॉजिकल लिंक कंट्रोल लेयर (LLC) : IEEE 802 समिति ने एक ऐसी लॉजिकल लिंक कंट्रोल (LCC) सबलेयर को भी डिफाईन किया है, जो सभी MAC स्टेंडड्र्स पर कार्य करें। LLC डाटालिंक लेयर पर HDLC की कुछ सेवाएँ प्रदान करने के लिए MAC लेयर द्वारा दी जा रही डाटाग्राम सेवा में वृद्धि कर सकती है

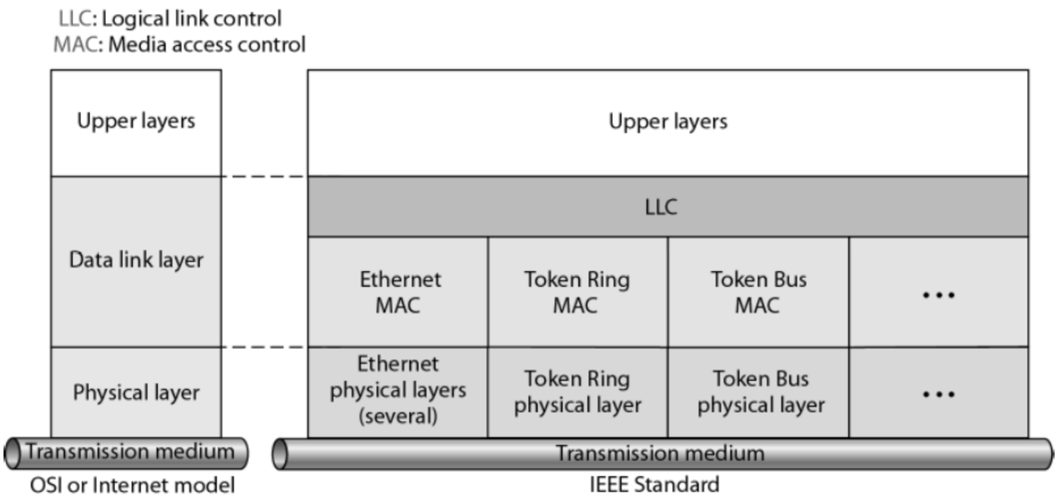
MAC डाटाग्राम सर्विस पर तीन HDLC सर्विसेज प्रदान किए जाने के लिए LCC का निर्माण होता हों।

MAC डाटाग्राम सर्विस पर HDLC सर्विसेज प्रदान किए जाने के लिए LLC का निर्माण होता है।

टाईप 1 LLC सर्विस अनएकनॉलेज्ड कनेक्शनरहित सर्विस है, जो अनुक्रम–रहित इंफॉर्मेशन को ट्रांसफर करने के लिए नंबररहित फ्रेम्स का उपयोग करती है। HDLC प्रोटोकॉल अपने कुछ संदेश विनिमयों में नंबररहित फ्रेम्स का उपयोग करते हैं। LANs में टाईप 1 LLC सर्विस काफी हद तक अत्यंत सर्वसामान्य होती है।

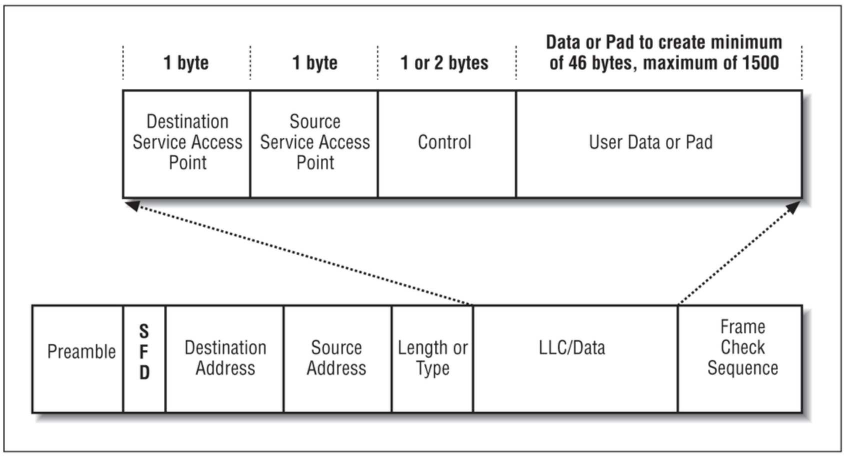
टाईप 2 LLC सर्विस इंर्फोमेशन फ्रेम्स का उपयोग करती है तथा HDLC के सिंक्रोनस बेलेंस्ड मोड के स्वरूप में विश्वसनीय कनेक्शन उन्मुखी सर्विस प्रदान करती है। कनेक्शन द्वारा ऍरर कंट्रोल, सिक्वेसिंग और फ्लों कंट्रोल प्रदान किए

जाने के लिए कनेक्शन सेटअप तथा रिलीज आवश्यक होता है। चित्र 4.22 में विश्वसनीय पैकेट ट्रांसफर सर्विस प्रदान किए जाने के लिए स्टेशन्स A तथा C पर दो टाईप 2 LLC एंटीटीज दर्शाई गई हैं। टाईप 2 ऑपरेशन उस समय उपयोगी होता है, जबकि एण्डसिस्टम विश्वसनीय सर्विस प्रदान करने के लिए ट्रांसपोर्ट लेयर प्रोटोकॉल का उपयोग नहीं कर रहे हों।



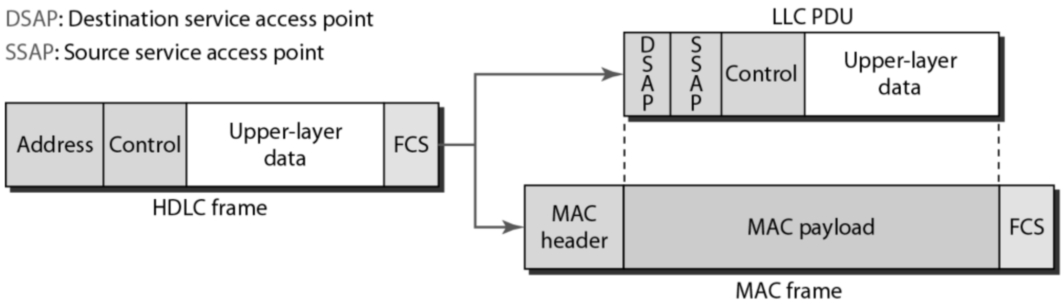
चित्र 4.22 : रिलाएबल पैकेट ट्रांसफर सर्विस

टाईप 3 LLC सर्विस एकनॉलेज्ड कनेक्शनरहित सर्विस अर्थात् एकनॉलेजमेंट्स के साथ प्रत्येक पृथक फ्रेम्स का कनेक्शनरहित ट्रांसफर प्रदान करती है। टाईप 3 LLC सर्विस प्रदान किए जाने के लिए HDLC द्वारा डिफाईन किए गए सेट में दो अतिरिक्त नंबररहित फ्रेम्स को जोड़ दिया जाता हैं।



चित्र 4.23 : LLC PDU स्ट्रक्चर

LLC द्वारा दी जाने वाली अतिरिक्त एड्रेसिंग MAC द्वारा दी गई एड्रेसिंग की पूरक होती है। LAN में कोई वर्कस्टेशन एक सिंगल MAC (भौतिक) एड्रेस रखता है। ऐसा वर्कस्टेशन किसी दिए गए समय पर विभिन्न अपर लेयर प्रोटोकॉल्स से प्रारंभ होने वाले किंतु उससी भौतिक कनेक्शन पर ऑपरेट होने वाले अनेक डाटा विनिमयों को एक साथ संभाल सकता है।



चित्र 4.24 : LLC, PDU, MAC

रेंडम एक्सेस :

रेंडम एक्सेस अथवा कंटेशन विधि सिस्टम्स में वहाँ प्रयुक्त की जाती है, जहाँ यूजर्स की अत्यधिक संख्या को एक ही ब्रॉडकॉस्ट चैनल के माध्यम से अन्य स्टेशन्स को मैसेजेज को एक ही ब्रॉडकॉस्ट चैनल के माध्यम से अन्य स्टेशन्स को मैसेजेज प्रेषित किए जाने वाले की जरूरत होती है। "रेंडम एक्सेस" शब्द का अभिप्राय ऐसे विशिष्ट अथवा पूर्व निर्धारित समय के नहीं होने से होता है, जब कोई स्टेशन विशेष ट्रांसमिट करे।

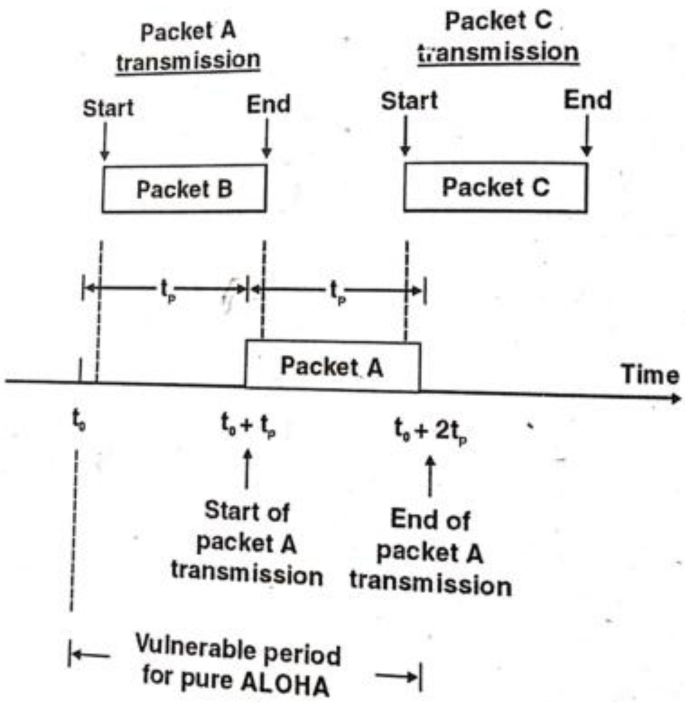
इस क्षेत्र में किए गए प्रारंभिंक कार्य से ALOHA स्कीम उत्पन्न हुई थी जिसमें प्रत्येक अलग–अलग यूजर किसी भी स्वेच्छिक समय पर, प्रेषित किए जाने का मैसेज आते ही डाटा भेज सकते हैं। यदि एक ही समय पर एकाधिक यूजर ट्रांसमिट करने के लिए प्रयारत हों तो मैसेजेज टकरा जाते हैं और उन्हें बाद में पुनः ट्रांसमिट करना पड़ता है। यह यथासंभव सरलतम तकनीक है, क्योंकि यह पूर्णतः एसिंक्रोनस है अर्थात इसमें यूजर्स के मध्य कोई सामंजस्य नहीं होता है।

कार्यकुशलता बढ़ाने के लिए स्लॉटेड ।स्ब्ः। नामक एक स्कीम प्रस्तावित की गई जिसने ।स्ब्ध्द। सिस्टम की क्षमता को दोगुना कर दिया। इसमें चैनल को विभिन्न एक समान टाईम एलॉट्स में विभाजित कर दिया गया। प्रत्येक इंटरवल को एक फ्रेम के ट्रांसमिशन टाईम के बराबर रखा गया। तदुपरांत सभी यूजर्स एक सेंट्रल क्लॉक अथवा अन्य विधियों के द्वारा सिंक्रोनाईज्ड होने लगे जिससे कि ट्रांसमिशन केवल टाईम स्लॉट के प्रारंभ होने पर ही शुरू हो सके।

अलोहा ALOHA :

ALOHA यथासंभव सरलतम ब्रॉडकॉस्ट प्रोटोकॉल है। सामान्यः वास्तविक ALOHA विधि को स्लॉटेड ALOHA स्कीम से पृथक करने के लिए प्योर ALOHA कहा जाता है।

1. प्योर AlOHA : प्योर ALOHA का मूल विचार सरल है, क्योंकि यूजर्स को जब कभी भी डाटा भेजने होते है, तो वह इन्हें तत्काल ट्रांसमिट कर देता है। यह पता लगाने के लिए कि ट्रांसमिशन सफलतापूर्वक हुआ है या नहीं, सेंडर को रिसीवर की ओर से प्राप्त होने वाली एकनॉलेजमेंट के लिए उस अवधि तक प्रतीक्षा करनी पड़ती है, जो दो प्रसारण अवधि $2t_{prop}$के बराबर समयावधि होती है यह वह समय है, जो एक पैकेट द्वारा सेंडर से रिसीवर से सेंडर से रिसीवर तक और पुनः रिसीवर से सेंडर तक यात्रा किए जाने में लगाता है।



चित्र 4.25 : अलोहा पैकेट ट्रांसमिशन

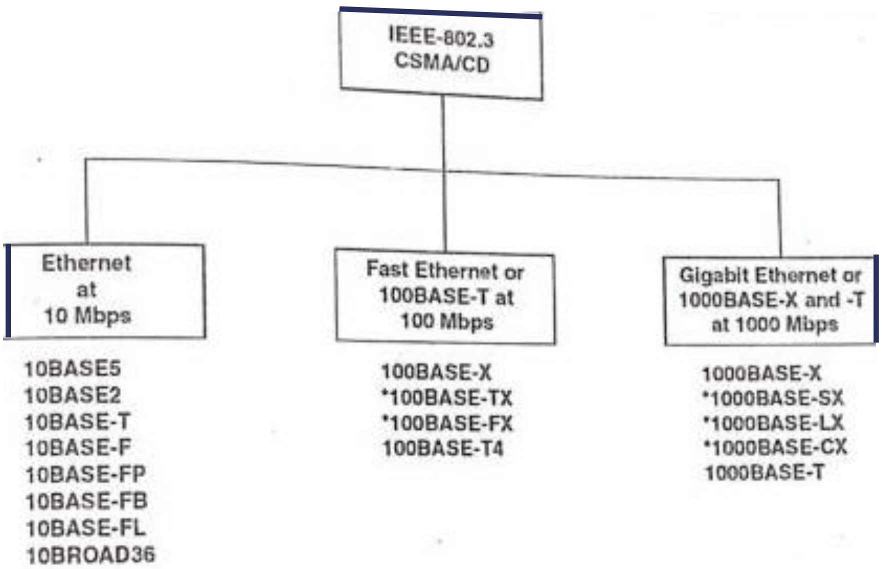
चित्र 4.25 में दर्शाए अनुसार विभिन्न यूजर्स प्रेषित किए गए पैकेट्स के मध्य पैकेट ट्रांसमिशन टाईम t_pके अंतगर्त टकराव हो रहा है। सबसे पहले हम यह मान लेते हैं कि सभी पैकेट्स एक समान लंबाई के हैं और ट्रांसमिशन के लिए प्रत्येक को एक टाईम यूनिट t_p(जिसे स्लॉट कहा जाता है) की आवश्यकता है। ध्यान दे कि यूजर द्वारा पैकेट A को t_0+t_p टाईम पर प्रेषित किए जाने का प्रयास प्रारंभ किया गया है और इसका समापन t_0+2t_p टाईम पर हो रहा है। यदि कोई अन्य यूजर t_0 और $t_0 + t_p$ के मध्य पैकेट B बनाना प्रारंभ करता है, तो पैकेट B का समापन पैकेट A के प्रारंभ से टकरा जाएगा।

5.1 प्रस्तावना :

1970 के प्रारंभ में जेरॉक्स पालो अल्टो शोध केन्द्र (PARC) में शोधकर्ताओं के एक समूह ने ईथरनेट लोकल एरिया नेटवर्क (LAN) पर चिंतन किया। 1980 में विस्तृत विकास के उपरांत डिजिटल इक्विपमेंट कॉर्पोरेशन, इंटेल कॉर्पोरेशन और जेरॉक्स कॉर्पोरेशन (DIX) द्वारा निर्मित एक संगठन ने वास्तविक ईथरनेट स्पेनेसिफिकेशन को सूत्रबद्ध किया। इस DIX ईथरनेट स्टेडर्ड को, जो कोएक्सियल केबल का उपयोग करते हुए 10 Mbps बस आधारित 1982 में कॉबिजन डिटेक्शन के साथ केरियर सेंस मल्टीपल एक्सेस (CSMA/CD) के लिए IEEE स्टेंडर्ड बना। IEEE-802.3 स्टेंडर्ड का मूल उद्देश्य व्यावसायिक और हलके औद्योगिक परिवेशों में उपयोग किया जाना था।

ईथरनेट का परिचय :

IEEE-802.3 स्टेंडर्ड्स कमेटी के परिणाम को चित्र 5.1 में स्पेसिफिकेशन के ऐसे परिवार के रूप में सूचीबद्ध किया गया है, जो गतियों और माध्यम की विविधता से बने हैं। स्टेंडर्ड्स हेतु नामकरण तीन भागों में किए गए है। प्रथम भाग में या तो 10, 100 अथवा 1000 है, जो उस गति (Mbps में) को सूचित करते हैं।



चित्र 5.1 : अलोहा पैकेट ट्रांसमिशन

ईथरनेट की बेसिक अवधारणाएँ :

ईथरनेट नेटवर्क पर सभी उपकरण कॉमन कम्यूनिकेशन मीडियम को टाईम शेयर करते हैं तथा सभी स्टेशन्स इस मीडियम को एक समान प्राथमिकता से एक्सेस करते हैं। इस मीडियम से एकाधिक स्टेशन्स, एक ही समय में डाटा प्राप्त कर सकते है, किंतु एक बार में केवल एक ही स्टेशन को ट्रांसमिट करने की अनुमति मिलती है। इसे पाने के लिए ईथरनेट CSMA/CD प्रोटोकॉल पर आधारित होता है। इस प्रोटोकॉल के साथ जब स्टेशन फ्रेम को ट्रांसमिट करेगा तो वह सर्वप्रथम यह पता लगाने के लिए मीडियम का श्रवण करेगा कि क्या कोई अन्य स्टेशन इस समय उसका उपयोग कर रहा है।

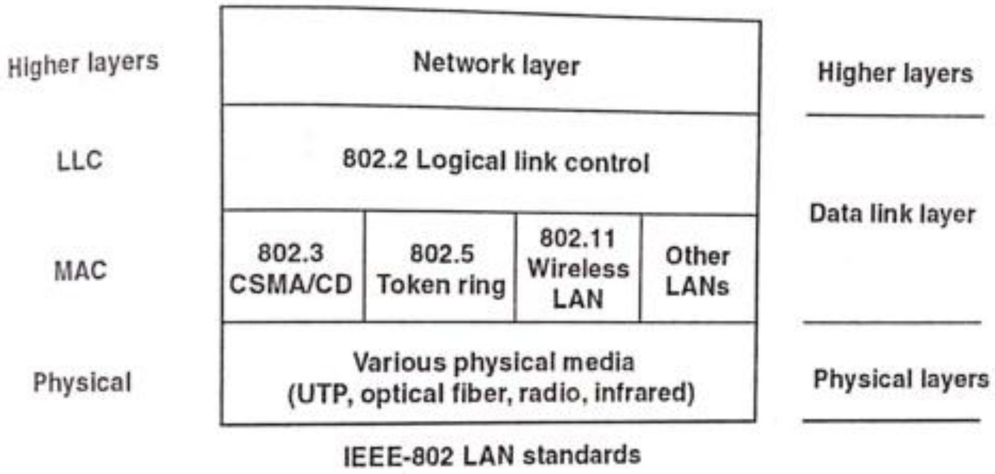
Symbol	Definition
T	Unshielded twisted pair
F	Optical fiber
FP	Optical fiber passive star
FS	Optical fiber backbone
FL	Optical fiber link
X	Two physical links between nodes
TX	Two pairs of STP or Cat-5 UTP
FX	Two optical fibers
T4	Four pairs of Cat-3 UTP
SX	Short wavelength duplex optical fiber link
LX	Long wavelength duplex optical fiber link
CX	One pair of short UTP wire

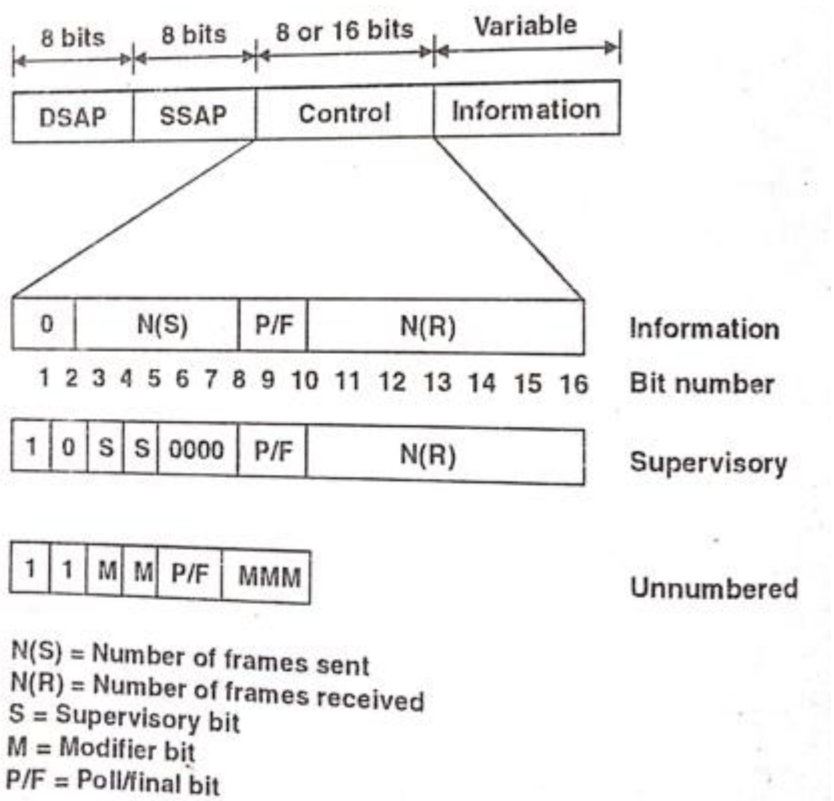
चित्र 5.2 : IEEE सिंबल

लॉजिकल लिंक कंट्रोल (LLC):

लॉजिकल लिंक कंट्रोल (LLC) लेयर IEEE-802 डाटा लिंक लेयर का ऊपरी भाग होती है तथा यह सभी LAN प्रोटोकॉल्स में एक समान होती है। (चित्र 5.3 देखें) यह लेयर मीडियम एक्सेस कंट्रोल (MAC) लेयर के ऊपर विद्यमान होती है। MAC नियंत्रित लिंक के आरपार अथवा MAC लेवल ब्रिजेस द्वारा जुड़े हुए LANs की श्रृंखला के सहायता देने के लिए एड्रेसिंग तथा कंट्रोल विधियाँ उपलब्ध कराना इसका मुख्य कार्य है।

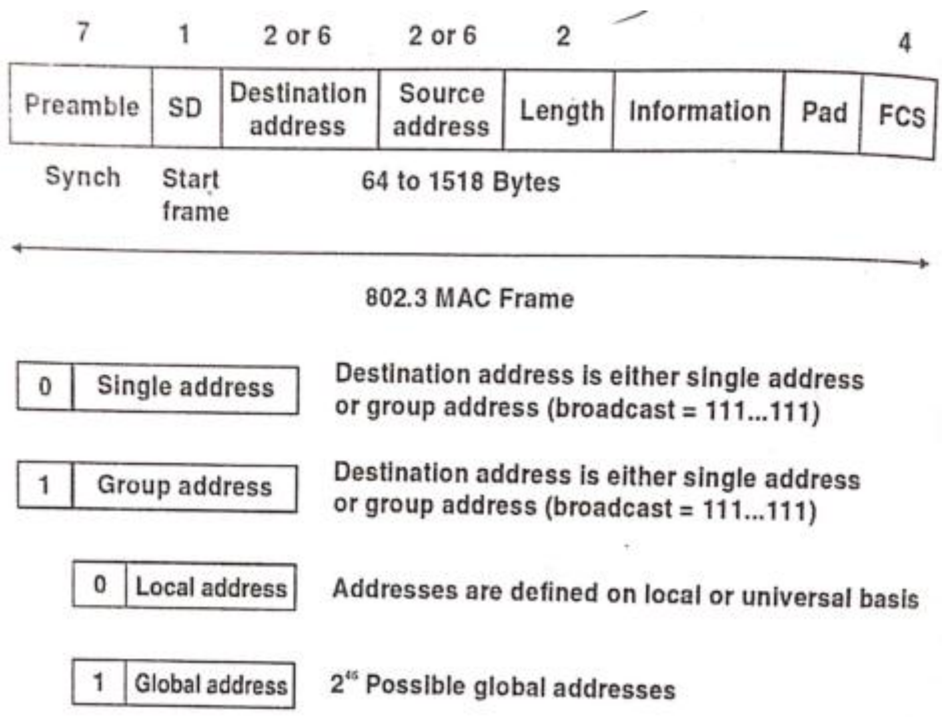
LLC प्रोटोकॉल हाई लेवल डाटा लिंक कंट्रोल (HDLC) प्रोटोकॉल पर आधारित है। यह साधारण उद्देश्य वाला वाला एक ऐसा प्रोटोकॉल है, जो OSI (ओपन सिस्टम इंटरकनेक्शन) रेफरेंस मॉडल की डाटा लिंक लेयर पर कार्य करता है। IEEE-802.3 स्टेडर्ड में LLC बिना एकनॉलेज के कनेक्शन रहित सेवा का उपयोग करता है और फ्रेम डिलीवरी के बेस्ट एफर्ट मोड पर निर्भर रहता है।





चित्र 5.3 : LLC फॉर्मेट डाटा यूनिट

चित्र 5.4 IEEE-802.3 के लिए MAC फ्रेम स्ट्रक्चर प्रदर्शित करता है। फ्रेम एक ऐसे सात अष्टपदीय (ऑक्टेल) प्रॉक्कथन के साथ प्रारंभ होती है, जो 10101010 अष्टपद को दोहराए। यह पेटर्न एक ऐसी स्क्वायर वेब को उत्पन्न करता है, जो रिसीवर्स को फ्रेम की शुरूआत के लिए सिंक्रोनाईज के उपरांत आता है, जो 10101011 पेटर्न से निर्मित होता है। डिलीमीटर में आने वाले दो लगातार 1st फ्रेम के प्रारंभ को स्पष्ट करते है।



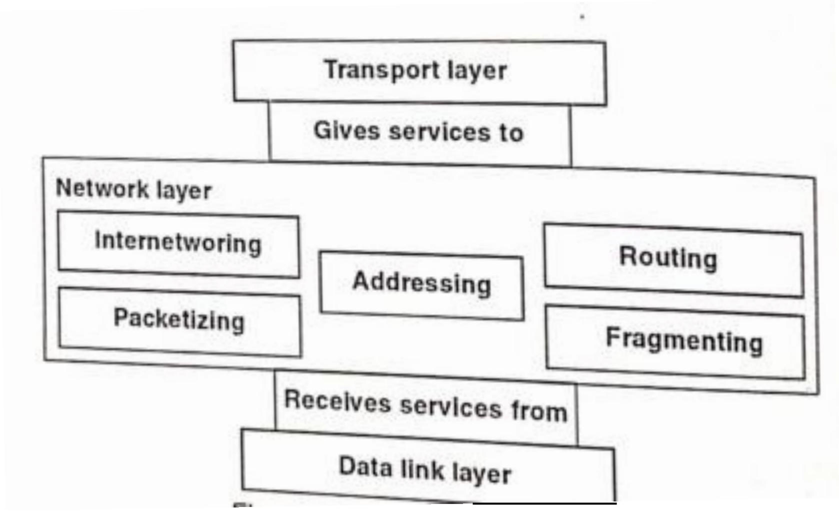
चित्र 5.4 : MAC फ्रेम स्ट्रक्चर

इसके बाद डेस्टिनेशन और सोर्स एड्रेस फील्ड्स जाती है। एड्रेस फील्ड्स छः बाईट्स लंबी होती है। डेस्टिनेशन एड्रेस की प्रथम बिट उन एकल एड्रेसेस और समूह एड्रेसेस के मध्य अंतर करती है, जो यूजर्स के समूह के लिए फ्रेम को मल्टीकॉस्ट करने हेतु प्रयुक्त किए जाते है। अगली बिट यह स्पष्ट करती है कि वह एड्रेस लोकल एड्रेस है अथवा ग्लोबल एड्रेस है। इस प्रकार छः बाईट वाले एड्रेसेस के प्रकरण में स्टेंडर्ड हमें 2^{46} ग्लोबल एड्रेसेस प्रदान करता है। प्रथम तीन बाईट्स NIC विक्रेता को प्रदर्शित करती है। इसलिए यह विधि 2^{24}= 16,777,215 एड्रेसेस प्रति विक्रेता तक की अनुमति देती है।

नेटवर्क लेयर कार्यप्रणालीः

नेटवर्क लेयर मुख्यतः किसी पैकेट को एक से दूसरे कम्प्यूटर तक स्थानांतरित करने के लिए प्रयुक्त की जाती है। यह होस्ट–टू–होस्ट डिलेवरी के लिए उत्तरदायी होती है।

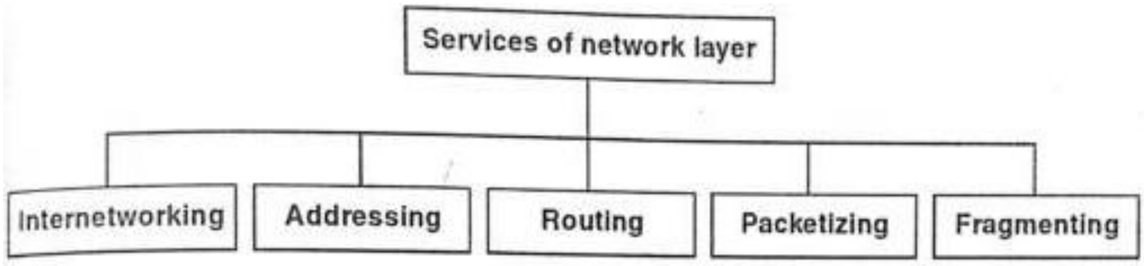
चित्र 5.5 में 5–लेयर इंटरनेट मॉडल में नेटवर्क लेयर की स्थिति को दर्शाया गया है। इस मॉडल में नेटवर्क लेयर तीसरी लेयर है। यह डाटा लिंक लेयर से सेवाएं स्वीकार करती है और ट्रांपसपोर्ट लेयर को सेवाएँ प्रदान करती है। डाटा लिंक लेयर से प्राप्त की जाने वाली मुख्य सेवा डाटा की नोड–टू–नोड डिलेवरी करना है।



चित्र 5.5 : नेटवर्क लेयर

नेटवर्क लेयर द्वारा प्रदान की जाने वाली सेवाएँः–

चित्र 5.6 में दर्शाए अनुसार नेटवर्क लेयर में सेवाओं का एक सुपरिभाषित सेट होता है।



चित्र 5.6 : नेटवर्क लेयर की सुविधाएँ

1. **इंटरनेटवर्किंग :** नेटवर्क लेयर की मुख्य सेवा अपर ट्रांसपोर्ट एवं एप्लीकेशन लेयर्स के लिए अलग–अलग फिजिकल नेटवर्क्स को एक सिंगल नेटवर्क जैसा स्वरूप देने हेतु परस्पर लॉजिकल सशक्तता और इंटरनेटवर्किंग प्रदान करता है।
2. **एड्रेसिंग :** नेटवर्क लेयर पर हमें सभी डिवाईसेस के मध्य ग्लोबल कम्यूनिकेशन की अनुमति प्रदान करने के लिए इंटरनेट पर प्रत्येक डिवाईस हेतु विशिष्ट पहचान की जरूरत होती है। यह टेलीफोन प्रणाली के समरूप ही है, जिसमें प्रत्येक टेलीफोन उपभोक्ता को एक विशिष्ट टेलीफोन नंबर दिया जाता है।

   नेटवर्क लेयर में प्रयुक्त किए जाने वाले एड्रेसेस विशिष्ट और होस्ट (कम्प्यूटर) अथवा इंटरनेट के राउटर के कनेक्शन को सार्वत्रिक रूप से परिभाषित करने वाले होने चाहिए।

3. राउटिंग : जब कभी भी किसी डेस्टिनेशन के लिए एकाधिक रूट्र्स होते हैं, तो हमें निर्णय लेना पड़ता है और किसी एक रूट का चयन करना पड़ता है। हमारा निर्णय सामान्यतः कुछ ऐसे मापदण्डों पर आधारित होता है, जो हमारे लिए महत्वपूर्ण होते हैं। यदि समय महत्वपूर्ण है, तो हम छोटे रूट का चयन कर सकते है। नेटवर्क मार्गो का एक ऐसा संयोजन भी होता है, जिसके माध्यम से प्च पैकेट्स अपने गंतव्यों तक पहुंचते है।

4. आमतौर पर प्रत्येक IP पैकेट विभिन्न रूट्र्स के माध्यम से ही अपने गंतव्य पर पहुँच सकता है। अंतर यह है कि पैकेट रूट का चयन नहीं कर सकता है, और जिस रूट का निर्णय लिया गया है उसके LANs और WANs को राउटर्स जोड़ देते हैं।
5. पैकेटाईजिंग : अपल लेयर प्रोटोकॉल्स से प्राप्त होने वाले पैकेट्स को एकत्र करके नेटवर्क लेयर उनके नए पैकेट्स बना देती है। IP (इंटरनेटवर्किंग प्रोटोकॉल) कहलाने वाले नेटवर्क लेयर प्रोटोकॉल द्वारा पैकेटाईजिंग सम्पन्न की जाती है।
6. फ्रेगमेंटिंग : विभिन्न नेटवर्क्स के माध्यम से डाटाग्राम यात्रा कर सकता है। प्रत्येक राउटर प्राप्त की गई फ्रेम से IP डाटाग्राम को डीकेप्स्यूलेट (विखंडित) करता है, उसे प्रोसेस करता है और फिर उसे अन्य फ्रेम में एनकेप्स्यूलेट (संयोजित) कर देता है।

कुछ महत्वपूर्ण शब्दावलियाँ :

1. **मल्टीकॉस्टिंग :** आज नेटवर्क में मल्टीकॉस्टिंग अर्थात् एक होस्ट से विभिन्न डेस्टिनेशन्स को डाटा की डिलेवरी करना एक महत्वपूर्ण कार्य है। मल्टीमीडिया की वजह से मल्टीकॉस्टिंग का नेटवर्क में अत्यंत महत्वपूर्ण स्थान बन गया है। ऑडियो और वीडियो के स्वरूप में मल्टीमीडिया को ऐसे अनेक गंतव्यों तक पहुंचने के लिए मल्टीकॉस्टिंग राउटर्स की जरूरत होती है, जो गंतव्य किसी समूह से संबंधित होते है।
2. **राउटिंग प्रोटोकॉल्स :** राउटिंग प्रोटोकॉल्स को डायनेमिक राउटिंग टेबल्स हेतु आवश्यकता के प्रतिक्रिया स्वरूप निर्मित किया गया है। राउटिंग प्रोटोकॉल नियमों और कार्य–प्रणालियों का एक ऐसा सेट होता है, जो किसी नेटवर्क में राउटर्स को एक–दूसरे के परिवर्तनों के बारे में सूचित करने की अनुमति देता है। यह राउटर्स को वह सब कुछ शेयर करने की अनुमति प्रदान करता है, जो वे नेटवर्क अथवा अपने आसपास के बारे में जानते हैं। इंफॉर्मेशन को शेयर किए जाने से, इंदौर में राउटर दिल्ली के नेटवर्क में आई विफलता के बारे में जान सकता है। राउटिंग प्रोटोकॉल्स में अन्य राउटर्स से प्राप्त होने वाली इंफॉर्मेशन को जोड़ने हेतु कार्य–प्रणालियों पर भी विचार किया जाता है।

3. **सपोर्टिंग प्रोटोकॉल्स :** IP जैसे किसी इंटरनेटवर्किंग प्रोटोकॉल को होस्ट–टू–होस्ट डिलेवरी उपलब्ध कराने में सहायता के लिए अन्य प्रोटोकॉल के समर्थन की आवश्यकता होती है। यह प्रोटोकॉल इंटरनेट कंट्रोल मैसेज प्रोटोकॉल (ICMP) कहलाता है।

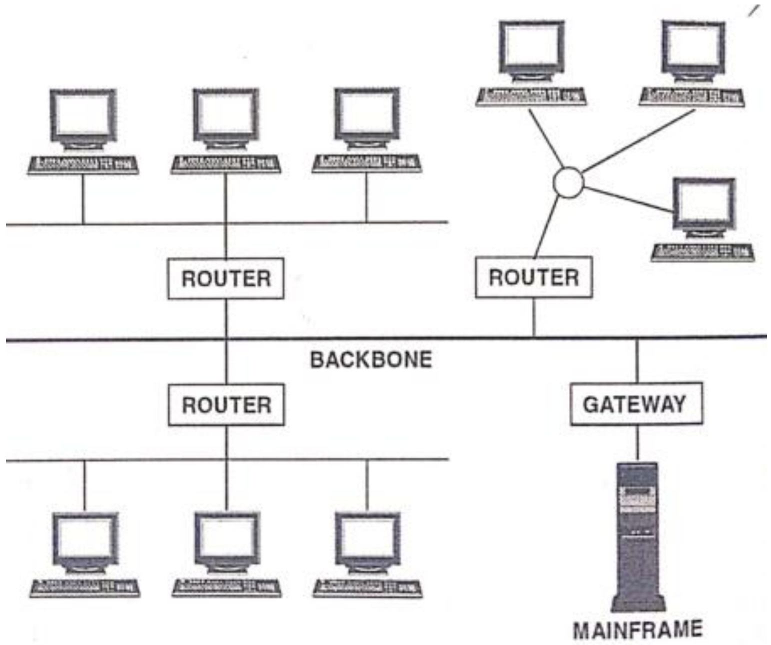
प्रस्तावनाः–LANs का निर्माण वैसे तो कम्प्यूटर्स और केबल्स से होता है, किंतु जैसे–जैसे टेक्नालॉजी विकसित होती जा रही है, अधिकाधिक उपकरणों की आवश्यकता होने लगी है। लंबी दूरियों को कवर करने के लिए आरंभिक कोएक्सियल केबल नेटवर्क्स में जब वृद्धि हुई तो सिग्नल्स को अधिक शक्ति प्रदान करने के लिए रिपीटर्स नामक डिवाईसेस को जोड़ा गया। आगे चल कर जब ईथरनेट नेटवर्क्स हेतु कोएक्सियल के स्थान पर अनावरित ट्विस्टेड पेयर (UTP) केबल प्रभावी माध्यम के रूप में कार्य करने लगे तो हब्स एक महत्वपूर्ण नेटवर्क घटक बन गए। जैसे ही नेटवर्क्स स्थानीय वर्कग्रुप्स के लिए एक उपकरण से बढ़कर कंपनी व्यापी संसाधनों के रूप में कार्य करने लगे तो वृहद नेटवर्क्स की रचना के क्रम में ब्रिजेस, स्विचेज और राउटर्स जैसे घटकों को निर्मित किया गया। इन डिवाईसेस के उपयोग से ऐसे नेटवर्क्स की रचना संभव हो पाई, जो अधिक लंबी दूरियों को कवर करें, अधिकतम कम्प्यूटर्स की मदद करें और नेटवर्क पर प्रत्येक सिस्टम के लिए बढ़ा हुआ बैंडविड्थ प्रदान करें।

होस्टः

होस्ट शब्द का अर्थ वह कम्प्यूटर है, जो यूजर को नेटवर्क पर अन्य होस्ट कम्प्यूटर्स के साथ कम्यूनिकेट करने की अनुमति देता है। व्यक्तिगत यूजर्स इलेक्ट्रॉनिक मेल, टेलनेट और थ्ज्च जैसे एप्लीकेशन प्रोग्राम का उपयोग करते हुए कम्यूनिकेट करते है। FTP को फाईल ट्रांसफर प्रोटोकॉल के लिए प्रयुक्त किया जाता है।

बैकबोन नेटवर्क :

नेटवर्क्स के समूह के साथ निरंतरता और कम्यूनिकेशन्स की समस्याएँ होती है। इसलिए इन सभी कम्यूनिकेशन्स लिंक्स को एक साथ जोड़ने के लिए एक उपाय की जरूरत होती है। इसका समाधान संपूर्ण संगठन के भीतर चलने वाला ब्रॉडबैंड अथवा फाईबर ऑप्टिक बैकबोन है। लोकल नेटवर्क्स के समूह और वाईड एरिया नेटवर्क्स की तदुपरांत इस बैकबोन में जोड़ दिया जाता है।



चित्र 5.7 : बैकबोन

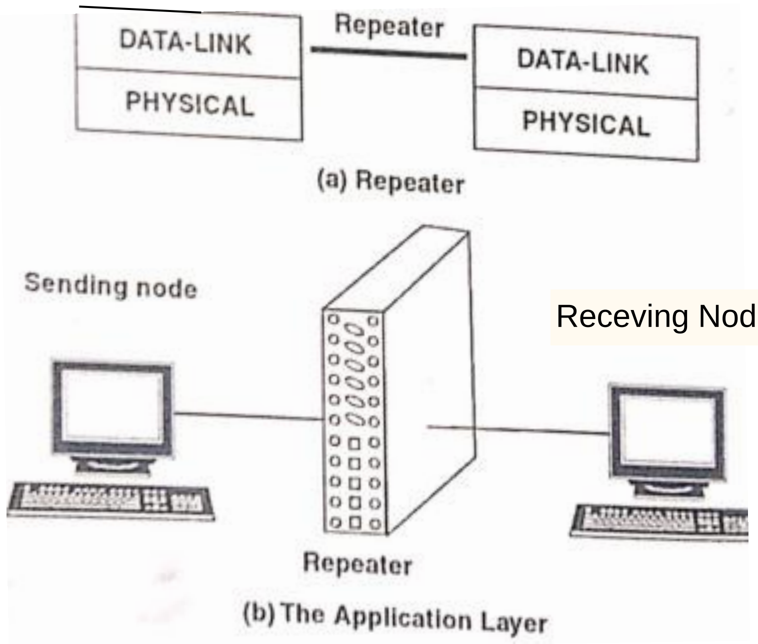
5.1.1 नेटवर्क लेयर की कनेक्शन डिवाइसेस :

एक नेटवर्क को दूसरे नेटवर्क से जोड़ने के लिए तथा ट्रांसमिशन की क्षमता बढ़ाने के लिए विभिन्न कनेक्टींग डिवाइसेस का उपयोग किया जाता है, जो निम्नानुसार है–

1. रिपीटर :

सभी ट्रांसमिशन माध्यम उनके द्वारा यात्रा करने वाली इलेक्ट्रो मेग्नेटिक वेव्स को क्षीण (कमजोर) कर देते है। इस प्रकार की क्षीणता की वजह से किसी भी माध्यम द्वारा ले जाए जा सकने वाले डाटा की दूरी सीमित हो जाती है। एक ऐसी डिवाईस जोड़ कर जो सिग्नल्स को एम्पलीफाई करे, उन्हें आगे बढ़ाने के लिए तैयार किया जा सकता है और

नेटवर्क के आकार में वृद्धि की जा सकती है। इस रीरि से जो डिवाईसेस सिग्नल्स को एम्प्लीफाई करती हैं, वे रिपीटर्स कहलाती हैं। सिग्नल्स को एम्प्लफाई करती है, वे रीपीटर्स कहलाती हैं। रिपीटर्स को एम्प्लीफॉयर्स और सिग्नल रीजनरेटिंग डिवाईसेस नामक दो श्रेणियों में वर्गीकृत किया जाता है। एम्पलीफॉयर्स संपूर्ण इनकमिंग सिग्नल्स और नॉईल दोनों को एम्प्लीफाई कर देते है। सिग्नल रीजनरेटिंग रिपीटर्स, इनकमिंग डाटा की यथार्थ प्रतिलिपि निर्मित करते हैं, उना पुननिर्माण करते है और केवल वांछित इंफॉर्मेशन को ही आगे बढ़ाते हैं।

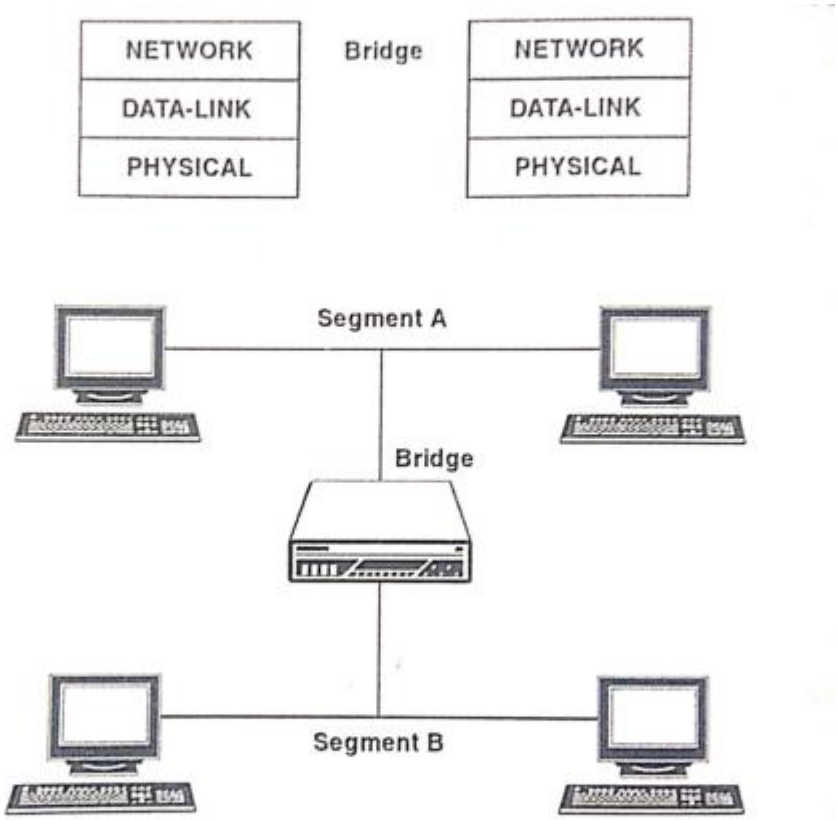


चित्र 5.8 : **एप्लीकेशन लेयर**

2. ब्रिज :

ब्रिज बुनियादी तौर पर दो ऐसे एक–समान नेटवर्क्स को जोड़ता है, जिनके नीचले स्तर पर कुछ भिन्न भौतिक तत्व होते हैं (चित्र 5.9 देखें)। उदाहरण के लिए ब्रिज लेयर–3 (नेटवर्क लेयर) पर भिन्न नीचली लेयर्स के साथ दो नेटवर्क्स को जोड़ सकता है, लेयर 3 के ऊपर सब कुछ समान होना चाहिए। वर्तमान में उपयोग किए जा रहे ब्रिज का एक श्रेष्ठ उदाहरण ब्रॉडबैंड टोकन नेटवर्क और बेसबैंड टोकन नेटवर्क के मध्य मिलता है। हार्डवेयर सिस्टम के अतिरिक्त उन पर सब कुछ एक समान होता है।

ब्रिज का उपयोग नेटवर्क को संभावित अधिकतम आकार तक बढ़ाता है। रिपीटर, जिसमें प्राप्त किए गए सभी सिग्नल्स को केवल आगे बढ़ाया भर जाता है, के विपरीत ब्रिज ऐसे उपयुक्त सेगमेंट का चयनात्मक रूप से पता लगाता है,



चित्र 5.9 : ब्रिज कनेक्शन

(a)ब्रिज A और B दोनों की सेगमेंट से सभी सिग्नल्स प्राप्त करता है (चित्र 5.9 देखें)।

(b) ब्रिज एड्रेसेस पढ़ता है और सेगमेंट A से आने वाले उन सभी सिग्नल्स की उपेक्षा (फिल्टर्स) कर देता है, जो सेगमेंट A के लिए एड्रेस किए गए है, क्योंकि उन्हें ब्रिज को पार करने की जरूरत नहीं होती है।

(c) सेगमेंट A से आने वाले उन सिग्नल्स को जो सेगमेंट B के कम्प्यूटर्स हेतु एड्रेस किए गए हैं, सेगमेंट B के लिए रीट्रांसमिट कर दिया जाता है।

(d) सेगमेंट B की ओर से आने वाले सिग्नल्स को भी इसी प्रकार से प्रोसेस किया जाता है।

3. हब्स :

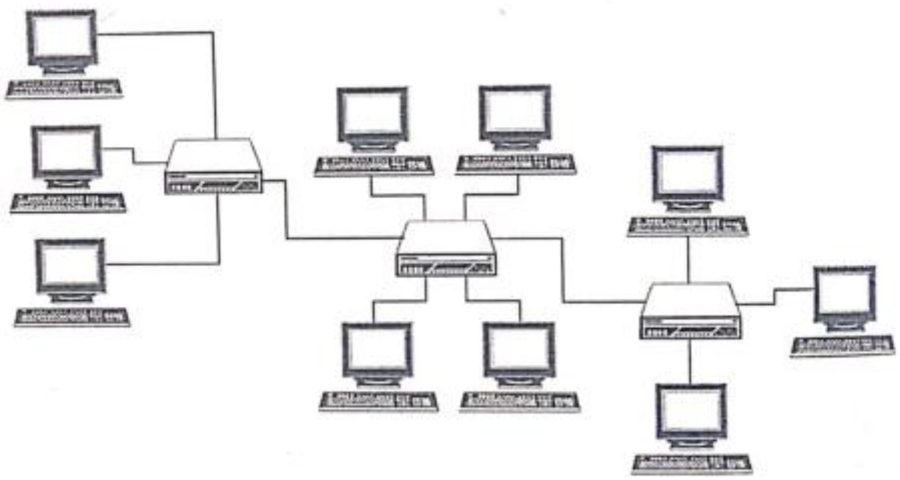
यह डिवाईस नेटवर्क के लिए ऐसे केबलिंग नेक्सस (गठबंधन) के रूप में कार्य करती है, जो स्टॉर टोपोलॉजी का उपयोग करता है। प्रत्येक कम्प्यूटर का उसका अपना केबल होता है, जो उसे केंद्रीय हब से जोड़ता है। हब का दायित्व यह देखना है कि उसके पोर्ट्स में से किसी एक पर आने वाला ट्रैफिक अन्य पोर्ट्स के माध्यम से आगे बढ़ जाए। नेटवर्क मीडियम के आधार पर हब इलेक्ट्रिकल सर्किटरी, ऑप्टिकल कम्पोनेट्स या फिर अन्य टेक्नॉलाजी का उपयोग इनकमिंग सिग्नल को आऊटगोइंग पोर्ट्स पर भेजने के लिए कर सकता है। फाईबर ऑप्टिक हब वस्तुतः प्रकाशीय स्पंदनों को विभाजित करने के लिए मिरर्स का उपयोग करता है।

हब या कन्सेन्टेटर शब्द मूलतः ईथरनेट नेटवर्क्स के संदर्भ में प्रयुक्त किया जाता है तथा टोकन रिंग नेटवर्क पर इसकी समरूप डिवाईस मल्टीस्टेशन एक्सेस यूनिट ;ड।न्द्ध कहलाती है।

हब को तीन प्रकार से वर्गीकृत किया जाता है–

(i) पेसिव हब : हब ऐसे केबल कनेक्शन्स प्रदान करता है, जो किसी पोर्ट के माध्यम से डिवाईस में इनपुट किए गए सभी सिग्नल्स को अन्य सभी पोर्ट्स पर प्रेषित करता है। यह पेसिव हब के रूप में जाना जाता है, क्योंकि यह केवल फिजिकल लेयर पर ही कार्य करता है,

(ii) रिपीटिंग (एक्टिव) हब्स : आज के ईथरनेट नेटवर्क्स पर प्रयुक्त होने वाले हब्स उनके पोर्ट्स में से किसी के माध्यम से उन्हें प्राप्त होने वाले सिग्नल्स को उसी समय डिवाईस में अन्य सभी पोर्ट्स के माध्यम से ट्रांसफर भी करते जाते हैं। ईथरनेट हब्स इनकमिंग सिग्नल्स को अन्य पोर्ट्स पर ट्रांसफर करने के साथ ही साथ उन्हें एम्पलीफाई करते हुए रिपीटिंग फंक्शनलिटी भी प्रदान करते हैं। वस्तुतः यदाकदा ईथरनेट हब्स को मल्टीपोर्ट रिपीटर्स के रूप में भी जाना जाता है। पेसिव हब के विपरीत रिपीटिंग (अथवा एक्टिव) हब को सिग्नल को बेहतर बनाने के लिए पॉवर सोर्स की जरूरत होती है।

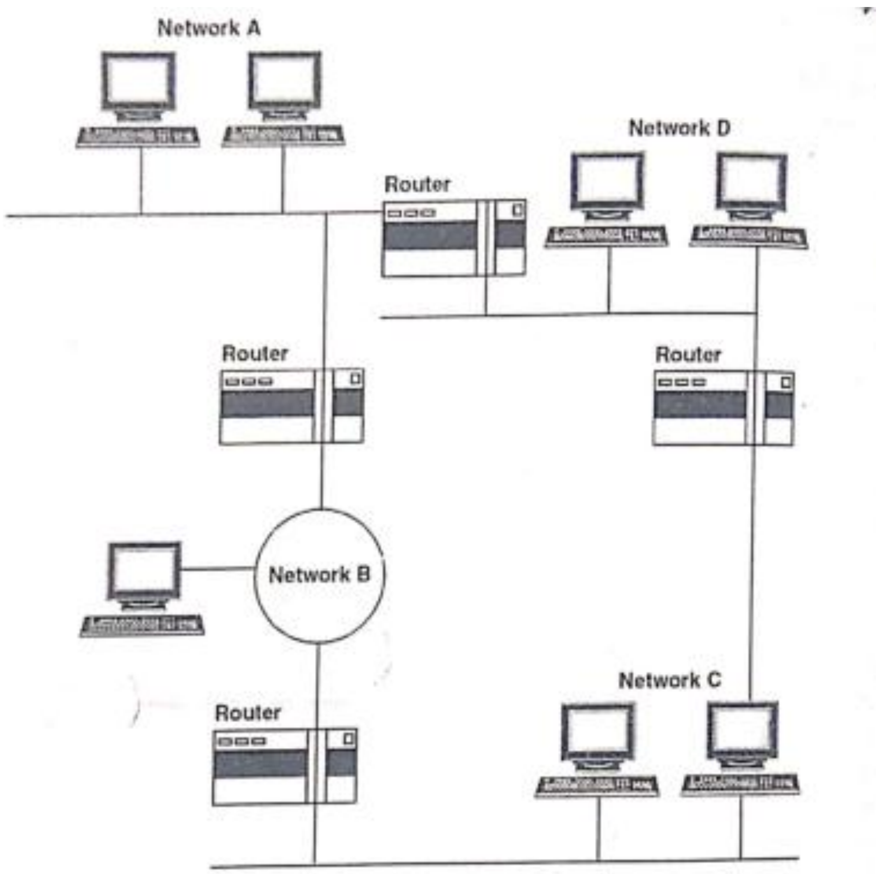


चित्र 5.10 : हब नेटवर्क

4. राउटर्स :

राउटर्स व डिवाईसेस होती है, जो दो या अधिक नेटवर्क्स को जोड़ती हैं। ये हार्डवेयर और सॉफ्टवेयर के संयोजन से बनते हैं। एक पृथक कम्प्यूटर, नेटवर्क सर्वर हार्डवेयर हो सकते हैं। हार्डवेयर में इंटरनेटवर्क के विभिन्न नेटवर्क्स हेतु फिजिकल इंटरफेसेज को शामिल किया जाता है। ऑपरेटिंग सिस्टम तथा राउटिंग प्रोटोकॉल किसी राउटर में सॉफ्टवेयर के दो मुख्य भाग होते है।

लॉजिकली तौर पर पृथक दो या अधिक नेटवर्क्स को जोड़ने के लिए राउटर्स लॉजिकल और फिजिकल एड्रेसिंग का उपयोग करते हैं। वे वृहद नेटवर्क को लॉजिकल नेटवर्क सेगमेंट्स में व्यवस्थित करते हुए यह कनेक्शन स्थापित करते है।



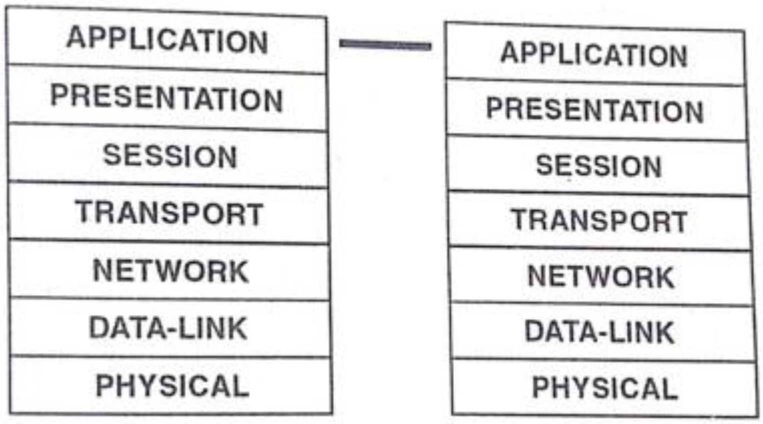
चित्र 5.11 : राऊटर नेटवर्क

5. ब्राउटर :

ब्राउटर वह राउटर है, जो ब्रीज भी हो सकता है। ब्राउटर सर्वप्रथम नेटवर्क प्रोटोकॉल इंफॉर्मेशन पर आधारित पैकेट को डिलीवर करने का अवसर देता है। यदि ब्राउटर पैकेट द्वारा उपयोग में लाए जा रहे प्रोटोकॉल की सहायता नहीं कर पाता है अथवा प्रोटोकॉल इंफॉर्मेशन पर आधारित पैकेट को डिलीवर नहीं कर सकता है, तो वह फिजिकल एड्रेस का उपयोग करते हुए उसे ब्रीज कर देता है। यदि किसी पैकेट में सही लॉजिकल एड्रेस नहीं होता है, तो एक वास्तविक राउटर उस पैकेट की उपेक्षा भर कर देगा। राउटर और ब्रीज दोनों होने की वजह से ब्राउटर अधिक उपयुक्त विकल्प हो सकता है।

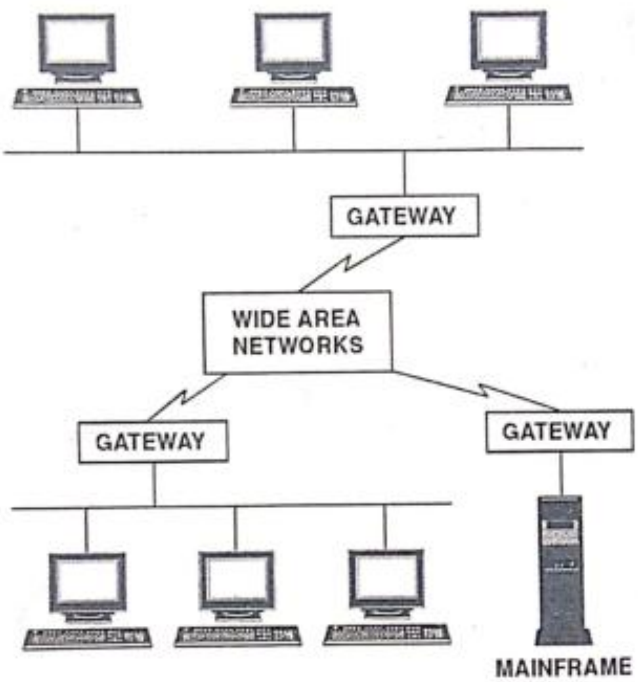
6. गेटवे :

पूर्णतः असमान नेटवर्क्स को जोड़ने के लिए गेटवे नामक डिवाईस प्रयुक्त की जाती है। OSI मॉडल की सभी सातों लेयर्स के लि गेटवेज, प्रोटोकॉल्स का रूपांतरण सम्पन्न करते है।



चित्र 5.12 : अलोहा पैकेट ट्रांसमिशन

LAN और SNA मेनफ्रेम कम्प्यूटर को कनेक्ट करना, प्रोटोकॉल्स को बदलना तथ दो पूर्णतः भिन्न सिस्टम्स के मध्य, पैकेट्स को ट्रांसमिट करना, गेटवे के सर्वसामान्य उपयोग है।

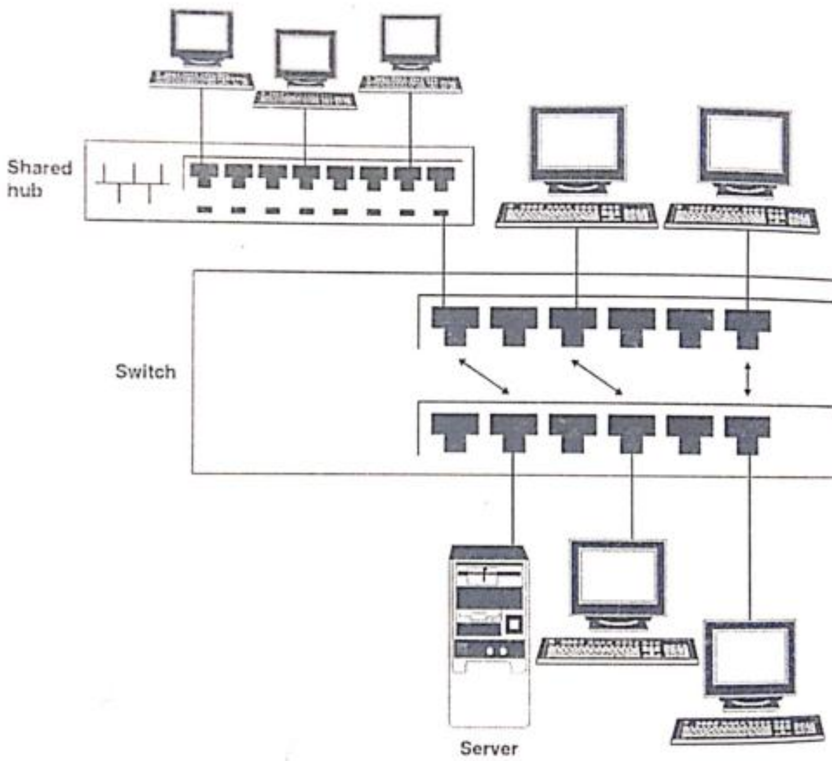


चित्र 5.13 : गेटवे फक्शन

7. स्विचेस :

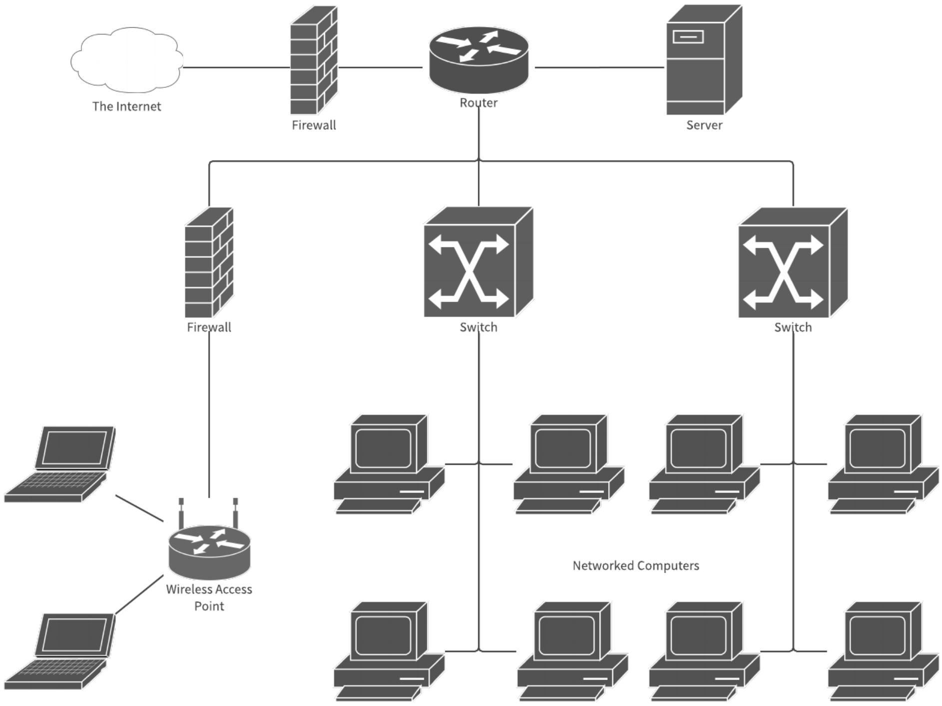
पारंपरिक इंटरनेटवर्क सरंचना ए ऐसे नेटवर्क की रचना करने के लिए राउटर्स द्वारा जुड़े हुए एकाधिक LAN का उपयोग करती है, जो कि एक सिंगल LAN से संभव नेटवर्क की तुलना में अधिक विशाल हो। राउटर्स प्रत्येक LANs पर ट्रेफिक के अलग–अलग समूह बना देते हैं और केवल उन्हीं पैकेट्स को आगे बढ़ाया जाता है, जो अन्य LANs के सिस्टम्स को एड्रेस किए गए होते है।

राउटर्स तो कई दशकों से विद्यमान हैं, किंतु LAN स्विच कहलाने वाली डिवाईस के नवीनतम प्रकार में क्रांतिकारी नेटवर्क डिजाईन होती है तथा इसने लगभग असीमित आकार वाले LANs का निर्माण किया जाना संभव कर दिया है। स्विच मुख्यतः एक ऐसी मल्टीपोर्ट ब्रीजिंग डिवाईस है, जिसमें प्रत्येक पोर्ट एक पृथक नेटवर्क सेगमेंट होता है। यह दिखने में हब जैसा ही होता है। स्विच अपने पोर्ट्स के माध्यम में इनकमिंग ट्रेफिक ग्रहण करता है।



चित्र 5.14 : स्विच के साथ कंप्यूटर नेटवर्क

स्विचेज OSI रेफरेंस मॉडल की लेयर 2, डाटा लिंक लेयर पर कार्य करते है, अतः इसके परिणामस्वरूप ये राउटर्स द्वारा जुड़ी हुई छोटे नेटवर्क्स की श्रृंखला के स्थान पर एक अकेला विशाल नेटवर्क बनाने के लिए प्रयुक्त किए जाते है। इसका अर्थ यह भी है कि स्विचेज किसी भी नेटवर्क लेयर प्रोटोकॉल की सहायता कर सकते है। ट्रांसपेरेंट ब्रिजेस की ही भांति स्विचेज भी नेटवर्क की टॉपोलॉजी को समझ सकते हैं और फॉरवर्डिंग व पैकेट फिल्टरिंग जैसे कार्यों को सम्पन्न करते हैं।



चित्र 5.15 : वाइड स्विच के साथ कंप्यूटर नेटवर्क

स्विच के प्रकार :

स्विचिंग दो मूलभूत प्रकार की होती है–

(i)कट–थ्रू

(ii)स्टोर एण्ड फॉरवर्ड।

(i) कटू–थ्रू स्विच किसी इनकमिंग पैकेट के केवल MAC एड्रेस को ही उसकी फॉरवर्डिंग टेबल के एड्रेस से तुलना करने के लिए पढ़ता है और डिस्टेनेशन के लिए उपलब्ध कराए गए एक्सेस पर पोर्ट के माध्यम से तत्काल ही उसे ट्रांसमिट करना प्रारंभ कर देता है।

ऍरर चेकिंग जैसी कोई अतिरिक्त प्रोसेसिंग किए बिना और संपूर्ण पैकेट प्राप्त होने के पूर्व ही स्विच, पैकेट को फॉरवर्ड कर देता है। इस प्रकार के स्विच सस्ते होते है और वर्कग्रुप अथवा डिपार्टमेंट लेवल पर सर्वाधिक साधारण तौर पर प्रयुक्त किए जाते हैं,

(ii) स्टोर एण्ड फॉरवर्ड स्विच अपने नाम के अनुरूप ही संपूर्ण इनकमिंग पैकेट को डेस्टिनेशन पोर्ट पर फॉरवर्ड किए जाने के पूर्व बफर मेमोरी में संग्रहीत कर लेता है। मेमोरी में स्विच द्वारा पैकेट की ब्ब् ऍरर्स और runts, gaints और jabber जैसी कंडीशन्स के लिए जाँच की जाती है। ऍरर होने पर किसी भी पैकेट को स्विच तत्काल ही उपेक्षित कर देता है और जो पैकेट्स बिना ऍरर्स वाले होते है, उन्हें सही पोर्ट के माध्यम से फॉरवर्ड कर दिया जाता है।

5.2 नेटवर्क लेयर प्रोटोकॉल

प्रस्तावनाः

TCP/IP मॉडल में नेटवर्क लेयर सर्वाधिक महत्वपूर्ण लेयर होती है क्योंकि यहीं वह स्थान होता है जहाँ पर अनेक फिजिकल नेटवर्क्स के आरपार सोर्स से डेस्टिनेशन होस्ट तक डाटा के स्थानांतरण की जिम्मेदारियों को प्रबंधित किया जाता है। जहाँ तक अपर लेयर्स का संबंध होता है, डाटा का स्थानांतरण पारदर्शी होना चाहिए, भले ही डेस्टिनेशन होस्ट उसी फिजिकल नेटवर्क पर हो अथवा अनेक फिजिकल नेटवर्क्स एक समान प्रोद्योगिकी और प्रोटोकॉल्स का उपयोग करें या नहीं करें।

इस अध्याय में नेटवर्क लेयर पर निम्नलिखित प्रोटोकॉल्स के विवरणों को प्रस्तुत किया गया है–

IP– इंटरनेट प्रोटोकॉल

ARP– एड्रेस रिजाल्यूशन प्रोटोकॉल

RARP–रिवर्स एड्रेस रिजाल्यूशन प्रोटोकॉल

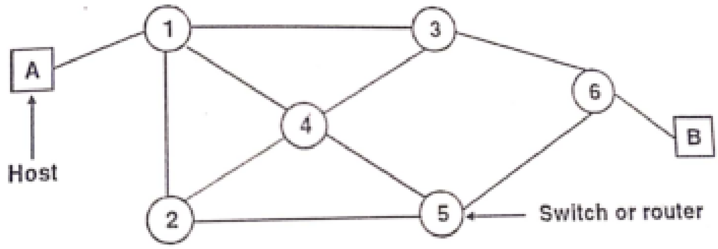
ICMP– इंटरनेट कंट्रोल मैसेज प्रोटोकॉल

इंटरनेट पर प्रत्येक सिस्टम को एक विशिष्ट IP एड्रेस के द्वारा पहचाना जाता है। यद्यपि यह केवल 4 बाईट की एक ऐसी संख्या मात्र होती है जो नेटवर्क तथा सर्विस के प्रकार के बारे में विभिन्न महत्वपूर्ण इंफॉर्मेशन संग्रहीत करती है। अतः सभी को इसे विस्तारपूर्वक समझना जरूरी होता है। किसी IP मॉड्यूल द्वारा लिए जाने वाले महत्वपूर्ण निर्णयों में से एक यह है कि इनकमिंग डाटागाम को कहाँ पर फॉरवर्ड किया जाए जिससे कि वह उसके डेस्टिनेशन होस्ट तक पहुंच जाए, दूसरे शब्दों में इसे राउटिंग कहते हैं।

5.2.1 पैकेट नेटवर्क में राउटिंग :

पैकेट स्विच्ड नेटवर्क चित्र 20.1 में दर्शाए अनुसार एक स्वेच्छिक जालनुमा पद्धति में कम्युनिकेशन लिंक्स द्वारा इंटरकनेक्टेड नोड्स (राउटर्स या स्विचेज) से मिलकर बनता है। जैसा इस चित्र में बताया गया है कि कोई पैकेट होस्ट A से होस्ट B तक विभिन्न संभावित मार्ग ले सकता है। उदाहरण के लिए तीन संभावित मार्ग 1–3–6, 1–4–5–6

और 1–2–5–6 होते है। यदि उद्देश्य हॉप्स की संख्या को प्रत्येक लिंक थोड़ा बहुत डिले उत्पन्न करती है और ऑब्जेक्टिव फंक्शन एण्ड–टू–एण्ड डिले को कम कर देता है तो फिर सर्वोत्तम मार्ग वह होता है जो हमें न्यूनतम एण्ड–टू–एण्ड डिले प्रदान करे।



चित्र 5.16 : पैकेट स्विच नेटवर्क

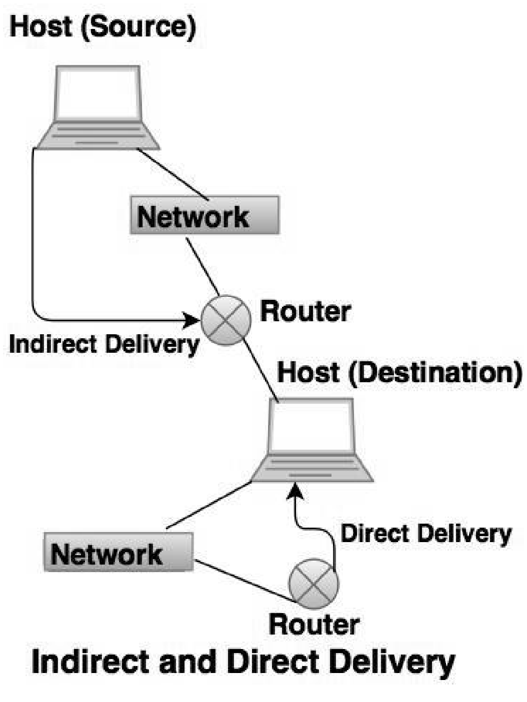
किसी अच्छे राउटिंग एल्गोरिथम के मुख्य कार्य ऐसे ऑब्जेक्टिव फंक्शन पर निर्भर करते हैं जिसे कोई व्यक्ति अनुकूलतम रूप से उपयोग करने का प्रयास कर रहा हो। सामान्यतः किसी राउटिंग एल्गोरिथम द्वारा निम्नलिखित में से एक या अधिक को पूर्ण किया जाना चाहिए–

1. पैकेट्स की त्वरित और स्टीक डिलीवरी : किसी राउटिंग एल्गोरिथम को सही तरह से कार्य करना चाहिए अर्थात् डेस्टिनेशन के लिए यदि कोई रूट मौजूद हो तो उसका पता लगाने में सक्षम होना चाहिए। इसके अतिरिक्त एल्गोरिथम को डेस्टिनेशन के लिए रूट का पता लगाने में अत्यधिक समय भी नहीं लेना चाहिए।
2. नोड या लिंक की विफलता के फलस्वरूप नेटवर्क टोपोलॉजी में परिवर्तनों हेतु अनुकूलनशीलता : किसी वास्तविक नेटवर्क में डिवाइसेज और ट्रांसमिशन लाइंस सामान्यतः फेल होती रहती है। अतः राउटिंग एल्गोरिथम को इस परिस्थिति को स्वीकार करने और नेटवर्क डिवाइस के विफल होने पर रूट्स को स्वचालित रूप से पुनः कॉन्फिगर करने में सक्षम होना चाहिए।

राउटिंग एल्गोरिथम का वर्गीकरण :

कोई भी व्यक्ति राउटिंग एल्गोरिथम को विभिन्न प्रकार से वर्गीकृत कर सकता है। अपनी प्रतिक्रियाशील क्षमता के अनुसार राउटिंग (1) स्टेटिक अथवा (2) डायनेमिक (अथवा अडेप्टिव) हो सकती है।

1. स्टेटिक राउटिंग में नेटवर्क टोपोलॉजी प्रारंभिक पाथ्स का पता लगाती है। तदुपरांत प्रीकम्प्यूटेउ पाथ्स राउटिंग टेबल पर मेन्युअली लोड कर दिए जाते हैं और शेष तुलनात्मक रूप से लंबी अवधि के लिए स्थिर बने रहते हैं। स्टेटिक राउटिंग तभी पर्याप्त हो सकता है जबकि नेटवर्क टोपॉलोजी तुलनात्मक रूप से स्थिर रहे और नेटवर्क का आकार छोटा हो।
2. डायनेमिक (अडेप्टिव) राउटिंग में प्रत्येक राउटर अपने समीपवर्ती राउटर्स के साथ निरंतर कम्युनिकेट करते हुए नेटवर्क की स्थिति को प्राप्त करता रहता है। अस्तु नेटवर्क टोपालॉजी में होने वाला कोई भी परिवर्तन तत्काल ही सभी राउटर्स को प्रसारित कर दिया जाता है। प्राप्त की जाने वाली सूचना के आनुसार प्रत्येक राउटर वांछित डेस्टिनेशन के लिए सर्वोतम पाथ्स की गणना कर सकता है। डायनेमिक राउटिंग का एक नुकसान यह है कि राउटर में जटिलता जुड़ जाती है।



चित्र 5.17 : इन डिरेक्टिंग रूटिंग

रूटिंग टेबल :

किसी नेटवर्क में राउटर्स को ढूंढने के लिए जो टेबल बनाई जाती है, उसे राउटिंग टेबल के रूप में जाना जाता है। इस टेबल का उपयोग IP राउटिंग को सरलता प्रदान करने के लिए किया जाता है। प्रत्येक होस्ट इस टेबल में डेस्टिनेशन IP नेटवर्क एड्रेस (एड्रेसेस) और अगले गेटवे (गेटवेज) के लिए रूट (रूट्स) के मध्य मेपिंग्स के सेट को संग्रहीत करता है।

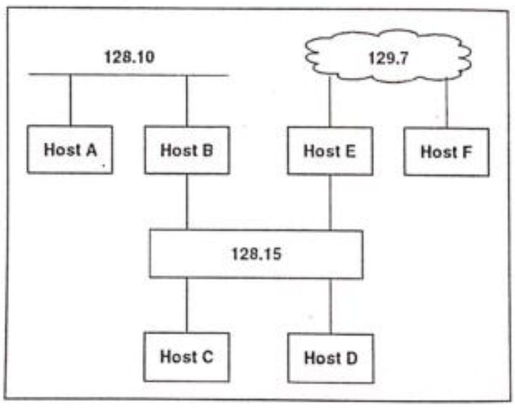
इस टेबल में मेपिंग्स के तीन प्रकार विद्यमान होते है –

1. लोकली अटेच किए गए नेटवर्क्स को विस्तृत करने वाले डायरेक्ट रूट्स।
2. एक या अधिक गेटवेज के माध्यम से पहुँच के योग्य होने वाले नेटवर्क्स को विस्तृत करने वाले इनडायरेक्ट रूट्स।
3. वह डिफॉल्ट रूट जो उपरोक्त दोनों ही प्रकार की मेपिंग्स में डेस्टिनेशन प्च नेटवर्क के उपस्थित नहीं होने पर प्रयुक्त किए जाने वाले रूट (डायरेक्ट या इनडायरेक्ट) से मिलकर बनता है।

चित्र 20.3 एक नमूना नेटवर्क को दर्शाता है। होस्ट D की राउटिंग टेबल निम्नलिखित (सांकेतिक) प्रविष्टियों से बनी हो सकती है –

Destination	Router
129.7.0.0	Host E
128.15.0.0	Direct
128.10.0.0	Host B
Default	Host B

Table 20.1 Routing Table of Host D



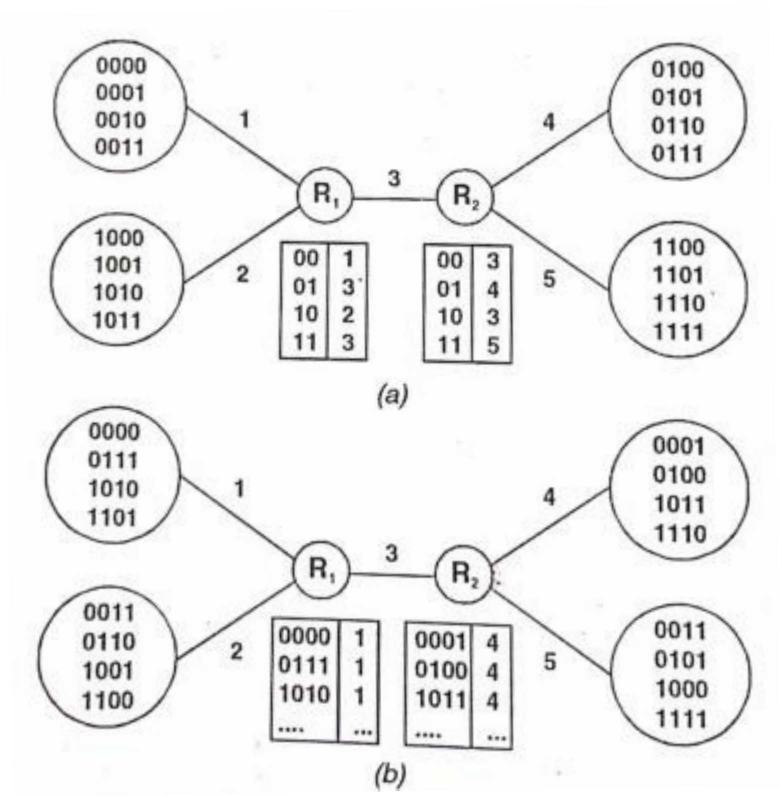
चित्र 5.18 : रूटिंग टेबल नेटवर्क

चूँकि D नेटवर्क 128.15.0.0 से सीधे ही जुड़ा होता है, अतः यह इस नेटवर्क के लिए डायरेक्ट रूट रखता है। नेटवर्क्स 129.7.0.0 और 128.10.0.0 पर पहुँचने के लिए, यद्यपि इसमें क्रमशः E और B द्वारा एक इनडायरेक्ट रूट होना चाहिए क्योंकि ये नेटवर्क्स सीधे जुड़े हुए नहीं हैं।

होस्ट F का राउटिंग टेबल में निम्नलिखित (सांकेतिक) प्रविष्टियाँ हो सकती हैं–

Destination	Router
129.7.0.0	Direct
Default	Host E

हाइअरार्किअल (पदानुक्रमिक) राउटिंग :



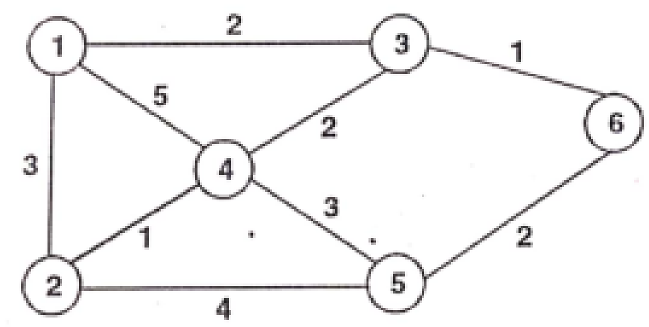
चित्र 5.19 : हिरार्चिकल रूटिंग

राउटर्स को जिस राउटिंग टेबल को रखना आवश्यक होता है उस का आकार न्यूनतम किया जा सकता है यदि एड्रेसेस के निर्धारण में पदानुक्रमिक उपागम प्रयुक्त की जाए। निश्चित रूप से, एक–दूसरे के समीप होने वाले होस्ट्स में ऐसे एड्रेसेस होने चाहिए जिनमें एक समान प्रीफिक्सेस होते हों। इस रीति में किसी पैकेट को कैसे रूट

किया जाना चाहिए, यह निर्णय लेने के लिए राउटर्स को एड्रेस के केवल एक भाग (अर्थात् प्रीफिक्स) का ही परीक्षण करने की आवश्यकता होती है। चित्र 5.19 पदानुक्रमिक एड्रेस असाइनमेंट और फ्लेट एड्रेस असाइनमेंट का उदाहरण प्रस्तुत करता है। भाग (a) में प्रत्येक चार साइट्स पर होस्ट्स में एक समान प्रीफिक्स होते हैं। अतः दो राउटर्स को केवल चार एंट्रीज के साथ टेबल्स को संभालना पड़ता है, जैसा कि चित्र में स्पष्ट किया गया है।

शॉर्टेस्ट–पाथ एल्गोरिथम्स :

नेटवर्क लेयर ापर नेटवर्क राउटिंग एक महत्वपूर्ण घटक होता है और यह प्रत्येक सोर्स से प्रत्येक डेस्टिनेशन तक के लिए सुगम पाथ्स (या रूट्स) का पता लगाने की समस्या से संबंधित होता है। राउटर अथवा पैकेट स्विच्ड फॉरवर्डिंग। राउटिंग फंक्शन में, एल्गोरिथम प्रत्येक डेस्टिनेशन के लिए एक अनुकूलतम पाथ का पता लगाता है। और परिणाम को राउटिंग टेबल में रखता है। फॉरवर्डिग फंक्शन में, राउटर प्रत्येक पैकेट को किसी इनपुट पोर्ट से राउटिंग टेबल में संग्रहीत सूचना के आधार पर उपयुक्त आउटपुट पोर्ट पर फारवर्ड करता है।



चित्र 5.20 : Example शॉर्टेस्ट पाथ अल्गोरिथम

अधिकांश राउटिंग एल्गोरिथम्स ऐसे शॉर्टेस्ट पाथ एल्गोरिथम्स की विभिन्नताओं पर आधारित होते हैं, जो कुछ परिणााम के आधार पर किसी पैकेट के लिए शॉटेस्ट पाथ का पता लगाने का प्रयास करते हैं। इन एल्गोरिथम्स के उद्देश्य को अच्छी तरह से समझने के लिए कम्युनिकेशन नेटवर्क को एक ऐसे ग्राफ के रूप में माने जो नोड्स के सेट (अथवा अनुलंब) और लिंक्स के सेट (अथवा किनारे, चाप या शाखाओं) से बना हो,

जहाँ प्रत्येक नोड किसी राउटर या पैकेट स्विच को दर्शाता हो और प्रत्येक लिंक दो राउटर्स के मध्य एक कम्यनुनिकेशन चैनल को दर्शाती हो। चित्र 5.20 ऐसा ही एक उदाहरण दर्शाता है। प्रत्येक लिंक के साथ ऐसी वेल्यू संबद्ध होती है जो उस लिंक के उपयोग की लागत (या परिणाम) को सूचित करती है।

1. बैलमन–फोर्ड एल्गोरिथम (डिस्टेंस–वेक्टर राउटिंग) :

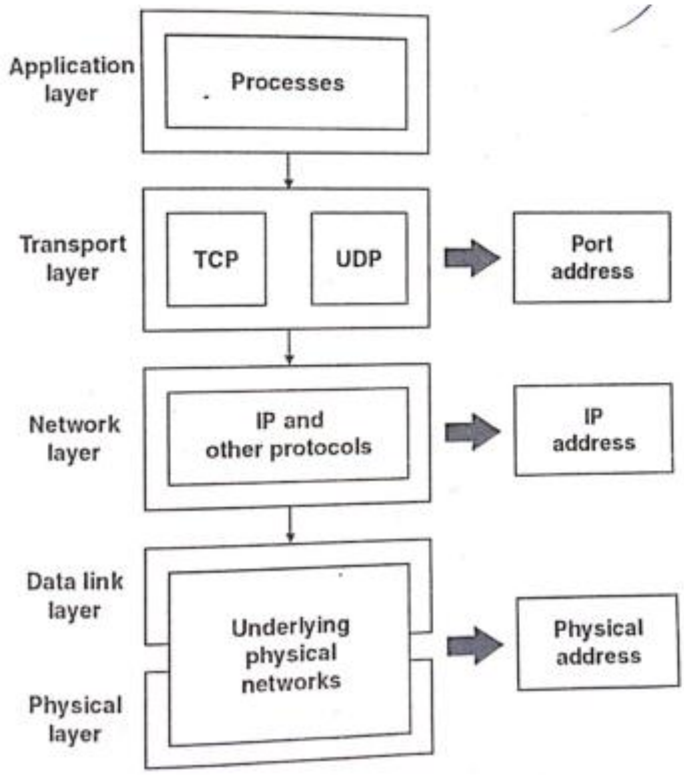
बैलमन–फोर्ड एल्गोरिथम (इसे फोर्ड–फल्कर्सन एल्गोरिथम भी कहा जाता है।) जिस सिद्धान्त का आधारति है वह समझने में आसान है, यदि कोई नोड A और N के मध्य शॉर्टेस्ट पाथ में होता है तब नोड A तक का पाथ भी शॉर्टेस्ट पाथ ही होना चाहिए। जैसा कि उदाहरण में प्रस्तुत है, मान लिजिए कि हम चित्र 5.20 में नोड 2 से नोड 6 (डेस्टिनेशन) तक के लिए शॉर्टेस्ट पाथ ढूढंना चाहते है। डेस्टिनेशन तक पहुँचने के लिए, नोड 2 से किसी पैकेट को सर्वप्रथम नोउ 1, नोड 4 या नोड 5 पर जाना ही पड़ता है। मान लिजिए कि कोई हमें नोड्स 1, 4 या 5 से डेस्टिनेशन (नोड 6) के लिए शॉर्टेस्ट पाथ्स क्रमशः 3, 3 और 2 बताता है। यदि पैकेट सबसे पहले नोड 1 से होकर जाता है, तो कुल दूरी (जिसे कुल लागत या परिमाण भी कहा जाता है) 3+3 अर्थात् 6 होती है। नोड 4 द्वारा कुल दूरी 1+3 अर्थात् 4 होती है। नोड 5 द्वारा कुल दूरी 4+2 अर्थात् 6 होती है। अतः यदि पैकेट नोड 4 पर पहले पहुँच जाए तो नोड 2 से डेस्टिनेशन नोड के लिए शॉर्टेस्ट पाथ प्राप्त किया जाता है।

TCP/IPमें एड्रेसिंग :

विभिन्न नेटवर्क लेयर प्रोटोकॉल को समझने से पहले किसी व्यक्ति के लिए ज्ब्ध्च्च मॉडल में विद्यमान एड्रेसिंग के विभिन्न प्रकारों को जानना आवश्यक होता है।

ज्ब्ध्च्च मॉडल में एड्रेसिंग के तीन विभिन्न लेवल्स होते है–

1. फिजिकल (लिंक) एड्रेस
2. इंटरनेटवर्क (IP)एड्रेस
3. ट्रांसपोर्ट अथवा पोर्ट एड्रेस



चित्र 5.21 : एड्रेसिंग लेयर

1. फिजिकल एड्रेस : यह LANया WANद्वारा परिभाषित डाटा लिंक लेयर पर किसी नोड का एड्रेस होता है। यह डाटा लिंक लेयर द्वारा भेजी जाने वाली फ्रेम में उपस्थित होता है। यह एड्रेस किसी विशेष नेटवर्क पर होस्ट सिस्टम का पता लगाता है।

फिजिकल एड्रेसेस या तो यूनीकास्ट (एकल प्राप्तकर्ता), मल्टीकास्ट (प्राप्तकर्ताओं का समूह) अथवा ब्रॉडकास्ट (इसे नेटवर्क में सभी प्राप्त करते हैं) हो सकते हैं। यद्यपि सभी नेटवर्क्स इनका समर्थन नहीं करते हैं। लोकप्रिय LAN में से एक, ईथरनेट इन सभी को सपोर्ट करता है।

2. इंटरनेट एड्रेस : फिजिकल नेटवर्क से स्वतंत्र इंटरनेट एड्रेसेस यूनिवर्सल कम्युनिकेशन सेवाओं के लिए आवश्यक होते हैं। फिजिकल नेटवर्क्स में विभिन्न एड्रेसिंग स्वरूप होते हैं, जो कि प्रयुक्त की जाने वाली नेटवर्क नकनीक पर निर्भर जिसका उपयोग करते हुए कोई व्यक्ति उस नेटवर्क की पहचान कर सके जिस पर इसे जोड़ा गया है, जो कि राउटिंग उद्देश्य के लिए आवश्यक होता है।

इंटरनेट एड्रेसेस को इस उद्देश्य के लिए ही डिजाइन किया गया है। वर्तमान में एक इंटरनेट एड्रेस 32 बिट (4 बाइट) का ऐसा एड्रेस होता है जो इंटरनेट से कनेक्ट किए गए किसी होस्ट को विशिष्ट रूप से पहचानता है।

3. पोर्ट एड्रेस : IPएड्रेस और फिजिकल एड्रेस सोर्स और डेस्टिनेशन सिस्टम को पहचानते है। ये इन सिस्टम्स पर प्रोसेस (कम्प्यूटर पर चल रहा को प्रोग्राम) को नहीं पहचानते हैं,, जिन पर डाटा वास्तविक रूप से प्रोसे के अनुरूप होता है। इंटरनेट कम्यूनिकेशन का मुख्य उद्देश्य दो विभिन्न सिस्टम पर चल रही दो प्रोसेसेज के मध्य एक कम्युनिकेशन लिंक प्रदान करना होता हैं उदाहरण के लिए, सिस्टम A से FTP (फाइल ट्रांसफर प्रोटोकॉल) क्लाइंट प्रोसेस के द्वारा भेजे गए डाटा को सिस्टम B पर FTP सर्वर प्रोसेस पर पहुँचना चाहिए।

5.2.2 इंटरनेट प्रोटोकॉल (IP):

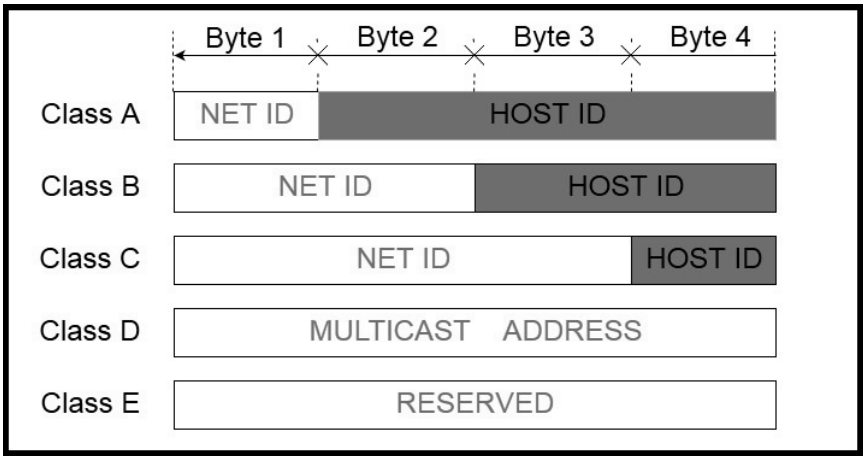
IPमॉड्यूल इंटरनेट प्रोद्योगिकी की सफलता का केन्द्र है। इंटरनेट प्रोटोकॉल अथवा IP एकाधिक फिजिकल नेटवर्क्स से एक सिंगल लॉजिकल नेटवर्क निर्मित करता है। दूसरे शब्दों में यह लेयर उच्चतम स्तरों को उसके निचले जटिल नेटवर्क आर्किटेक्चर से बचाए रखती है। अतः इंटरनेट प्रोटोकॉल (IP)अत्यधिक महत्वपूर्ण प्रोटोकॉल होता है। उच्चतम लेयर्स केवल एक वर्चअल अथवा लॉजिकल नेटवर्क पर ही कार्य करती है और इन्हें फिजिकल नेटवर्क कहाँ स्थित है, उसके आर्किटेक्चर इत्यादि के बारे में जानना आवश्यक नहीं होता है।

यह एक अविश्वनीय और कनेक्शन रहित डाटाग्राम प्रोटोकॉल है जो बेस्ट एफर्ट डिवीवरी सर्विस देता है। बेस्ट एफर्ट शब्द का अर्थ है कि IP हमें कोई ऍरर चेकिंग या ट्रेकिंग प्रदान नहीं करता है। IP आंतरिक लेयर्स की अविश्वसनीयता का अनुमान लगता है और उसके डेस्टिनेशन के लिए ट्रांसमिशन प्राप्त करने के लिए बिना किसी गारंटी के सर्वोतम कार्य करता है। IPयह मानता है कि अपर लेयर प्रोटोकॉल्स विश्वसनीयता संबंधी मामलों को आवश्यकता होने पर प्रबंधित कर लेंगे। वस्तुतः ट्रांसपोर्ट लेयर पर TCP प्रोटोकॉल हमें एप्लीकेशन लेयर के लिए विश्वसनीयता और कनेक्शन उन्मुखी सर्विस प्रदान करता है।

IP एड्रेसिंग योजना :

TCP/IP प्रोटोकॉल स्टेक में, एड्रेसिंग को इंटरनेट प्रोटाकॉल(IP) द्वारा प्रदर्शित किया जाता है। IP मानक यह निर्दिष्ट करता है कि प्रत्येक होस्ट को एक विशिष्ट 32 बिट संख्या प्रदान की जाए जिसे होस्ट का इंटरनेट प्रोटोकॉल एड्रेस के रूप में जाना जाता है, इसे आमतौर पर संक्षिप्त में IPएड्रेस या इंटरनेट एड्रेस भी कहा जाता है। इंटरनेट पर भेजा गया प्रत्येक पैकेट सेंडर (सोर्स) के साथ ही साथ लक्षित प्राप्तकर्ता (डेस्टिनेशन) के 32 बिट IPएड्रेस से मिलकर बनता है।

IP एड्रेसेज की क्लासेज :



चित्र 5.22 : IP एड्रेसिंग क्लासेज

Address Class	RANGE	Default Subnet Mask
A	1.0.0.0 to 126.255.255.255	255.0.0.0
B	128.0.0.0 to 191.255.255.255	255.255.0.0
C	192.0.0.0 to 223.255.255.255	255.255.255.0
D	224.0.0.0 to 239.255.255.255	Reserved for Multicasting
E	240.0.0.0 to 254.255.255.255	Experimental

चित्र 5.23 : IP एड्रेसिंग क्लासेज

एक बार IP एड्रेसेज के लिए कोई आकार चुने जाने और प्रत्येक एड्रेस को दो भागों में विभक्त करने का निर्णय ले लिए जाने के बाद, IPके डिजाइनर्स को यह पता करना पड़ता है कि प्रत्येक भाग में कितनी बिट्स रखना है। प्रीफिक्स को इंटरनेट में प्रत्येक फिजिकल नेटवर्क के लिए एक विशिष्ट नेटवर्क नंबर प्रदान किए जाने की अनुमति प्रदान करने हेतु पर्याप्त बिट्स की आवश्यकता होती है। सफिक्स को किसी नेटवर्क से जोड़े गए प्रत्येक कम्प्यूटर पर एक विशिष्ट सफिक्स प्रदान किए जाने की अनुमति के लिए प्रर्याप्त बिट्स की आवश्यकता होती है।

चित्र 5.23 पाँच एड्रेस क्लासेज को दर्शाता है कि प्रारंभिक बिट्स प्रत्येक क्लास को पहचाहनने के लिए प्रयुक्त की जाती है। चित्र में बाएँ से दाएँ की ओर नंबरिंग बिट्स के TCP/IPप्रोटोकॉल्स में प्रयुक्त परिपाटी का पालन किया गया है और प्रथम बिट के लिए शून्य उपयोग किया जा रहा है।

क्लासेज A, Bऔर C को प्राइमरी क्लासेज कहा जाता है, क्योंकि ये होस्ट एड्रेसेज के लिए प्रयुक्त की जाती है। क्लास D मल्टीकास्टिंग के लिए प्रयुक्त होती है, जो कम्प्यूटर्स के किसी समूह को वितरण की अनुमति प्रदान करती है। IPमल्टीकास्टिंग का उपयोग करने के लिए होस्ट्स के किसी समूह को मल्टीकास्ट एड्रेस को साझा करने के लिए सहमत होना चाहिए। एक बार जब मल्टीकास्ट ग्रुप सेट हो जाता है, तो मल्टीकास्ट एड्रेस पर भेजे गए किसी भी पैकेट की प्रतिलिपि को समूह में मौजूद प्रत्येक होस्ट को वितरित कर दिया जाएगा।

जैसा कि चित्र दर्शाता है, प्राइमरी क्लासेज किसी एड्रेस को प्रीफिक्स और सफिक्स में विभाजित करने के लिए ऑक्टेट सीमाओं का उपयोग करती है। क्लास A सीमा को पहले और दूसरे और तृतीय और चतुर्थ ऑक्टेट्स के मध्य सीमा स्थित करती है।

क्लास A:

यदि प्रथम बिट 0 होता है, तब प्रदान किया गया एड्रेस क्लास A एड्रेस होता है। प्रथम बिट का शेष भाग netid को परिभाषित करता है। बाइट 2 से 4 4, उस फिजिकल नेटवर्क पर सिस्टम के hostidका पता लगाते है। netid में 7 बिट्स होते हैं, जिसका अर्थ होता है कि क्लास A एड्रेस के साथ कुल 2^7= 128 नेटवर्क्स हो सकते हैं। चूँकि hostid

में 3 बाइट्स (24 बिट्स) शेष है, अतः ऐसा प्रत्येक नेटवर्क 2^{24}= 16777216 होस्ट्स को अनुकूलित कर सकता है।

क्लास B :

यदि IPएड्रेस की प्रथम दो बिट्स 10 होती है।, तो प्रदान किया गया एड्रेस क्लास B एड्रेस होता है। यहाँ hostid 16 बिट्स (2 बाइट्स) लंबा होता है और शेष 14 बिट्स netid के लिए होती हैं। इसका अर्थ है कि यहाँ कुल 2^{14}= 16384 क्लास B नेटवर्क्स और ऐसे प्रत्येक नेटवर्क पर 2^{16}= 65536 होस्ट्स होते है। जैसा कि क्लास A के लिए पहले बताया गया है, इनमें से कुद विशेष उद्देश्य के लिए आरक्षित रहते है।

क्लास C :

यदि IP एड्रेस की प्रथम तीन बिट्स 110 होती हैं तो प्रदान किया गया एड्रेस क्लास C एड्रेस होता है। अगले 21 बिट्स netid को परिभाषित करते है और शेष 8 बिट्स उस नेटवर्क पर hostid का पता लगाते है। अतः कुल 2^{21}= 2,097,152 क्लास C नेटवर्क्स और ऐसे प्रत्येक नेटवर्क पर 2^{8}= 256 होस्ट्स होते हैं। जैसा कि पहले ही बताया गया है उनमें से कुछ विशेष उद्देश्य के लिए आरक्षित होते है।

क्लास D :

क्लास D मल्टीकास्टिंग के लिए बनाया गया एक विशेष प्रकार का एड्रेस होता है। इसमें netid अथवा hostid के नोटेशन नहीं होते हैं। प्रथम 4 बिट्स (1110) यहाँ मौजूद क्लास को परिभाषित करती हैं। शेष 28 बिट्स इंटरनेट पर मल्टीकास्ट एड्रेस को विशिष्ट तौर पहचानते है।

क्लास E :

यह इंटरनेट ऑथोरिटी द्वारा विशेष उद्देश्यों के लिए आरक्षित रखी गई क्लास होती है। इस क्लास में कोई netid अथवा hostid नहीं होते हैं। इस क्लास के प्रथम चार बिट्स 1111 होते हैं।

क्लास का निर्धारण :

किसी एड्रेस की क्लास का निर्धारण करने के लिए दो तरीके हैं जो इसे प्रदर्शित करने वाले स्वरूप पर निर्भर होते हैं।

यदि एड्रेस के आधारा पर बिट्स के क्लास को पहचाना जा सकता हैं।

- यदि प्रथम 0 बिट्स हो तो वह क्लास A होती है।
- यदि प्रथम 2 बिट्स 10 हों – क्लास B
- यदि प्रथम 3 बिट्स 110 हों – क्लास C
- यदि प्रथम 4 बिट्स 1110 हों – क्लास D
- यदि प्रथम 4 बिट्स 11111 हों –क्लास E

सामान्यतः एड्रेसेस डेसिमल नोटेशन में प्रदान किए जाते हैं, जिन्हें क्लास का पता लगाने के लिए निम्निलिखित विधियों की आवश्यकता होती है।

- क्लास A– पहली संख्या 0 और 127 के मध्य होती है
- क्लास B– पहली संख्या 128 और 191 के मध्य होती है।
- क्लास C– पहली संख्या 192 और 223 के मध्य होती है।
- क्लास D– पहली संख्या 224 और 239 के मध्य होती है।
- क्लास E – पहली संख्या 240 और 255 के मध्य होती है।

ARP मैसेज फॉर्मेट :

ARP मैसेजेस को पैकेट मे लाए जा रहे प्रोटोकॉल को पहचाहने के लिए ईथर टाइप या SNAP लोकल कोड वेल्यू मान के समान ही 0806 का उपयोग करते हुए सीधे डाटा लिंक लेयर फ्रेम्स में ट्रांसमिट किया जाता है। सभी ARP मैसेज प्रकारों के लिए एक ही फॉर्मेट होता है, जिसे चित्र 20.14 में दर्शाया गया है।

<table>
<tr><td>1 2 3 4 5 6 7 8</td><td>1 2 3 4 5 6 7 8</td><td>1 2 3 4 5 6 7 8</td><td>1 2 3 4 5 6 7 8</td></tr>
<tr><td colspan="2">Hardware Type</td><td colspan="2">Protocol Type</td></tr>
<tr><td>Hardware Size</td><td>Protocol Size</td><td colspan="2">Op Code</td></tr>
<tr><td colspan="4">Sender Hardware Address</td></tr>
<tr><td colspan="2">Sender Hardware Address (cont'd)</td><td colspan="2">Sender Protocol Address</td></tr>
<tr><td colspan="2">Sender Protocol Address (cont'd)</td><td colspan="2">Target Hardware Address</td></tr>
<tr><td colspan="4">Target Hardware Address (cont'd)</td></tr>
<tr><td colspan="4">Target Protocol Address</td></tr>
</table>

चित्र 5.24 : ARP मैसेज फॉर्मेट

फील्ड्स के कार्य निम्नानुसार है –

1. हार्डवेयर टाइप (2 बाइट्स) : यह सेंडर, हार्डवयेर, एड्रेस और टारगेट हार्डवेयर एड्रेस फील्ड्स में उपस्थित हार्डवेयर एड्रेस के प्रकार को दर्शाता है। ईथरनेट के लिए हेक्साडेसिमल वेल्यू 0001 होती है।

2. प्रोटोकॉल टाइप (2 बाइट्स) : यह सेंडर प्रोटोकॉल एड्रेस और टारगेट प्रोटोकॉल एड्रेस और टारगेट प्रोटोकॉल एड्रेस फील्ड्स में उपस्थित प्रोटोकॉल एड्रेसेज के प्रकार को प्रदर्शित करता है। IPएड्रेस के लिए हेक्साडेसिमल वेल्यू 0800 होती है।
3. हार्डवेयर साइज (1 बाईट) : यह सेंडर हार्डवेयर एड्रेस और टारगेट हार्डवेयर एड्रेस फील्ड्स मे विद्यमान हार्डवेयर एड्रेसेज के आकार (बाइट्स में) को निर्दिष्ट करता है। ईथरनेट हार्डवयेर एड्रेसेज के लिए वेल्यू 6 होती है।
4. प्रोटोकॉल साइज (1 बाईट) : यह सेंउर प्रोटोकॉल एड्रेस और टारगेट प्रोटोकॉल एड्रेस फील्ड्स में उपस्थित प्रोटोकॉल एड्रेसेज के आकार (बाइट्स में) को प्रदर्शित करता है। IP एड्रेसेज के लिए मान 4 होती है।
5. Opcode (2 बाइट्स) : यह निम्नलिखित वेल्यूज का उपयोग करते हुए पैकेट में उपस्थित मैसेज के प्रकार को निर्दिष्ट करता है 7

   (i) ARPरिक्वेस्ट

   (ii) ARP रिप्लाई

   (iii) RARP रिक्वेस्ट

   (iv) RARP रिप्लाई

6. सेंडर हार्डवेयर एड्रेस : यह मैंसेज भेजने वाले सिस्टम के हार्डवेयर (जैसे कि ईथरनेट) एड्रेस को रिक्वेस्ट्स और रिप्लाइज दोनों में प्रदर्शित करता है।
7. सेंडर प्रोटोकॉल एड्रेस : यह मैसेज भजने वाले सिस्टम के प्रोटोकॉल (जैसे कि IP) एड्रेस को रिक्वेस्ट्स और रिप्लाइज दोनों में प्रदर्शित करता है।

RARP :

RARP (रिवर्स एड्रेस रेजॉल्यूशन प्रोटोकॉल) प्रत्येक TCP/IPसिस्टम पर प्रयुक्त किए जाने वाले ARP (एड्रेस रेजॉल्यूशन प्रोटोकॉल) के विपरीत कार्य करता है। जब ARPनेटवर्क लेयर IPएड्रेसेज को डाटा लिंक लेयर हार्डवेयर एड्रेसेज में रूपांतरित करता है तो RARP सिस्टम के हार्डवेयर एड्रेस को प्रसारित करते हुए और RARP सर्वर से पुनः IP एड्रेस को प्राप्त करते हुए कार्य करता है।

RARP सर्वर किसी नेटवर्क सेगमेंट पर सभी सिस्टम्स के टॉस्क फोर्स के RFC 903दस्तावेज में परिभाषित की गई यह अवधारणा माइक्रोशॉफ्ट की आवश्यकताओं के लिए निम्नलिखित कारणों से पर्याप्त नहीं थी –

RARP क्लाइंट द्वारा उत्पन्न किए जाने वाले ब्रॉउकास्ट मैसेजेस पर निर्भर होता है क्योंकि डिस्क रहित वर्कस्टेशन के लिए RARPसर्वर के एड्रेस को संग्रहीत करना अर्थपूर्ण नहीं होता है। इसलिए चूँकि लोकल नेटवर्क पर ब्रॉडकास्ट सीमित होते है। अस्तु प्रत्येक नेटवर्क सेगमेंट पर वर्कस्टेशन्स को कार्य करने के लिए उस सेगमेंट पर एक RARPसर्वर होना ही चाहिए।

IP एड्रेसेज के साथ केवल क्लाइंट सिस्टम्स को ट्रांसमिट करने के लिए RARP सक्षम होता है। वर्तमान नेटवर्क्स पर उपयोगी होने के लिए प्रोटोकॉल को अन्य कॉन्फिग्युरेशन पेरामीटर्स जैसे कि नेम सर्वर्स और डिफाल्ट गेटवेज के लिए वेल्यूज को भी साथ ही साथ प्रदान करना चाहिए।

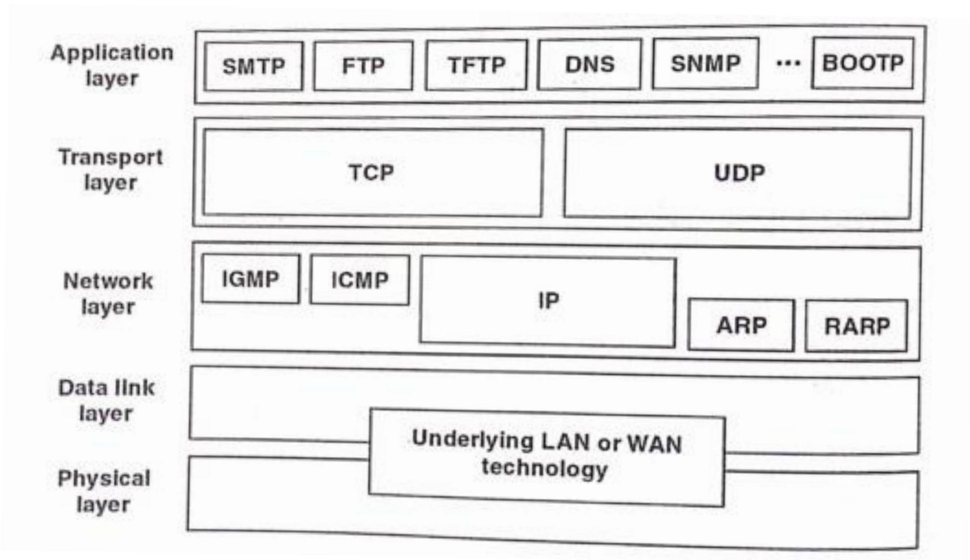
6.1 ट्रांसपोर्ट लेयर एक परिचय :

ट्रांसपोर्ट लेयर TCP/IPप्रोटोकॉल मॉडल का हृदय है। यहाँ कार्यों का संबंध प्रोसेस–टू–प्रोसेस कम्यूनिकेशन, विश्वसनीयता, स्ट्रीम डाटा सेवाएँ प्रदान किए जाने से होता है। ये वे सेवाएँ हैं, जो नेटवर्क के आर–पार कम्यूनिकेटिंक कार्य को एप्लीकेशन प्रोग्राम की दृष्टि से सरल बनाती हैं।

ट्रांसपोर्ट लेयर पर दो प्रोटोकॉल्स परिभाषित किए जाते हैं –

1. UDP– यूजर डाटाग्राम प्रोटोकॉल
2. TCP– ट्रांसमिशन कंट्रोल प्रोटोकाल

ट्रांसपोर्ट लेयर प्रोटोकॉल्स और शेष लेयर्स के मध्य संबंध को चित्र 6.1 में दर्शाया गया है।



चित्र 6.1: ट्रांसपोर्ट लेयर

1. UDP : दोनों में से UDP सबसे सरल है तथा यह हमें प्रोसेस–टू–प्रोसेस कम्यूनिकेशन सेवा और अल्प मात्रा में ऍरर चैकिंग प्रदान करता है। इसकी सरलता और अविश्वसनीय सेवा की वजह से यह कार्य–कुशल है तथा इसीलिए उन्हीं एप्लीकेशन्स में प्रयुक्त किया जाता है, जहाँ पर संपूर्ण विश्वसनीयता महत्वपूर्ण नहीं

होती है। यह मुख्यतः मल्टीमीडिया एप्लीकेशन में उपयोगी रहता है, जिनमें ध्वनि व वीडियों डाटा ट्रांसमिट किए जाते हैं ओर जिन्हें अधिक विश्वसनीयता की आवश्यकता नहीं होती हैं, किंतु डाटा तेज गति से ट्रांसफर किया जाना जरूरी होता हैं। यदि कुछ डाटा लुप्त अथवा करप्टेड हो जाए तो भी इंफॉर्मेशन की क्षति अल्प मात्रा में ही होती है।

UDP के खण्ड में पोर्ट संख्या (एड्रेस) की अवधारणा और सॉकेट एड्रेस की व्याख्या की जाएगी। इसके बाद UDPडाटाग्राम फॉर्मेट के बारे में एक खण्ड रहेगा।

2. TCP : TCPवह प्रोटोकॉल है, जो नेटवर्क के आर–पार कम्यूनिकेटिंग के कार्य को एप्लीकेशन प्रोग्राम (प्रोसेस) के दृष्टिकोण से सरल बनाता है। एप्लीकेशन प्रोग्राम लिखने वाला डेवलपर ऐसे विभिन्न बोझिल कार्यों को लेकर चिंतित नहीं होता है, जिनमें किसी भी अवसर पर डाटा लॉस होता हो या डाटा के क्रमानुसार प्राप्त न होने अथवा फ्लों कंट्रोल से संबंधित मामले शामिल होते हों। TC इन सभी को संभालता हैं और एक भरोसेमंद, कनेक्शन उन्मुखी, स्ट्रीम डाटा सेवा एण्ड प्रोसेस के लिए प्रदान करता है। इसमें फ्लों कंट्रोल भी उसके भीतर ही बना होता है।

TCP की मूल अवधारणा :

TCP असंभव से प्रतीत होने वाले कार्य सम्पन्न करता है : वह अन्य कम्प्यूटर को डाटा भेजे जाने के दौरान IP द्वारा उपलब्ध कराई गई अविश्वसनीय डाटाग्राम सेवा का उपयोग करता करता है, किंतु एप्लीकेशन प्रोग्राम्स के लिए हमें एक भरोसेमंद डाटा डिलीवरी सेवा देता है। हमें कार्यकुशल डाटा ट्रासफर प्रदान करने के लिए TCP इंटरनेट में होने वाले लॉस या डिले की क्षतिपूर्ति करता है तथा यह कार्य वाले लॉस या डिले की क्षतिपूर्ति करता है तथा यह कार्य वह उसके अंतगर्त आने वाले नेटवर्क्स और राउटर्स पर कोई अतिरिक्त भार डाले बिना ही सम्पन्न करता है।

6.2 ट्रांसमिशन कंट्रोल प्रोटोकॉल :

विश्वसनीयता ट्रांसपोर्ट प्रोटोकॉल का उत्तरदायित्व है, डाटा को भेजने तथा प्राप्त करने के लिए एप्लीकेशन ट्रांसपोर्ट सर्विस से कम्यूनिकेट करती है। TCP/IPसमूह में ट्रांसमिशन कंट्रोल प्रोटोकॉल (TCP)हमें भरोसेमंद ट्रांसपोर्ट सेवा प्रदान करता है, इसलिए महत्वपूर्ण है। हालांकि अन्य प्रोटोकॉल्स भी बनाए गए है, पर सामान्य उद्देश्य वाले किसी ट्रांसफर प्रोटोकॉल ने बेहतर कार्य प्रमाणित नहीं किया है। परिणामस्वरूप अधिकांश एप्लीकेशन TCP का उपयोग करने के लिए ही बनाई जाती हैं।

हम संक्षेप में कह सकते हैं कि ट्रांसफर प्रोटोकॉल हमें वह विश्वसनीयता प्रदान करते हैं, जो अनेक एप्लीकेशन के लिए मूलभूत रूप से महत्वपूर्ण होती है।

एप्लीकेशन को TCP द्वारा प्रदान की जानेवाली सेवा :

एप्लीकेशन प्रोग्राम के दृष्टिकोण के अनुरूप TCP द्वारा दी जाने वाली सेवा की सात मुख्य विशेषताएँ होती है –

1. कनेक्शन अनुकूलन : TCP हमें ऐसी कनेक्शन उन्मुखी सेवा प्रदान करता है, जिसमें एप्लीकेशन को सर्वप्रथम डेस्टिनेशन से कनेक्शन के लिए रिक्वेस्ट करना पड़ती है और फिर उस कनेक्शन का उपयोग डाटा ट्रांसफर के लिए किया जाता है।

2. पॉईंट–टू–पॉईंट कम्यूनिकेशन : प्रत्येक TCP कनेक्शन में बिल्कुल सही दोएण्ड–पॉईंट्स होते हैं।

3. सम्पूर्ण विश्वसनीयता : TCP यह सुनिश्चित करता है कि कनेक्शन के आर–पार भेजा जाने वाला डाटा बिल्कुल ठीक उसी प्रकार से डिलीवर हो जैसा कि उसे भेजा गया था, न तो कोई डाटा छूट पाए और न ही वह क्रम से हट कर हो।

4. फुल डुप्लेक्स कम्यूनिकेशन : TCP कनेक्शन, डाटा को दोनों ही दिशा में प्रवाहित होने तथा दोनों ही एप्लीकेशन प्रोग्राम को किसी भी समय डाटा भेजने की अनुमति देता हैं। TCP दोनों ही दिशाओं मे आऊटगोइंग तथा इनकमिंग डाटा संग्रहीत कर सकता है।

5. स्ट्रीम इंटरफेस : हम कह सकते हैं कि TCP हमें ऐसा स्ट्रीम इंटरफेस प्रदान करता है, जिसमें कोई एप्लीकेशन एक संपूर्ण कनेक्शन पर ऑक्टेट्स (आठ–आठ के समूह) की निरंतर सीक्वेंस भेजती है। अर्थात् TCP हमें रेकॉर्ड्स का नोटेशन प्रदान नहीं करता है तथा यह भी सुनिश्चित नहीं करता है कि रिसीविंग एप्लीकेशन को डाटा उसी आकार के टुकड़ों में डिलीवर किया जाए जिस तरह से सेंडिंग एप्लीकेशन ने उन्हें ट्रांसफर किया था।

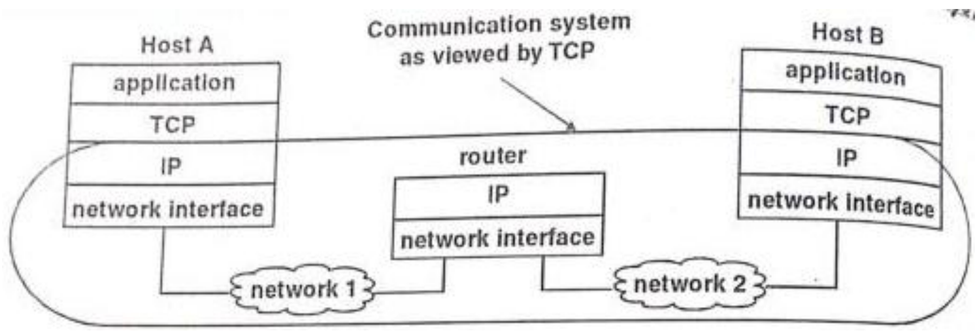
6. भरोसेमंद कनेक्शन स्टार्टअप : दो एप्लीकेशन द्वारा एक कनेक्शन निर्मित किए जाने के दौरान TCP की आवश्यकता होती है। दोनों को ही इस नए कनेकशन के लिए सहमत होना चाहिए। दोनों को ही इस नए कनेक्शन के लिए सहमत होना चाहिए। पूर्ववर्ती कनेक्शन्स में प्रयुक्त किए गए ड्प्लीकेट पैकेट्स को वैध रिसपांसेस के रूप में नहीं देखा जाएगा या उनके द्वारा नए कनेक्शन में अनय कहीं हस्तक्षेप नहीं किया जा सकेगा।

7. सम्मानजनक कनेक्शन शटडाउन : किए जाने की रिक्वेस्ट करता है। कनेक्शन बंद किए जाने के पूर्व TCP संपूर्ण डाटा की विश्वसनीय डिलीवरी की गारंटी देता है।

एण्ड–टू–एण्ड सेवा तथा डाटाग्राम :

TCP मैसेजेस को ले जाने के लिए IPका उपयोग करता है। सभी TCP मैसेज एक IP डाटाग्राम में उपस्थित होते हैं तथा इंटरनेट के आर–पार भेजे जाते हैं। जब डेस्टिनेशन होस्ट पर डाटाग्राम आता है, तो IP द्वारा TCP को डाटा को डाटा पास किया जाता है। चूँकि TCP द्वारा मैसेजेस को ले जाने के लिए ही IPका उपयोग किया जाता है, इसलिए IPमैसेजेस को पढ़ने या समझने का प्रयास नहीं करता है। इस प्रकार TCPद्वारा IPको एक ऐसे पैकेट कम्यूनिकेशन के दो एण्ड पॉईंट्स पर होस्टस को कनेक्ट करें और IPद्वारा प्रत्येक TCP मैसेज को ट्रांसफर किए जाने वाले डाटा के रूप में लिया जाता है।

TCP और IPसॉफ्टवेयर के मध्य संबंध को दर्शाने वाले दो होस्ट्स और राउटर के साथ इंटरनेट के एक उदाहरण से चित्र 21.2 द्वारा समझाया गया है।

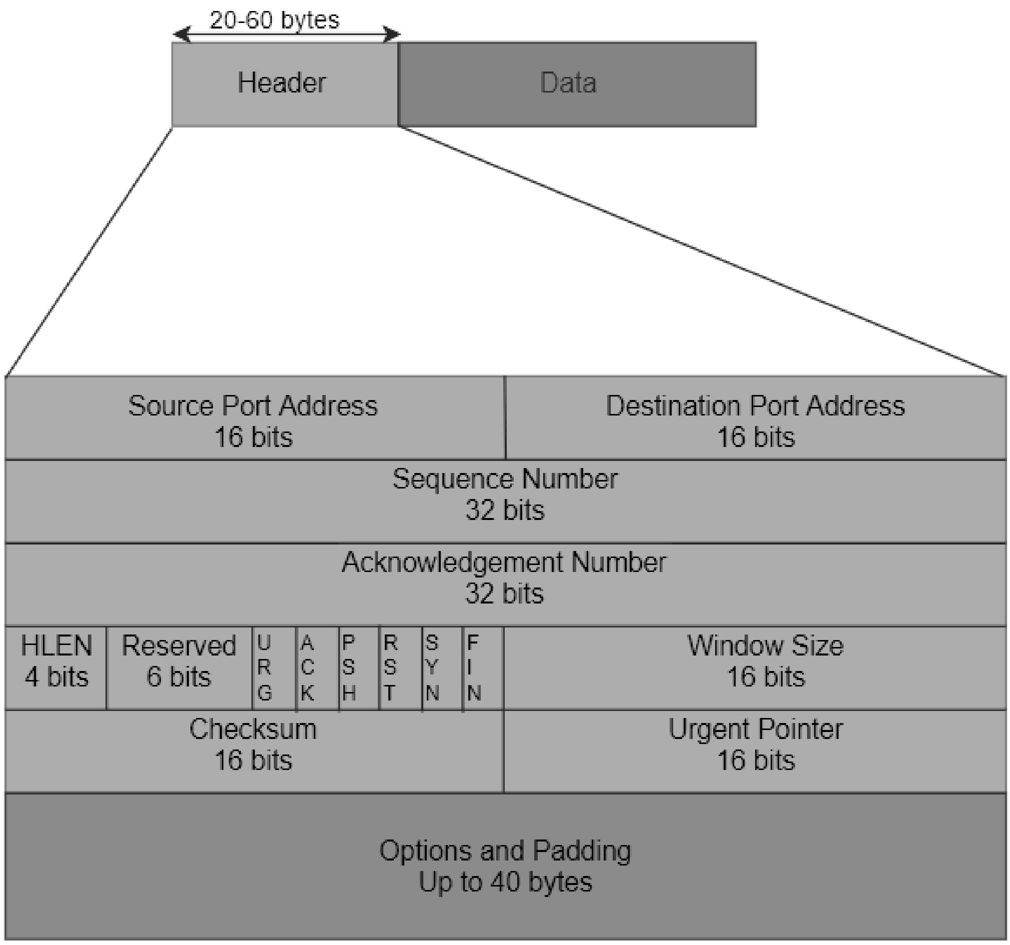


चित्र 6.2: ट्रांसपोर्ट लेयर कम्युनिकेशन TCP प्रोटोकॉल के साथ

6.2.1 TCP सेगमेंट :

IPमें डाटा की एक यूनिट जो एक बार में ट्रांसमिट की जाती है, IPडाटाग्राम कहलाती है।UDP में भी इसे डाटाग्राम के रूप में जाना जाता है अर्थात् UDP में भी इसे डाटाग्राम के रूप में जाना जाता है अर्थात् UDP डाटाग्राम। किन्तु TCP में ट्रांसफर किए जाने वाले डाटा की एक यूनिट को TCP सेगमेंट के रूप में जाना जाता है। चूँकि TCP हमें स्ट्रीम उन्मुखी डाटा सेवा प्रदान करता है, इसलिए यह ट्रांसफर की यूनिट के लिए सेगमेंट की अवधारणा का उपयोग करता है।

20 से 60 बाईट वाले हैडर के उपरांत एल्पीकेशन प्रोग्राम के डाटा से सेगमेंट निर्मिट होता है। यदि कोई विकल्प नहीं होते है, तो हेडर 20 बाईट्स का होता है और यदि यह कुद विकल्पों से बना हो तो 60 बाईट्स तक का होता है। कुद हेडर फील्ड्स की व्याख्या निम्नानुसार हैं –



चित्र 6.3: TCP सेग्मेंट्स

1. सोर्स पोर्ट एड्रेस : यह 16 बिट (2 बाईट्स) की फील्ड है, जो सेगमेंट भेजने वाले होस्ट में एप्लीकेशन प्रोग्राम की पोर्ट संख्या को परिभाषित करती है। यह UDP हेडर में सोर्स पोर्ट एड्रेस जैसे ही एक समान उद्देश्य के रूप में कार्य करती है।

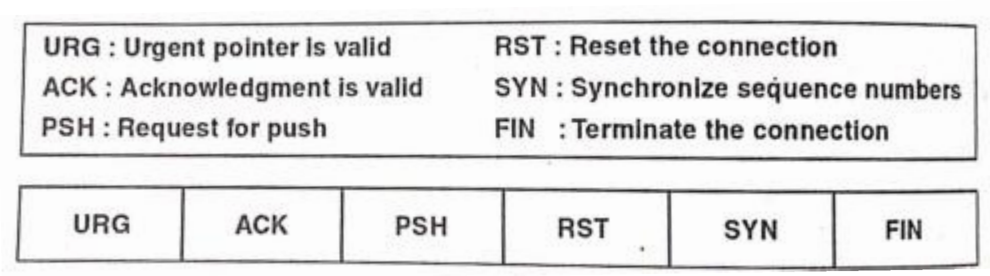
2. डेस्टिनेशन पोर्ट एड्रेस : यह 16 बिट (2 बाईट्स) की फील्ड है, जो सेगमेंट प्राप्त करने वाले होस्ट में एप्लीकेशन प्रोग्राम की पोर्ट संख्या को परिभाषित करती है।

3. सीक्वेंस नंबर : 32 बिट (4 बाईट्स) की यह फील्ड उस संख्या को परिभाषित करती है, जो इस सेगमेंट में धारित डाटा के प्रथम बाईट को प्रदान किया जाता है। जैसा हम जानते ही हैं कि TCP एक स्ट्रीम ट्रांसपोर्ट प्रोटोकॉल है।

4. एकनॉलेजमेंट नंबर : 32 बिट (4 बाईट्स) की यह फील्ड उस बाईट संख्या को परिभाषित करती है, जिसकी दूसरे सिरे पर की जा रही प्रोसेस से सेगमेंट के सोर्स को

प्राप्त होने की अपेक्षा रही है। यदि होस्ट दूसरे होस्ट की ओर से बाईट संख्या n को सफलापूर्वक प्राप्त करता रहता है, तो वह एकनॉलेजमेंट नंबर के रूप में n+1को परिभाषित करेगा, जो दूसरे होस्ट की स्ट्रीम पर n+1लोकेशन से प्रारंभ होने वाले डाटा की अपेक्षा को दर्शाता है।

5. हेडर लेंथ : यह चार बिट फील्ड TCP हेडर की लंबाई को दर्शाती है। यह TCP हेडर में चार बाईट शब्दों की संख्या के बराबर होती है। हेडर की लंबाई 20 और 60 बाईट्स के मध्य हो सकती है। अतः इस फील्ड की वेल्यू 5(5×4=20)और 15 (15×4=60) के मध्य हो सकती है।

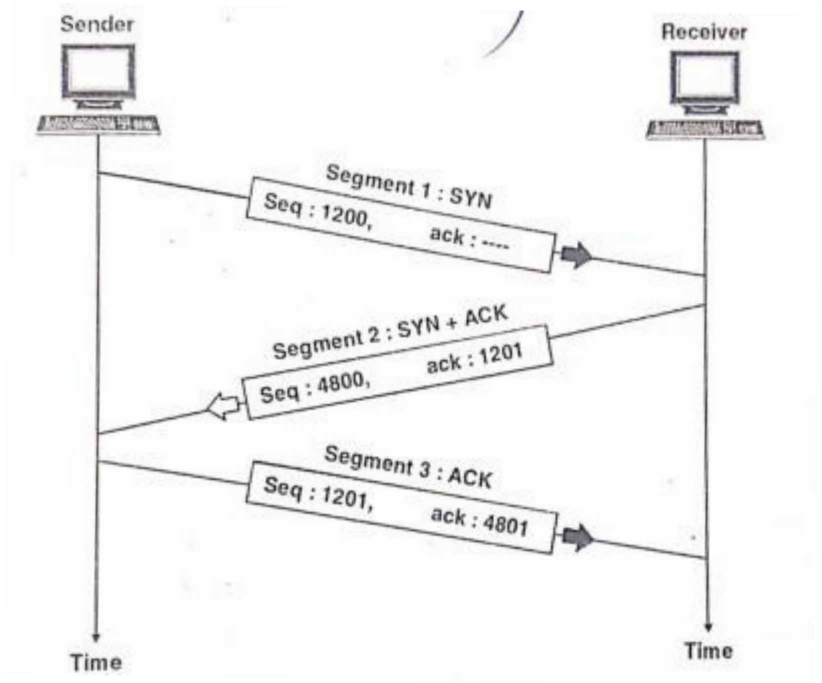


चित्र 6.4: कण्ट्रोल बिट

6.2.2 थ्री–वे हैंडशेकिंग :

ऊपर उललेखित की गई कनेक्शन स्थापना थ्री–वे हैंडशेकिंग कहलाती है। इस प्रोसीजर में क्लाईट कहलाने वाला एक एप्लीकेशन प्रोग्राम, ट्रांसपोर्ट लेयर प्रोटोकॉल के रूप में TCP का उपयोग करते हुए सर्वर कहलाने वाले दूसरे एप्लीकेशन प्रोग्राम से कनेक्शन निर्मित करना चाहता है।

थ्री–वे हैंडशेकिंग प्रोसीजर सर्वर के साथ प्रारंभ होता है। सर्वर प्रोग्राम अपने TCP को अवगत कराता है कि वह कनेक्शन स्वीकार करने के लिए तैयार है। यह पेसिव ओपन के लिए एक रिक्वेस्ट कहलाती है।



चित्र 6.5: थ्री वे हैंडशेकिंग प्रोसेस

क्लाईंट प्रोग्राम, एक्टिव ओपन के लिए एक रिक्वेस्ट निर्मिट करता है। सर्वर से कनेक्ट होने की इच्छा रखने वाला क्लाईंट अपने TCP को अवगत कराता है कि उसे एक विशिष्ट सर्वर से जुड़ने की आवश्यकता है। अब क्लाईंट्स TCPचित्र 6.5 में दर्शाए अनुसार थ्री–वे हैंडशेकिंग प्रक्रिया प्रारंभ कर सकते है।

प्रक्रिया के चरण निम्नानुसार हैं :

क्लाईंट द्वारा SYNबिट सेट के साथ भेजे गए प्रथम सेगमेंट को SYN सेगमेंट के रूप में जाना जाता है। सेगमेंट में सोर्स और डेस्टिनेशन पोर्ट संख्याएँ सम्मिलित रहती हैं। डेस्टिनेशन पोर्ट संख्या उस सर्वर को स्पष्ट रूप से परिभाषित करती है, जिसके साथ क्लाइंट को कनेक्टेड होने की आवश्यकता है। सेगमेंट में क्लाईंट की ओर सर्वर को भेजे जाने वाले डाटा के बाईट्स की नंबरिंग के लिए प्रयुक्त किया जाने वाला क्लाईंट का इनिशियलाईजोशन सीक्वेंस नंबर (ISN)भी सम्मिलित रहता है।

सर्वर द्वितीय सेगमेंटSYNतथा ACK सेगमेंट प्रेषित करता है। इस सेगमेंट का दोहरा उद्देश्य होता है। पहला, यह ACK फ्लैग और एकनॉलेजमेंट नंबर फील्ड का उपयोग करते हुए प्रथम सेगमेंट प्राप्त होने की अभिस्वीकृति देता है। क्लाईंट का इनिशियलाईजेशन

सीक्वेंस नंबर प्लस वन ही एकनॉलेजमेंट होता है। सर्वर को क्लाईट की विंडो साईज को भी परिभाषित करना पड़ता हैं। दूसरा, सेगमेंट को सर्वर के लिए इनिशयलाईजेशन सेगमेंट के रूप में प्रयुक्त किया जाता है। यह सर्वर के लिए इनिशियलाईजेशन सेगमेंट और सर्वर से भेजी गई बाईट्स की संख्या हेतु प्रयुक्त होने वाले इनिशियलाईजेशन सीक्वेंस नंबर से निर्मित होता है।

क्लाईंट तृतीय सेगमेंट भेजता हैं। यह केवल एक ACKसेगमेंट होता है। यह ACKफ्लैग और एकनॉलेजमेंट नंबर फील्ड का उपयोग करते हुए द्वितीय सेगमेंट प्राप्त होने की अभिस्वीकृति देता है।

6.3 यूजर डाटाग्राम प्रोटोकॉल (UDP):

यह ध्यान रखा जाना चाहिए कि उपलब्ध वर्तमान फिजिकल नेटवर्क टेक्नॉलाजी अत्यंत ही विश्वसनीय है। इनमें ऍरर की जॉंच–पड़ताल करने वाली तकनीक अंतः निर्मित होती है। फिर भी यह विश्वसनीयता बिल्कुल सटीक नहीं होती है, यह विभिन्न एण्ड एप्लीकेशन के लिए महत्वपूर्ण है। कुछ सीमा तक, डाटा के गुम अथवा करप्ट होने को सहन किया जा सकता है। इन सभी एप्लीकेशन को एक ऐसी विधि को आवश्यकता होती है, जिसके द्वारा वे नेटवर्क के आर–पार एक एप्लीकेशन प्रोग्राम या प्रोसेस से किसी अन्य होस्ट पर दूसरे को डाटा भेज सकें।

UDP वह प्रोटोकॉल है, जो इस अंतर को पाटता है। UDP हमें होस्ट–टू–होस्ट कम्यूनिकेशन के स्थान पर प्रोसेस–टू–प्रोसेस कम्यूनिकेशन प्रदान करता है।

UDP एक कनेक्शन रहित अविश्वसनीय ट्रांसपोर्ट प्रोटोकॉल है। यह प्रोसेस–टू–प्रोसेस कम्यूनिकेशन के अतिरिक्त IP सेवाओं में और कुछ भी नहीं जोड़ता है। यह अल्प सीमा तक ऍरर चैकिंग भी सम्पन्न कर लेता है

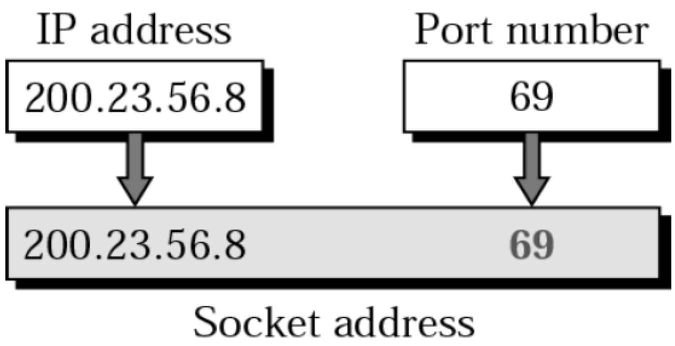
प्रोसेस–टू–प्रोसेस कम्यूनिकेशन :

UDP का अध्ययन करने के पूर्व पहले हमें होस्ट–टू–होस्ट कम्यूनिकेशन और प्रोसेस–टू–प्रोसेस कम्यूनिकेशन को जानना तथा उनके मध्य अंतर को समझना होगा।

IPदो होस्ट्स के मध्य कम्यूनिकेशन के लिए जिम्मेदार होता है। नेटवर्क लेयर प्रोटोकॉल के रूप में, IP केवल डेस्टिनेशन होस्ट सिस्टम के लिए ही मैसेज ग्रहण कर सकता है। यह एक अपूर्ण डिलीवरी होती है। मैसेज को अब भी सही प्रोसेस अथवा प्रोग्राम के चल रहे इंस्टेंस को संभलाए जाने की जरूरत है।

पोर्ट नंबर्स :

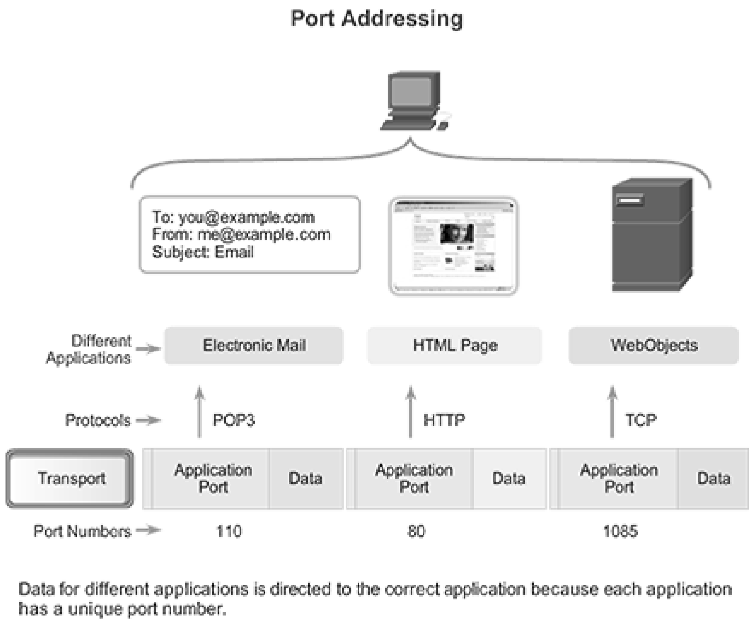
TCP/IP मॉडल में, TCP/IP कम्यूनिकेशन सेवा की आवश्यकता रखने वाली प्रत्येक प्रोसेस को पोर्ट नंबर नामक एक 16 बिट (2 बाईट) नंबर प्रदान किया जाता है। TCP/IP स्टैंडर्ड इस विशिष्ट पोर्ट नंबर को जानी पहचानी नेटवर्क एप्लीकेशन प्रोसेस में से कुछ के लिए परिभाषित करता है। इसी के चलते होस्ट मशीन पर चल रही नेटवर्क एप्लीकेशन प्रोसेस को विशिष्ट तौर पर पहचानना संभव हो पाता है।



चित्र 6.6: पोर्ट नंबर **एड्रेसिंग**

कम्यूनिकेशन के लिए हमें निम्न को परिभाषित करना आवश्यक होता है –

- लोकल होस्ट
- लोकल प्रोसेस
- रिमोट होस्ट
- रिमोट प्रोसेस



चित्र 6.7: पोर्ट नंबर **एड्रेसिंग**

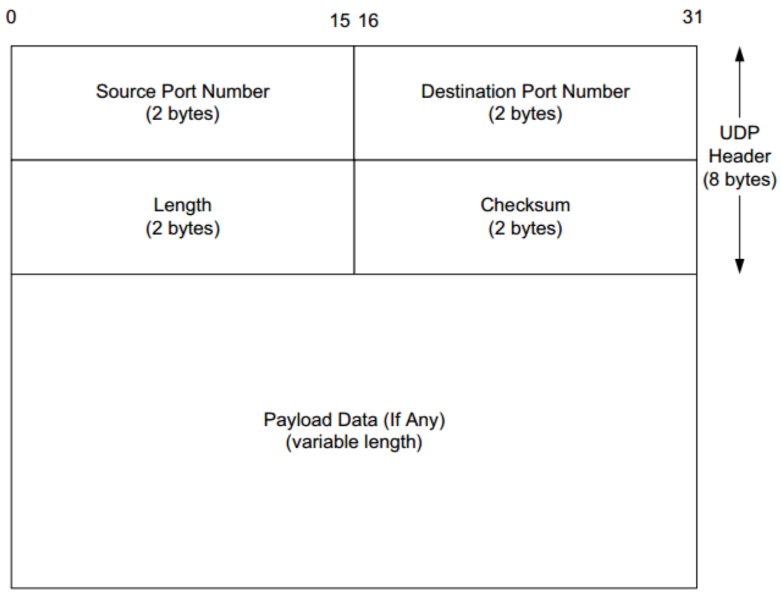
IP एड्रेसेस का उपयोग करते हुए लोकर और रिमोट होस्ट पहचाने जाते हैं। प्रोसेसेज को परिभाषित करने के लिए हमें सेकण्ड आयडेंटिफॉयर्स, जो पोर्ट नंबर्स कहलाते है, की आवश्यकता होती है। TCP/IP प्रोटोकॉल समूह में पोर्ट नंबर्स 2 और 65,535 के मध्य पूर्ण संख्या (इंटीजर्स) होते हैं।

क्लाईंट प्रोग्राम को क्लाईंट होस्ट पर चल रहे UDP सॉफ्टवेयर द्वारा रेंडमलरी चुना गया एक पोर्ट नंबर प्रदान किया जाता है। यह क्षणिक पोर्ट नंबर होता है।

सर्वर प्रोसेस को भी एक पोर्ट नंबर दिया जाना आवश्यक है। यह पोर्ट नंबर रेंडमली नहीं चुना जा सकता है। यदि सर्वर साईट पर सर्वर प्रोसेस चलाने वाले कम्प्यूटर को पोर्ट नंबर के रूप में एक रेंडम नंबर प्रदान कर दिया जाता है, तो क्लाईंट की वह प्रोसेस जिसे उस सर्वर को एक्सेस किए जाने की आवश्यकता है और उसकी सेवाओं का उपयोग करना चाहती है, पोर्ट नंबर नहीं जान पाएगी। सामान्यतः इसका एक समाधान यह हो सकता है कि एक विशेष पैकेट भेजा जाए, किंतु विशिष्ट सर्वर के पोर्ट नंबर की रिक्वेस्ट की जाए, किंतु इसे अधिक ओवरहेड की जरूरत होती है। TCP/IP ने सर्वर्स के लिए यूनिवर्सल पोर्ट नंबर्स का उपयोग किए जाने का निर्णय लिया है, ये वेल–नोन पोर्ट नंबर्स कहलाते है।

6.3.1 UDP डाटाग्राम :

यूजर डाटाग्राम के रूप में पहचाने जाने वाले UDP पैकेट्स में आठ बाईट्स का एक फिक्स्ड साईज का हेडर होता है। चित्र 6.8 यूजर डाटाग्राम का फॉर्मेट दर्शाता है।



चित्र 6.8: UDP सेगमेंट

1. सोर्स पोर्ट नंबर : यह UDP डाटाग्राम को ट्रांसमिट करने वाले सोर्स प्रोसेस का पोर्ट नंबर होता है। यह 16 बिट्स (2 बाईट) लंबा होता है। यदि सोर्स प्रोसेस एक क्लाईंट है (रिक्वेस्ट भेजने वाला क्लाईंट) तो अधिकांश मामलों में पोर्ट नंबर एक क्षणिक पोर्ट नंबर होता है। यदि सोर्स प्रोसेस एक सर्वर है। (रिस्पांस भेजने वाला सर्वर) तो अधिकांश मामलों मं पोर्ट नंबर एक वेल–नोन पोर्ट नंबर होता है।

2. डेस्टिनेशन पोर्ट नंबर : यह उस डेस्टिनेशन प्रोसेस का पोर्ट नंबर होता है, जिसके लिए वह UDP डाटाग्राम बनाया गया है। यह भी 16 बिट्स लंबा होता है। इसकी विशेषताएँ सोर्स पोर्ट नंबर के समरूप ही होती हैं।

3. लैंथ : 16 बिट की यह फील्ड, हेडर और डाटा सहित UDP डाटाग्राम की कुल लंबाई परिभाषित कर सकती हैं। इसकी न्यूनतम लंबाई 8 बाईट्स होती है, जो यह स्पष्ट करती है कि यूजर डाटाग्राम में कोई डाटा नहीं है, बल्कि मात्र हेडर ही है। किंतु यह ध्यान दिया जाना चाहिए कि प्च के पास उसके डाटाग्राम के लिए 65,535 बाईट्स की सीमित होती है। अतः डाटा की लंबाई 0 से 65,507 (65,535–20–8) बाईट्स (बीस बाईट्स IP हेडर के लिए और 8 बाईटस UDP हेडर के लिए) के मध्य हो सकती है।

4. चैकसम : यह फील्ड संपूर्ण यूजर डाटाग्राम (हेडर सहित डाटा) में ऍरर्स का पता लगाने के लिए प्रयुक्त की जाती है। IP जैसे लेयर प्रोटोकॉल्स के विपरीत, जो हमें केवल उनके हेडर के लिए ही चैकसम प्रदान करते हैं, यह हमें ऐसे डाटाग्राम के लिए चैकसम प्रदान करता है, जिसमें यूजर प्रोसेस द्वारा भेजा गया डाटा भी शामिल होता है।

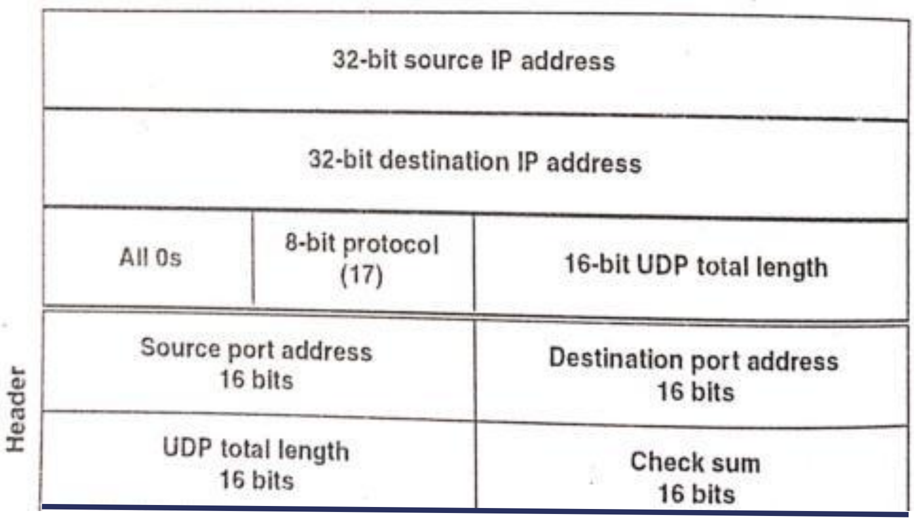
UDP चैकसम की गणना :

चैकसम गणना के पीछे, IP चैकसम गणना के समान ही अंकगणित होता है। तथापि, UDP चैकसम की गणना IP और ICMP हेतु एक की गणना से भिन्न होती है। यहाँ चैकसम में तीन सेक्शन्स सम्मिलित किए जाते हैं –

1. स्यूडो हेडर : स्यूडो हेडर IP पैकेट के हैडर का वह भाग होता है, जिसमें यूजर डाटाग्राम Os की कुद फील्ड्स के साथ ट्रांसमिशन के लिए एनकेप्स्यूलेट किया जाता है।

2. UDP हेडर : इस UDP डाटाग्राम के लिए हेडर।

3. यूजर डाटा : अपर लेयर द्वारा भेजा गया डाटा।



चित्र 6.9: चेकसम फील्ड

सोर्स पर चैकसम की गणना :

सोर्स होस्ट सिस्टम पर चैकसम की गणना करने के लिए सेंडर (भेजने वाला) इन चरणों का अनुपालन करता है –

1. UDP यूजर डाटाग्राम के साथ स्यूडो–हेडर जोड़ना।

2. यदि बाईट्स की कुल संख्या सम नहीं हे, तो पेडिंग (सभी Os) की एक बाईट जोड़ना। पेडिंग केवल चैकसम की गणना किए जाने के उद्देश्य से ही की जाती है और इसके उपरांत उसे अनदेखा कर दिया जाएगा।

3. चैकसम फील्ड्स को शून्य से भरना।

4. कुल बिट्स को 16 बिट (दो बाईट) वर्ड्स सेक्शन्स में विभाजित करना।

5. एक के पूरक अंकगणित का उपयोग करते हुए सभी 16 बिट सेक्शन्स को जोड़ना।

6. परिणाम को एक के पूरक में लेना (Os को 1s में और सभी वास्तविक 1s को Os में बदलना) जो एक 16 बिट चैकसम नंबर हो।

6.3.2 UDP के उपयोग :

UDP प्रोटोकॉल के कुछ उपयोग निम्नानुसार हैं –

1. UDP उस प्रोसेस के लिए सहायक है, जिसे साधारण रिक्वेस्ट–रिस्पांस कम्यूनिकेशन की आवश्यकता होती है और फ्लो व ऍरर कंट्रोल से थोड़ा ही संबंध होता हो। यह आमतौर पर FTP जैसी उस प्रोसेस के लिए प्रयुक्त नहीं की जाती है, जिसे आवश्यक रूप से ऍरर और फ्लो कंट्रोल के साथ विपुल मात्रा में डाटा भेजने की जरूरत हो।
2. UDP उस प्रोसे के लिए उपयोगी रहती है, जिसके साथ आंतरिक फ्लो और ऍरर कंट्रोल विधि हो। उदाहरण के लिए, ट्रिविअल फाईल ट्रांसफर प्रोटोकॉल ()TFTP प्रोसेसे में फ्लो और ऍरर कंट्रोल सम्मिलित रहते हैं। यह UDP का आसानी से उपयोग कर सकती है।

3. UDP मल्टीकॉस्टिंग और ब्रॉडकॉस्टिंग के लिए उपयोगी ट्रांसपोर्ट प्रोटोकॉल है। UDP सॉफ्अवेयर में मल्टीकॉस्टिंग और ब्रॉडकॉस्टिंग क्षमताएँ अंतःनिर्मित होती है, किंतु TCP सॉफ्टवेयर में नहीं।
4. SNMP जैसी मैनेजमेंट प्रोसेस के लिए UDP को प्रयुक्त किया जाता है।
5. रूटिंग इंफॉर्मेशन प्रोटोकाल (RIP) जैसे कुछ रूट अपडेटिंग प्रोटोकॉल्स के लिए UDP को प्रयुक्त किया जाताह ै।
6. आजकल की महत्वपूर्ण मल्टीमीडिया एप्लीकेशन जैसे –VoIP (वॉइस ओवर IP– जिसका उपयोग करके कोई व्यक्ति जिसके पास टेलीफोन हो, वह इस प्रोटोकाल के माध्यम से टेलीफॉन कॉल लगाकर किसी दूसरे व्यक्ति से बातचीत कर सकता है) और एप्लीकेशन लेयर पर डाटा ट्रांसफर के लिए वीडियो कॉन्फ्रेसिंग एप्लीकेशन RTP (रीयल टाईम प्रोटोकॉल) के रूप में पहचाने जाने वाले प्रोटोकॉल का उपयोग करते है।

7.1 एप्लीकेशन लेयर का परिचय :

TCP/IP में लेयर्स यथार्थतः OSI लेयर्स से संबंधित नहीं होती हैं। इसके कारणों में से एक यह हो सकता है कि TCP/IP प्रोटोकॉल समूह OSI मॉडल के पहले ही डिजाइन कर लिए गये थे। TCP/IP प्रोटोकॉल समूह OSI मॉडल के पहले ही डिजाइन कर लिए गए थे। TCP/IP में एप्लीकेशन लेयर संयुक्त रूप से OSI मॉडल की सेशन, प्रेजेंटेशन और एप्लीकेशन लेयर्स के समकक्ष है। इसका अभिप्राय यह है कि इन तीनों लेयर्स से संबंधित संपूर्ण कार्यप्रणाली को एक अकेली एप्लीकेशन लेयर में ही हेंडल किया जाता है। किंतु यह ध्यान रखना चाहिए कि विभन्न एप्लीकेशन को सेशन और प्रेजेंटेशन लेयर्स द्वारा प्रस्तुत की जाने वाली सेवाओं की आवश्यकता नहीं होती है। जिन एप्लीकेशन को इन सेवाओं की आवश्यकता नहीं होती है। जिन एप्लीकेशन्स को इन सेवाओं की जरूरत है, वे इसे हेंडल कर सकती हैं।

एप्लीकेशन लेयर के कार्य :

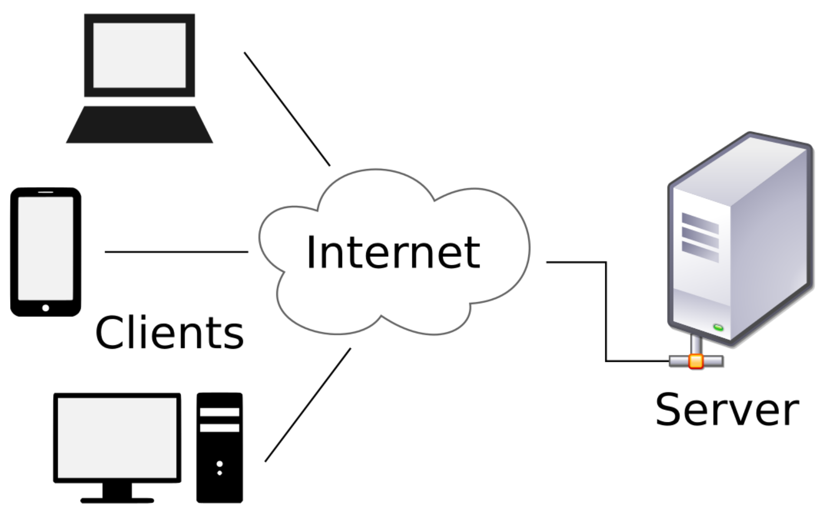
एप्लीकेशन लेयर में वह प्रोटोकॉल सन्निहित होता है, जो यूजर को नेटवर्क एक्सेस करने की अनुमति प्रदान करें। एप्लीकेशन लेयर पर विभिन्न प्रकार के प्रोटोकॉल्स संचालित किए जाते है, जिनमें से कुछ तालिका में दिए गए हैं।

एप्लीकेशन लेयर प्रोटोकॉल्स में ई–मेल, ब्राउजर्स तथा ऑफिस एप्लीकेशन्स जैसे एण्ड यूजर एप्लीकेशन प्रोग्राम्स को सम्मितित नहीं किया जाता है, क्योंकि ये यूजर के कम्प्यूटर में ही विद्यमान होते हैं। इनके स्थान पर प्रोटोकॉल्स में नेटवर्क आधारित वे सेवाएँ शामिल होती है, जो इन एप्लीकेशन्स को सपोर्ट करती है।

7.2 क्लाइंट सर्वर मॉडल :

TCP/IO अथवा इंटरनेट का उद्देश्य यूजर्स को डाटा कम्यूनिकेशन सेवाएँ प्रदार करना है। किसी अन्य होस्ट से इंफॉर्मेशन एक्सेस करने के दौरान भौगोलिक दूरियो की वजह से जो बाधाँए उत्पन्न होनी चाहिए।

यदि लोकल होस्ट कम्प्यूटर पर यूजर किसी दूरस्थ स्थित कम्प्यूटर से सेवा ग्रहण करने का प्रयास करता है, तो कम्प्यूटर इस विशिष्ट कार्य को सम्पन्न करने के लिए कुछ खास–प्रोग्राम्स को निष्पादित करेगा। इनमें से एक प्रोग्राम वर्ड प्रोसेसिंग करेगा, एक प्रोग्राम वेबसाईट को ब्राउस करेगा तथा इसी प्रकार अन्य कार्य होंगे।

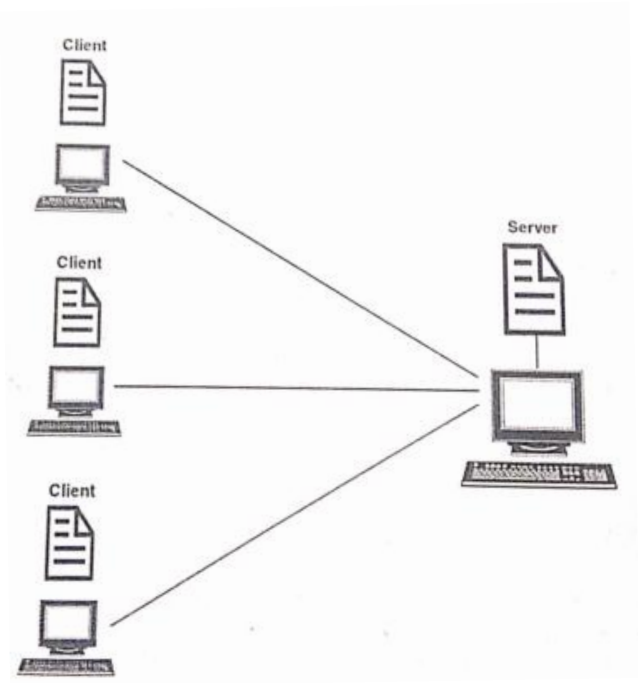


चित्र 7.1: क्लाइंट सर्वर मॉडल

दूसरे शब्दों में, डाटा कम्यूनिकेशन को ग्रहण करने के लिए कम्प्यूटर एक ऐसा प्रोग्राम चलाता है, जो डेस्टिनेशन कम्प्यूटर पर विद्यमान अन्य प्रोग्राम से सेवा के लिए रिक्वेस्ट करे। इसका अभिप्राय यह है कि इंटरनेट द्वारा जुड़े हुए दो कम्प्यूटर्स अपने–अपने प्रोग्राम चलाते हैं, एक सेवा प्रदान करने के लिए और दूसरा सेवा हेतु रिक्वेस्ट करने के लिए।

क्लाइंट :

क्लाइंट वह प्रोग्राम है, जो सर्वर से सेवा का आग्रह करते हुए लोकल होस्ट कम्प्यूटर पर चलाया जाए। क्लाइंट प्रोग्राम इन मायनों में सीमित होता है कि इसे यूजर (अथवा अन्य एप्लीकेशन प्रोग्राम) द्वारा प्रारंभ किया जाता है ओर सेवा पूर्ण हो जाने पर टर्मिनेट कर दिया जाता है। दूरस्थ होस्ट के IP एड्रेस और उस मशीन पर चल रहे विशिष्ट सर्वर प्रोग्राम के प्रसिद्ध पोर्ट एड्रेस का उपयोग करते हुए क्लाइंट कम्यूनिकेशन चैनल ओपन करता है इसे एक्टिव ओपन कहा जाता है।



चित्र 7.2: क्लाइंट सर्वर

सर्वर :

सर्वर वह प्रोग्राम है, जो दूरस्थ होस्ट कम्प्यूटर पर क्लाइंट्स को सेवा प्रदान करें। जब इसे प्रारंभ किया जाता है, तो यह क्लाइंट्स की ओर से आने वाली रिक्वेस्ट्स के लिए चैनल ओपन करता है, किंतु यह किसी सेवा को तक तक प्रारम्भ नहीं करता है, जब तक कि उसे ऐसा करने के लिए आग्रह न किया जाए। इसे पेसिव ओपन कहते है।

सर्वर प्रोग्राम एक असीमित प्रोग्राम है। जब इसे प्रारंभ किया जाता है, तो यह अनंत काल तक चलता रहता है, बशर्ते कि कोई समस्या उत्पन्न न हो जाए। यह क्लाइंट्स की ओर से आने वाली रिक्वेस्ट्स की प्रतीक्षा करता है। जैसे ही रिक्वेस्ट आती है, यह उस रिक्वेस्ट पर आगामी खण्ड में विवेचित अनुसार या तो पुनरावृत्ति करते हुए अथवा समवर्ती रूप में प्रतिक्रिया करता है।

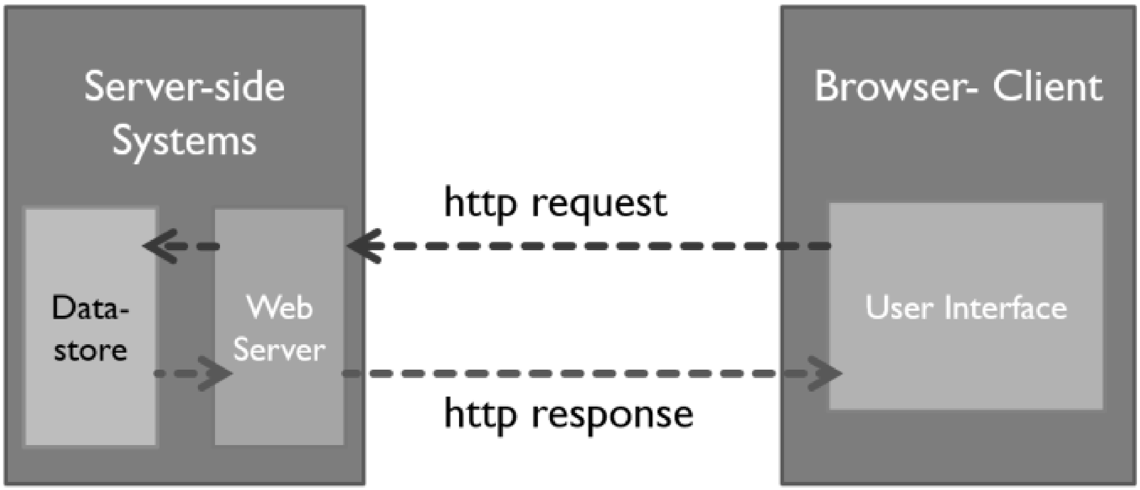
समवर्तिता :

यहाँ समवर्तिता (कॉनकरेंसी) शब्द एक साथ एक ही समय में चलने की क्षमता की ओर संकेत करता है। क्लाइंट्स और सर्वर्स दोनों ही कॉनकरेंट मोड में चल सकते हैं। क्लाइंट्स और सर्वर में समवर्तिता भिन्न–भिन्न होती है, जिसकी व्याख्या आगे दी जा रही है।

क्लाइंट्स में समवर्तिता :

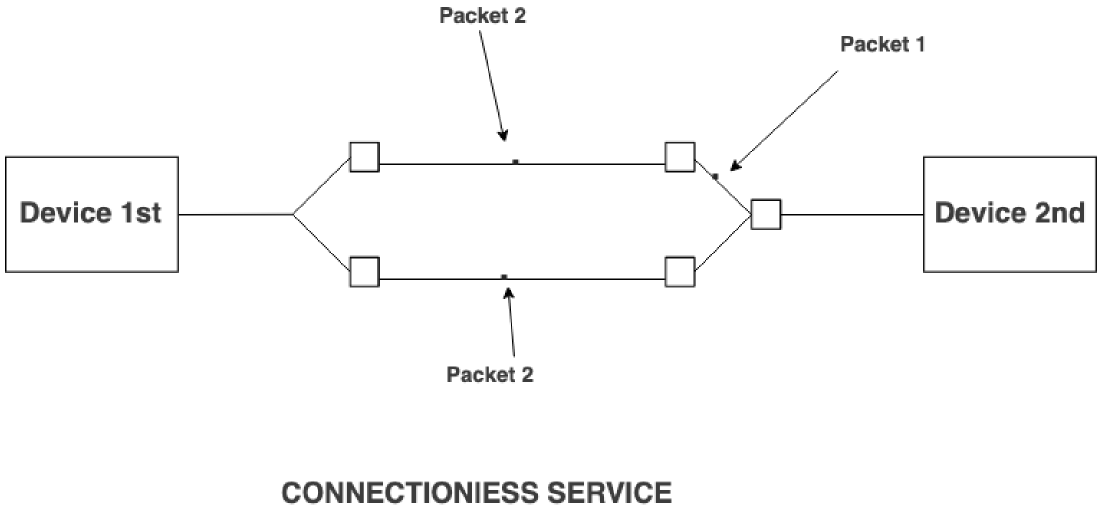
किसी कम्प्यूटर पर क्लाइंट्स या तो पुनरावृत्ति करते हुए (इटरेटिवली) अथवा समवर्ती रूप में (कॉनकरेंटली) चल सकते हैं। क्लाइंट्स के पुनरावृत्ति करते हुए चलने का अभिप्राय उनका एक के बाद एक चलना है। एक क्लाइंट प्रारंभ होता है, चलता है और इससे पहले कि कम्प्यूटर दूसरा क्लाइंट प्रारंभ करें, वह समाप्त हो जाता है।

सर्वर्स में समवर्तिता :



चित्र 7.3: **कनेक्शनलेस कम्युनिकेशन**

चूँकि एक इटरेटिव सर्वर एक बार में केवल एक ही रिक्वेस्ट को प्रोसेस कर सकता है, अस्तु वह रिक्वेस्ट प्राप्त करता है, उसे प्रोसेस करता है और दूसरी रिक्वेस्ट को हेंडल करने के पूर्व ही वह आग्रहकर्ता को रिस्पांस भेज देता है,। इस बीच में यदि किसी अन्य क्लाइंट की ओर से रिक्वेस्ट आती है, तो वह या तो उसे अस्वीकृत कर देता है या फिर जब तक वह सर्वर प्रथम रिक्वेस्ट को पूर्ण न कर दें, तब तक उस रिक्वेस्ट को प्रतीक्षारत रखता है।



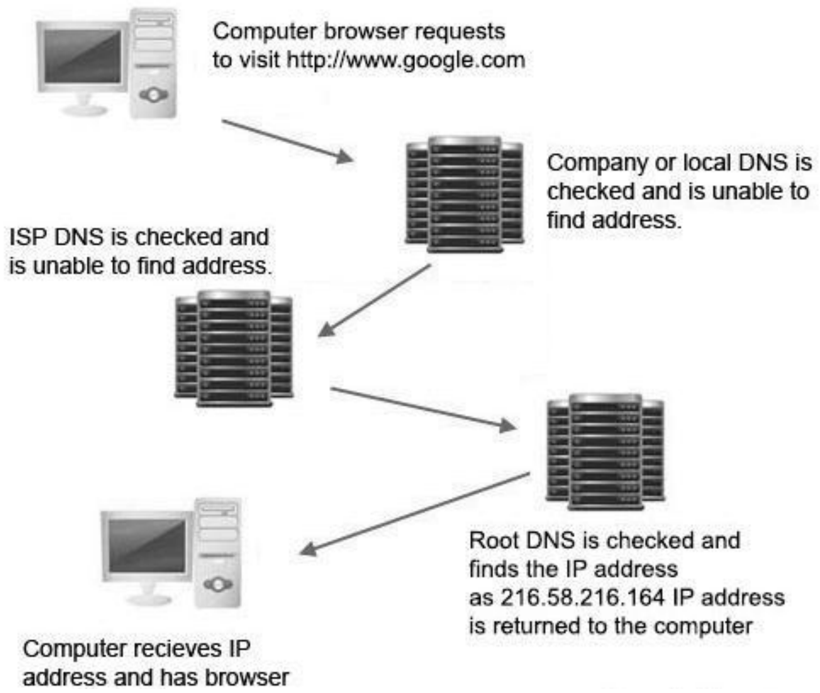
चित्र 7.4: कनेक्शनलेस ओरिएंटेड

7.3 डोमेन नेम सिस्टम

प्रस्तावना :

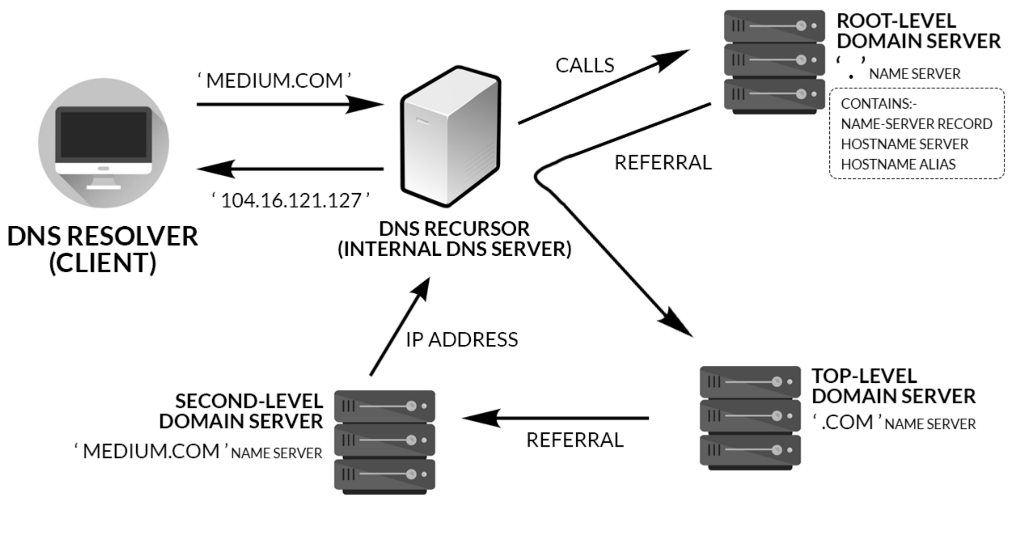
चूँकि TCP/IPमें IP एड्रेसेस बुनियादी अंग होते हैं, अस्तु इंटरनेट का उपयोग करने वाला कोई भी व्यक्ति यह जानता है कि यूजर्स को IP एड्रेसेस याद रखने या इंटर करने की आवश्यकता नहीं होती है। इसके अतिरिक्त कम्प्यूटर्स को भी सांकेतिक नाम दिए जाते हैं। एप्लीकेशन सॉफ्टवेयर यूजर को किसी विशिष्ट कम्प्यूटर की पहचान बनाने के लिए सांकेतिक नामों में किस एक को इंटर करने की अनुमति देता है।

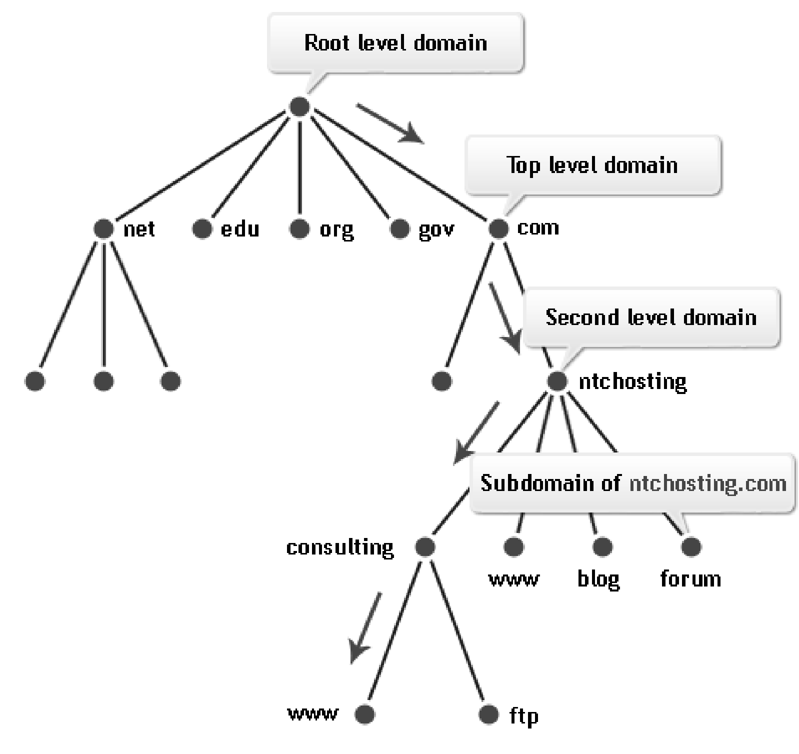
सांकेतिक नाम भले ही मानव के लिए उपयुक्त हो, किंतु कम्प्यूटर्स के लिए वे अनुपुक्त होते हैं। सांकेतिक नाम की तुलना में IP एड्रेस के बायनरी स्वरूप के अधिक सघन होने की वजह से उनके परिचालन में अल्प कम्प्यूटेशन की आवश्यकता होती है। किसी नाम की तुलना में एक एड्रेस कम मेमोरी लेता है और इसके नेटवर्क के आरपार प्रेषित करने में कम ही जरूरत होती है।



चित्र 7.5: डोमेन नेम सिस्टम

वह सॉफ्टवेयर जो कम्प्यूटर के नामें को उनके अनुरूप इंटरनेट एड्रेसेस में बदलता है, क्लाईंट–सर्वर आदान–प्रदान का एक रोचक उदाहरण प्रस्तुत करता है। नामों को डाटाबेस एक ही कम्प्यूटर में नही रखा जाता हे। इसके स्थान पर नामों संबंधी इंफॉर्मेशन इंटरनेट पर विभिन्न साईट्स पर स्थित सर्वर्स के अत्यंत व्यापक सेट के मध्य वितरित कर दी जाती है।





चित्र 7.6: रुट डोमेन नेम सिस्टम

DNS :

नेम रजिस्ट्रेशन और रिजॉल्यूशन के लिए होस्ट टेबल्स के उपयोग से उत्पन्न होने वाली समस्याओं से निपटने हेतु ARPANET के लिए उत्तरदायी लोगों ने पूर्णतः नई विधि निर्मित करने का निर्णय लिया। प्रथम दृष्टि में उनका प्राथमिक लक्ष्य विरोधाभासी प्रतीत होता है था – एक ऐसी विधि निर्मित करना जो उडमिनिस्ट्रेटर्स को बिना डुप्लीकेट नेम्स प्रदान करने में सहायक हो तथा सिंगल एक्सेस पाईंट पर निर्भर हुए बिना ही होस्ट नेम इंफॉर्मेयशन को दुनियाभर में अन्य एडमिनिस्ट्रेटर्स के उपलब्ध करा सके।

डोमेन नेमिंग:

डोमेन नेम सिस्टम द्वारा होस्टस् के नाम हेतु नेम स्पेस को प्रयुक्त करने तथा होस्ट नेम इंफॉर्मेशन से बनने वाले डाटाबेस दोनों में हाईअरर्किकल सिस्टम का उपयोग करते हुए वाछिंत लक्ष्य प्राप्त किया जाता हैं।

DNS नेम स्पेस ऐसे डोमेन पर आधारित होता हैं, जो कुछ इस प्रकार के हाईअरर्किकल स्ट्रक्चर में विद्यमान होते हैं, जैसे किसी फाईल सिस्टम में डायरेक्ट्री ट्री

होती है। डोमेन इस तरह से डॉयरेक्टरी के समरूप होता हैं कि वह या तो सबडोमेन (सबडॉयरेक्टरीज) का अथवा होस्ट्स (फाईल) से बना होता हैं। इससे जो स्ट्रक्चर बनता हैं, वह DNS ट्री (देखें चित्र 7.6) कहलाता हैं। सुपूर्ण इंटरनेट पर नेटवर्क एडमिनिस्ट्रेटर्स को विशिष्ट डोमेन हेतु उत्तरदायित्व प्रदान किए जाने का परिणाम संपूर्ण नेटवर्क के सिस्टम के मध्य फैले हुए डिस्ट्रीब्यूटेड डाटाबेस के रूप में सामने आता हैं।

इसका परिणाम यह होता हैं कि इंटरनेट पर प्रत्येक कम्प्यूटर की एक ऐसे DNS नेम द्वारा विशिष्ट पहचान बन जाती है, जो होस्ट नेम के साथ DNS ट्री की जड़ तक आने वाले उसकेसमस्त पेंरेट डोमेन्स के नाम से बनाता हैं। इन्हें पीरियड्स (.) के द्वारा पृथक किया जाता है। पीडियड्स के मध्य प्रत्येक नेम्स 63 केरेक्टर्स तक लंबे हो सकते है और संपूर्ण DNS नेम की कुल लम्बाई 255 केरेक्टर्स की हो सकती है। इसमें होस्ट और नेम्स केस सेंसिटिव नहीं होते हैं तथा लन वेल्यू (कोई केरेक्टर नहीं) को छोड़कर कोई भी वेल्यू ले सकते है, जो DNS ट्री की जड़ को दर्शाती हो।

कम्प्यूटर की संरचना :

जैसा हम जानते हैं कि इंटरनेट पर प्रयुक्त होने वाली नामकरण विधि डोमेन नेम सिस्टम (DNS) कहलाती है। वाक्य रचना के अनुसार प्रत्येक कम्प्यूटर नेम पीरियड्स द्वारा पृथक किए गए अल्फा –न्यूमेरिक सेगमेंट्स की सीक्वेंस से बनाता हैं। उदाहरणार्थ ABC विश्वविद्यालय के कम्प्यूटर विज्ञान विभाग में किसी कम्प्यूटर का डोमेन नेम होगा–

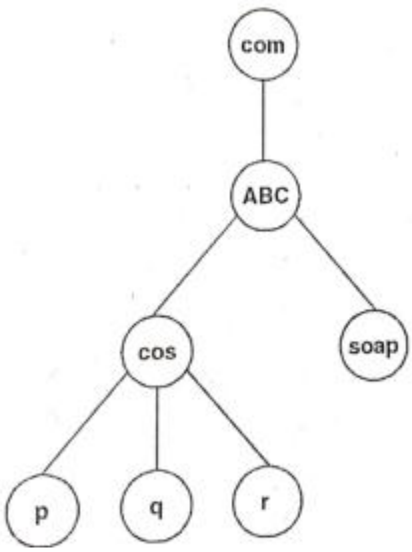
डोमेन नेम हाईअरार्किकल (पदानुक्रम अनुरूप) होते हैं। नेम का सर्वाधिक महत्वपूर्ण भाग में किसी पृथक कम्प्यूटर का नाम होता है। डोमेन नेम के अन्य सेगमेंट्स (खण्ड) उस समूह की पहचान होते है, जिसके पास उस नेम का स्वामित्व होता है।

डोमेन नेम सिस्टम सर्वाधिक महत्वपूर्ण सेगमेंट के लिए वेल्यूज प्रदर्शित करता हैं, जिसे DNS का टॉप लेवल कहते हैं। तालिका में संभावित टॉप लेवल डोमेन्स को सूचीबद्ध किया गया हैं। नेम स्पेस को और अधिक विभाजित करने तथा व्यावसायिक डोमेन में उत्पन्न होने वाली भीड़भाड़ को दूर करने के लिए 1997 में सात अतिरिक्त टॉप लेवल डोमेन प्रस्तावित केए गए थे। प्रस्तावित नेम्स में firm, dtore, web, arts, rec, info और nom शामिल थे।

Domain Name	Assigned to
Com	Commercial organization
edu	Educational institution
gov	Government organization
mil	Military group
net	Major network support center
org	Organization other than those above
arpa	Temporary ARPA domain (still used)
int	International organization
country code	A country

संगठन के अंतर्गत डोमेन नेम्स :

एक बार किसी संगठन को उपयुक्त डोमेन प्राप्त हो जाने के बाद वह संगठन तय कर सकता है कि अतिरिक्त हाईअरार्किकल संरचना बनाई जाए अथवा नहीं। हो सकता है के लघु कॉपोरेशन अतिरिाक्त हाईअरार्किकल का चुनाव नहीं करें, जबकि वृहद संगठन विभिन्न स्तरों का चयन कर सकता है। उदाहरण के लिए, यदि ABC कॉपेरेशन लघु हैं, तो हो सकता हैं कि वह सारे नाम इस रूप में रखने का निर्णय लें–

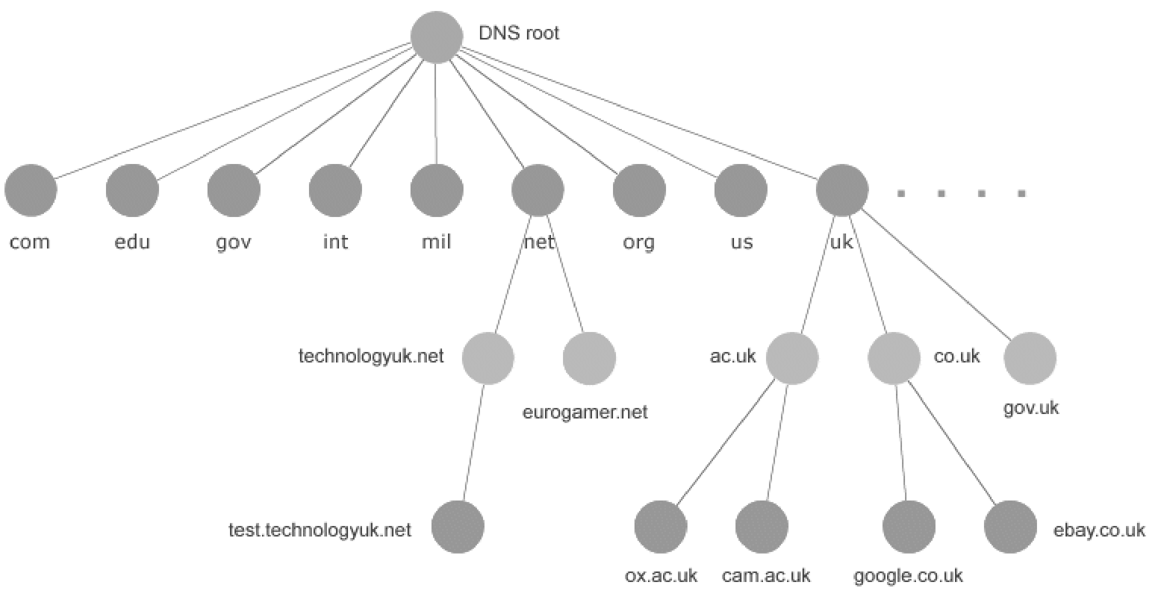


चित्र 7.7: डोमेन डिस्ट्रीब्यूशन

DNS क्लाईंट सर्वर मॉडल :

डोमेन नेमिंग सिस्टम के मुख्य फीचर्स में से एक स्वायत्तता हैं। सिस्टम को इस प्रकार से निर्मित किया जाता है कि प्रत्येक संगठन कम्प्यूटर्स को नेम्स आवंटित कर सकता है अथवा उन नेम्स को केन्द्रीय प्राधिकारी को सूचना दिए बिना बदल भी सकता है। नेमिंग हाईअरार्की किसी संगठन को किसी उपयुक्त सफिक्स के साथ समस्त नेम्स को नियंत्रित किए जाने की अनुमति देते हुए, स्वायत्तता प्राप्त करने में सहायता प्रदान करती है। इस प्रकार देवी अहिल्या विश्वविद्यालय ऐसा कोई भी नेम निर्मित करने अथवा उसे बदलने के लिए स्वतंत्र है, जो davv.edu के साथ समाप्त होता है।

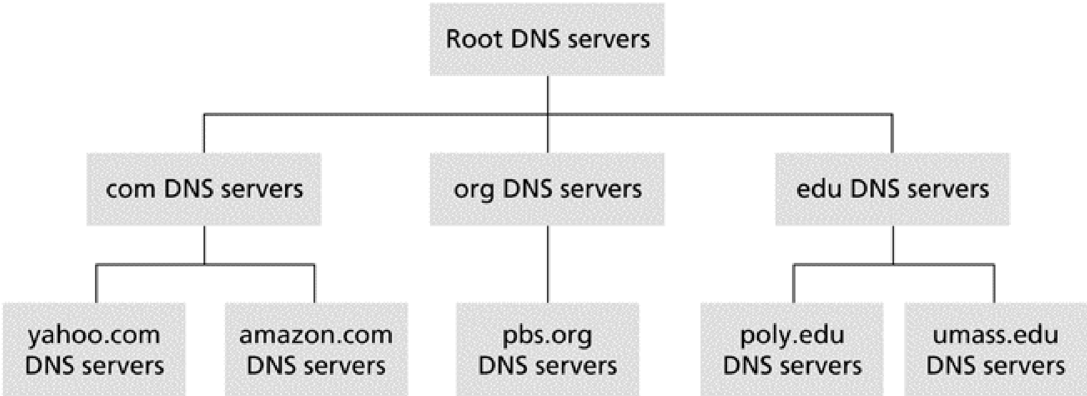
जब कभी भी किसी एप्लीकेशन को कोई नाम IP एड्रेस में ट्रांसलेट किए जाने की आवश्यकता होती है, तो वह एप्लीकेशन नेमिंग सिस्टम की क्लाईंट बन जाती है। कलाईंट द्वारा बदला जाने वाला नेम DNS रिक्वेस्ट मैसेज में रखा जाता है। सर्वर रिक्वेस्ट को DNSसर्वर को प्रेषित किया जाता है। सर्वर रिक्वेस्ट में से नेम प्राप्त करता है, और परिणामी एड्रेस को रीप्लाई मैसेज में एप्लीकेशन को लौटा देता है।



चित्र 7.8: डोमेन DNS डिस्ट्रीब्यूशन

DNS नेम पंजीयन :

जैसा हम जानते हैं कि नेम रिजॉल्यूशन वह प्रक्रिया है, जिसके द्वारा DNS डाटाबेस से किसी होस्ट नेम के लिए IP एड्रेस इंफॉर्मेशन प्राप्त की जाती है। वह प्रक्रिया जिसके द्वारा डाटाबेस में होस्ट नेम्स और उनके एड्रेसेस जोड़े जाते हैं, नेम रजिस्ट्रेशन कहलाती है। यह DNS सर्वर पर नए संसाधन रेकॉर्ड्स निर्मित किए जाने की प्रक्रिया है, जिससे कि वे नेटवर्क पर अन्य सभी DNS सर्वर्स के लिए उपलब्ध हो जाए।



चित्र 7.9: रूट DNS

किसी परम्परागत DNS सर्वर पर नेम रजिस्ट्रेशन की प्रक्रिया निश्चित रूप से निम्न तकनीकी होती है। ऐसी कोई विधि नहीं होती है, जिसके द्वारा सर्वर नेटवर्क पर सिस्टम का पता लगाते हुए उनके होस्ट नेम्स तथा IP एड्रेसेज को संसाधन के रेकॉर्ड्स में दर्ज कर ले।

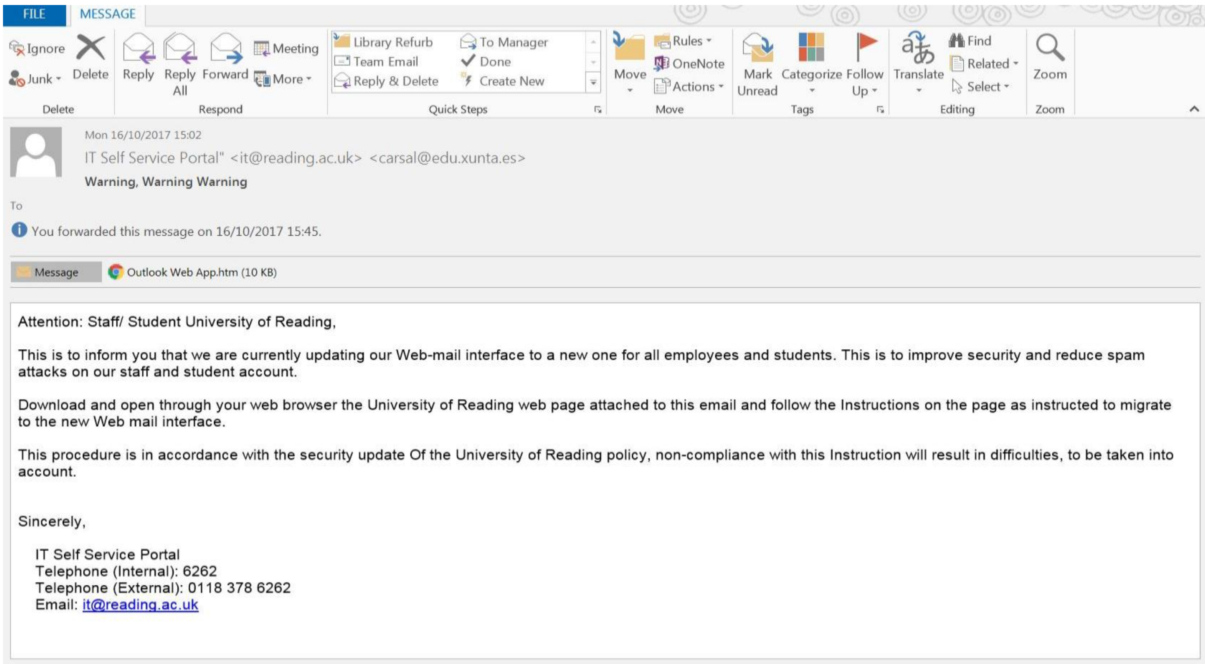
चित्र 7.10: डोमेन रजिस्ट्रेशन

DNS सेवाएँ प्राप्त करना :

इंटरनेट से जुड़े हुए निजी नेटवर्क पर हम अब भी अपने ISP के DNS सर्वर्स का उपयोग कर सकते है। यदि हम अपना स्वयं का डोमेन नहीं चला रहे हैं, तो नेटवर्क को केवल नेम्स को एड्रेस में रिज़ॉल्व किए जाने के लिए DNS सर्वर्स की क्लाईंट क्षमताओं की ही आवश्यकता होगी। एक ऐसा संगठन जो एक इंटरनेट डोमेन की होस्टिंग कर रहा हो, के पास ऐसा DNS सर्वर्स होना चाहिए जो उस डोमेन के लिए रजिस्टार्स को फॉल्ट के प्रति सहनशीलता के उद्देश्य से दो DNS सर्वर्स के एड्रेसेस की आवश्यकता होती है।

7.4 ई–मेल एड्रेसिंग :

प्रारंभिक ई–मेल यूजर्स के लिए ई–मेल एड्रेस फॉर्मेट शीघ्र ही अत्यंत सामान्य हो गया। किसी इंटरनेट ई–मेल एड्रेस में दो भाग शामिल होते हैं – (1) यूजर नेम और (2) डोमेन नेम। इन्हें रूंजरू संकेत / से पृथक किया गया है, जैसे कि ई–मेल नेम ab@mydomain.comहै। जैसे URLs को Web ओर FTP साईट्स की पहचान करने के लिए प्रयुक्त किया जाता है, वैसे ही किसी ई–मेल एड्रेस में डोमेन नेम किसी विशिष्ट यूजर के लिए ई–मेल सेवाओं को प्रदान करने वाले संगठन की पहचान कराता है।

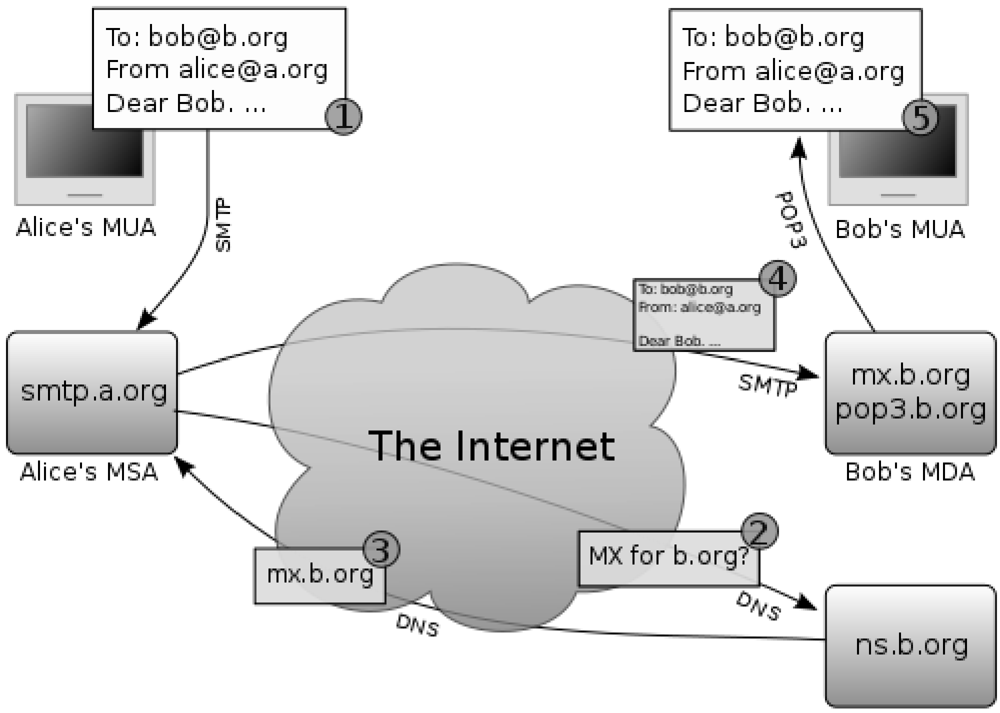


चित्र 7.11: ईमेल सरंचना

1. यूजर नेम : ई–मेल का यूजर नेम वाला भाग डोमेन को सेवा प्रदान करने वाले मेल सर्वर पर निर्मित मेल बॉक्स का नाम दर्शाता है। यूजर नेम प्रायः नेम्स और/अथवा प्रारंभिक अक्षरो के मिले–जुले रूप से बनता है, जो संगठन में व्यक्तिगत यूजर की पहचान करता है।

2. डोमेन नेम : चूँकि मेल सर्वस की पहचान करने के लिए इंटरनेट ई–मेल स्टेंडर्ड डोमेन नेम्स पर निर्भर होता है, अस्तु डोमेन नेम सिस्टम (DNS) इंटरनेट ई–मेल आर्किटेक्चर का एक आवश्यक अंग है।

DNS सर्वर्स विभिन्न प्रकार की इकाईयों में इंफॉर्मेशन संग्रहीत करता है, जिन्हें रिसोर्स रेकॉर्ड्स कहते हैं। उग रिसोर्स रेकॉर्ड इनमें से एक है, जिसे किसी विशिष्ट डोमेन में ई–मेल सर्वर को किसी ई–मेल क्लाईंट की ओर से एक आऊअगोईंग मैसेज प्राप्त होता है, तब स्थिति में वह वह तत्संबंधित प्रेषक का एड्रेस पड़ता है और उस एड्रेस में डोमेन के लिए सर्वर Mx रिसॉर्स रेकॉर्ड का अनुरोध करते हुए एक DNS सर्वर डेस्टीनेशन डोमेन के लिए ई–मेल सर्वर के IP एड्रेस के साथ प्राप्ति स्वीकृति भेजता है।



चित्र 7.12: इंटरनेट में ईमेल कनेक्शन

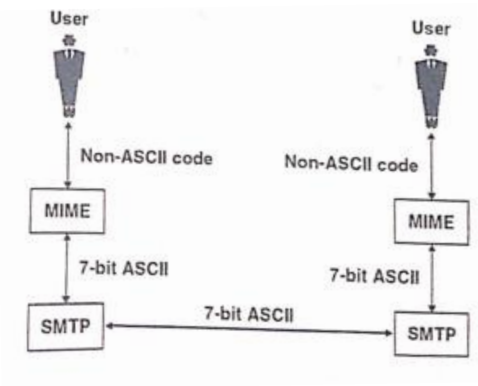
ई–मेल सर्वर प्रॉडक्ट्स सामान्यतः दो श्रेणियों में रखे जाते हैं – (1) वे जो पूर्णतः इंटरनेट ई–मेल के लिए निर्मित किए जाते हैं और (2) वे जो इंटरनेट ई–मेल सेवाओं के साथ ही अधिक व्यापक आंतरिक ई–मेल सेवाएँ भी प्रदान करते हैं। प्रथम श्रेणी में तुलनात्मक रूप से सरल ऐसी एप्लीकेशन आती हैं, जो SMTP को समर्थन प्रदान करती हैं ओर इसके साथ ही उनमें या तो POP3 अथवा IMAP सम्मिलित हो सकते हैं या नहीं हो सकते है।

यदि सम्मिलित नहीं है, तो हम POP3 अथवा IMAP सर्वर को खरीद कर इंस्टॉल भी कर सकते हैं, जिससे कि हमारे यूजर्स अपने मेल एक्सेस कर सकें। इंटरनेट पर सर्वाधिक प्रयुक्त किए जाने वाले सर्वसामान्य SMTP सर्वर्स में से एक फ्री यूनिक्स प्रोग्राम है, जो सेण्डमेल कहलाता है।

मल्टीपरपज इंटरनेट मेल इक्सटेशन्स (MIME) :

SMTP एक सरल मेल ट्रांसफर प्रोटोकॉल है। इसकी सरलता के साथ कुछ कीमत भी चुकानी पड़ती है। SMTP केवल 7–बिट ASCII फॉर्मेट में ही मैसेजेस प्रेषित कर सकता है। उसकी अपनी सीमाएँ हैं। यह बायनरी फाईल्स, वीडियों अथवा ऑडियों प्रेषित करने हेतु भी प्रयुक्त नहीं किया जा सकता।

मल्टीपरपज इंटरनेट मेल इक्सटेशन्स (MIME) एक ऐसा पूरक प्रोटोकॉल है, तो non-ASCII डाटा को SMTP के माध्यम से प्रेषित किए जाने की अनुमति प्रदान करता है। MIME मेल प्रोटोकॉल नहीं है ओर यह SMTP का केवल एक एक्सटेंशन मात्र है।

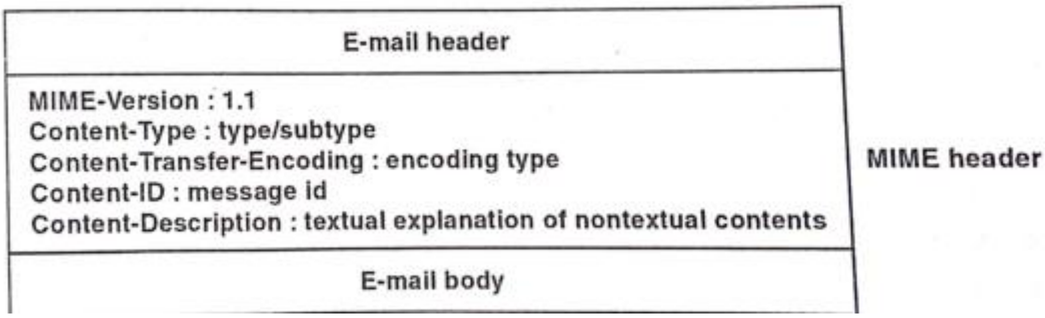


चित्र 7.13: MIME प्रोटोकॉल

Non-ASCII डाटा को MIME सेंटर साईट पर ASCII डाटा में बदलता हैं और उसे क्लाईट SMTP पर इंटरनेट के माध्यम से प्रेषित किए जाने के लिए डिलीवरी करता हैं। रिसविंग साईट पर SMTP सर्वर ASCII डाटा प्राप्त करता हैं और उसे मूल डाटा में रूपांतरित किए जाने के लिए MIME को प्रदान करता हैं।

MIME हमें ऐसे पाँच हेडर्स प्रदान करता हैं, जिन्हें रूपातंरण के मापदण्डों को परिभाषित करने के लिए मूल SMTP हेडर सेक्शन में जोड़ा जा सकता है–

1- MIME - Version
2- Content - Type
3- Content - Transfer-Encoding
4- Content-id
5- Content-Description



1. MIME-Version

यह हमें प्रयुक्त किए जा रहें MIME का वर्शन प्रदान करता है। वर्तमान वर्शन 1.1 हैं।

2 Content-Type

यह हमें मैसेज की बॉडी में प्रयुक्त किए जा रहे डाटा का प्रकार प्रदान करता हैं। कंटेंट टाईप और कंटेंट सबटाईप को स्लेश (/) द्वारा पृथक किया जाता है। सबटाईप के आधार पर हेडर में अन्य मापदंड (पेरामीटरर्स) सन्निहित हो सकते हैं।

Type	Subtype	Description
Text	Plain	Unformatted text
Multipart	Mixed	Body contains ordered parts of different data types
	Parallel	Same as above, but no order
	Digest	Similar to mixed, but the default is message/RFC822
	Alternative	Parts are different versions of the same message
Message	RFC822	Body is an encapsulated message
	Partial	Body is a fragment of a bigger message
	External-body	Body is a reference to another message
Image	JPEG	Image is in JPEG format
	GIF	Image is in GIF
Video	MPEG	Video is in MPEG format
Audio	Basic	Single channel encoding of voice at 8 KHz
Application	PostScript	Adobe PostScript
	Octet-stream	General binary data (8-bit bytes)

(i) **TEXT :** मूल मैसेज 7 – बिट ASCII फॉर्मेट में होता है और MIME द्वारा रूपांतरण की कोई आवश्यकता नहीं होती हैं। वर्तमान में केवल एक सबटाईप प्लेन ही प्रयुक्त किया जा रहा है।

(ii) **Multipart :** बॉडी एकाधिक स्वतंत्र भागों से निर्मित होती हैं। मल्टीपार्ट हेडर प्रत्येक भाग के मध्य की सीमा को परिभाषित किए जाने के लिए आवश्यक होता हैं। यह सीमा मापदंड या पेरामीटर की भाँति प्रयुक्त की जाती हैं। यह एक ऐसा स्ट्रींग टोकन हैं, जो प्रत्येक भाग के पूर्व स्वतंत्र लाईन पर अपने आप को दोहराता हैं तथा इसका प्रारम्भ दो हाईफंस (––) से होता है।

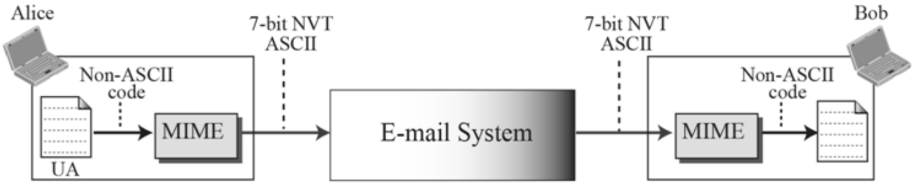
```
Content-type: text/plain; charset=us-ascii (Plain text)

Content-type: text/plain; charset="us-ascii"
```

(iii) **Message :** मैसेजटाईप में बॉडी अपने आप में एक संपूर्ण मैसेज, मेल मैसेज का एक पाईंटर के रूप में डिर्फान होती है। वर्तमान में तीन सबटाईप प्रयुक्त किए जाते हैं –RFC822, partial अथवा external vody / RFC822 सबटाईप को तब प्रयुक्त किया जाता हैं, जब बॉडी किसी अन्य मैसेज में जोड़ दी गई हो। partial सबटाईप को तब प्रयुक्त

किया जाता हैं, जबकि मूल मैसेज को विभिन्न मेल मैसेजेज में खंडित कर दिया गया हो और यह मेल मैसेजेज भी किसी खण्ड में एक हो । इन खण्डों को डेस्टिनेशन पर MIME द्वारा पुनः जोड़ा जाता हैं। इसमें तीन मानदंड (पेरामीटरर्स) Id, number और total जोड़ने पड़ते है।

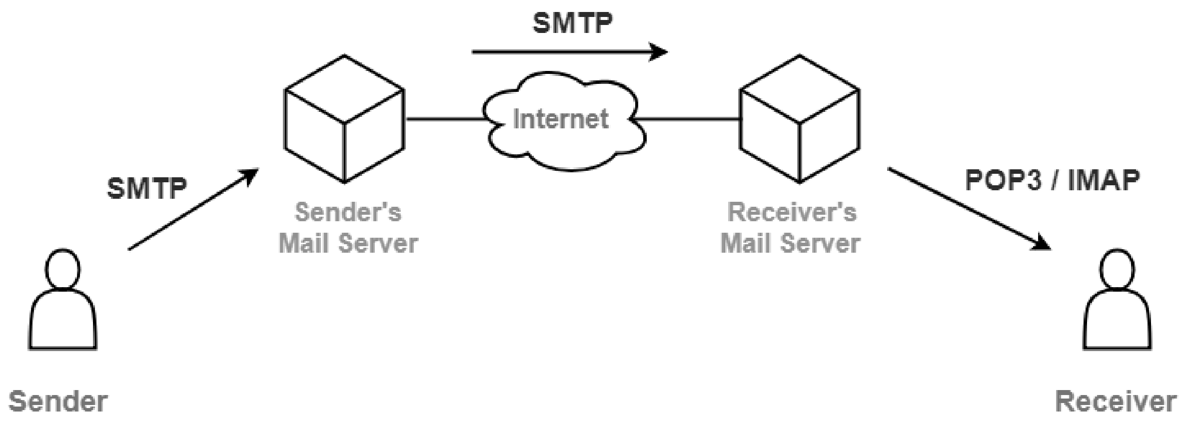
```
MIME-message-headers := entity-headers
                        fields
                        version CRLF
                        ; The ordering of the header
                        ; fields implied by this BNF
                        ; definition should be ignored.
```



चित्र 7.14: चेकसम फील्ड

सिंपल मेल ट्रांसफर प्रोटोकॉल (SMTP) :

SMTP एक एप्लीकेशन लेयर प्रोटोकॉल है, जिसे IETF के RFC 821 डॉक्यूमेंट में मानकीकृत किया गया है। SMPT मैसेजेज को किसी भी विश्वसनीय ट्रांसपोर्ट प्रोटोकॉल द्वारा स्थानांनतरण किया जा सकता है, किंतु इंटरनेट और अधिकांश निजी नेटवर्क्स पर इन्हें सर्वर पर सुविख्यात पोर्ट नंबर 25 का उपयोग करते हुए TCP प्रोटोकॉल द्वारा स्थानातंरण किया जाता है। HTTP और FTP की SMTP मैसेजेज भी प्रोटोकॉल स्टैक की लोयर लेयर्स के प्रोटोकॉल द्वारा प्रयुक्त किए जाने वाले हेडर्स और फील्ड्स के स्थान पर ASCII टेक्सट कमांड्स पर आधारित होते है।



चित्र 7.15: SMTP कनेक्शन

SMTP कमांड्स :

एक बार TCP कनेक्शन स्थापित हो जाता हैं, तो सेंडर SMTP कम्प्यूटर रिसीवर SMTP को वह SMTP कमांड्स ट्रांसमिट करना प्रारम्भ कर देता हैं, जो उसके द्वारा ग्रहण किए जाने वाले प्रत्येक कंमाड के लिए एक रिप्लाई मैसेज और न्यूमेरिक कोड से प्रतिक्रिया देता हैं।

सेंडर SMTP द्वारा प्रयुक्त किए जाने वाले कमांड्स और उनके फंक्शन निम्नानुसार होते हैं–

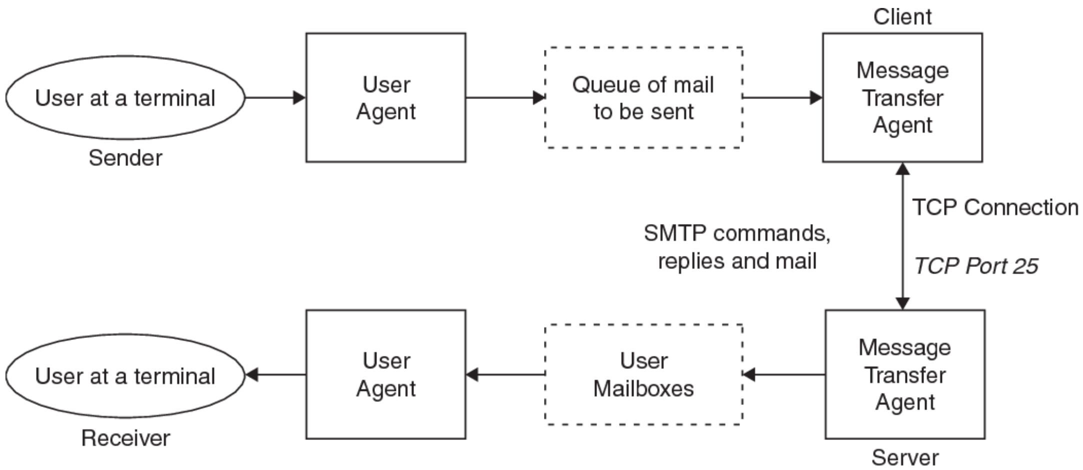
1. HELLO (HELO) :सेंडर SMTP द्वारा रिसीवर SMTP को स्वंय की पहचान कराने के लिए उसके होस्ट नेम को स्वयं की पहचान कराने के लिए उसके होस्ट नेम को ऑर्ग्यूमेंट के रूप में प्रेषित करते हुए प्रयुक्त किया जाता है। रिसीवर SMTP अपना स्वयं का होस्ट नेम ट्रांसमिट करते हुए प्रतिक्रिया देता है।

2 MAIL (MAIL) : इसे उस ट्रांजेशन को प्रारंभ करने के लिए प्रयुक्त किया जाता है, जिसमें मेल बॉक्स में किसी मेल मैसेज को भेजे जाने के लिए मेल सेंडर के एड्रेस को ऑर्ग्यूमेंट के रूप में और होस्ट्स की उस सूची को दर्शाया जाता है, जिसके माध्यम से मेल मैसेज को रूट (जिसे सोर्स रूट कहते हैं) किया जाता है।

3. RECIPIENT (RCPT) :यह मेल मैसेज के ग्रहणकर्ता की पहचान ग्रहणकर्ता के मेल बॉक्स एड्रेस को ऑर्ग्यूमेंट की तरह उपयोग करते हुए करता है। यदि मैसेज एकाधिक प्राप्तकर्ताओं को प्रेषित किया गया है, यदि मैसेज एकाधिक प्राप्तकर्ताओं को प्रेषित किया गया है, तो सेंडर SMTPप्रत्येक एड्रेस के लिए एक स्वतंत्र RCPTकमांड उत्पन्न करता है।
4. DATA (DATA) :यह वास्तविक ई–मेल मैसेज डाटा से बना होता है। इसके उपरांत एक CRLF, एक पीरियड (.)तथा एक अन्य CRLF(<CRLF>.<CRLF>)आता है, जो मैसेज स्ट्रींग के समापन को निर्दिष्ट करता है।
5. SEND (SEND): यह उस ट्रांजेक्शन को प्रारंभ करने के लिए प्रयुक्त किया जाता है, जिसमें मेंल को यूजर के टर्मिनल पर भेजा जाना है। MAIL कमांड की ही भाँति ऑर्ग्यूमेंट सेंडर के मेल बॉक्स एड्रेस और सोर्स रूट से निर्मिट होता है।
6. SEND OR MAIL (SOML) :इसे ऐसा ट्रांजेक्शन प्रारंभ किए जाने के लिए प्रयुक्त किया जाता है, जिसमें मेल मैसेज को यूजर के टर्मिनल पर तब डिलीवर किया जाता है, जबकि वे वर्तमान में सक्रिय हों ओर मैसेजेस को प्राप्त करने के लिए कॉन्फिग्यूर किए गए हों।
7. SEND and MAIL (SAML) :इसे एक ऐसा ट्रांजेक्शन प्रारंभ करने के लिए प्रयुक्त किया जाता है, जिसमें यदि यूजर का टर्मिनल वर्तमान में सक्रिय है और मैसेजेस को प्राप्त करने के लिए कॉन्फिग्यूर किया गया है, तो मेल मैसेज को यूजर के टर्मिनल पर, यूजर के मेल बॉक्स को भेज दिया जाता है।
8. RESET (RSET) : यह रिसीवर SMTPको वर्तमान मेल ट्रांजेक्शन को रोकने और उस ट्रांजेक्शन को रोकन और उस ट्रांजेक्शन से सभी सेंडर, रेसिपियंट तथा मेल डाटा इंर्फोमेशन को अनदेखा करने के निर्देश देता है।
9. VERIFY (VRFY) : सेंडर SMTP इसे यह सुनिश्चित करने के लिए प्रयुक्त करता है कि ऑर्ग्यूमेंट एक वैध यूजर की ही पहचान करे। यदि ऐसे यूजर का अस्तित्व है, तो रिसीवर SMTPयूजर के पूर्ण नाम तथा मेल बॉक्स एड्रेस के साथ प्रतिक्रिया प्रदान करता है।

10. EXPAND (EXPN) : सेंडर SMTP इसे यह सुनिश्चित करने के लिए प्रयुक्त करता है कि ऑर्ग्यूमेंट किसी वैघ मैलिंग लिस्ट की ही पहचान करें। यदि ऐसे लिस्ट विद्यमान है, तो रिसीवर SMTP उस लिस्ट के मेम्बर्स के पूर्ण नामों और मेलबॉक्स एड्रेसेज के साथ प्रतिक्रिया प्रदान करता है।

11. HELP (HELP) : यह सेंडर SMTP (मान लें कि एक क्लाईंट) द्वारा रिसीवर SMTP की ओर से हेल्प इंफॉर्मेशन की रिक्वेस्ट करने के लिए प्रयुक्त किया जाता है। एक वैकल्पिक ऑर्ग्यूमेंट उस विषय को निर्दिष्ट कर सकता है, जिसके लिए सेंडर SMTP को सहायता की जरूरत है।



चित्र 7.16: SMTP कनेक्शन कम्युनिकेशन

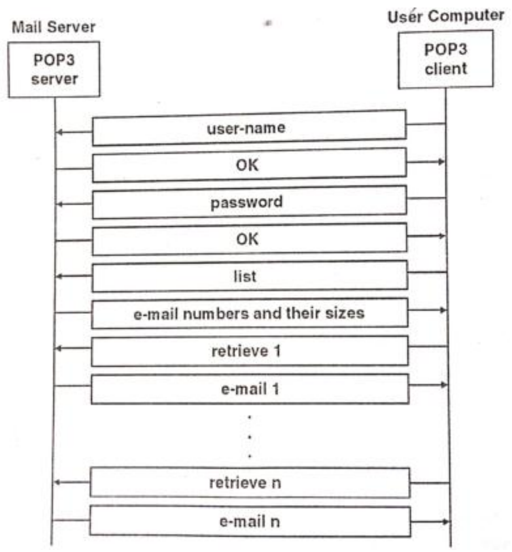
मेल एक्सेस प्रोटोकॉल्स :

दूरस्थ यूजर एजेंट मेल एक्सेस प्रोटोकॉल का उपयोग, मेल बॉक्स को एक्सेस करने तथा मेल प्राप्त करने के लिए करता है। वर्तमान में दो मेल प्राप्त करने के लिए करता है। वर्तमान में दो मेल एक्सेस प्रोटोकॉल्स उपलब्ध हैं – (1) पोस्ट ऑफिस प्रोटोकॉल्स, वर्शन 3 (POP3) और (2) इंटरनेट मेल एक्सेस प्रोटोकॉल, वर्शन 4 (IMAP4) ।

1. (POP3) :

पोस्ट ऑफिस प्रोटोकॉल, वर्शन 3 (POP3) सरल है, किंतु यह कार्यकारी तौर पर सीमित है। क्लाईंट POP3 सॉफ्टवेयर रेसिपियेंट कम्प्यूटर पर इंस्टॉल किया जाता है तथा सर्वर POP3 सॉफ्टवेयर मेल सर्वर पर इंस्टॉल होता है।

RFC 1939 डॉक्यूमेंट में परिभाषित किए गए अनुसार पोस्ट ऑफिस प्रोटोकॉल, वर्शन 3 (POP3) ऐसे क्लाईंट अधिकांश मामलों में क्लाईंट्स को मेल बॉक्स सेवा की आवश्यकता होने का कारण यह है कि वे लगातार इंटरनेट से जुड़े नहीं रह सकते हैं और इसीलिए जब कभी कोई दूरस्थ SMTP स्वीकार करने में सक्षम नहीं हों। च्व्च्3 सर्वर निरंतर जुड़ा रहता है और ऑफ लाईन यूजर्स के लिए मैसेजेस को ग्रहण करने के लिए सदैव ही उपस्थित रहता है। तदुपरांत सर्वर मैसेजेस को एक इलेक्ट्रोनिक मेल बॉक्स में तब तक रखता है, जब तक कि यूजर सर्वर से कनेक्ट होकर उनके लिए रिक्वेस्ट न करें।



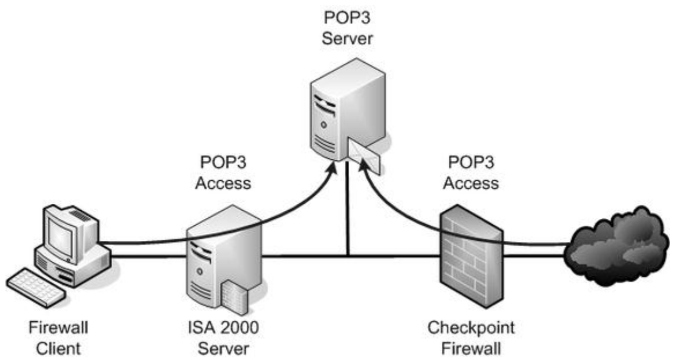
चित्र 7.17: POP3 मेल एक्सेस प्रोटोकॉल्स

एक POP3 क्लाईंट/सर्वर सेशन तीन विभिन्न अवस्थाओं से गुजरकर पूरा होता है– (i) प्रमाणीकरण या ऑथोराईजेशन अवस्था (ii) ट्राजेक्शन अवस्था और ;पपपद्ध अपडेट अवस्था। इन अवस्थाओं की व्याख्या निम्नानुसार है–

(i) प्रमाणीकरण या ऑथोराईजेशन अवस्था : च्व्च्3 सैशन तब प्रारंभ होता है, जबकि क्लाईंट किसी सक्रिय सर्वर के साथ एक ज्ब्च् कनेक्शन स्थापित करता है। एक बार ज्ब्च् थ्री वे हेंडशेक सम्पन्न हो जाता है, तो सर्वर क्लाईंट को एक ग्रीटिंग प्रेषित करता है, जो सामान्यतः एक + OK रिप्लाई के स्वरूप में होता है। इसी बिंदु पर सेशन, ऑथोराईजेशन अवस्था में प्रविष्ठ होता हैं,

(ii) ट्रोजेक्शन अवस्था : एक बार सेशन ट्रांजेक्शन अवस्था में प्रवेश कर जाए तो क्लाईंट उस सर्वर को कमांड्स ट्रांसमिट करना प्रारंभ कर सकता है, जिससे वह उन मेल मैसेजेस को प्राप्त करेगा, जो मेल बॉक्स में प्रतीक्षारत रहते हैं। जब सर्वर ट्रांजेक्शन अवस्था में प्रवेश करता है, तब वह क्लाईंट के मेल बॉक्स में प्रत्येक मैसेज के आकार को नोट करता है।

(iii) अपडेट अवस्था : एक बार जब क्लाईंट के द्वारा मेल बॉक्स में मैसेजेस को प्राप्त करने और ट्रांजेक्शन अवस्था से संबंधित अन्य गतिविधियाँ सम्पन्न कर ली जाती है, तब वह सर्वर को फन्प्ज कमांड भेजता है, जिसके फलस्वरूप सेशन ट्रांजेक्शन से अपडेट अवस्था में पहुंच जाता है। अपडेट अवस्था में प्रविष्ट होने के उपरांत सर्वर उन सभी मैसेजेस को डिलिट कर देता है, जो डिलिट किए जाने के लिए चिन्हित किए हुए होते हैं और क्लाईंट के बॉक्स पर अपने विशिष्ट नियंत्रण को मुक्त कर देता है।

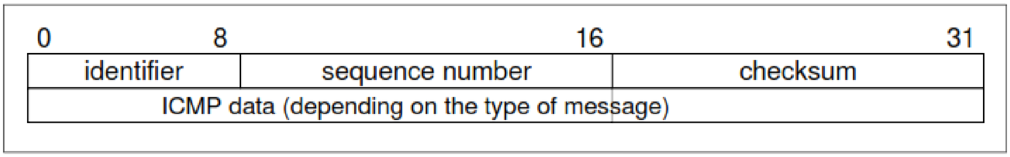


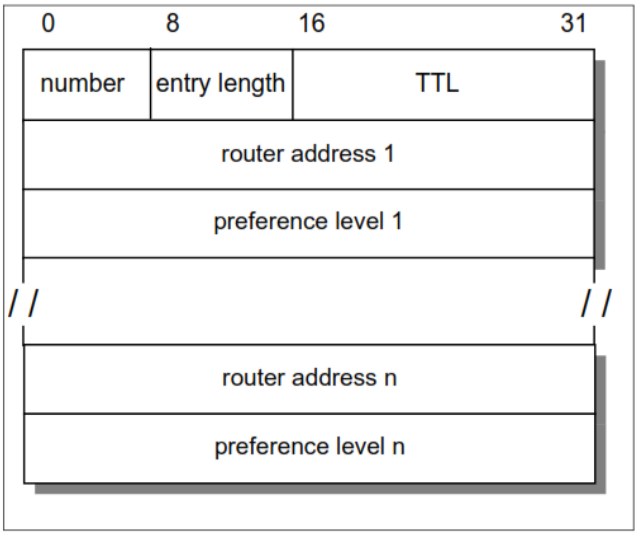
चित्र 7.18: POP3

2. इंटरनेट मैसेज एक्सेस प्रोटझेकॉल (IMAP) :

POP3 तुलनात्मक रूप से एक सरल प्रोटोकॉल है। यह क्लाईंट्स को केवल सर्वाधिक मूलभूत मेलबॉक्स सेवा प्रदान करता है। लगभग सभी परिस्थितियां में, च्व्च्3 सर्वर को एक ऐसे अस्थायी स्टोरेज मीडियम के रूप में प्रयुक्त किया जाता है, जहाँ से ई–मेल क्लाईंट्स अपने मैसेजेस को डाऊन लोड कर दिया जाता है। कि क्लाईंट को इस प्रकार से कॉन्फिगर किया जाना संभव होता है कि वह डाउनलोड करने के बाद मैसेजेस को डिलिट न करें, किंतु क्लाईंट अगले सेशन में उन्हें फिर से डाऊन लोड करता ही है।

RFC 2060 में परिभाषित किया गया इंटरनेट मैसेज एक्सेस प्रोटोकॉल (IMAP), वर्शन 4, एक ऐसी मेल बॉक्स सेवा है, जिसे च्व्च्3 सक्षमताओं को सुधारे जाने के आधार पर निर्मित किया गया है।

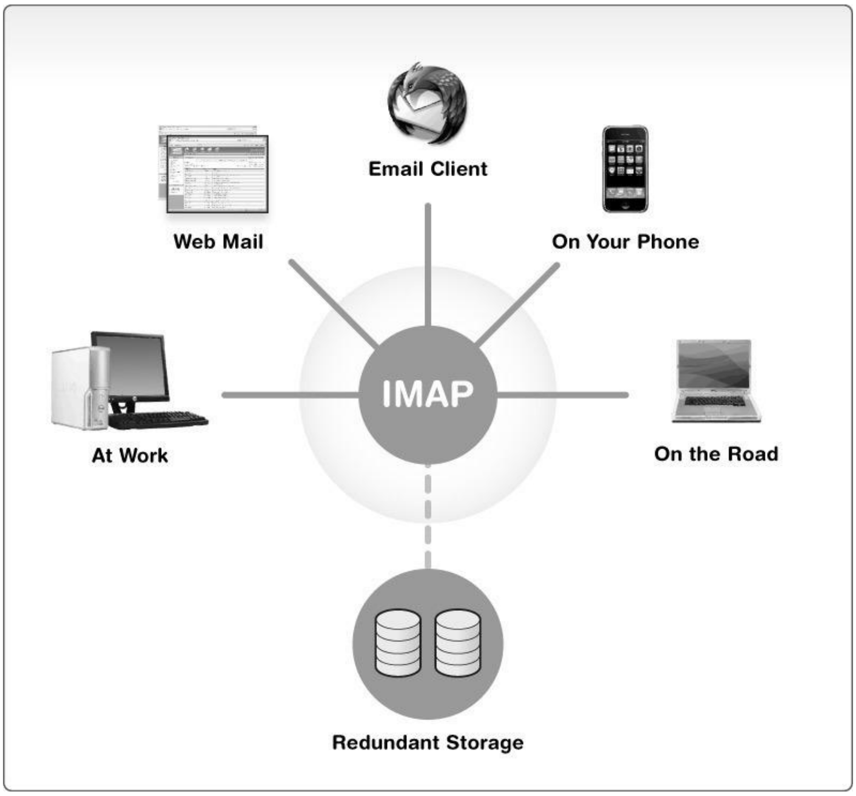




चित्र 7.19: मैसेज एक्सेस प्रोटोकॉल

POP3 की भाँति ही IMAP इस अर्थ में कार्य करता है कि यह टेक्स्ट आधारित कमांड्स और रिस्पांसेज को उपयोग में लाता है, किंतु IMAP सर्वर काफी सीमा तक POP3 से अधिक फंक्शन्स प्रदान करता है।

IMAP और POP3 के मध्य सबसे बड़ा अंतर यह है कि IMAP को ई–मेल मैसेजेस को सर्वर पर स्थायी रूप से संग्रहीत करने के लिए निर्मित किया गया है तथा यह कमांड्स के चयन हेतु ऐसे व्यापक विकल्प प्रदान करता है, जो क्लाईंट्स को अपने मैसेजेस को एक्सेस करने तथा उन्हे परिचालित करने में सहायता प्रदान करते हैं।



चित्र 7.20: मैसेज एक्सेस प्रोटोकॉल

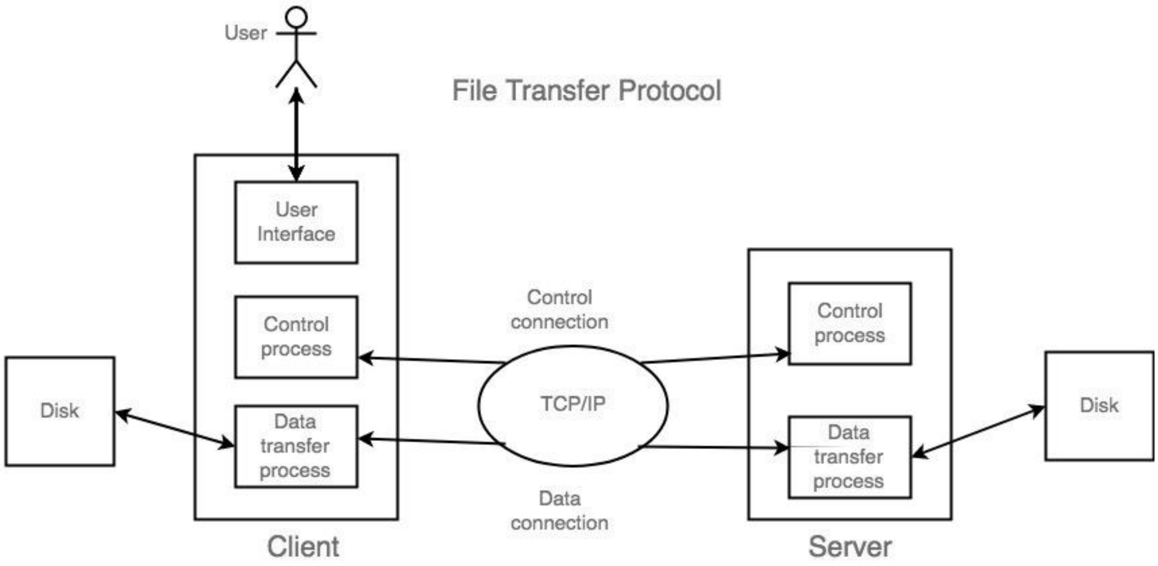
सर्वर पर क्लाईंट की ई–मेल के संग्रहण को व्यावहारिक बनाने के लिए IMAP में अनेक संगठनात्मक और निष्पादनात्मक विशेषताएँ निहित होती है, जिनमें निम्न शामिल हैं–

1. यूजर्स अपने मेल बॉक्सेस में फोल्डर्स बना सकते है और अपने ई–मेल मैसेजेस को फोल्डर्स में ले जाते हैं, जिससे कि एक संगठित स्टोरेज हायरार्की बनाई जा सके।
2. यूजर्स अपने मेल बॉक्सेस में मैसेजेस की ऐसी सूची प्रदर्शित कर सकते हैं, जो केवल हेडर इंफॉर्मेशन से ही बनी हो और फिर उन्हें पूरी तरह डाऊनलोड करने की आवश्यकता होने पर मैसेजेस को चुना जा सकता है।
3. यूजर्स हेडर फील्ड्स की विषय–सामग्री के आधार पर मैसेजेस के लिए सर्च कर सकते हैं। यह विषय–सामग्री मैसेज सब्जेक्ट या मैसेज की बॉडी होती है।

FTP सर्वर्सः

FTP अर्थात् फाईल ट्रांसफर प्रोटोकॉल एक एप्लीकेशन लेयर TCP/IP प्रोटोकॉल है। यह किसी प्रमाणित क्लाईंट को सर्वर से जुड़ने तथा किसी अन्य मशीन से या उस मशीन को फाईल्स ट्रांसफर कने में मदद करता है। FTP नेटवर्क पर किसी अन्य सिस्टम से ड्राईव को शेयर किए जाने जैसा नहीं है। एक्सेस कुछ बुनियादी फाईल मैनेजमेंट कमांड्स तक सीमित रहता है और प्रोटोकॉल का मुख्य कार्य फाईल्स को हमारे लोकल सिस्टम पर कॉपी करना ही है, न कि सर्वर में जा कर उनका एक्सेस करना।

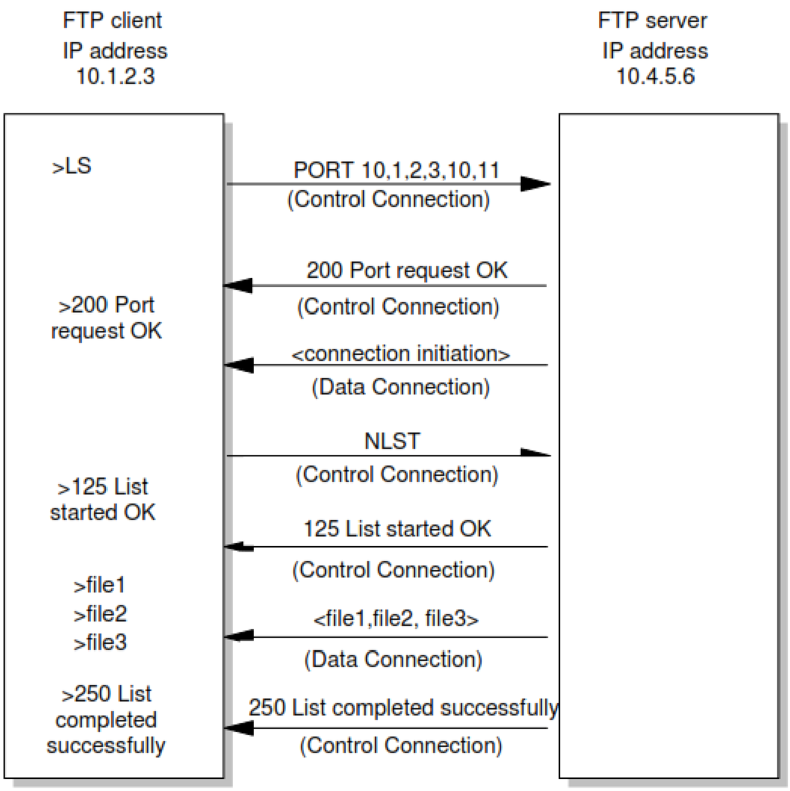
HTTP की भाँति FTP भी अपनी ट्रांसपोर्ट सेवाओं के लिए TCP प्रोटोकॉल का उपयोग करता है और अपने यूजर इंटरफेस के लिए ASCII टेक्स्ट कमांड्स पर निर्भर रहता है। जैसे कि FTP क्लाईंट विंडोस में सम्मिलित होते हैं, वैसे ही UNIX पर सभी वास्तविक थ्ज्च इम्प्लीमेंटेशन्स केरेक्टर आधारित होते हैं। अब अनेक ग्राफिकल FTP क्लाईंट्स ऐसे भी उपलब्ध हैं, जो सर्वर पर यथोचित टेक्स्ट कमांड्स की उत्पत्ति और ट्रांसमिशन को स्वचलित बनाते हैं।



चित्र 7.21: फाईल ट्रांसफर प्रोटोकॉल

FTP कनेक्शन्स :

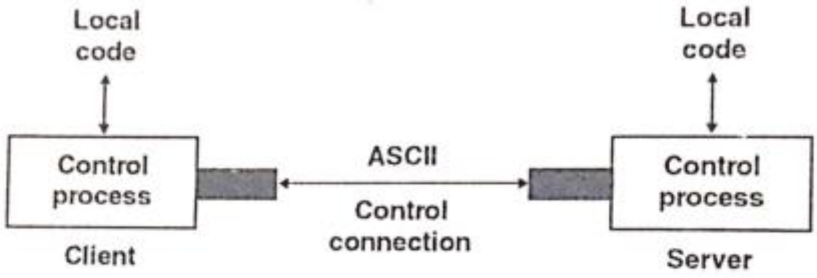
निम्नानुसार दो प्रकार के FTP कनेक्शन्स होते हैं– (1) कंट्रोल कनेक्शन और (2) डाटा कनेक्शन।



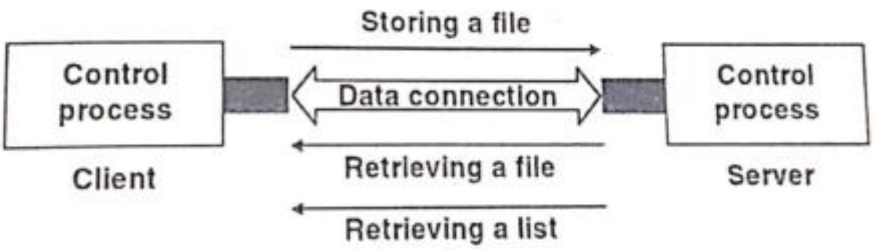
चित्र 7.22: FTP कनेक्शन्स :

ये कनेक्शन विभिन्न रणनीतियों और विभिन्न पोर्ट नंबर्स का उपयोग करते है।

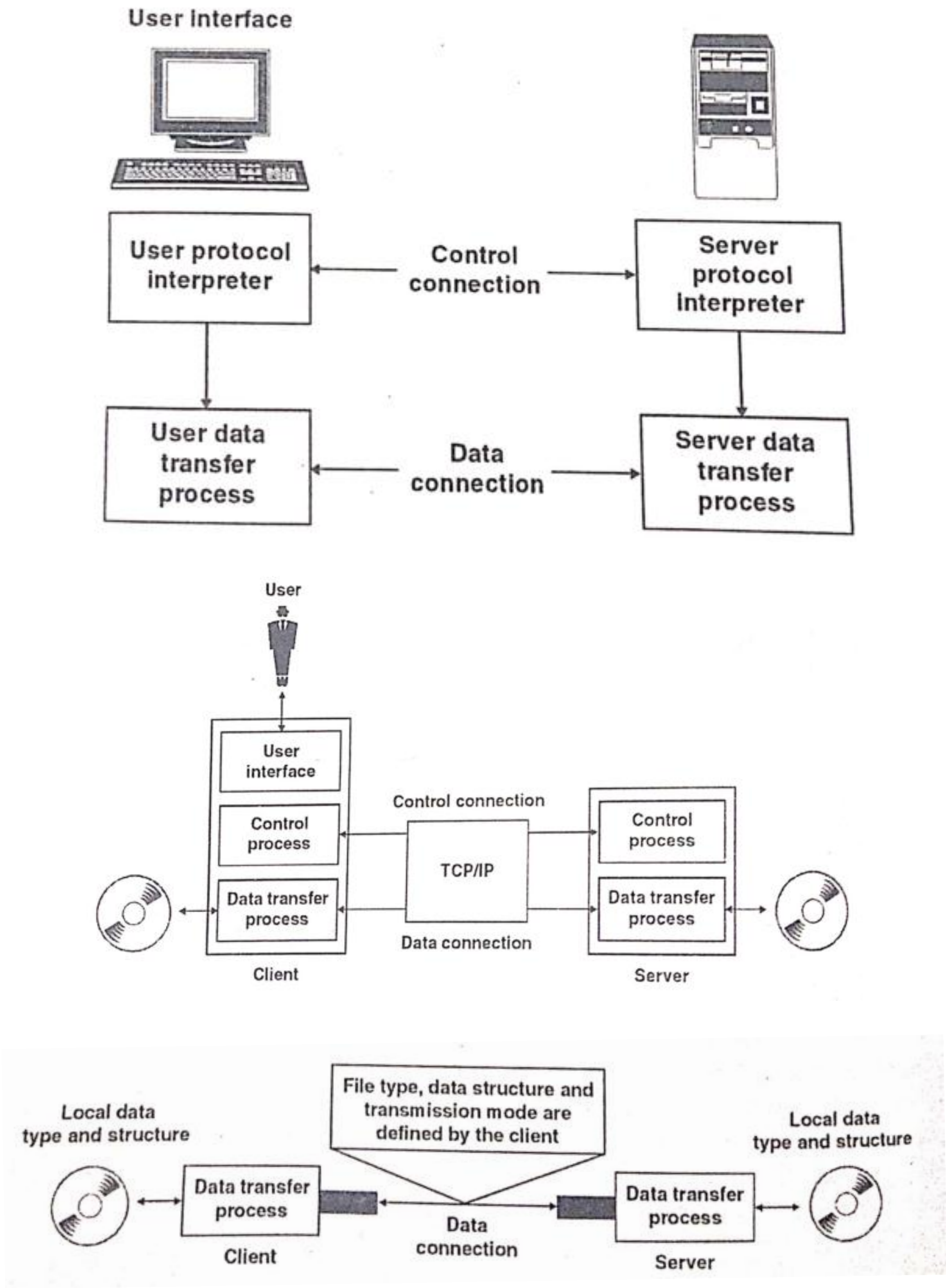
(1) कंट्रोल कनेक्शन : कंट्रोल कनेक्शन को भी उसी प्रकार से निर्मित किया जाता है, जैसे कि अब तक वर्णित किए गए अन्य एप्लीकेशन प्रोग्राम्स को निर्मित किया गया था। पूरी प्रक्रिया के दौरान कनेक्शन खुला रहता है। IP द्वारा प्रयुक्त की जाने वाली सर्विस टाईप minimize dealy हैं,



(2) डाटा कनेक्शन : डाटा कनेक्शन सर्वर साईट पर सुपरिचित पोर्ट 20 का उपयोग करता है। जब डाटा ट्रांसफर के लिए तैयार हो जाता है, तो डाटा कनेक्शन खुल जाता है। जब इसकी आवश्यकता नहीं होती तो यह बंद हो जाता है।



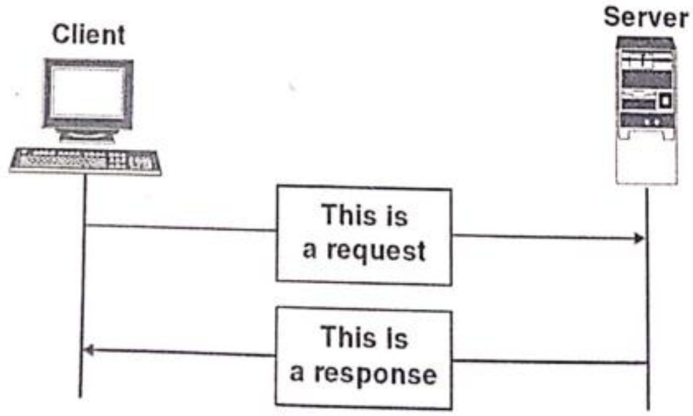
एक सेशन के दौरान डाटा कनेक्शन कई बार खुल और बंद हो सकता है। कंट्रोल कनेक्शन एक बार ही खुलता व बंद होता है। IP द्वारा प्रयुक्त की जाने वाली सर्विस टाईप maximize throughput है।



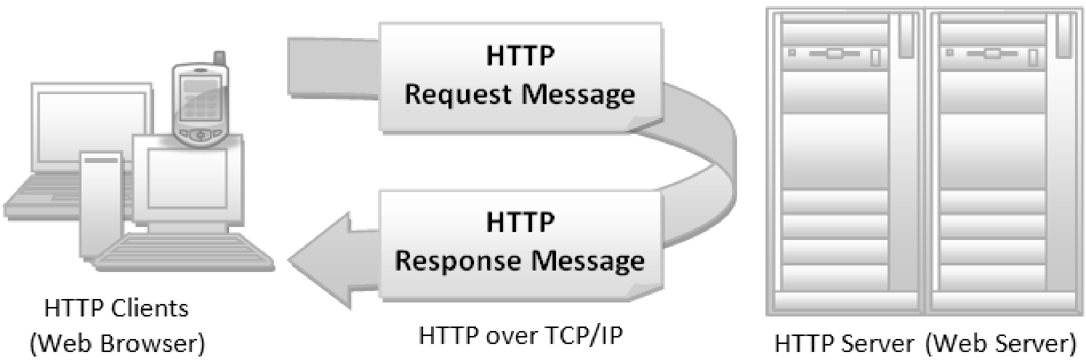
चित्र 7.23: FTP कनेक्शन कम्युनिकेशन TCP में

7.5 एचटीटीपी HTTP :

वेब सर्वर्स और उसके ब्राउजर क्लाईंट्स के मध्य कम्यूनिकेशन एक एप्लीकेशन लेयर प्रोटोकॉल द्वारा दिया जाता है, जिसे हायपर टेक्स्ट ट्रांसफर प्रोटोकॉल (HTTP) कहते हैं।

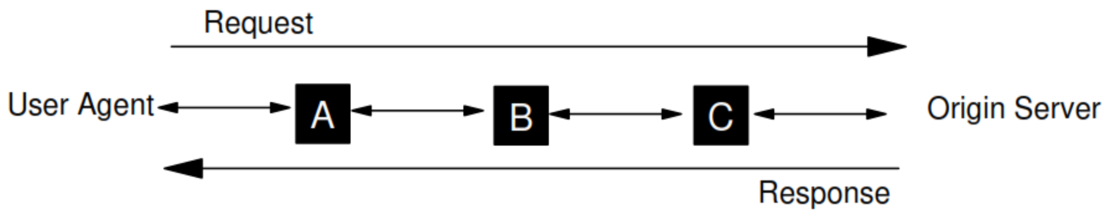


HTTP तुलनात्मक रूप से सरल ऐसा प्रोटोकॉल है, जो सर्वर से क्लाईंट्स तक फाईल्स को ट्रांसफर करने के लिए ट्रांसपोर्ट लेयर पर TCP प्रोटोकॉल द्वारा प्रदान की जाने वाली सेवाओं का लाभ लेता है। जब कोई क्लाईंट ब्राउजर में URL टाईप करके अथवा हायपर लिंक क्लिक करके वेब सर्वर से जुड़ता है, तो सिस्टम एक HTTP रिक्वेस्ट मैसेज उत्पन्न करता है और उसे सर्वर को भेज देता है।



चित्र 7.24: एचटीटीपी प्रोटोकॉल

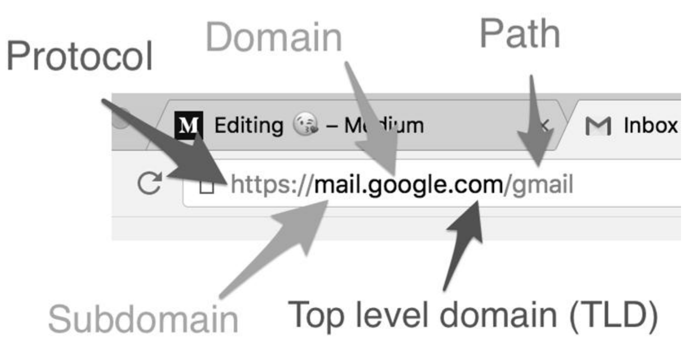
एक बार TCP कनेक्शन स्थापित हो जाने पर ब्राउजर और सर्वर भ्ज्ज्च मैसेजेस का आदान–प्रदान कर सकते हैं। HTTP केवल दो मैसेज टाईप्स से बना होता है : (1) रिक्वेस्ट्स और (2) रिस्पांसेज।



HTTP मैसेजेस ASCII टेक्स्ट स्ट्रिंग्स का स्वरूप लेते हैं न कि असंगत कोड किए गए फील्ड्स वाले विशिष्ट हेडर्स का। हम किसी वेब सर्वर को टेलनेट क्लाईंट से जोड़कर सर्वर को सीधे ही HTTP कमांड के द्वारा फाईल के लिए अनुरोध कर सकते हैं।

यूनिफार्म रिसोर्स लोकेटर Uniform Resource Locator (URL) :

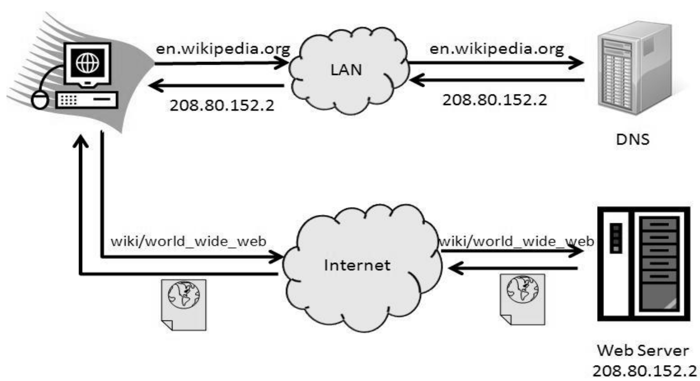
वह क्लाईंट जिसे वेब पेज पर एक्सेस की आवश्यकता है, उसे एक एड्रेस वांछित होता है। पूरी दुनिया भर में फैले हुए डॉक्यूमेंट्स के एक्सेस में सहायता पाने के लिए HTTP यूनिफॉर्म रिसोर्स लोकेटर्स की अवधारणा का उपयोग करता है। इंटरनेट पर किसी भी प्रकार की इंफॉर्मेशन को प्रदर्शित करने के लिए न्त्स् एक स्टेंडर्ड है।



1. **मेथड :**मेथड वह प्रोटोकॉल है, जो डॉक्यूमेंट को प्राप्त करने के लिए प्रयुक्त किया जाता है। अनेक विभिन्न प्रोटोकॉल्स डॉक्यूमेंट को प्राप्त कर सकते है। FTP और HTTP उनमें से ही हैं।
2. **होस्ट कम्प्यूटर :** होस्ट वह कम्प्यूटर होता है, जहाँ इंफॉर्मेशन अवस्थित होती है। यद्यपि कम्प्यूटर का नाम एक उपनाम भी हो सकता है। सामान्यतः वेब पेजेस कम्प्यूटर्स में संग्रहीत होते हैं और कम्प्यूटर्स को ऐसे उपनाम प्रदान कर दिए जाते हैं, जो आमतौर पर www केरेक्टर्स के साथ प्रारंभ होते हैं।
3. **पोर्ट :** URL वैकल्पिक रूप से सर्वर का पोर्ट नंबर रख सकता है। यदि पोर्ट विद्यमान है, तो उसे होस्ट और पाथ के मध्य इंसर्ट किया जाता है तथा इसे विसर्ग चिन्ह (:) द्वारा होस्ट से पृथक किया जाता है।
4. **पाथ :** पाथ फाईल का वह पाथ नेम होता है, जहाँ पर इंफॉर्मेशन अवस्थित होती है। ध्यान दें कि पॉथ में ही स्लैशेज (//) विद्यमान हो सकते है, जो यूनिक्स ऑपरेटिंग सिस्टम में डायरेक्ट्रीज को सबडायरेक्ट्रीज तथा फाईल्स से अलग करते है।

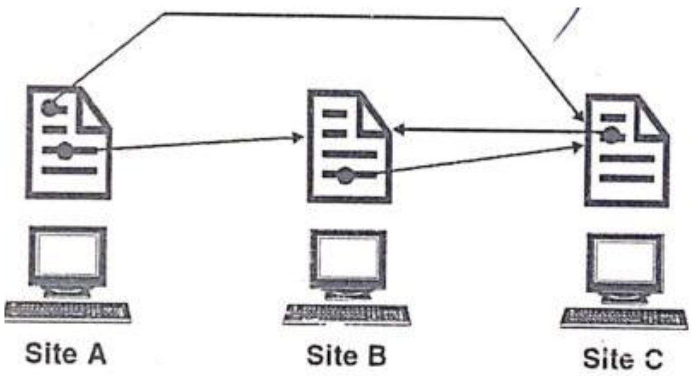
7.5.1 वर्ल्ड वाईड वेब (www):

वर्ल्ड वाईड वेब (WWW) दुनिया भर में फैली और आपस में जुड़ी हुई इंफॉर्मेशन का कोष है। WWW में लचीलेपन, पोर्टेबलिटी और यूजर के अनुकूल विशेषताओं का एक ऐसा अनोखा संयोजन है, जो इसे इंटरनेट द्वारा प्रदान की जाने वाली अन्य सेवाओं से अलग करता है।



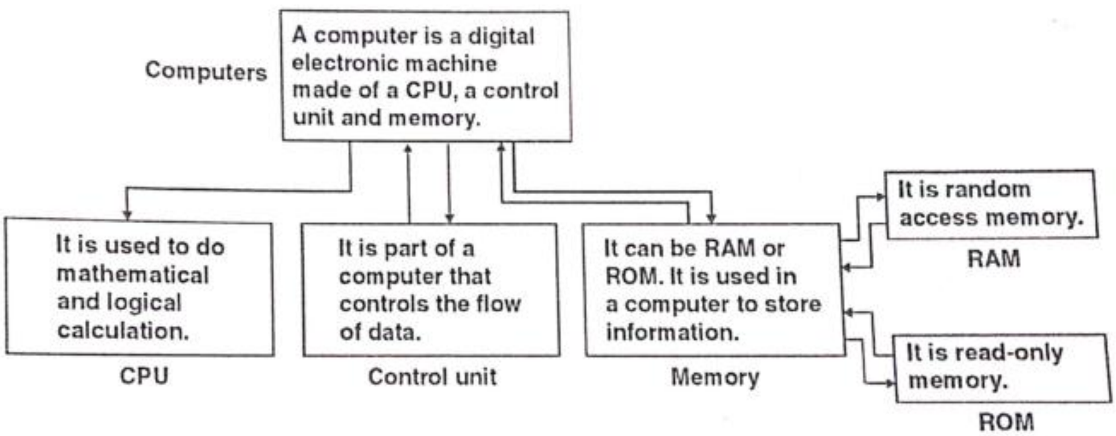
चित्र 7.25: WWW कनेक्शन

आज WWW एक ऐसी डिस्ट्रिब्यूटेड क्लाईंट सर्वर सेवा है, जिसमें ब्राउजर का उपयोग करने वाला क्लाईट सर्वर का उपयोग करते हुए सेवा को एक्सेस कर सकता है। प्रदान की जाने वाली यह सेवा वेबसाईट्स कहलाने वाल अनेक लोकेशन्स पर डिस्ट्रिब्यूटेड होती है।

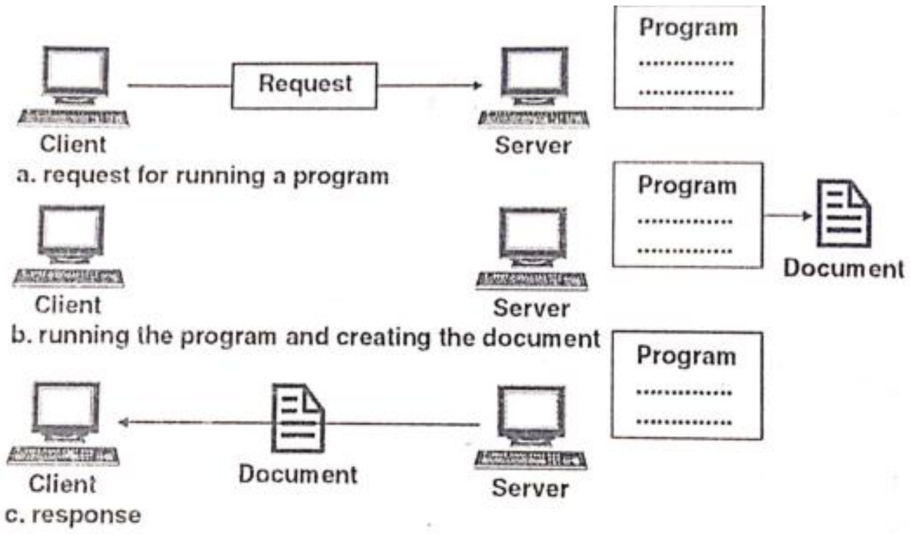


हायपरटेक्स्ट और हायपरमीडिया :

WWW, हायरपटेक्स्ट और हायपरमीडिया की अवधारणा का उपयोग करता है। किसी हायरपटेक्स्ट पर्यावरण में इंफॉर्मेशन को डॉक्यूमेंट्स के ऐसे सेट में रखा जाता है, जो पॉईंटर्स की अवधारणा का उपयोग करते हुए आपस में जुड़े होते हैं।



चित्र 7.26: हायरपटेक्स्ट और हायपरमीडिया



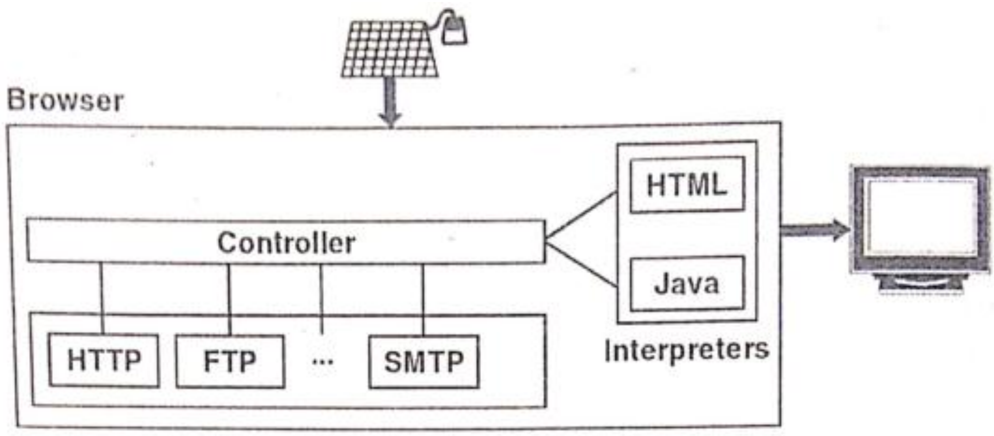
चित्र 7.27: हायरपटेक्स्ट और हायपरमीडिया **कनेक्शन**

एक आयटम को किसी अन्य डॉक्यूमेंट के साथ पॉईंटर द्वारा संबद्ध किया जा सकता है। डॉक्यूमेंट के माध्यम से ब्राउज कर रहा रीडर अन्य डॉक्यूमेंट्स से जुड़े आयटम्स का चयन करते हुए अन्य डॉक्यूमेंट्स में जा सकता है। चित्र 7.27 हॉयपरटेक्स्ट की अवधारणा को दर्शाता है।

जहाँ हायपरटेक्स्ट डॉक्यूमेंट्स केवल टेक्स्ट से ही निर्मित होता हैं, वहीं हायपरमीडिया डॉक्यूमेंट्स में चित्र, ग्राफिक्स और ध्वनि भी सम्मिलित हो सकते है।

7.5.1.1 ब्राउजर आर्किटेक्चर :

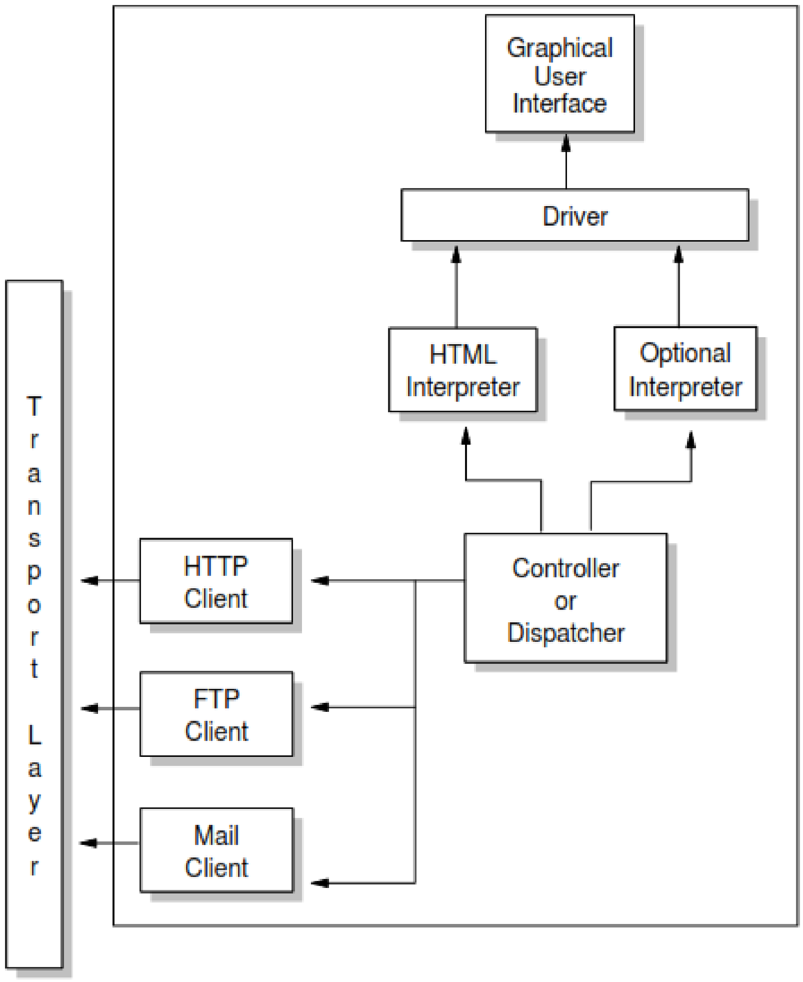
विभिन्न विक्रेतागण हमें ऐसे व्यावसायिक ब्राउजर्स प्रदान कराते हैं, जो वेब डॉक्यूमेंट की व्याख्या तथा उन्हें डिस्पले करते हैं और लगभग सभी समान आर्किटेक्चर का उपयोग करते हैं। प्रत्येक ब्राउजर सामान्यतः तीन हिस्सों का बना होता है– (1) कंट्रोलर, (2) क्लाईंट प्रोग्राम्स और (3) इंटरप्रेटर्स।



चित्र 7.28: वेब ब्राउजर्स डॉक्यूमेंट

कंट्रोलर की–बोर्ड अथवा माऊस से इनपुट ग्रहण करता है और डॉक्यूमेंट एक्सेस करने के लिए क्लाईंट प्रोग्राम्स का उपयोग करता है। डॉक्यूमेंट एक्सेस हो जाने के उपरांत कंट्रोलर इंटरप्रेटर्स में से एक का उपयोग करते हुए स्क्रीन पर डॉक्यूमेंट को डिस्पले करता है। क्लाईंट प्रोग्राम्स पूर्व में विवेचित किए गए प्रोटोकॉल्स जैसे कि भ्ज्ज्च् FTP अथवा SMTP में से एक हो सकता है।

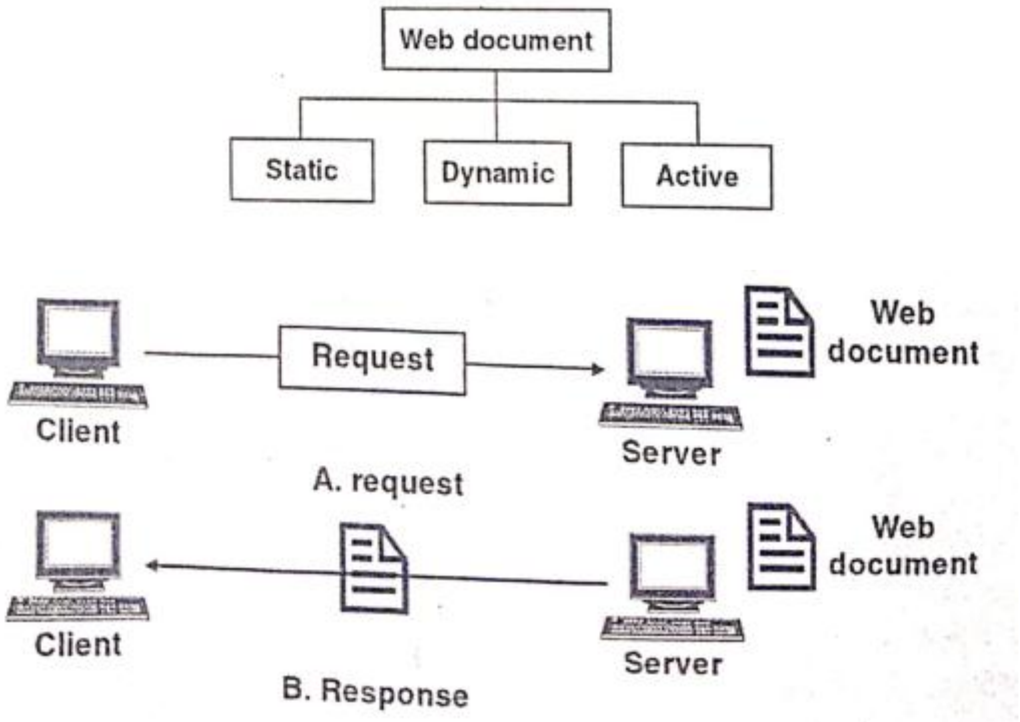
HTML – (स्टेटिक डॉक्यूमेंट का उदाहरण) : हायपरटेक्स्ट मॉर्कअप लेंग्वेज (HTML) वेब पेजेस को निर्मित करने की लेंग्वेज है। मॉर्कअप लेंग्वेज शब्दावली पुस्तक प्रकाशन उद्योग से आई है। किसी पुस्तक को टाईप सेट करने और मुद्रित किए जाने के पूर्व एक कॉपी एडिटर उसकी पांडुलिपि को पढ़ता है तथा उस पर अनेक चिन्ह लगा देता है। यह चिन्ह डिजाईनर को बताते है कि वह टेक्स्ट को किस तरीके से फॉर्मेट करेगा।



चित्र 7.29: ब्राउजर्स **कनेक्शन**

HTML जैसी मॉर्कअप लेंग्वेज हमें फाईल में ही फॉर्मेटिंग निर्देशों को अंतः स्थापित करने की अनुमति प्रदान करती है। निर्देशों को टेक्स्ट के साथ संग्रहीत कर लिया जाता है। इस प्रकार से कोई भी ब्राउजर निर्देशों को पढ़ सकता है और प्रयुक्त किए जा रहे वर्क स्टेशन के अनुसार टेक्स्ट को फॉर्मेट कर सकता है।

भ्ज्डर हमें मुख्य टेक्स्ट और निर्देशों दोनों की फॉर्मेटिंग करने के लिए केवल ASCII केरेक्टर्स के उपयोग की ही अनुमति प्रदान करता है। इस प्रकार से प्रत्येक कम्प्यूटर संपूर्ण डॉक्यूमेंट को एक ASCII डॉक्यूमेंट के रूप में प्राप्त कर सकता है।



चित्र 7.30: वेब पेज की संरचना

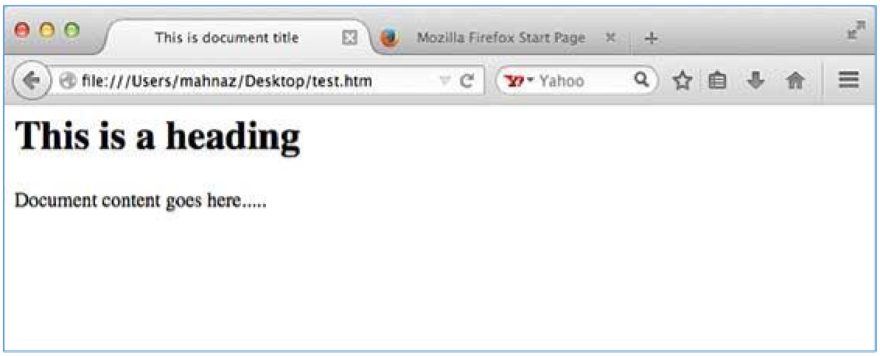
वेज पेज की सरंचना :

वेब पेज दो भागों में निर्मित होता है – हेड और बॉडी।

```
<!DOCTYPE html>
<html>
<head>
<title>This is document title</title>
</head>
<body>
<h1>This is a heading</h1>
<p>Document content goes here.....</p>
</body>
</html>
```

```
Document declaration tag
<html>
   <head>
       Document header related tags
   </head>

   <body>
       Document body related tags
   </body>
</html>
```

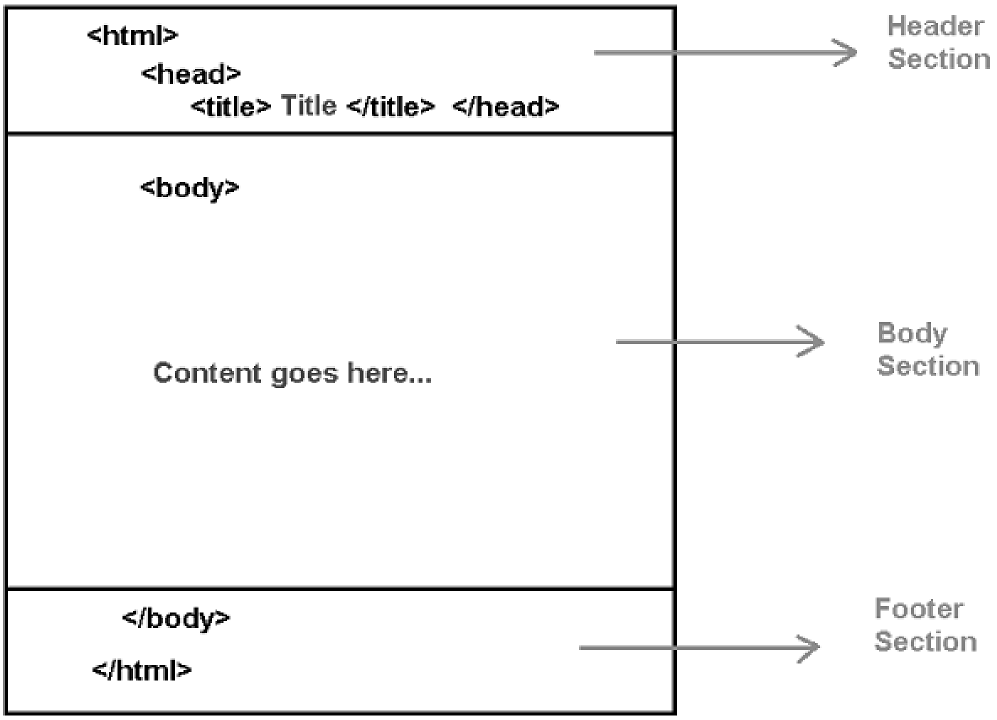


चित्र 7.31: वेब पेज की संरचना (HTTP कोडिंग)

हेड : हेड वेब पेज का प्रथम भाग है। हेड में पेज का शीर्षक और वह अन्य पेरामीटर्स होते हैं, जिनका ब्राउजर उपयोग करता है।

बॉडी : पेज का वास्तविक डाटा बॉडी में होता है। यह टेक्स्ट और टैग्स से निर्मित होता है। जहाँ टेक्स्ट किसी पेज में विद्यमान वास्तविक इंफॉर्मेशन होती है, वहीं टैग्स डॉक्यूमेंट की बनावट को परिभाषित करते हैं।

टैग्स : ब्राउजर टैग्स के आधार पर ही टेक्स्ट की सरंचना के बारे में निर्णय लेता है। ये टैग्स वे चिन्ह होते हैं, जो टेक्स्ट के बीच–बीच में विद्यमान होते हैं। टैग दो चिन्हों (<and>) के भीतर बंद होता है तथा सामान्यतः जोड़ियों में होते हैं।

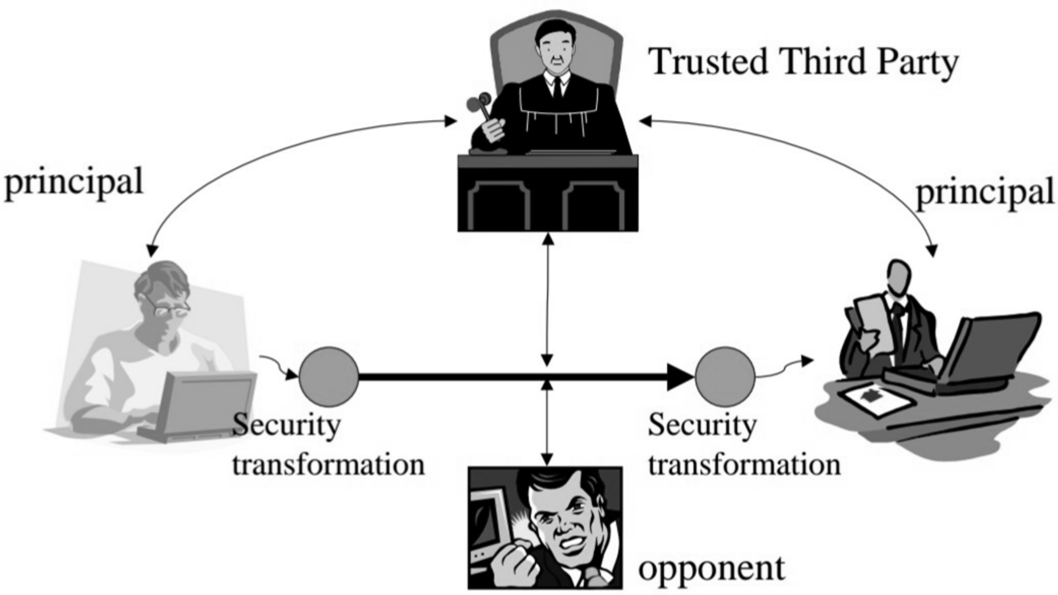


7.6 इंटरनेट सुरक्षा Internet Security

इंटरनेट सुरक्षा का अर्थ है – नेटवर्क तथा नेटवर्क पर उपलब्ध सूचना, डाटा या सॉफ्टवेयर को अनधिकृत व्यक्तियों (Unauthorized persons) की पहुंच से दूर रखना तथा केवल विश्वसनीय उपयोगकर्ताओं द्वारा ही इनका उपयोग सुनिश्चित करना।

आजकल इंटरनेट का उपयोग ऑनलाइन बैंकिंग और ई-कॉमर्स में काफी जोरों पर है, ऐसे में नेटवर्क की सिक्योरिटी अधिक महत्त्वपूर्ण हो जाती है।

कंप्यूटर का उपयोग गोपनीय संवाद भेजने से लेकर ई-बिजनेस तक में काफी तेजी से बढ़ रहा है। एक तरफ जहां इससे काफी सुविधाएं बढ़ी हैं, वहीं दूसरी ओर सिक्योरिटी से संबंधित परेशानियों से भी दो-चार होना पड़ रहा है। नेटवर्क को सिक्योर रखना एक बड़ी चुनौती बन गया है, ताकि नेटवर्क ट्रैफिक से होकर गुजरने वाला मैसेज सुरक्षित अपने गंतव्य तक पहुंच सके।



चित्र 7.32: इंटरनेट सिक्योरिटी स्ट्रक्चर

आज बात करते हैं नेटवर्क सिक्योरिटी से संबंधित कुछ ऐसी ही कॉमन टर्म्स की, जिनके बारे में हमें बराबर सुनने को मिलता रहता है। नेट यूजर्स के रूप में इन टर्म्स की जानकारी होना तो हमारे लिए जरूरी है ही, साथ ही आजकल इंटरव्यू के दौरान भी इन कॉन्सेप्टों के बारे में आपसे पूछा जा सकता है।

जब भी हम नेटवर्क के संदर्भ में सिक्योरिटी की बात करते हैं तो हमारा उद्देश्य इस बात को सुनिश्चित करना होता है कि नेटवर्क ट्रैफिक से होकर गुजरने वाले मैसेज को कोई अनाधिकृत व्यक्ति एक्सेस न कर सके। आजकल इंटरनेट का उपयोग ऑनलाइन बैंकिंग और ई-कॉमर्स में काफी जोरों पर है, ऐसे में नेटवर्क की सिक्योरिटी और भी अधिक महत्त्वपूर्ण हो जाती है। नेटवर्क सिक्योरिटी प्रॉब्लम को आमतौर पर हम चार कैटेगरीज में रख सकते हैं।

7.6.1 सिक्योरिटी मुद्दे

प्राइवेसी: किसी मैसेज को भेजने वाले तथा इसे पाने वाले व्यक्ति की कॉन्फिडेंशिएलिटी इसके तहत आती है। भेजा जाने वाला मैसेज केवल अधिकृत यूज़र को ही डिलीवर होना चाहिए। प्राइवेसी के लिए आमतौर पर मैसेज को इनक्रिप्ट किया जाता है।

मैसेज ऑथेंटिकेशन: आप जिस मैसेज को प्राप्त करते हैं, आपको यह पता होना चाहिए कि वह मैसेज किसी अधिकृत स्रोत से ही भेजा गया है। कभी-कभी कोई गलत व्यक्ति भी अपने आप को यह साबित करने की कोशिश करता है कि वास्तव में मैसेज का असली सेंडर वही है। मैसेज ऑथेंटिकेशन के लिए आजकल डिजिटल सिग्नेचर का प्रचलन जोरों पर है।

मैसेज इंटिग्रिटी: कभी-कभी ऐसा भी होता है कि नेटवर्क ट्रैफिक से गुजरते हुए मैसेज को 'हैक' कर उसे परिवर्तित कर दिया जाता है यानी ऑरिजनल मैसेज को ही बदल दिया जाता है। मैसेज इंटिग्रिटी से तात्पर्य है कि कोई मैसेज बिना किसी परिवर्तन के बिलकुल उसी फॉरमेट में रिसीवर (मैसेज पाने वाला) को प्राप्त होना चाहिए।

नॉन रिपुडिएशन (Non Repudiation) : इसका मतलब होता है कि मैसेज पाने वाला व्यक्ति यह साबित करने में सक्षम होना चाहिए कि उसने जो मैसेज पाया है, वह किसी स्पेसिफिक सेंडर द्वारा ही भेजा गया है। मतलब है कि मैसेज भेजने वाला व्यक्ति बाद में इस बात से इंकार न कर सके कि वह मैसेज उसके द्वारा नहीं भेजा गया है।

फायरवाल

नेटवर्क सिक्योरिटी के संदर्भ में फायरवाल भी काफी प्रसिद्ध विषय है। फायरवाल एक ऐसी तकनीक है, जिसके उपयोग से अनऑथराइज्ड इंटरनेट यूज़र्स को किसी इंट्रानेट यानी प्राइवेट नेटवर्क को एक्सेस करने से रोका जा सकता है। इस तरह हमारा इंटर्नल नेटवर्क सुरक्षित रहता है। इसे आप हार्डवेयर और सॉफ्टवेयर, दोनों ही रूप में इंप्लिमेंट कर सकते हैं। आमतौर पर हम चाहते हैं कि हमारा प्राइवेट नेटवर्क बाहरी दुनिया से एक्सेस न किया जा सके। ऐसे में फायरवाल काफी काम आता है। इतना ही नहीं, वायरस, स्पैम, मेक्रोज आदि से भी फायरवाल कंप्यूटर नेटवर्क की सुरक्षा करता है।

डिजिटल सिग्नेचर

डिजिटल सिग्नेचर के बारे में आपने जरूर सुना होगा। वास्तव में है तो यह भी सिग्नेचर ही, लेकिन इलेक्ट्रॉनिक फॉरमेट में। ज्यों-ज्यों फाइनेंशियल और अन्य एक्टिविटीज में नेट का उपयोग जोर पकड़ता जा रहा है, ऑनलाइन फ्रॉड की घटनाएं भी उसी तेजी से नजर आ रही हैं। ऐसे में डिजिटल सिग्नेचर एक उपयोगी टूल है। जिस प्रकार किसी प्रिंटेड डॉक्यूमेंट पर सिग्नेचर इस बात की पुष्टि करता है कि डॉक्यूमेंट वैध और सही है, ठीक उसी प्रकार इलेक्ट्रॉनिक डॉक्यूमेंट्स (ई-फॉर्म) पर डिजिटल सिग्नेचर इस बात का सूचक है कि डॉक्यूमेंट ऑथेंटिकेटेड और वैलिड है। डिजिटल सिग्नेचर की सहायता से किसी मैसेज की ऑथेंटिकेशन, इंटिग्रिटी और नॉन रिपुडिंएशिएशंस सुनिश्चित किया जा सकता है।

7.6.2 सिक्योरिटी नीतियां

कम्प्यूटर सिस्टम तथा नेटवर्क में धोखे से या बार – बार प्रयास कर (Trial and error Method) या सॉफ्टवेयर द्वारा पासवर्ड लीक होने की संभावना बनी रहती हैं। इससे बचने के लिए –

- पासवर्ड नियमित अंतराल पर बदलते रहना चाहिए।
- पासवर्ड बहुत छोटा नहीं होना चाहिए।
- पासवर्ड जितना बड़ा होगा, बार – बार प्रयास कर उसे प्राप्त करना उतना ही कठिन होगा।
- पासवर्ड में अक्षरों (Letters), अंकों (Numbers) तथा विशेष चिन्हों (Special Characters) का मिश्रण होना चाहिए।
- पासवर्ड में Capital Letters तथा Small Letters का मिश्रण भी प्रयोग किया जाना चाहिए।

7.6.3 नेटवर्क सिक्योरिटी टूल (फ़ायरवॉल)

Firewall हमारे कंप्यूटर की सुरक्षा के लिए होती है जो हमारे कंप्यूटर में वायरस को आने से या हमारे कंप्यूटर से वायरस जाने से रोकती है . अगर हम इंटरनेट का इस्तेमाल कर रहे है तो कई वेबसाइट हमारे कंप्यूटर में वायरस डालने की कोसिस करती है , जिस हमारी कंप्यूटर की Firewall रोक लेती है और हमारे कंप्यूटर को सुरक्षित रखती है . Firewall एक किस्म का Antivirus ही होता है .जो हमारी विंडो में Installed होता है.

अगर आप अपने कंप्यूटर में एक बढ़िया कंपनी का एंटीवायरस इंस्टॉल करते हैं तो आप अपने कंप्यूटर को ज्यादा सुरक्षित बना सकते हैं वैसे तो आप Free का एंटीवायरस भी इंस्टॉल कर सकते हैं लेकिन फ्री के एंटीवायरस में आपको वह सभी सुरक्षा के फीचर नहीं मिलेंगे जो आपके कंप्यूटर को चाहिए होते हैं तो कुछ पैसे लगाकर और एक बढ़िया प्रीमियम कंपनी का अच्छा एंटीवायरस अपने कंप्यूटर में इंस्टॉल कर लीजिए.नीचे आपको एंटीवायरस के या Firewall के क्या-क्या फायदे हैं यह आपको बताया गया है.

Firewall के क्या क्या फायदे है

जैसा की Firewall एक एंटीवायरस होता है जो आपके कंप्यूटर को सुरक्षित रखता है , लेकिन ये जरूर नहीं कि ये सिर्फ आपके कंप्यूटर को इंटरनेट से सुरक्षित रखेगा.

1. अगर आपका कंप्यूटर किसी दूसरे कंप्यूटर से नेटवर्किंग के द्वारा जुड़ा हुआ है और एप्प फाइल शेयर कर रहे है तो उस टाइम भी Firewall आपके कंप्यूटर को दूसरे कंप्यूटर से आने वाले वायरस से बचाएगा
2. Firewall सिर्फ आपके कंप्यूटर को दूसरे से नहीं बचता बल्कि अगर आपके कंप्यूटर में वायरस है तो वो उसे भी दुसरे कंप्यूटर में जाने से रोकता है .
3. अगर आप अपने कंप्यूटर को सुक्षित रखना चाहते है तो उसमें बढ़िया एंटीवायरस इंस्टाल करके रखे
4. कंपनी का एंटीवायरस इनस्टॉल करके रखे अगर आप इंटरनेट ज्यादा इस्तेमाल करते है तो कोशिस करे ही प्रीमियम एंटीवायरस का इस्तेमाल करे जो आपको ज्यादा Fearure देता है और आपके कंप्यूटर को Safe रखता है

Firewall कितने प्रकार के होते है – Types Of Firewall In Hindi?

सामान्यतः दो प्रकार के होते हैं हार्डवेयर और सॉफ्टवेयर. लेकिन इसके अलावा कुछ और स्टैंडर्ड में भी Firewall के प्रकार बताए जाते हैं जैसे की Packet Filters, Stateful Inspection, Proxys. लेकिन यहां पर हम सिर्फ 3 बड़े Firewall के बारे में ही बात करेंगे. जिसका इस्तेमाल सबसे ज्यादा किया जाता है.

Hardware Firewall

आजकल इंटरनेट Router में पहले से ही लगे हुए आते है जिस से आपके इन्टरनेट से आने वाले वायरस से सुरक्षा और भी बढ़ जाती है. बड़ी बड़ी कंपनियों में सभी कंप्यूटर एक ही नेटवर्क से जुड़े होते हैं तो इस तरह अगर किसी एक कंप्यूटर में वायरस आ जाता है तो वह उन सभी कंप्यूटर में आ जाएगा जो उस नेटवर्क के साथ में जुड़ गया है तो इसी वायरस से बचने के लिए उस नेटवर्क के मॉडल के ऊपर ही एक फ़ायरवॉल लगा दिया जाता है जिससे कि उस नेटवर्क पर ही किसी तरह के वायरस का असर नहीं होता है और उस नेटवर्क को ज्यादा सुरक्षित बनाया जाता है .

Sofware Firewall

हम एंटीवायरस को कहते है जो हमारे कंप्यूटर में पहले से इनस्टॉल होता है या हम उसे खरीद कर भी इनस्टॉल कर सकते है . एक साधारण फायरवाल हमारे विंडो के साथ में पहले ही आता है लेकिन हमारी विंडो को और ज्यादा सुरक्षित करने के लिए और इंटरनेट से भी वायरस ना आ जाए इसलिए हमें दूसरे सॉफ्टवेयर का भी इस्तेमाल करना पड़ता है इंटरनेट पर आपको ऐसे बहुत सारे सॉफ्टवेयर फ्री में मिल जाएंगे जोकि आपके कंप्यूटर को वायरस आने से ही बचाएंगे जैसे कि : – Avast, McAfee,Norton, QuickHeal इत्यादि .

प्रॉक्सी Firewall दूसरी Firewall के मुकाबले बहुत ज्यादा सुरक्षित होती है .लेकिन स्पीड और काम करने के मामले में यह फायरवाल थोड़ा सा धीरे काम करता है. और यह सभी नेटवर्क प्रोटोकॉल के साथ में Compatible भी नहीं होता है. प्रोटोकॉल को फायरवाल से पास होने के लिए हर एक प्रोटोकॉल और नेटवर्क के लिए एक नया Proxy Agent बनाना पड़ता है. Internal Protected Network की टोपोलॉजी को प्रॉक्सी फायरवाल की मदद से

छुपा लिया जाता है.क्योंकि Proxy Services दुनिया के बाहरी IP एड्रेस को कंप्यूटर से सीधा कम्युनिकेट नहीं कर सकते. जिससे हमारा कंप्यूटर एक्सटर्नल नेटवर्क से आने वाले डाटा से प्रभावित नहीं होता और ज्यादा सुरक्षित रहता है.

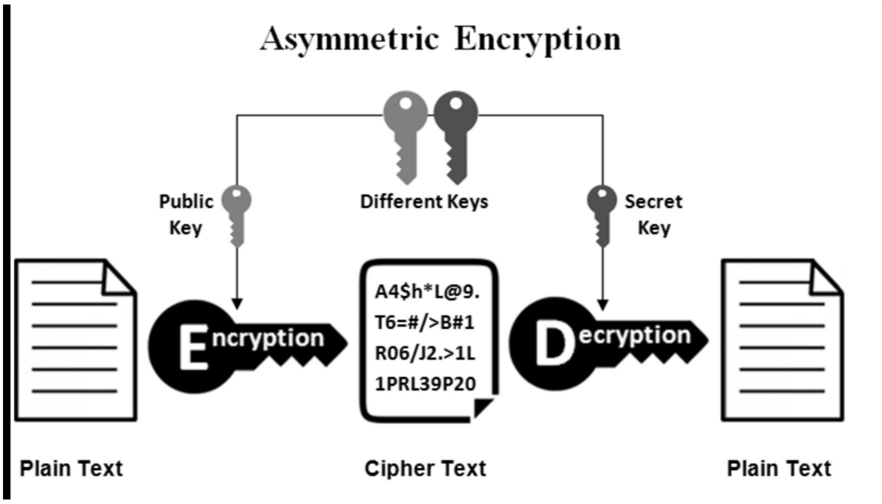
Firewall क्यों जरुरी है

फ़ायरवॉल एक सुरक्षा कवच की तरह काम करता है जैसे की हमारे घरों में दीवार होती है उसी तरह हमारे कंप्यूटर में फायरवाल या एंटीवायरस एक दीवार का काम करता है. अगर हमारे घर के चारों तरफ आग लग जाती है तो दीवारों के कारण वह आग हमारे घर के अंदर नहीं आ सकती. इसी तरह अगर हमारे कंप्यूटर में बाहर से कोई हानिकारक फाइल या वायरस आने की कोशिश करें तो फायर या एंटीवायरस उसे रोक लेता है. तो इसका सीधा सा मतलब है कि हमारे कंप्यूटर को ज्यादा सुरक्षित रखने के लिए हमें फ़ायरवॉल या एंटीवायरस की जरूरत पड़ती है.

7.7 क्रिप्टोग्राफ़ी

सूचना या डाटा को इंटरनेट पर भेजने से पहले उसे गुप्त कोड में परिवर्तित करना तथा प्राप्तकर्ता द्वारा उसे प्रयोग से पूर्व पुन: सामान्य सूचना में परिवर्तित करना क्रिप्टोग्राफी कहलाता हैं। यह इंटरनेट पर डाटा सुरक्षा का एक महत्वपूर्ण आधार है। सूचना या डाटा को गुप्त संदेशों में बदलने की प्रक्रिया Encryption कहलाती हैं। जबकि इनक्रिप्ट किए गए डाटा या सूचना को पुन: सामान्य सूचना में बदलना Decryption कहलाता हैं। क्रिप्टोग्राफी से डाटा स्थानान्तरण के दौरान डाटा चोरी होने या लीक होने की संभावना नहीं रहती है।

इन्टरनेट की दुनिया में एन्क्रिप्शन (Encryption) और डिक्रिप्शन (Decryption) शब्द बहुत प्रचलित शब्द है इन्टरनेट एक ऐसा जाल है जहाँ पर पर कुछ भी सुरक्षित नहीं है इसलिए इन्टरनेट में डाटा को सुरक्षित रखने के लिए एन्क्रिप्शन यूज़ किया जाता है,अगर आप एन्क्रिप्शन का यूज़ नहीं करते है तो आपका डाटा कोई भी हैक सकता है और उसका प्रयोग गलत कामो के लिए कर सकता है|



चित्र 7.33: **क्रिप्टोग्राफ़ी प्रक्रिया**

7.8 क्रिप्टोग्राफ़ी RSA अल्गोरिथम:

RSA एल्गोरिथ्म क्या है?

RSA अल्गोरिथम एक asymmetric क्रिप्टोग्राफ़ी अल्गोरिथम है। Asymmetric का यहाँ पर अर्थ हुआ ये दो अलग-अलग key पर कार्य करता है-पब्लिक key एउर प्राइवेट key.

जैसा कि इसके नाम से पता चलता है, पब्लिक key को सभी को दिया जाता है जबकि प्राइवेट करी को प्राइवेट रखा जाता है।

Asymmetric क्रिप्टोग्राफ़ी का उदाहरण:

1. एक क्लाइंट (जैसे कि ब्राउज़र) अपने पब्लिक key को सर्वर को भेजता है और कुछ डाटा के लिए निवेदन करता है।
2. उसके बाद सर्वर क्लाइंट के पब्लिक key का प्रयोग कर के उस डाटा को एन्क्रिप्ट करता है और उस एन्क्रिप्ट किये हुए डाटा को भेजता है।
3. उसेक बाद क्लाइंट उस डाटा को प्राप्त कर के डिक्रिप्ट करता है।

चूँकि ये असिमेट्रिक है, इसीलिए ब्राउज़र के अलावे कोई भी इसे डिक्रिप्ट नहीं कर सकता भले ही किसी थर्ड पार्टी के पास ब्राउज़र का पब्लिक key ही क्यों न हो।

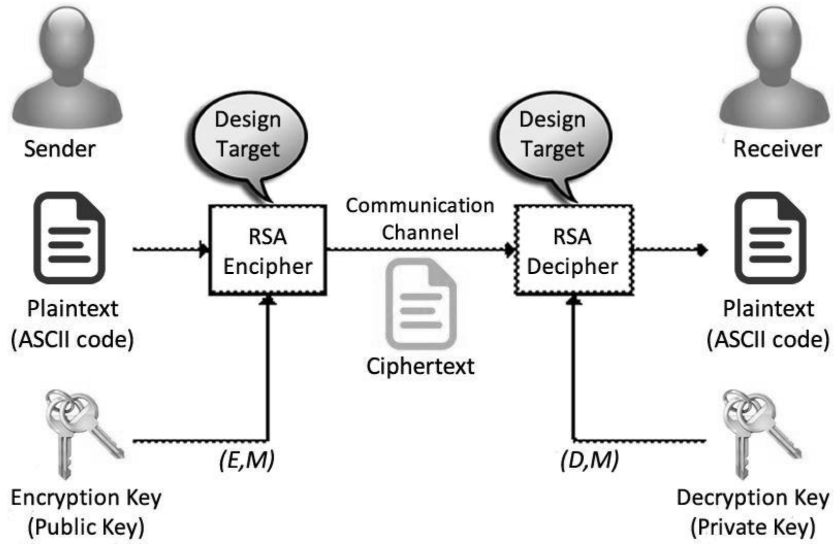
RSA अल्गोरिथम की कार्यप्रणाली (working of rsa algorithm in hindi)

RSA अल्गोरिथम का विचार इस बात पर आधारित है कि बड़े इन्टिजर को फैक्टर करना काफी मुश्किल काम है। पब्लिक key दो संख्याओं को मिला कर बना होता है जिसमे से एक संख्या दो बड़े प्राइम संख्या का गुना होता है।

एक प्राइवेट key को भी इतनी दो प्राइम संख्या से मिलाकर बनाया जाता है। इसीलिए अगर कोई बड़ी संख्या को फैक्टर कर सकता है तो प्राइवेट key को कोम्प्रोमाईज़ किया जा सकता है।

इसीलिए एन्क्रिप्शन की पूरी मजबूरी key के आकार पर निर्भर करती है और अगर हम key साइज़ को दुगुना या तिगुना करते हैं तो एन्क्रिप्शन की मजबूती भी काफी ज्यादा बढ़ जाती है।

RSA के key अधिकतर 1024 या 2048 बिट लम्बे होते हैं लेकिन अब एक्सपर्ट लोगों का मन्ना है कि निकट भविष्य में 1024 बिट के key को तोड़ा जा सकता है। लेकिन अभी तक तो ऐसा कुछ नहीं हुआ है।



चित्र 7.34: RSA अल्गोरिथम

RSA अल्गोरिथम का मैकेनिज्म :

पब्लिक key generate करने के लिए:

- दो प्राइम संख्या चुने। Suppose **P = 53 and Q = 59**.
  पब्लिक key का पहला भाग : **n = P*Q = 3127**.
- हमे एक छोटा एक्स्पोनेंट भी चाहिए, जैसे **e** :
  लेकिन e को होना चाहिए:
    - एक इन्टिजर
    - और n का फैक्टर नहीं होना चाहिए।
    - **1 < e < Φ(n)** [Φ(n) को नीचे बताया गया है],
      अब मानते हैं कि ये 3 के बराबर होगा।
- हमारा पब्लिक key n और eइ से बना है।

प्राइवेट key generate करने के लिए:

- हमे कैलकुलेट करना है Φ(n) :
  जैसे कि, **Φ(n) = (P-1)(Q-1)**
  इसीलिए, Φ(n) = 3016
- अब प्राइवेट key का कैलकुलेशन, **d** :
  d = (k*Φ(n) + 1) / e for some integer k
  k = 2 के लिए, d का मान होगा 2011.

अब हमारे पास है हमारे पब्लिक key (n = 3127 and e = 3) और प्राइवेट Key (d = 2011)।

RSA का उदाहरण (rsa algorithm example in hindi)

आइये अब हम **"HI"** को एन्क्रिप्ट कर के देक्लहते हैं कि ये प्रक्रिया कैसे काम करती है:

- पहले अक्षर को संख्या में बदले : H = 8 and I = 9
- इसीलिए **Encrypted Data c = 89^{e} mod n**.
  अब हमारा एन्क्रिप्ट किया हुआ डाटा होगा 1394

अब हम **1394** को डिक्रिप्ट करेंगे:

- **Decrypted Data = c^{d} mod n**.
  इसीलिए हमारे एन्क्रिप्ट किया हुआ डाटा होगा 89

8 = H और I = 9 i.e. "HI".

RSA अल्गोरिथम का कोड

RSA अल्गोरिथम का C कोड:

```
RSA असिमेट्रिक क्रिप्टोग्राफ़ी का प्रोग्राम
// algorithm. For demonstration values are
// relatively small compared to practical
// application
#include<stdio.h>
#include<math.h>
// Returns gcd of a and b
int gcd(int a, int h)
{
    int temp;
    while (1)
    {
        temp = a%h;
        if (temp == 0)
          return h;
        a = h;
```

```
        h = temp;
    }
}
// Code to demonstrate RSA algorithm
int main()
{
    // दो रैंडम प्राइम संख्या
    double p = 3;
    double q = 7;
    //पब्लिक key का पहला भाग
    double n = p*q;
    // पब्लिक key का दूसरा भाग पता करने के लिए
    // e stands for encrypt
    double e = 2;
    double phi = (p-1)*(q-1);
    while (e < phi)
    {
        // e must be co-prime to phi and
        // smaller than phi.
        if (gcd(e, phi)==1)
            break;
        else
            e++;
    }
    // Private key (d stands for decrypt)
    // choosing d such that it satisfies
    // d*e = 1 + k * totient
    int k = 2;  // A constant value
    double d = (1 + (k*phi))/e;
    // Message to be encrypted
    double msg = 20;
    printf("Message data = %lf", msg);
```

```
    // Encryption c = (msg ^ e) % n
    double c = pow(msg, e);
    c = fmod(c, n);
    printf("\nEncrypted data = %lf", c);
    // Decryption m = (c ^ d) % n
    double m = pow(c, d);
    m = fmod(m, n);
    printf("\nOriginal Message Sent = %lf", m);
    return 0;
```

संदर्भ ग्रंथो की सूची

a) Kurose, J.F. and K.W. Ross (2003) Computer Networking: A Top Down Approach Featuring the Internet, Addison Wesley.

b) Tanenbaum, A.S. (2002) Computer Networks, Prentice Hall.

c) Sally Floyd and Van Jacobson, "On Traffic Phase Effects in Packet-Switched Gateways", Internetworking: Research and Experience, volume 3

d) S. Keshav, An Engineering Approach to Computer Networking.

e) J. Walrand & P. Varaiya, High-Performance Communication Networks.

f) वैज्ञानिक तथा तकनीकी शब्दावली आयोग द्वारा प्रकाशित मूलभूत शब्दावली

g) Rigney, C. and Willens, S. and Rubens, A. and Simpson, W.: RFC 2865: Remote Authentication Dial In User Service (RADIUS), 2000

h) Phaal, P. and Panchen, S. and McKee, N.: RFC 3176: InMon Corporation's sFlow: A Method for Monitoring Traffic in Switched and Routed Networks.

i) Trammell, B. and Boschi, E.: RFC 5103: Bidirectional Flow Export Using IP Flow Information Export (IPFIX).

j) Roesch, M.: Snort – Lightweight Intrusion Detection for Networks

k) Patton, S. and Yurcik, W. and Doss, D.: An Achilles' Heel in Signature-Based IDS Squealing False Positives in SNORT.

l) Goodall, J. and Lutters, W. and Rheingans, P. and Komlodi, A.: Preserving the Big Picture: Visual Network Traffic Analysis with TNV.

m) Northcutt, S. and Frederick, K. and Winters, S. and Zeltser, L. and Ritchey, R.: Inside Network Perimeter Security: The Definitive Guide to Firewalls, VPNs, Routers, and Intrusion Detection Systems, New Rider's Publishing

n) Deering, S. and Hinden, R.: RFC 2460: Internet Protocol, Version 6 (IPv6) Specification

वैज्ञानिक तथा तकनीकी शब्दावली आयोग के अंतर्गत डाटा कम्युनिकेशन की मूलभूत शब्दावली

band eliminating filter	बैंड निरसन निस्यंदक
band limiting filter	बैंड सीमन निःस्यंदक
band pass filter	बैंड पारक निःस्यंदक
band separation	बैंड पृथकन
band splitting	बैंड विपाटन
band splitting privacy device	बैंड विपाटन गोपनीयता युक्ति
band spread	बैंड विस्तरण
band width compression	बैंड चौड़ाई संपीडन
band width conversion factor	बैंड चौड़ाई रूपांतरणांक
band width economy	बैंड चौड़ाई मितव्ययिता
bar	पट्टी
barochamber	दाब कक्ष
barred	1. रोधित 2. वारित
base band amplifier	आधार बैंड प्रवर्धक
base band circuit	आधार बैंड परिपथ
base band frequency range	आधार बैंड आवृत्ति परास
base band frequency spectrum	आधार बैंड आवृत्ति स्पेक्ट्रम
base band interference	आधार बैंड व्यतिकरण
base band interference noise power	आधार बैंड व्यतिकरण रव शक्ति
base band noise	आधार बैंड रव
base band output signal	आधार बैंड निर्गम संकेत
base band reference frequency	आधार बैंड संदर्भ आवृत्ति
base band signal to thermal noise ratio	आधार बैंड संकेत-ताप रव
base band spectrum	आधार बैंड स्पेक्ट्रम
base band terminal equipment	आधार बैंड अंतक उपस्कर
base band transmission	आधार बैंड संचरण
base insulator	आधार विद्युत् रोधी
base plate	आधार प्लेट
base station	आधार स्टेशन
basic booster assembly	आधारी अभिवर्धक समुच्चय
basic channel spacing	आधारी चैनल अंतरण
basic channel unit	आधारी चैनल इकाई
basic field strength measurement	आधारी क्षेत्र प्रबलता माप
basic receiver	आधारी अभिग्राही
basic reference atmosphere	आधारी संदर्भ वायुमंडल
basic thermal radiation	आधारी ताप विकिरण
basic uni-directional system	आधारी एकदिशिक तंत्र
BCD time code	बी.सी.डी. काल कूट
beacon	बीकन
beacon receiver	बीकन अभिग्राही
beacon track	बीकन पथ
beam	किरणपुंज
beam area	किरणपुंज क्षेत्र
beam axis	किरणपुंज अक्ष

beam cluster	किरणपुंज गुच्छ
beam control	किरणपुंज नियंत्रण
beam coupling	किरणपुंज युग्मन
beam crossover	किरणपुंज संक्रमण
beam divergence	किरणपुंज अपसरण
beam focusing	किरणपुंज फोकसन
beam hopping	किरणपुंज प्लुति
beam isolation	किरणपुंज विलगन
beam jitter	किरणपुंज जिटर
beam sensor	किरणपुंज संवेदक
beam separation	किरणपुंज पृथकन
beam slewing	किरणपुंज द्रुतघूर्णन
beam splitter	किरणपुंज विपाटक
beam spread	किरणपुंज विस्तरण
beam switching	किरणपुंज स्विचन
beam wave guide feed	किरणपुंज तरंगपथक प्रभरण
bearer circuit	धारक परिपथ
bearing retainer	दिक्मान अवधारक
bearing swing	दिक्मान प्रदोल
beat	विस्पंद
beat frequency	विस्पंद आवृत्ति
beat frequency interference	विस्पंद आवृत्ति व्यतिकरण
beat frequency oscillator	विस्पंद आवृति दोलित्र
beat note	विस्पंदी स्वर
bend	बंक
bending angle	बंकन कोण
bias	अभिनति, बायस
bias distortion (asymmetrical distortion)	बायस विरूपण (असममित विरूपण)
bi-directional interruption	द्विदिशिक अंतरायन
bi-directional link	द्विदिशिक कड़ी
biennialization	द्विवर्षीकरण
bifilar helix	द्वितंतु कुंडलिनी
bifold solar array	द्विवलन सौर सरणी
binary check digit	द्वि-आधारी परीक्षण अंक
binary coded decimal	द्वि-आधारी कूटलिखित दशमलव
binary coded matrix	द्वि-आधारी कूटलिखित आव्यूह
binary digital signal	द्वि-आधारी अंकीय संकेत
binary signal	द्वि-आधारी संकेत
bio medicine	जैव औषध
bio-instrumentation harness	जैव यंत्रीकरण सज्जा
bioastronautics	जैव अंतरिक्षयानिकी
biodynamics	जैवगतिकी
bi orthogonal signalling	द्विलांबिक संकेतन
biosatellite	जैव उपग्रह
biosphere	जैवमंडल

bi-directional transmission	द्विदिशिक संचरण
bi-phase modulation	द्वि-कला मॉडुलन
bi-phase phase shift keying	द्वि-कला कला विस्थापन कुंजीयन
bi-phase system	द्वि-कला तंत्र
bi-propellant apogee motor	द्वि-प्रणोदक अपभू मोटर
bistatic mode	द्विस्थितिक विधा
bistatic radar equation	द्विस्थितिक रेडॉर समीकरण
bit distortion	द्वयंक विरूपण
bit insertion facility	द्वयंक निवेशन सुविधा
bit rate conversion	द्वयंक दर रूपांतरण
bit rate reduction	द्वयंक दर ह्रास
bit synchronism	द्वयंक तुल्यकालन
bit timing recovery	द्वयंक काल पुनः प्राप्ति
black body	कृष्णिका
black body temperature	कृष्णिका ताप
blade antenna	पंखाकृति ऐन्टेना
blanking	लोपन
blanking interval	लोपन अंतराल
blast area	स्फोटन क्षेत्र
blast shield	स्फोटन ढाल
blind transmission	अंध संचरण
blip	ब्लिप
block code	खंड कूट
block control signal	खंड नियंत्रण संकेत
block decoding scheme	खंड विकोडन योजना
blocked call attempt	अवरूद्ध आह्वान प्रयास
block house	सुदृढ़ गृह
blocking	अवरोधन
blocking loss	अवरोधन हानि
blocking shadow	अवरोधन छाया
blunt nose vehicle	कुंठित नासा यान
blur	अस्पष्ट
blurred indication	अस्पष्ट सूचन
body	1. पिंड 2. काय
body flexure	पिंड आनमन
body mounted array	पिंडारोपित सरणी
body mounted solar array	पिंडारोपित सौर सरणी
body stabilized spacecraft	पिंड स्थायीकृत अंतरिक्षयान
Boltzmann constant	बोल्ट्समान स्थिरांक
boost	अभिवर्धन
booster	अभिवर्धक
booster charge	अभिवर्धक आवेश
boot lace lens antenna	बूट फीता लेन्स ऐन्टेना
bore sight direction	प्रकाशीय संरेख दिशा
bore sight displacement	प्रकाशीय संरेख विस्थापन
bothway (telegraph) circuit	उभयपथी (तार) परिपथ
bothway circuit availability	उभयपथी परिपथ उपलब्धता

bothway telephone circuit	उभयपथी टेलीफोन परिपथ
boundary condition	परिसीमा प्रतिबंध
boundary layer separation	परिसीमा स्तर पृथकन
branching filter	शाखन निस्यंदक
branching network	शाखन जालक्रम
breadboard model	प्रयोगपट्ट मॉडल
breadboard testing	प्रयोगपट्ट परीक्षण
break-in on a transmission (Q-code)	संचरण-व्यवधान (क्यू-कोड)
break-in operate time	प्रचालन काल विच्छेदन
break-in-service	सेवा-व्यवधान
break-up charge	संखंडन आवेश
breakdown	भंग, भंजन
breakdown of internal down time	आंतरिक व्यवरोधकाल भंजन
breakdown of maintenance time	अनुरक्षणकाल भंजन
bridge	सेतु
bridging loss	सेतुबंधन हानि
bridging phase	सेतुबंधन प्रावस्था
bright spot	दीप्त बिंदु
brightness	दीप्ति
Brinell hardness	ब्रिनेल कठोरता
British Thermal Unit	ब्रिटिश ऊष्मा मात्रक
broad band filter	विस्तृत बैंड फिल्टर
broad band horn	विस्तृत बैंड हार्न
broad band service	विस्तृत बैंड सेवा
broad band single side band frequency division multiplexing	विस्तृत बैंड एकपार्श्व बैंड आवृत्ति विभाजन बहुसंकेतन
broad band spread-spectrum system	विस्तृत बैंडप्रसारी स्पैक्ट्रम तंत्र
broad band system	विस्तृत बैंड तंत्र
broad pulse	विस्तृत स्पंद
broadcast call	प्रसारण कॉल
broadcaster	प्रसारण कर्त्ता
broadcasting channel	प्रसारण चैनल
broadcasting coverage	प्रसारण व्याप्तिक्षेत्र
broadcasting from satellite	उपग्रह प्रसारण
broadcasting network	प्रसारण जालतंत्र
broadcasting reception	प्रसारण अभिग्रहण
broadcasting satellite	प्रसारण उपग्रह
broadcasting-satellite band	प्रसारण-उपग्रह बैंड
broadcasting satellite channel	प्रसारण उपग्रह चैनल
broadcasting satellite for experimental purpose	प्रायोगिक उद्देशीय प्रसारण उपग्रह
broadcasting-satellite service	प्रसारण-उपग्रह सेवा
broadcasting-satellite service for community reception	सामुदायिक अभिग्रहणार्थ प्रसारण-उपग्रह सेवा
broadcasting-satellite signal	प्रसारण-उपग्रह संकेत
broadcasting- satellite space station	प्रसारण-उपग्रह अंतरिक्ष केंद्र

broadcasting satellite system	प्रसारण-उपग्रह तंत्र
broadcasting-satellite system for community reception	सामुदायिक अभिग्रहणार्थ प्रसारण उपग्रह तंत्र
broadcasting-satellite transponder	प्रसारण-उपग्रह ट्रांसपोंडर
broadcasting satellite transmission	प्रसारण-उपग्रह संचरण
broadcasting schedule	प्रसारण अनुसूची
broadcasting service	प्रसारण सेवा
broadcasting signal	प्रसारण संकेत
broadcasting station	प्रसारण केंद्र.
broadside antena	निरक्षीय ऐन्टेना
broadside array	निरक्षीय सरणी
buffer amplifier	बफ़र प्रवर्धक
buffer capacity	बफ़र धारिता
buffer fund	बफ़र निधि
buffer memory	बफ़र स्मृति
buffer stage	बफ़र अवस्था
built-in antenna	अन्तर्निर्मित ऐन्टेना
built-in redundancy	अन्तर्निर्मित अतिरिक्तता
buried conductor	भूनिक्षिप्त चालक
burn	दाह
burn period	दाह काल
burn-out	पूर्ण ज्वलन
burried radial conductor	भूनिक्षिप्त त्रिज्य चालक

burst duration	प्रस्फोट अवधि
burst error correcting capability	प्रस्फोट त्रुटि संशोधन क्षमता
burst error correcting code	प्रस्फोट त्रुटि संशोधन कूट
burst length	प्रस्फोट दैर्ध्य
burst noise	प्रस्फोट रव
burst of noise	रव प्रस्फोट
burst synchronisation	प्रस्फोट तुल्यकालन
burst synchronisation signal	प्रस्फोट तुल्यकालन संकेत
burst transmission	प्रस्फोट संचरण
burst-mode carrier	प्रस्फोट विधा वाहक
busy hour call	व्यस्त घंटा भार
busy period	व्यस्त अवधि
busy traffic period	व्यस्त ट्रैफिक अवधि
by-pass	उपमार्ग
byte interleafing	बाईट अंतः पत्रण
byte time source	बाईट काल स्रोत
byte timing	बाईट कालन
cable	केबिल
cable circuit	केबिल परिपथ
cable connection	केबिल संयोजन
cable distribution	केबिल वितरण
cable distribution installation	केबिल वितरण अधिष्ठान
cable distribution network	केबिल वितरण जालक्रम

cable distribution system केबिल वितरण तंत्र
cable network केबिल जालक्रम
cable television केबिल टेलीविज़न
cable television system केबिल टेलीविजन तंत्र
cable termination केबिल समापन
caesium beam frequency standard सीज़ियम किरणपुंज आवृत्ति मानक
caesium clock सीज़ियम घड़ी
caesium frequency standard सीजियम आवृत्ति मानक
caging device पिंजरन युक्ति
calculator परिकलित्र
calendar day कैलेण्डर दिवस
calender year कैलेण्डर वर्ष
calibrated frequency scale अंशांकित आवृत्ति स्केल
calibrated generator अंशांकित जनित्र
calibrated noise generator अंशांकित रव जनित्र
calibrated signal generator अंशांकित संकेत जनित्र
calibrated standard radio frequency signal generator अंशांकित मानक रेडियोआवृत्ति संकेत जनित्र
calibrating signal अंशांकन संकेत
calibrating source अंशांकन स्रोत
calibration अंशांकन
calibration band width अंशांकन बैंड-चौड़ाई
calibration level अंशांकन स्तर
calibration service अंशांकन सेवा
calibration signal generator अंशांकन संकेत जनित्र
call कॉल, आह्वान
call booking service आह्वान बुकिंग सेवा
call confirmation आह्वान संपुष्टि
call congestion ratio आह्वान संकुलन अनुपात
call connected signal आह्वान संबद्‌ध संकेत
call connected signal आह्वान संबद्ध संकेत
call finder आह्वान अन्वेषी
call handling आह्वान प्रहस्तन
call information analysis आह्वान सूचना विश्लेषण
call operator signal आह्वान प्रचालक संकेत
call processing delay आह्वान प्रक्रमण विलम्ब
call progress indicator आह्वान प्रगति सूचक
call progress signal आह्वान प्रगति संकेत
call progress signal आह्वान प्रगति संकेत
call request signal आह्वान अनुरोध संकेत
call restriction service आह्वान निषिद्ध सेवा
call sequence आह्वान अनुक्रम
call success rate आह्वान सफलता दर
call trace आह्वान अनुरेखन
call waiting आह्वान प्रतीक्षा
call-in-progress signal आह्वान प्रगति संकेत
called line identification facility आहूत लाईन अभिनिर्धारण सुविधा

called station	आहूत केंद्र
called subscriber identification	आहूत- अभिदाता अभिनिर्धारण
called terminal	आहूत टर्मिनल
caller	आह्वान कर्त्ता
calling channel	आह्वान चैनल
calling frequency	आह्वान आवृत्ति
calling party identity message	आह्वानकर्त्ता अभिज्ञान संदेश
calling rate	आह्वान दर
calling signal	आह्वान संकेत
calling terminal	आह्वान टर्मिनल
calling tone	आह्वान टोन
calls per busy hour	आह्वान प्रति व्यस्त घंटा
cancellation	निरसन
cancellation ratio	निरसन अनुपात
canceller	निरसक
cantilevered mode	कैंटीलीवर विधा
capacitive reactance	धारिता प्रतिघात
capacitor	संधारित्र
capsule	कैप्सूल
carrier	वाहक
carrier deviation	वाहक विचलन
carrier energy dispersal technique	वाहक ऊर्जा परिक्षेपण तकनीक
carrier filter	वाहक निस्यन्दक, वाहक फिल्टर
carrier frequency	वाहक आवृत्ति
carrier frequency assignment	वाहक आवृत्ति नियतन
carrier frequency beat	वाहक आवृत्ति विस्पन्द
carrier frequency offset	वाहक आवृत्ति ऑफसैट
carrier modulation	वाहक मॉडुलन
carrier noise degradation	वाहक रव निम्नन
carrier operated device antinoise	वाहक प्रचालित युक्ति-प्रतिरव
carrier oscillator	वाहक दोलित्र
carrier phase reversal	वाहक कला व्युत्क्रमण
carrier phase shift	वाहक कला विस्थापन
carrier power flux density	वाहक शक्ति अभिवाह घनत्व
carrier re-insertion	वाहक पुनर्निवेशन
carrier recovery circuit	वाहक पुनःप्राप्ति परिपथ
carrier reduction	वाहक लघुकरण
carrier rejection filter	वाहक अस्वीकरण निस्यन्दक
carrier sense signal	वाहक संवेद संकेत
carrier sense system	वाहक संवेद तंत्र
carrier sensitivity	वाहक संवेदकता
carrier separation	वाहक पृथकन
carrier source stability	वाहक स्रोत स्थायित्व
carrier system	वाहक तंत्र
carrier to intermodulation-noise	वाहक-अंतरमॉडुलन रव अनुपात

carrier to system thermal noise ratio	वाहक-तंत्र ताप रव अनुपात
carrier voltage	वाहक वोल्टता
carrier-to noise ratio	वाहक-रव अनुपात
carry-over	अग्रनयन
Carson's rule band width	कार्सन बैंड चौड़ाई नियम
cartridge	कार्ट्रिज
cascaded circuit	प्रपाती परिपथ
case shift	केस विस्थापन
cassette	कैसेट
catalytic chamber	उत्प्रेरक कक्ष
cathode follower	कैथोड अनुगामी
cathode follower amplifier	कैथोड अनुगामी प्रवर्धक
cathode ray direction finder	कैथोड किरण दिशान्वेषी
cathode ray display	कैथोड किरण प्रदर्श
cathode ray oscilloscope (oscillograph)	कैथोड किरण दोलनदर्शी (दोलनलेखी)
cathode ray screen	कैथोड किरण पर्दा
cathode ray tube	कैथोड किरण नली
cathode resistor	कैथोड प्रतिरोधक
cavity	कोटर
cavity backed slot dipole antenna	कोटर दोषित द्विक ऐन्टेना
cavity klystron	कोटर क्लाइस्ट्रोन
C-band frequency	सी-बैंड आवृत्ति
CCIR computer based interim method	सी.सी.आई.आर. कंप्यूटर आधारित अंतरिम विधि
celestial ascending node	खगोलीय आरोही नोड
celestial body	खगोलीय पिंड
celestial horizon	खगोलीय क्षितिज
celestial radio source	खगोलीय रेडियो स्रोत
celestial X-ray source	खगोलीय ऐक्स-रे स्रोत
cell	सैल, कोष्ठिका
cell matrix	कोष्ठिका आव्यूह
cellular system	सैलुलर तंत्र
central angular zone	केंद्रीय कोणीय क्षेत्र
central control	केंद्रीय नियंत्रण
central control room	केंद्रीय नियंत्रण कक्ष
central frequency standard	केंद्रीय आवृत्ति मानक
central network control station	केंद्रीय जालक्रम नियंत्रण केन्द्र
central processing unit (CPU)	केंद्रीय प्रक्रमण एकक (सी.पी.यू.)
central radio office (CRO)	केंद्रीय रेडियो कार्यालय (सी.आर.ओ.)
central reference clock	केंद्रीय संदर्भ कालद
centralized automatic message accounting	केंद्रीकृत स्वतः सूचना लेखाकार्य
centralized clock interface	केंद्रीकृत कालद अंतरापृष्ठ
centralized inter exchange signalling	केंद्रीकृत अंतरकेंद्र संकेतन
centre frequency (of a band)	केंद्र आवृत्ति (बैंड का)
centre guard band	केंद्र रक्षक बैंड

centre of thrust	प्रणोद केंद्र
centrifugal potential	अपकेंद्री विभव
ceramic	सिरेमिक
Cerenkov counter	सेरेनकोव गणित्र
cessation of emmission	उत्सर्जन विराम
Cessegrain antenna	कैसेग्रेन ऐन्टेना
Cessegrain horn	कैसेग्रेन शृंग
chaff cloud	भ्रामक अभ्र
changeback code field	पृष्ठ परिवर्तन कूट क्षेत्र
changing colour sequence	परिवर्ती वर्णानुक्रम
channel	1. चैनल 2. प्रणाल
channel address word	चैनल पता शब्द
channel allocation strategy	चैनल नियतन व्यूह रचना
channel allocation time	चैनल नियतन समय
channel arrangement	चैनल विन्यास
channel capacity	चैनल क्षमता
channel centre frequency	चैनल केंद्र आवृत्ति
channel command word	चैनल समादेश शब्द
channel designator	चैनल संज्ञापक
channel distribution	चैनल वितरण
channel efficiency	चैनल दक्षता
channel failure	चैनल भंग
channel filter	चैनल निस्यंदक
channel identification	चैनल अभिनिर्धारण
channel isolation	चैनल विलगन
channel multiplexing equipment	चैनल बहुसंकेतन उपस्कर
channel noise power	चैनल रव शक्ति
channel selection filter	चैनल चयन निःस्यंदक
channel selection switch	चैनल चयन स्विच
channel separation	चैनल पृथकन
channel sharing analysis	चैनल सहभागन विश्लेषण
channel vocoder	चैनल वाक् कोडित्र
channel width	चैनल चौड़ाई
channelization	चैनलन, प्रणालन
channelized frequencies	चैनलीकृत आवृत्तियां, प्रणालीकृत आवृत्तियां
channelling	1. चैनलन 2. प्रणालन
characteristic admittance	अभिलक्षणिक प्रवेश्यता
characteristic chamber length	अभिलक्षणिक कक्ष दैर्ध्य
characteristic frequency	अभिलक्षणिक आवृत्ति
characteristic impedance	अभिलक्षणिक प्रतिबाधा
charge transfer device	आवेश अंतरण युक्ति
charge-discharge cycle	आवेश-विसर्जन चक्र
charged particle telescope	आवेशित कण दूरदर्शक
chip	चिप
chrominance signal	वर्णकत्व संकेत
chromosphere	वर्णमंडल

closed earth-track orbit	संवृत भू-पथ कक्षा
closed private network	संवृत निजी जालक्रम
closed-loop null-seeking system	संवृत-पाश शून्य अन्वेषी तंत्र
closely-coupled antenna	संवृततः युग्मित ऐन्टेना
cloud climatology	मेघ जलवायु विज्ञान
cluster analysis	गुच्छ विश्लेषण
clustering	गुच्छन
clutter	संकुल ध्वनि, कोलाहल
coalescence	संलयन
coarse pre-tuning	अपरिष्कृत पूर्व-समस्वरण
coarse sensor	अपरिष्कृत संवेदक
coarse stellar reference	अपरिष्कृत तारकीय संदर्भ
coast earth station	तट भू केंद्र
coast station	तट केंद्र
coastal antenna	तटीय ऐन्टेना
coastal refraction	तटीय अपवर्तन
coaxial	समाक्ष
coaxial cassette	समाक्ष कैसेट
coaxial pair	समाक्ष युगल
co-channel carrier	सहप्रणाल वाहक
co-channel digital signal	सहप्रणाल अंकीय संकेत
co-channel digital systems	सहप्रणाल अंकीय पद्धति
co-channel frequency sharing	सहप्रणाल आवृत्ति सहभाजन
co-channel interference	सहप्रणाल व्यतिकरण
co-channel isolation	सहप्रणाल विलगन
co-channel operation	सहप्रणाल प्रचालन
co-channel protection ratio	सहप्रणाल रक्षण अनुपात
co-channel spacing	सहप्रणाल अंतरण
co-channel transmitter	सहप्रणाल ट्रांसमीटर, सहप्रणाल प्रेषित्र
co-coverage network	सहव्याप्त जालक्रम
code	1. कोड, कूट 2. संकेत 3. संहिता
code conversion processor	कोड रुपांतरण संसाधित्र
code converter	कोड रूपांतरित्र
code division multiplexing	कोड भाजन बहुसंकेतन
code II operator	कोड II प्रचालक
code number	कोड संख्या
code violation detection	कोड उल्लंघन संसूचन
coded data information	कोडित आंकड़ा सूचना
coded information	कोडित सूचना
coded time information	कोडित समय सूचना
coding rate	कोडन दर
coding strategy	कोडन कार्यनीति
coding system	कोडन तंत्र
coding-decoding technique	कोडन-विकोडन तकनीक
co-direction frequency assignment	सहदिशा आवृत्ति समनुदेशन
co-direction frequency system	सहदिशा आवृत्ति तंत्र
co-frequency channel arrangement	सह-आवृत्ति चैनल व्यवस्था
co-frequency orthogonally polarized channel system	सह-आवृत्ति लांबिकतः ध्रुवीकृत चैनल पद्धति

coherence band width	संसक्तता बैंडचौड़ाई
coherence of frequency	आवृत्ति संसक्तता
coherence of phase	कला संसक्तता
coherent communication system	संसक्त संचार तंत्र
coherent detection	संसक्त संसूचन
coherent detector	संसक्त संसूचक
coherent electromagnetic energy	संसक्त विद्युत्-चुंबकीय ऊर्जा
coherent modulation	संसक्त मॉडुलन
coherent phase shift keying	संसक्त कला विस्थापन कुंजीयन
coherent PSK modulation	संसक्त पी.एस.के. मॉडुलन
coherent PSK transmission	संसक्त पी.एस.के. संचरण
coherent signal	संसक्त संकेत
cold gas jet system	शीत गैस प्रधार तंत्र
cold gas system	शीत गैस तंत्र
collect call	मूल्यदेय कॉल, कलेक्ट कॉल
collection area	संग्रहण क्षेत्र
collection optics	संग्रहण-प्रकाशिकी
collective antenna	सामूहिक ऐन्टेना
collimating telescope	समांतरकारी दूरदर्शक
collimation tower	समांतरण मीनार
collimator	समांतरित्र
collision frequency	संघट्ट आवृत्ति
colloid thruster	कोलॉइड प्रणोदक
colorimetry	वर्णमिति
colour	वर्ण, रंग
colour bar signal	वर्ण-धारी संकेत
colour code	वर्णकोड, वर्ण कूट
colour coding	वर्ण कोडन
colour film	रंगीन फिल्म
colour film recording	रंगीन फिल्म रिकार्डिंग
colour picture	रंगीन चित्र
colour signal	वर्ण संकेत
colour telecine equipment	रंगीन दूरदर्शन चलचित्र उपस्कर
colour television receiver	रंगीन दूरदर्शन अभिग्राही
colour television signal	रंगीन दूरदर्शन संकेत
colour TV programme	रंगीन टी.वी. कार्यक्रम
coma aberration	कॉमा विपथन
comb filter	कंघा फिल्टर
combined AM-PM signal	संयुक्त ए.एम-पी.एम संकेत
combined receiver	संयुक्त अभिग्राही
combined standard deviation	संयुक्त मानक विचलन
combiner	संयोजक
combining process	संयोजन प्रक्रम
combustion engine ignition circuit	दहन इंजन प्रज्वलन परिपथ
combustion unit	दहन एकक

earth receiving station	भू-अभिग्राही केंद्र
earth reflection	भू-परावर्तन
earth resistance	भू-प्रतिरोध
earth resource survey operational system	भू–संसाधन सर्वेक्षण प्रचालन तंत्र
earth resources satellite	भू-संसाधन उपग्रह
earth resources technology satellite	भू-संसाधन-प्रौद्योगिकी उपग्रह
earth sensor	भू-संवेदक
earth's equatorial bulge	भू-विषुवतीय उभार
earth's gravitational field	भू-गुरुत्वीय क्षेत्र
earth's gravity	भू-गुरुत्व
earth's infrared image	भू-अवरक्त प्रतिबिम्ब
earth's magnetic field	भू-चुंबकीय क्षेत्र
earth's radius	भू-त्रिज्या
earth's-satellite telemetering	भू-उपग्रह दूरमापन
earth spike	भू-स्पाइक
earth station	भू-केंद्र
earth station receiver	भू-केंद्र अभिग्राही
earth station transmitter	भू-केंद्र प्रेषित्र
earth storable propellant	भू-संचयी नोदक
earth strains	भू-विकृति; भू-वितति
earth track of a satellite	उपग्रह भू-पथ
earth tracking station	भू-अनुवर्तन केंद्र
earth-ionosphere waveguide	भू-आयन मंडल तरंगपथक
earth-oriented antenna	भू-अभिविन्यस्त ऐन्टेना
earth-oriented geosynchronous satellite	भू-अभिविन्यस्त भूतुल्यकालिक उपग्रह
earth-oriented spacecraft	भू-अभिविन्यास अंतरिक्षयान
earth-pointing yaw axis	भू-दिष्ट पार्श्ववर्तन अक्ष
earth-stabilized communication antenna	भू-स्थायीकृत संचार ऐन्टेना
earth-synchronous orbit	भू-तुल्यकालिक कक्षा
earth-to-space transmissions	भू-से-अंतरिक्ष प्रेषण
earth/moon liberation centre	पृथ्वी-चंद्रमा विमोचन केंद्र
earthing	भू-संपर्कन
earthing system	भू-संपर्कन तंत्र
earthlight	भू-दीप्ति
easterly launching	पूर्वोन्मुखी प्रमोचन
eccentric orbit	उत्केंद्री कक्षा
eccentricity	उत्केंद्रकता
echo amplitude	प्रतिध्वनि आयाम
echo control	प्रतिध्वनि नियंत्रण
echo delay time	प्रतिध्वनि विलंब काल
echo distortion noise	प्रतिध्वनि विरूपण रव
echo disturbance	प्रतिध्वनि विक्षोभ
echo path	प्रतिध्वनि पथ
echo pulse	प्रतिध्वनि स्पंद

error density	त्रुटि सघनता
error detection	त्रुटि संसूचन
error detection coding	त्रुटि संसूचन कोडन
error generation process	त्रुटि जनन प्रक्रम
error index of a measurement method	मापन विधि त्रुटि सूचकांक
error message	त्रुटि संदेश
error of prediction	प्रागुक्ति-त्रुटि
error protection code	त्रुटि रक्षण कोड
error rate-time distribution	त्रुटि दर-काल वितरण
error sensor	त्रुटि संवेदक
error susceptibility	त्रुटि संवेद्यता
error-burst correction	त्रुटि प्रस्फोट संशोधन
error-concealment processes	त्रुटि प्रच्छादन प्रक्रम
error-rate scatter-diagram	त्रुटि दर प्रकीर्णन आरेख
escape velocity	पलायन वेग
estimated junction frequency	आकलित संधि आवृत्ति
estimated time of arrival	आकलित आगमन समय
estimated time of departure	आकलित प्रस्थान समय
european broadcasting area	यूरोपीय प्रसारण क्षेत्र
european maritime area	यूरोपीय समुद्री क्षेत्र
even pulse	सम स्पंद
even-order components of a signal	संकेत समक्रम घटक
excess attenuation	अधिक्षीणन

exchange	**1. विनिमय 2. केंद्र, एक्सचेंज**
exchange of communications	**संसूचना-विनिमय**
exchange of traffic	**यातायात-विनिमय**
excited state	**उत्तेजित अवस्था**
exciter	**उत्तेजक**
exclusive digital selective calling frequency	**अपवर्जी अंकीय वरणात्मक वार्ता आवृत्ति**
executing command	**कार्यकारी कमान**
exhaust line	**निष्कासन पथ**
exhaust plasma	**निष्कासन प्लाज्मा**
exhaust plume	**निष्कासन पिच्छ**
exhuast velocity	**निष्कासन वेग**
exit cone (of a nozzle)	**(तुंड का) निगर्म शंकु**
exobasis	**बहिःआधार**
exobiology	**बहिर्जैविकी**
exosphere	**बहिर्मंडल**
expander	**1. प्रसारक 2. प्रसारित्र**
expansion buffer	**1. प्रसारण बफ़र 2. प्रसंरण बफ़र**
expansion wave	प्रसरण तरंग
experiment electronics	प्रयोग इलेक्ट्रॉनिकी
experiment sensor	प्रयोग संवेदक
experimental attenuation statistics	प्रायोगिक क्षीणन आंकड़े
experimental communication satellite	प्रायोगिक संचार उपग्रह

experimental earth exploration satellite	प्रायोगिक भू-अन्वेषण उपग्रह
experimental space communication earth station	प्रायोगिक अंतरिक्ष संचार भू-प्रेक्षण स्थल
experimental station	प्रायोगिक प्रेक्षण केंद्र
explosive decompression	विस्फोटी विसंपीडन
exponential distribution function	चरघातांकी बंटन फलन
exponential factor	चरघातांकी कारक
exponential probability law	चरघातांकी प्रायिकता नियम
exponential reference atmosphere	चरघातांकी संदर्भ वायुमंडल
express voice channel	द्रुत वाक् चैनल
express voice circuit	द्रुत वाक् परिपथ
extended area service	विस्तारित क्षेत्र सेवा
extended-bandwidth system	विस्तारित बैंड चौड़ाई तंत्र
extended frequency range	विस्तारित आवृत्ति परास
extended Kalman filter	विस्तारित कालमैन निस्यंदक
extended range reflection	विस्तारित परास परावर्तन
extended range telescope	विस्तारित परास दूरदर्शक
extent of a frequency range	आवृत्ति परास विस्तृति
external cable duct	बाह्य केबिल वाहिनी
external noise factor	बाह्य रव गुणक
external noise figure	बाह्य रवांक
extra bit capacity	अतिरिक्त द्वयांक धारिता
extraction filter	निष्कर्षण फिल्टर
extra-diffraction transmission loss	विवर्तनेतर संचरण हानि
extragalactic radio source	परागांगेय रेडियो स्रोत
extragalactic radio wave	परागांगेय रेडियो तरंगें
extrapolated curve	बहिर्वेशित वक्र
extra-terrestrial body	पार्थिवेतर पिंड
extraterrestrial noise	पार्थिवेतर रव
extra-terrestrial radiation	पार्थिवेतर विकिरण
extravehicular activity	यानेतर क्रियाकलाप
extremely high frequencies	अत्यंत उच्च आवृत्तियां
eye aperture	नेत्र द्वारक
eye diagram	नेत्र आरेख
factor of non-linear distortion	अरैखिक विरूपण कारक
fading	म्लानन
fading curve	म्लानन वक्र
fading duration	म्लानन अवधि
fading frequency	म्लानन आवृत्तिं
fading of signal	संकेत म्लानन
fading power spectrum	म्लानन शक्ति स्पेक्ट्रम
fading probability	म्लानन प्रायकिता
fading ratio	म्लानन अनुपात
fading safety factor-FSF	म्लानन सुरक्षा गुणक
fading simulator	म्लानन अनुकारी
failure corrective action	विफलता संशोधी क्रिया

instantaneous voltage	तात्क्षणिक वोल्टता
instructions	अनुदेश
instructions for the International Telephone Service	अंतर्राष्ट्रीय टेलीफोन सेवार्थ अनुदेश
instructions for the operation of the International Public Telegram Service	अंतर्राष्ट्रीय पब्लिक तार सेवा-प्रचालनार्थ अनुदेश
integrated circuit micro-processor	एकीकृत परिपथ सूक्ष्म संसाधित्र
integrated communication system	एकीकृत संचार तंत्र
integrated data processing	एकीकृत आंकड़ा प्रक्रमण तंत्र
integrated services digital network	एकीकृत सेवा अंकीय जालक्रम
integrated services network	एकीकृत सेवा जालक्रम
integrated switching and transmission network	एकीकृत स्विचन तथा संचरण जालक्रम
integrator	समाकलक
intelligence	1. आसूचना 2. बुद्धि
intensity of speech	वाक्-तीव्रता
inter stage	जड़ अवस्था
inter-carrier receiver	अंतरावाहक अभिग्राहित्र
inter-carrier reception	अंतरावाहक अभिग्रहण
inter-carrier sound	अंतरावाहक ध्वनि
inter-cell switching	अंतरासेल स्विचन
inter-channel interference	अंतराचैनल व्यतिकरण
inter-satellite band isolation	अंतराउपग्रह बैंड विलगन
inter-satellite interference	अंतराउपग्रह व्यतिकरण
inter-satellite link acquisition	अंतराउपग्रह लिंक अधिग्रहण
inter-satellite link	अंतराउपग्रह लिंक
inter-satellite relay system	अंतराउपग्रह रिले तंत्र
inter-satellite service	अंतराउपग्रह सेवा
inter-satellite spacing	अंतराउपग्रह अंतराल
inter-satellite system	अंतराउपग्रह तंत्र
inter-service channel	अंतरासेवा चैनल
inter-service interference	अंतरासेवा व्यतिकरण
inter-site coupling loss	अंतरास्थल युग्मन हानि
inter-symbol interference	अंतराप्रतीक व्यतिकरण
intercepted signal	अपरोधित संकेत
interception of radio communication	रेडियो संचार का अपरोधन
interchange circuit	विनिमय परिपथ
interconnection frequency	अंतःसंयोजन आवृत्ति
intercontinental clock synchronization	अंतरामहाद्वीपीय कालद तुल्यकालन
interdigital transducer	अंतरांगुलि ट्रांसड्यूसर
interface	अंतरापृष्ठ
interface between different layer	विभिन्न परतवर्ती अंतरापृष्ठ
interface circuit	अंतरापृष्ठीय परिपथ
interface equipment	अंतरापृष्ठीय उपस्कर
interface module	अंतरापृष्ठीय मॉड्यूल
interference	व्यतिकरण

interference between two channels	द्विचैनल मध्य व्यतिकरण
interference coupling	व्यतिकरण युग्मन
interference density	व्यतिकरण घनत्व
interference flux	व्यतिकरण अभिवाह
interference from co-channel	सह-चैनल से व्यतिकरण
interference immunity of a signal	संकेत प्रतिरक्षण व्यतिकरण
interference matrix	व्यतिकरण आव्यूह
interference noise per telephone channel	प्रति टेलीफोन चैनल व्यतिकरण रव
interference on a co-channel basis	समचैनल आधारक व्यतिकरण
interference peak	व्यतिकरण शिखर
interference potential	व्यतिकरण शक्यता
interference power density	व्यतिकरण शक्ति घनत्व
interference power flux density	व्यतिकरण शक्ति अभिवाह घनत्व
interference safety margin	व्यतिकरण सुरक्षा उपांत
interference sector	व्यतिकरण सेक्टर
interference sensitivity factor	व्यतिकरण सुग्राहिता गुणक
interference source	व्यतिकरण स्रोत
interference suppressor	व्यतिकरण संदमक
interference supression	व्यतिकरण संदमन
interference tone	व्यतिकरण टोन
interference zone	व्यतिकरण अंचल
interfering channel	व्यतिकारी चैनल
interfering emission	व्यतिकारी उत्सर्जन
interfering field	व्यतिकारी क्षेत्र
interfering frequency	व्यतिकारी आवृत्ति
interfering power flux	व्यतिकारी शक्ति अभिवाह
interfering radio-frequency signal	व्यतिकारी रेडियो आवृत्ति संकेत
interfering signal carrier	व्यतिकारी संकेत वाहक
interfering transmission	व्यतिकारी संचरण
interleaved carrier frequency	अंतरापत्रित वाहक आवृत्ति
interleaved channel	अंतरापत्रित चैनल
interleaved channel analogue system	अंतरापत्रित चैनल अनुरूप तंत्र
interleaved channel digital system	अंतरापत्रित चैनल अंकीय तंत्र
interleaved frequency	अंतरापत्रित आवृत्ति
intermediate distribution frame	मध्यवर्ती वितरण फ्रेम
intermediate failure	मध्यस्थ विफलता
intermediate freqeuncy selectivity	मध्य आवृत्ति वरणात्मकता
intermediate frequence characteristics	मध्य आवृत्ति अभिलक्षण
intermediate frequence response curve	मध्य आवृत्ति अनुक्रिया वक्र
intermediate frequency	मध्य आवृत्ति
intermediate frequency circuit	मध्य आवृत्ति परिपथ
intermediate frequency interconnection	मध्य आवृत्ति अंतर्योजन
intermediate frequency output	मध्य आवृत्ति निर्गम
intermediate frequency passband	मध्य आवृत्ति पारणबैंड

ion stream	आयन धारा
ion thruster	आयन प्रणोदक
ion-acoustic wave	आयन-ध्वनिक तरंग
ionization	आयनन
ionization density	आयनन घनत्व
ionization sheet	आयनन शीट
ionization trace	आयनन अनुरेख
ionized argon laser	आयनित आर्गन लेसर
ionized atmosphere	आयनित वायुमंडल
ionized regions of the atmosphere	आयनित वायुमंडल प्रदेश
ionopause	आयनमंडल सीमा
ionosonde	आयनसोंद
ionospheric wave	आयनमंडलीय तरंग
isochronous telegraph distortion	समकालिक टेलीग्राफ विरूपण
jumper	झंपक
junction	संधि
junction cable	संधि केबिल
junction diode	संधि डायोड
junction frequency	संधि आवृत्ति
junction group	संधि समूह
justification control signal	न्यायसंगत नियंत्रण संकेत
justification digit time slot	न्यायसंगत अंक काल खांचा
justification error	न्यायसंगत त्रुटि
justification frame	न्यायसंगत फ्रेम
justification frame structure	न्यायसंगत फ्रेम संरचना
justification service digit	न्यायसंगत सेवा अंक
justification time slot	न्यायसंगत काल खांच
justified satellite link	न्यायसंगत उपग्रह लिंक
key	कुंजी
key down position	अनुत्तेजित अवस्था
keyboard	कुंजी पटल
keyboard selection	कुंजीपटल वरण
keyboard transmitter	कुंजीपटल प्रेषित्र
keyed carrier	कुंजीयित वाहक
keyed numeral	कुंजीयित संख्यांक
keyed pilot	कुंजीयित मार्गदर्शी
keyed signal	कुंजीयित संकेत
keying	कुंजीयन
keying cycle	कुंजीयन चक्र
keying filter	कुंजीयन फिल्टर
keying speed	कुंजीयन गति
kicker magnet	प्रक्षेपक चुंबक
land cable	थल केबिल
land earth station	थल भू-केंद्र
land mobile service	थल गतिशील सेवा
land mobile station	थल गतिशील केंद्र

line filter	लाइन फिल्टर
line folding	लाइन वलन
line identification by the network	जालक्रम अभिनिर्धारित लाइन
line link frame	लाइन लिंक फ्रेम
line synchronizing pulse	लाइन तुल्यकालन स्पंद
line-of sight microwave link	दृष्टिरेखा सूक्ष्मतरंग लिंक
line-time waveform distortion	लाइन-काल तरंगरूप विरूपण
line-up	पंक्तिबद्धता, लाइनअप
line-up condition	पंक्तिबद्धता अवस्था, लाइन-अप अवस्था
link	कड़ी, लिंक
local battery	स्थानीय बैटरी
local call	स्थानीय कॉल
local clock pulse	स्थानीय कालद स्पंद
local gravity gradient vector	स्थानीय गुरुत्व प्रवणता सदिश
local mode	स्थानीय विधा
local mode service signal	स्थानीय विधा सेवा संकेत
local mode signal	स्थानीय विधा संकेत
local oscillator	स्थानिक दोलित्र
local oscillator frequency	स्थानिक दोलित्र आवृत्ति
local oscillator output signal	स्थानिक दोलित्र निर्गम संकेत
local oscillator radiation	स्थानिक दोलित्र विकिरण
local procedure error	स्थानीय प्रक्रिया त्रुटि
local telephone circuit	स्थानीय टेलीफोन परिपथ
local user terminal	स्थानीय उपभोक्ता टर्मिनल
local vertical error	स्थानीय ऊर्ध्व त्रुटि
locating	स्थान निर्धारण
location of spurious response	भ्रामक अनुक्रिया स्थिति निर्धारण
locus of frequencies	आवृत्तियों का बिंदुपथ
logarithmic amplifier	लघुगणकीय प्रवर्धक
logarithmic compressor	लघुगणकीय संपीडित्र
logarithmic display	लघुगणकीय प्रदर्श
logarithmic interpolation	लघुगणकीय अंतर्वेशन
logarithmic ratio	लघुगणकीय अनुपात
logic unit	तर्क एकक
logical channel (packet mode operation)	तर्कसंगत चैनल (पैकेट विधा प्रचालन)
logical channels for incoming calls only	केवल आगमी कॉलों हेतु तर्कसंगत चैनल
logical channels for out-going calls only	केवल निर्गमनी कॉलों हेतु तर्कसंगत चैनल
long distance communication	सुदूर संचार
long distance diffraction	सुदूर विवर्तन
long distance transmission	सुदूर संचरण
long haul circuit	दीर्घ कर्षण परिपथ
long haul terrestrial system	दीर्घ कर्षण पार्थिव तंत्र
long inter-satellite link	दीर्घ अंतरउपग्रह संपर्क
long term frequency stability	दीर्घकालिक आवृत्ति स्थायित्व

long-range interference	दीर्घ परासी व्यतिकरण
long-term interference	दीर्घकालिक व्यतिकरण
loop	पाश, लूप
loop bandwidth	पाश बैंड-चौड़ाई
loop bandwidth	पाशबैंड चौड़ाई
loop gain stability	पाश लब्धि स्थायित्व
loop input signal-to-interference ratio	पाश निवेश संकेत और व्यतिकरण अनुपात
loop lock ambiguity	लूप लॉक संदिग्धता
loop mean-square phase error	पाश कला त्रुटि वर्ग माध्य
loop propagation time	पाश संचरण काल
loop radiator	पाश विकिरक
loop receiving antenna	पाश ग्राही ऐन्टेना
loop system	पाश तंत्र
loop time delay of a route	मार्ग पाशकाल-विलंब
loop-like structure	पाशवत् संरचना
loop-type direction finder	पाश प्ररुपी दिशान्वेषी
looped signal	पाशित संकेत
looped-back clock	पाशित-पृष्ठ कालद
looping	पाशन
loss	हानि, ह्रास
loss/frequency characteristic	ह्रास/आवृत्ति लक्षण
loss/frequency distortion	ह्रास/आवृत्ति विरूपण
lossless antenna	ह्रासहीन ऐन्टेना
loss of block phase	रुद्ध कला ह्रास
loss of carrier signal	वाहक संकेत ह्रास
loss of circuit time	परिपथ काल ह्रास
loss of frame alignment	फ्रेम संरेखण ह्रास
loss of multiframe alignment	बहुफ्रेम अनुयोजन ह्रास
loss of multiframe signal	बहुफ्रेम संकेत ह्रास
loss of synchronism	तुल्यकालत्व ह्रास
loss on exchange	विनिमय ह्रास
lost circuit time	नष्ट परिपथ समय
low coupling	निम्न युग्मन
low cycle fatigue	निम्न चक्र श्रांति
low decay rate	निम्न क्षय दर
low frequency	निम्न आवृत्ति
low frequency ground wave	निम्न आवृत्ति भू-तरंग
low-frequency noise	निम्न आवृत्ति रव
low-frequency power	निम्न आवृत्ति शक्ति
low-frequency triangular waveform	निम्न आवृत्ति त्रिभुजाकार तरंगरूप
low frequency wave analyser	निम्न आवृत्ति तरंग विश्लेषित्र
low gravity	निम्न गुरुत्व
low index angle modulation	निम्न सूचकांक कोण मॉडुलन
low-index FM systems	निम्न सूचकांक एफ.एम. आवृत्ति मॉडुलन
low-index modulation	निम्न सूचकांक मॉडुलन

maritime mobile-satellite service	समुद्री चल-उपग्रह सेवा
maritime mobile-satellite system	समुद्री चल-उपग्रह तंत्र
maritime orbital test satellite	समुद्री कक्षीय जांच उपग्रह
maritime satellite	समुद्री उपग्रह
mark and space filter	चिह्न और अंतरिक्ष फिल्टर
mark and space frequency	चिह्न और अंतरिक्ष आवृत्ति
mark frequency	चिह्न आवृत्ति
marked cycle	चिह्नित चक्र
matrix	मैट्रिक्स, आधात्री
maximum mean power	अधिकतम माध्य शक्ति
maximum multi-path propagation delay speed	अधिकतम बहु-पथ संचरण विलंब चाल
maximum observed frequence	अधिकतम प्रेक्षित आवृत्ति
maximum permissible interference power level	अधिकतम अनुमेय व्यतिकरण शक्ति स्तर
maximum permissible level of interference	अधिकतम अनुमेय व्यतिक्रम स्तर
maximum permissible overall frequency error	अधिकतम अनुमेय समग्र आवृत्ति त्रुटि
maximum power density	अधिकतम शक्ति घनत्व
maximum power point tracking	अधिकतम शक्ति बिंदु अनुवर्तन
maximum sensitivity	अधिकतम सुग्राहिता
maximum signal deviation	अधिकतम संकेत विचलन
maximum signal direction finding	अधिकतम संकेत दिशा निर्धारण
maximum usable frequency	अधिकतम उपयोज्य आवृत्ति
maximum usable sensitivity	अधिकतम उपयोज्य सुग्राहिता
mean access time	माध्य अभिगम काल
mean anomaly	माध्य असंगति
mean atomic time scale	माध्य परमाण्विक समय मान
mean attenuation	माध्य क्षीणन
mean busy hour	माध्य व्यस्त काल
mean call duration	माध्य कॉल अवधि
mean delay of calls delayed	विलंबित कॉलों का माध्य विलंब
mean down time (space)	माध्य व्यवरोध काल
mean failure intensity	माध्य विफलता तीव्रता
mean long term loss	माध्य दीर्घावधि हानि
mean time scale	माध्य समय मान
mean time to failure	विफलता हेतु माध्य समय
mean time to restoration	पुनःस्थापन हेतु माध्य समय
mean value	माध्य मूल्य
measured signal	मापित संकेत
measurement instrument	मापन यंत्र
median signal strength	मध्य संकेत सामर्थ्य
median transmission loss	मध्य संचरण हानि
median unwanted carrier	मध्य अवांछित वाहक
medium capacity digital system	मध्यम क्षमता अंक तंत्र
medium frequencies	मध्यम आवृत्तियाँ
medium sensitivity frequency modulation receiver	मध्यम सुग्राहिता आवृत्ति मॉडुलन अभिग्राही

memory	स्मृति
memory capacity	स्मृति सामर्थ्य
memory dumping	स्मृति सन्निक्षेपण
message	संदेश
message alignment	संदेश संरेखण
message bit stream	संदेश द्वयंक धारा
message compression	संदेश संपीडन
message confirmation signal	संदेश पुष्टि संकेत
message error rate monitor	संदेश त्रुटिदर मानीटर
message of cancellation	निरसन संदेश
message relay	संदेश रिले
message routing	संदेश अनुमार्गण
message spacing	संदेश अंतराल
message switching	संदेश स्विचन
message transfer control	संदेश अंतरण नियंत्रण
message transfer delay	संदेश अंतरण विलंब
meter	1. मापी 2. मीटर
micro computer	सूक्ष्म कंप्यूटर
micro processor	सूक्ष्म संसाधित्र
microcomponent	सूक्ष्म घटक
micropulsation frequency	सूक्ष्मस्पंदन आवृत्ति
microwave absorber	सूक्ष्मतरंग अवशोषक
microwave antenna	सूक्ष्मतरंग ऐन्टेना
microwave background	सूक्ष्मतरंग पृष्ठभूमि
microwave beam	सूक्ष्मतरंग किरणपुंज
microwave data transmission	सूक्ष्मतरंग आंकड़ा संचरण
microwave feeder	सूक्ष्मतरंग प्रभरक
microwave frequency generator	सूक्ष्मतरंग आवृत्ति जनित्र
microwave generator	सूक्ष्मतरंग जनित्र
microwave integrated circuit	सूक्ष्मतरंग एकीकृत परिपथ
microwave link	सूक्ष्मतरंग कड़ी
microwave link analyser	सूक्ष्मतरंग कड़ी विश्लेषित्र
microwave network	सूक्ष्मतरंग जालक्रम
minimum intermediate frequency rejection ratio	न्यूनतम मध्यवर्ती आवृत्ति अस्वीकरण अनुपात
minimum moment of inertia	न्यूनतम जड़त्व आघूर्ण
minimum permissible basic transmission loss	न्यूनतम अनुमेय मूल संचरण हानि
minimum permissible transmission loss	न्यूनतम अनुमेय संचरण हानि
minimum signal	न्यूनतम संकेत
minimum signal element duration	न्यूनतम संकेत अवयव अवधि
minimum usable power flux-density	न्यूनतम उपयोज्य शक्ति अभिवाह घनत्व
minimum useful frequency separation	न्यूनतम उपयोगी आवृत्ति पृथकन
minimum-shift keying	न्यूनतम विस्थापन कुंजीयन
	कुमार्गण

multi path intermodulation noise	बहुपथी अंतरामॉडुलन रव
multi-address call	बहु-पता कॉल
multi-address telex call	बहु-पता टेलेक्स कॉल
multi-band antenna	बहुबैंड ऐन्टेना
multi-band satellite	बहुबैंड उपग्रह
multi-channel	बहु-चैनल
multi-channel carrier	बहु-चैनल वाहक
multi-channel equipment	बहु-चैनल उपस्कर
multi-channel frequency division emission	बहु-चैनल आवृत्ति-विभाजन उत्सर्जन
multi-channel frequency-division system	बहु चैनल आवृत्ति-विभाजन तंत्र
multi-channel modulation	बहु-चैनल मॉडुलन
multi-channel modulation index	बहु-चैनल मॉडुलनांक
multi-channel multiplex telephony	बहुचैनल मल्टीप्लेक्स टेलीफोनी
multi-channel peak deviation	बहु-चैनल उच्चतम विचलन
multi-channel phase deviation	बहु-चैनल प्रावस्था विचलन
multi-channel r.m.s. deviation	बहु-चैनल आर.एम.एस. विचलन
multi-channel radio-relay system	बहु-चैनल रेडियो-रिले तंत्र
multi-channel signal	बहु-चैनल संकेत
multi-channel system	बहु-चैनल तंत्र
multi-channel technique	बहु-चैनल तकनीक
multi-channel telegraph system	बहु-चैनल टेलीग्राफ तंत्र
multi-channel telephone traffic	बहु-चैनल टेलीफोन यातायात
multi-channel telephony	बहु-चैनल टेलीफोनी
multi-channel telephony system	बहु-चैनल टेलीफोनी तंत्र
multi-channel voice frequency telegraphy	बहु-चैनल वाक् आवृत्ति टेलीग्राफी
multi-frequency selection signalling	बहु आवृत्ति वरण संकेतन
multi-frequency signalling	बहु आवृत्ति संकेतन
multi-frequency signalling system	बहु-आवृत्ति संकेतन तंत्र
multi-frequency voice frequency telegraphy	बहुआवृत्ति वाक् आवृत्ति टेलीग्राफी
multi-frequency-shift keying technique	बहुआवृत्ति-विस्थापन कुंजीयन तकनीक
multi-function control code signal	बहुप्रकार्य नियंत्रण कोड संकेत
multi-functional monitoring equipment	बहुप्रकार्यात्मक मानीटरन उपस्कर
multi-hop FM equipment	बहुपद एफ. एम. उपस्कर
multi-level digital signal	बहुस्तरी अंकीय संकेत
multi-level error coding	बहुस्तरी त्रुटि कोडन
multi-level PSK modulation	बहुस्तरी पी.एस.के. मॉडुलन
multi-line protection switching	बहुरेखीय रक्षण स्विचन
multi-line switching equipment	बहुरेखीय स्विचन उपस्कर
multi-lingual format	बहुभाषी संरूप
multi-mode horn	बहुविधा शृंग
multi-range instrument	बहुपरासी यंत्र
multi-relay links	बहु रिले कड़ी
multi-satellite link	बहुउपग्रह कड़ी

multi-satellite system	बहुउपग्रह तंत्र
multi-section radio link	बहुभागीय रेडियो लिंक
multi-sectioned filter	बहुभागी फिल्टर
multi-slot	बहु-खांच
multi-standard receiver	बहुमानक अंभिग्राही
multipath signal	बहुपथी संकेत
multiple modulation	बहुमॉडुलन
multiple phase shift keying	बहुप्रावस्था विस्थापन-कुंजीयन
multiple signal selectivity	बहुसंकेत वरणात्मकता
multiple signal unit	बहुसंकेत यूनिट
multiple use circuit	बहु उपयोग परिपथ
multiple-access mode	बहुअभिगम विधा
multiple-access network	बहुअभिगम जालक्रम
multiple-access satellite	बहुअभिगम उपग्रह
multiple-access system	बहुअभिगम तंत्र
multiple-access terminal	बहुअभिगम टर्मिनल
multiple-band configuration	बहुबैंड विन्यास
multiple-channel group transmission by FM	FM द्वारा बहुचैनल समूह संचरण
multiple-channel telephone group	बहु-चैनल टेलीफोन समूह
multiple-route system	बहुमार्ग तंत्र
multiple-scattered signals	बहुप्रकीर्णित संकेत
multiple-source interference	बहुस्रोत व्यतिकरण
multiplex	मल्टीप्लेक्स, बहुसंकेत
multiplex carrier telephony	मल्टीप्लेक्स वाहक टेलीफोनी
multiplex equipment	मल्टीप्लेक्स उपस्कर
multiplex hierarchy	मल्टीप्लेक्स पदानुक्रम
multiplex link	मल्टीप्लेक्स कड़ी
multiplex noise	मल्टीप्लेक्स रव
multiplex signal	मल्टीप्लेक्स संकेत
multiplex structure	मल्टीप्लेक्स संरचना
multiplex telephony	मल्टीप्लेक्स टेलीफोनी
multiplex terminal	मल्टीप्लेक्स टर्मिनल
multiplex terminal equipment	मल्टीप्लेक्स टर्मिनल उपस्कर
multiplexd signal	बहुसंकेतित सिगनल
multiplexing arrangement	बहुसंकेतन व्यवस्था
multiplexing chain	बहुसंकेतन शृंखला
multiplexing loss	बहुसंकेतन हानि
multiplicative complex envelope factor	गुणनात्मक जटिल-अन्वालोप गुणक
multiplicative distortion	गुणनात्मक विरूपण
multiplicative noise	गुणनात्मक रव
multiprocessing	बहु संसाधन
mutilated signal	विकृत संकेत
mutilation of telegraphic signals	टेलीग्राफ संकेत विकृति
mutual coupling	अन्योन्य युग्मन
mutual impedance effect	अन्योन्य प्रतिबाधा प्रभाव
mutual impedence	अन्योन्य प्रतिबाधा

on-off keying modulation	चालू-बंद कुंजीयन मॉडुलन
on-off keying of the modulating audio frequencies	मॉडुलन श्रव्य आवृत्तियों का चालू-बंद कुंजीयन
on-off signal	चालू-बंद संकेत
one way	एकधा
one-bit code	एक द्वयंक कोड
one-frame memory	एक फ्रेम स्मृति
one-way operation	एकधा प्रचालन
one-way technique	एकधा तकनीक
one-way telephone channel	एकधा टेलीफोन चैनल
open circuit	विवृत परिपथ
open circuit voltage	विवृत परिपथ वोल्टता
operating frequency	प्रचालन आवृत्ति
operation console	प्रचालन कन्सॉल
operation mode	प्रचालन विधा
operational circuit	प्रचालन परिपथ
operational satellite circuit	प्रचालनीय उपग्रह परिपथ
operational staff	प्रचालनीय स्टाफ
operator	प्रचालक
optical fibre	प्रकाशिक तंतु
optical filter	प्रकाशिक निःस्यंदक
optical frequency	प्रकाशिक आवृत्ति
optical link	प्रकाशिक कड़ी
optical maser	प्रकाशिक मैसर
optical projection	प्रकाशिक प्रक्षेप
optical track	प्रकाशिक पथ
optical transmission	प्रकाशिक संचरण
optical wavelength	प्रकाशिक तरंग दैर्ध्य
orbit	कक्षा
order of priority of communication	संचार प्राथमिकता क्रम
order-wire	आदेश तार
order-wire communication	आदेश तार संचार
ordinary private communication	साधारण निजी संचार
ordinary private telegram	साधारण निजी तार
out going	बहिर्गामी
out-of-band	बैंड बाह्य
out-of-band interference	बैंडबाह्य व्यतिकरण
out-of-band signalling	बैंडबाह्य संकेतन
outgoing repeater	बहिर्गामी पुनरावर्तक
output electronics	निर्गम इलेक्ट्रॉनिकी
output processor	निर्गम संसाधित्र
output syntax	निर्गम वाक्यविन्यास
output waveform	निर्गम तरंगरूप
overall amplitude/frequency response	समग्र तरंगदैर्ध्य/आवृत्ति अनुक्रिया
overall circuit interruption time	समग्र परिपथ अंतरायन काल

overall communication integrity	समग्र संचार अखंडता
overall cross talk	समग्र संकर वार्ता
overall distortion	समग्र विरुपण
overall frequency response curve	समग्र आवृत्ति अनुक्रिया वक्र
overall loss	समग्र हानि
overall noise factor	समग्र रव गुणक
overall transmission loss	समग्र संचरण हानि
overhead wire	शिरोपरितार
overlap of marking and spacing signals	चिह्नन एवं अंतरण संकेतों की अतिव्याप्ति
overlap signalling	अतिव्यापी संकेतन
overlapping channel	अतिव्यापी चैनल
overload distortion	अतिभार विरुपण
ove-modulation	अधिमॉडुलन
packet level interface	वेष्टक स्तर अंतरापृष्ठ
packet retransmission	वेष्टक पुनःप्रसारण
packet-like data transmission	वेष्टक-सम आंकड़ा संचरण
parallel polarization	समांतर ध्रुवण
parallel system	समांतर तंत्र
parallel-twin transmission line	समांतर-युगल सचरण रेखा
parameter	प्राचल
parameter block separator	प्राचल ब्लॉक पृथकित्र
parameter circuit compatibility	प्राचल परिपथ संगतता
parameter name	प्राचल नाम

parametric amplifer	प्राचली प्रवर्धक
parametric oscillation	प्राचली दोलन
parasitic frequency modulation	परजीवी आवृत्ति मॉडुलन
parasitic oscillation	परजीवी दोलन
parasitic phase modulation	परजीवी कला मॉडुलन
parity bit	समता द्वयंक
parity check bit	समता परीक्षण द्वयंक
parity check coding	समता-परीक्षण कोडन
parity check element	समता परीक्षण अवयव
parity check symbol	समता परीक्षण प्रतीक
parity check-code	समता परीक्षण कोड
parity checking	समता परीक्षण
parity error	समता त्रुटि
parity unit	समता एकक
partial error	आंशिक त्रुटि
partial failure	आंशिक विफलता
partial response line code	आंशिक अनुक्रिया रेखा कोड
partially closed user group	आंशिकतः संवृत उपयोक्ता वर्ग
passive atomic frequency standard	निष्क्रिय परमाणु आवृत्ति मानक
passive filter circuit	निष्क्रिय फिल्टर परिपथ
passive measurement	निष्क्रिय माप
passive microwave radiometry	निष्क्रिय सूक्ष्मतरंग विकिरणमिति
passive microwave sensor	निष्क्रिय सूक्ष्मतरंग संवेदक

spool	चरखी, स्पूल
spot wobble	प्रबिंदु प्रदोलन
spread	विस्तार
spurious	भ्रामक
squelch	रवअवरोध, रवअवरोधन
squelching	रवअवरोधन, रवावरोधन
squesch	मौन करना
squib	फुलझड़ी युक्ति
squint	तिर्यक्
stable liberation point	स्थायी मोचन बिंदु
staging	मंचन
stand-by	आपातोपयोगी
stand-by redundancy	आपातोपयोगी अतिरिक्तता
standard earth station	मानक भू-केंद्र
standard software	मानक प्रक्रियासामग्री, मानक सॉफ्टवेयर
standing wave	अप्रगामी तरंग
star field	तारक क्षेत्र
Stark effect	स्टार्क-प्रभाव
start-stop	आरंभ-विराम
state concept	अवस्था संकल्पना
static terrain	स्थैतिक भू-भाग
station keeping	अप्रगामी अनुरक्षण
stationary satellite	स्थिर उपग्रह

status	अवस्थिति
steady	स्थिर
steerability	कर्षणीयता, परिचालनीयता
steering	1. स्टीयरिंग; 2. परिचालन
stellar reference system	तारकीय संदर्भ तंत्र
step	सोपान
stepped zone	सोपानित अंचल
stereo	त्रिविम, स्टीरिओ
stereophony	त्रिविम ध्वनिकी
stereoscopy	त्रिविमदर्शी
still picture broadcasting system	अचल चित्र प्रसारण तंत्र
stochastic frequency fluctuation	प्रसंभाव्य आवृत्ति उच्चावचन
storage	भंडारण
stored data transmission	भंडारित आंकड़ा प्रेषण
stowage	अस्थायी संचय
straggling	विचरण
stratopause	समताप सीमा
stratosphere	समताप मंडल
stratospheric sounding unit	समतापमंडलीय परिज्ञापन एकक
stray capacitance	अवांछित धारिता
streaking	रेखण
stretch	तनन
strut	आलंबन स्तंभ

synchronized	तुल्यकालित
synchronous detector	तुल्यकालिक संसूचक
synchrotron emission	सिंकोट्रॉन उत्सर्जन
syncrhonization	तुल्यकालन
synoptic view	साररूप दृश्य
syntax	वाक्यविन्यास
synthesis programme	संश्लेषण क्रमादेश
system alarm	तंत्र अलार्म
system bandwidth limiting frequency	तंत्र बैंडचौड़ाई सीमक आवृत्ति
system configuration	तंत्र विन्यास
system cycle	तंत्र चक्र
system inhomogeneity	तंत्र असमांगता
system linearity	तंत्र रैखिकता
system of rotation	घूर्णन-तंत्र
system pilot tone	तंत्र प्रारंभक टोन
system reliability	तंत्र विश्वसनीयता
tamed frequency modulation	साधित आवृत्ति मॉडुलन
tandem exchange	अनुबद्ध एक्सचेन्ज
tandem hop	अनुबद्ध प्लुति
tandem launch	अनुबद्ध प्रमोचन
tandem links	अनुबद्ध कड़ी
tandem path	अनुबद्ध पथ
tandem satellite connection	अनुबद्ध उपग्रह संयोजन
tandem signal unit	अनुबद्ध संकेत एकक
tandem system	अनुबद्ध तंत्र
tape recorder	टेप रिकार्डर
technical criteria for frequency sharing	आवृत्ति सहभाजन का तकनीकी निकष
technological constraintt	प्रौद्योगिकीय व्यवरोध
telecino (television cinema)	दूरदर्शन चल-चित्र
telecommand	दूर आदेश
telecommunication circuit	दूर संचार परिपथ
telecommunication geostationary satellite	दूरसंचार भू-तुल्यकाली उपग्रह
telecommunication network	दूरसंचार जालक्रम
teledrawing	दूरआरेखण
telegram	तार, टेलीग्राम
telegraphic distortion	टेलीग्राफीय विरुपण
telegraphy	टेलीग्राफी
telemetry	दूरमिति
telephone	टेलीफोन, दूरभाष
telephone data transmission	दूरभाष आंकड़ा प्रेषण
telephone dial	टेलीफोन डायल
telephone exchange	टेलीफोन एक्सचेन्ज, दूरभाष केंद्र
telephone traffic	टेलीफोन यातायात
telephony	दूरभाष विज्ञान, टेलीफोनी
teleprocessing	दूरभाष संसाधन

telerecording equipment	दूरअभिलेखन उपस्कर
teletex	टेलीटेक्स
television	दूरदर्शन, टेलीविजन
television signal	दूरदर्शन संकेत
telewriter	दूर लेखक
telex	टेलेक्स
tensile strength	तनन सामर्थ्य
terminal	टर्मिनल
terminal equipment	टर्मिनल उपस्कर
terminal impedance	टर्मिनल प्रतिबाधा
terminal telegraphic equipment	टर्मिनल टेलीग्राफ-उपस्कर
termination	समापन
terrestrial	पार्थिव
tesla coil	टेस्ला कुंडली
test call	परीक्षण कॉल
test tone	परीक्षण टोन
thermal noise	तापीय रव
thermo-couple	तापवैद्युत युग्म
thermo-stat	तापस्थापी
thermoionic equipment	तापायनी उपस्कर
threshold	देहली
threshold noise	देहली रव
threshold value	देहली मान
through connection	सीधा योजन
time and frequency data analysis	काल और आवृत्ति आंकड़ा विश्लेषण
time code generator	काल कूट जनित्र
time congestion	काल संकुलन
time constant	कालांक
time diagram	काल आरेख
time discrimination	काल विविक्तीकरण
time division modulation	काल विभाजन मॉडुलन
time division multiple access	काल विभाजन बहु-अभिगम
time domain	काल प्रांत
time frame	काल फ्रेम
time reference signal	समय संदर्भ संकेत
time signal dissemination via satellites	उपग्रह द्वारा समय संकेत विकीर्णन
time signal satellite service	समय संकेत उपग्रह सेवा
time slot	समय खांचा
time slot bit	समय खांचा द्वयंक
time slot sequence integrity	समय खांचा अनुक्रम अखंडता
time unit	काल इकाई
timer	कालद, कालमापित्र, टाइमर
timing	1. काल समंजन 2. काल मापन
tone control	स्वरक नियंत्रण
tone generation	स्वरक जनन
torque	बलाघूर्ण

total audio output	संपूर्ण श्रव्य निर्गम
total conductivity	संपूर्ण चालकता
total impulse	संपूर्ण आवेग
total multiplex signal band	संपूर्ण मल्टीप्लेक्स संकेत बैंड
total noise	संपूर्ण रव
total SSB power	संपूर्ण एस.एस.बी. शक्ति
total traffic capacity	संपूर्ण यातायात क्षमता
total utilization factor	संपूर्ण उपयोग कारक
tower	मीनार, टॉवर
tracking	अनुपथन, अनुवर्तन
tracking and data relay satellite	अनुपथन और आंकड़ा रिले उपग्रह
tracking and data relay satellite system	अनुपथन और आंकड़ा रिले उपग्रह तंत्र
tracking, telemetry and command	अनुपथन, दूरमिति और समादेश
tracking, telemetry, command and monitoring	अनुपथन, दूरमिति, समादेश और मॉनीटरन
traffic	यातायात, परियात
traffic handling capacity	यातायात प्रहस्तन क्षमता
trailer	ट्रेलर
trainee	प्रशिक्षु, प्रशिक्षणार्थी
training standard	प्रशिक्षण मानक
trajectory	प्रक्षेपपथ
transducer	ट्रांसड्यूसर
transfer loop	अंतरण पाश
transfer oscillator	अंतरण दोलित्र
transfer ratio	अंतरण अनुपात
transient effect	क्षणिक प्रभाव
transient emission	क्षणिक उत्सर्जन
transistor	ट्रांजिस्टर
transistorized equipment	ट्रांजिस्टरित उपस्कर
transit	पारगमन
transit between mark and space	चिह्न-रिक्ति मध्य संक्रमण
transit traffic	पारगमन यातायात
translation frequency	स्थानांतरीय आवृत्ति
transmission	प्रेषण, संचरण
transmission bandwidth	प्रेषण बैंड चौड़ाई
transmission carrying multiplexed voice channels	बहुसंकेतित ध्वनि चैनलवाही प्रेषण
transmission channel	प्रेषण चैनल
transmission characteristic	प्रेषण अभिलक्षण
transmission circuit	प्रेषण परिपथ
transmission coefficient	प्रेषण गुणांक
transmission efficiency	प्रेषण दक्षता
transmission gain	प्रेषण लब्धि
transmission in time-division multiplex	काल विभाजन मल्टीप्लेक्स प्रेषण
transmission loss	प्रेषण हानि
transmission medium	प्रेषण माध्यम

transmission performance	प्रेषण निष्पादन	triggering lead pulse	ट्रिगरन लीड स्पंद
transmission through the earth	भू-प्रेषण	triggering signal	ट्रिगरन संकेत
transmission unit	प्रेषण यूनिट	trop-pause	क्षोभमंडल सीमा
transmissivity	पारगम्यता	tropical year	सायन वर्ष
transmit end	प्रेषण सिरा	tropical zone	ऊष्ण कटिबंध
transmitter distortion	प्रेषित्र विरुपण	tropical zone fading	ऊष्ण कटिबंध क्षीणन
transmitter output power	प्रेषित्र निर्गम शक्ति	tropo-sphere	क्षोभमंडल
transmitter pass band	प्रेषित्र पारण बैंड	tropospheric propagation	क्षोभमंडलीय संचरण
transmitter unwanted side band	प्रेषित्र अवांछित पार्श्व बैंड	tropospheric propagation medium	क्षोभमंडलीय संचरण माध्यम
transmitting antenna	प्रेषी ऐन्टेना	true attenuation	यथार्थ क्षीणन
transmitting antenna gain	प्रेषी ऐन्टेना लब्धि	true value	यथार्थ मान
transmitting frequency	प्रेषण आवृत्ति	trunk	ट्रंक
transmitting standard	प्रेषण मानक	trunk exchange	ट्रंक एक्सचेंज
transmitting station	प्रेषण केंद्र	trunked system	ट्रंक-तंत्र
transmitting-receiving station	प्रेषण अभिग्राही केंद्र	trunking	ट्रंकन
transonic	पारध्वनि	truth table	सत्य सारणी
transparency	पारदर्शिता	tumbling	अवपातन
transponder	ट्रांसपॉन्डर, प्रेषानुकर	tuning	समस्वरण
transportable radio equipment	वहनीय रेडियो उपस्कर	tunnel-diode	सुरंग-डायोड
transposition error	पक्षांतरण त्रुटि	turbulent fluctuations	प्रक्षुब्ध उच्चावचन
travelling wave	प्रगामी तरंग	twisted pair	व्यावर्तित युगल
travelling wave tube	प्रगामी तरंग नलिका	two-way communication	द्वि-दिक् संचार
trigger circuit	ट्रिगर परिपथ, प्रवर्तक परिपथ	two-way continuity check	द्विक सातत्य जांच

UHF band	परा-उच्च आवृत्ति बैंड
unbalance (satellite)	असंतुलन (उपग्रह)
undocking (of two space vehicles)	(दो अंतरिक्ष यानों का) विलगन
unperforated tape	अछिद्रित टेप
unsuccessful call attempt	असफल कॉल प्रयास
uplink (=air borne plateform)	उत्कड़ी, अपलिंक
utility satellite	उपयोगी उपग्रह
vacancy	रिक्ति
value added tax (VAT)	अतिरिक्त मूल्य कर
vecoder	विकोडर, विकोडित्र
vecoding	विकोडिंग
vibrator	कंपित्र
videography	वीडियोलेखन, वीडियोग्राफी
videotex	वीडियोटेक्स
vocoder (voice coder)	वाक् कोडित्र
voice-frequency link	वाक् आवृत्ति कड़ी
voice-operated transmitter keyer	वाक्-प्रचालित ट्रांसमीटर कुंजीयक
weather satellite	मौसम उपग्रह
weight impulse	भार आवेग
wire	तार
wireless hearing aid	बेतार श्रव्य सहाय
work load	कार्यभार
working medium	कार्यकारी माध्यम
x-band	x-बैंड
young's modulus	यंग का गुणांक
z-axis modulation (=intensity modulation)	तीव्रता मॉडुलन
zero frequency	शून्य आवृत्ति