MASTER OF SCIENCE (COMPUTER SCIENCE)

COMPUTER NETWORK

UNIT-I

PREVIOUS YEARS QUESTIONS

प्रश्न 1 – *डाटा कम्यूनिकेशन के मूलभूत तत्व को लिखिये।*
Write down the main elements of data communication.

उत्तर–संचार प्रणाली में निम्नलिखित भाग होते हैं–

(1) सैण्डर (Sender)—सैण्डर अथवा स्रोत व्यक्ति प्रेषण हेतु डाटा प्रदान करता है। यह डाटा कोई फाइल, चित्र, ध्वनि अथवा कोई चलचित्र भी हो सकता है।

(2) संचार माध्यम (Medium)—सूचनाओं को एक स्थान से दूसरे स्थान तक स्थानान्तरण करने के लिये संचार माध्यम की आवश्यकता होती है। प्रायः यह संचार टेलीफोन लाइन के माध्यम से होता है।

संचार माध्यम दो प्रकार का होता है–

(a) निर्देशित संचार माध्यम (Guided Communication Medium)—इसके अन्तर्गत संचार तारों का प्रयोग किया जाता है; जैसे ट्विस्टेड-तार युग्म, कोएक्सिअल केबिल, फाइबर ऑप्टिक केबिल आदि।

(b) अनिर्देशित संचार माध्यम (Unguided Communication Medium)—इसके अन्तर्गत तारों का प्रयोग नहीं किया जाता; जैसे रेडियो तरंगें, माइक्रोवेव तरंगें, उपग्रह संचार आदि।

(3) प्राप्तकर्त्ता (Receiver)—यह एक ऐसी डिवाइस होती है जो संचार माध्यम से प्राप्त डाटा को Receive करती है।

(4) संचार प्रोटोकॉल (Communication Protocol)—प्रोटोकॉल वे तकनीकी नियम अथवा निर्देश हैं, जिनके द्वारा उपकरणों के मध्य संकेतों के संचार का संचालन किया जाता है। यह नियम सूचनाओं के संचार को नियन्त्रित करते हैं। इन नियमों तथा विधियों के समूह को संचार प्रोटोकॉल कहते हैं। ☐

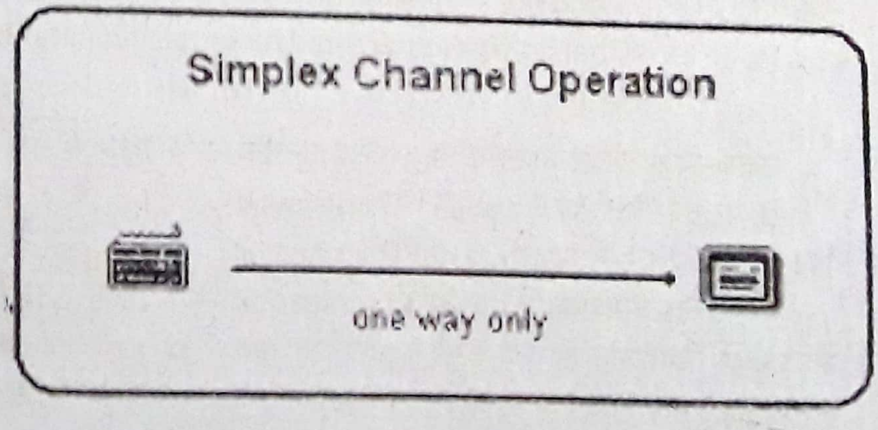
प्रश्न 2 – *Communication/Transmission media की अवस्थायें को बताइये।*
Explain communication/Transmission media mode.

अथवा (Or)

Simplex, Half Duplex और Full Duplex से आप क्या समझते हैं? बताइये।
What do you understand by simplex, Half duplex and full duplex? Explain.

उत्तर–डाटा संचार माध्यम की तीन अवस्थाएं होती हैं–

(1) सिम्प्लेक्स (Simplex)—डाटा संचार की इस अवस्था में आंकड़ों का प्रसारण सदैव एक ही दिशा में होता है। एक विशेष उपकरण द्वारा प्रेषित किये जाते हैं तथा अन्य उपकरण केवल अभिग्रहण की क्रिया करते हैं। इस प्रणाली में प्रेषक (Sender) उपकरण के द्वारा अभिग्रहण नहीं किया जाता है तथा अभिग्रहण (Receiver) उपकरण द्वारा प्रेषण नहीं किया जा सकता है।

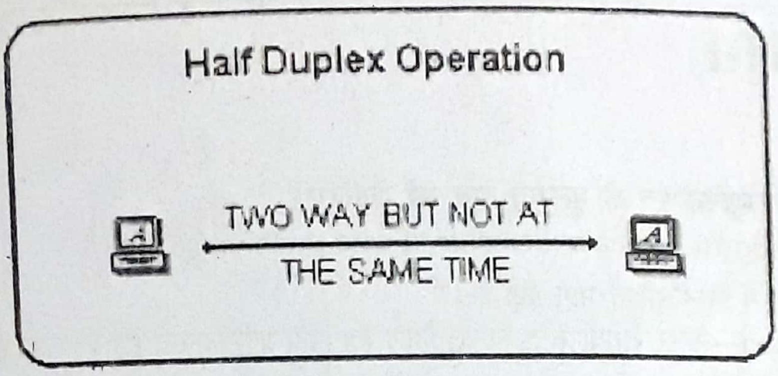


Scanned by CamScanner

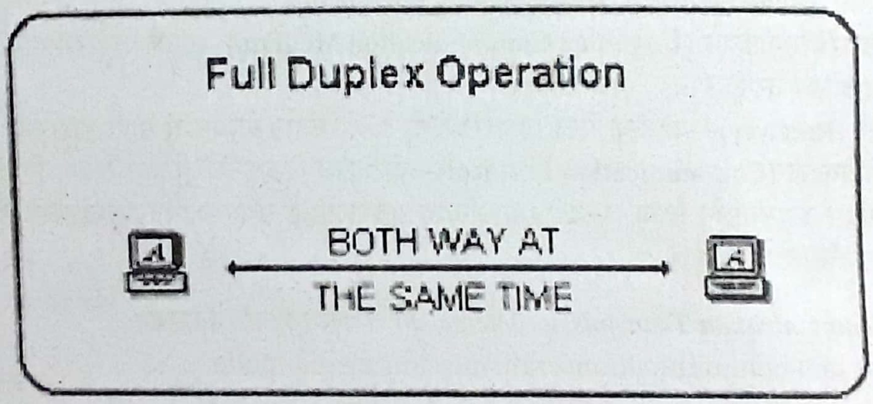
उदाहरणार्थ; रेडियो, टेलीविजन प्रसारण प्रणाली इसी प्रकार की होती है। कम्प्यूटर के की-बोर्ड के द्वारा डाटा को केवल की-बोर्ड से कम्प्यूटर की ओर प्रेरित किया जाता है। इस प्रणाली का मुख्य उपयोग इसके सस्तेपन के कारण है। इसके द्वारा वृहत्-क्षेत्र में प्रसारण सम्भव होता है परन्तु जिन डिवाइसेज में डाटा एक ही दिशा में संचारित होता है, इस Simplex लाइन का प्रयोग अनुपयुक्त है।

(2) अर्द्ध-ड्यूप्लेक्स (Half Duplex)—इस अवस्था में डाटा का संचरण दोनों दिशाओं में सम्भव होता है लेकिन एक समय में एक ही दिशा में डाटा का संचरण होता है। उदाहरणार्थ; स्थानीय क्षेत्रीय नेटवर्क में अर्द्ध-ड्यूप्लेक्स प्रणाली का उपयोग होता है।

कम्प्यूटर क्षेत्र में हार्ड डिस्क पर डाटा लिखने तथा पढ़ने की प्रणाली में डाटा का आदान-प्रदान अर्द्ध-ड्यूप्लेक्स अवस्था में ही होता है। जब हार्ड डिस्क पर डाटा सेव किया जाता है तो उस समय डाटा पढ़ा नहीं जा सकता और जब डाटा पढ़ा जा रहा हो, तब उस समय डाटा सेव नहीं किया जा सकता है।



(3) पूर्ण ड्यूप्लेक्स (Full Duplex)—इस अवस्था में एक ही समय में डाटा का संचरण दोनों दिशाओं में सम्भव है। इस प्रणाली में एक ही समय में प्रेषण तथा अभिग्रहण दोनों कार्य किये जा सकते हैं। इस प्रणाली में प्रेषक (Sender) तथा प्राप्तकर्त्ता दोनों के लिये दो भौतिक रूप की आवश्यकता होती है। उदाहरणार्थ, आधुनिक दूरभाष प्रणालियां पूर्ण ड्यूप्लेक्स सुविधा का उपयोग करती हैं।



प्रश्न 3 — ***Serial और Parallel Transmission/Communication से आप क्या समझते हैं? विस्तार से समझाइये।***

What do you understand by serial and parallel Transmission/Communication? Explain in detail.

उत्तर–किसी दो डिवाइसों के मध्य डाटा ट्रान्समिशन दो प्रकार से सम्पन्न होता है–

(i) पैरेलल ट्रांन्समिशन (Parallel Transmission)

(ii) सीरियल ट्रांन्समिशन (Serial Transmission)

पैरेलल ट्रान्समिशन (Parallel Transmission)—Parallel Transmission में बाइनरी डाटा (0 और 1) को Bits के समूह में संगठित कर लिया जाता है तथा संगठित डाटा एक साथ Transmit किया जाता है। Parallel Transmission में n-bits भेजने के लिये n-wire का प्रयोग किया जाता है; अर्थात् यदि हमें 8 bit डाटा भेजना है तो 8 तारों का प्रयोग करना होगा।

Scanned by CamScanner

Parallel Transmission की गति Serial Transmission से अत्यधिक होती है, परन्तु यह अत्यन्त महंगा होता है।

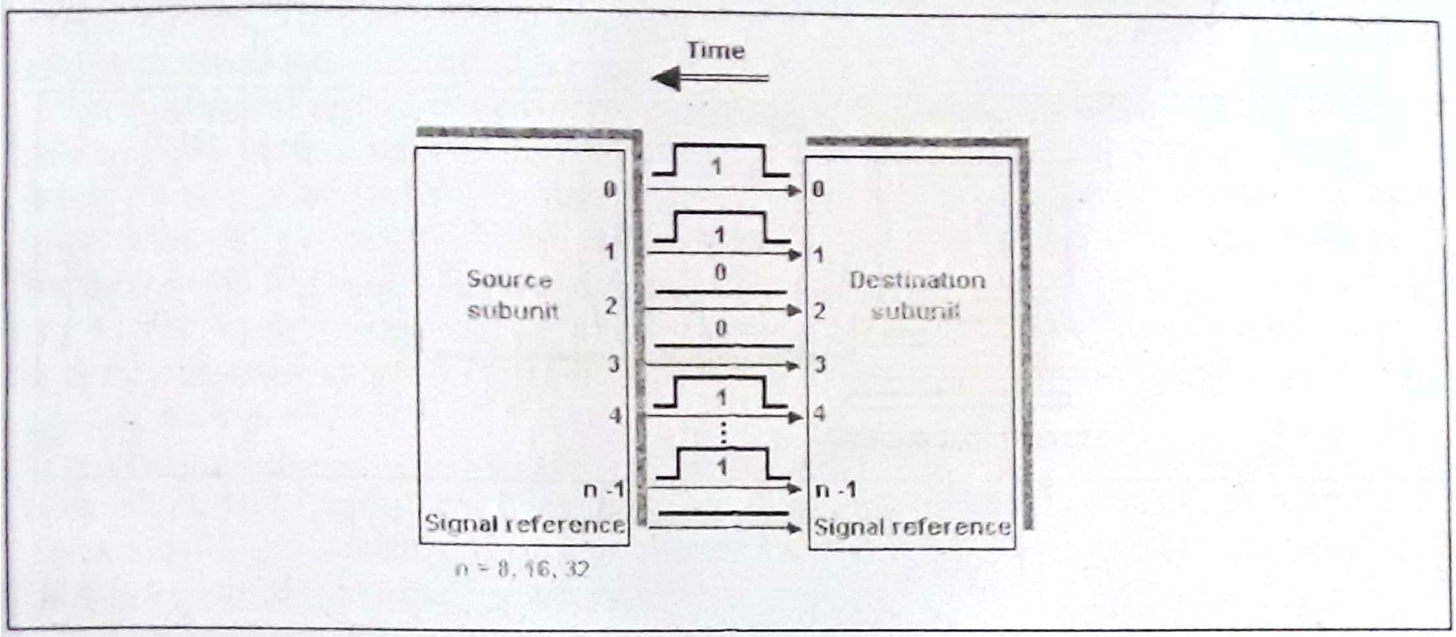


Fig. : Parallel Transmission Mode

सीरीयल ट्रान्समिशन (Serial Transmission)—Serial Transmission में एक-एक करके Bits भेजी जाती हैं, ये बिट्स एक-दूसरे का अनुसरण करती हैं।

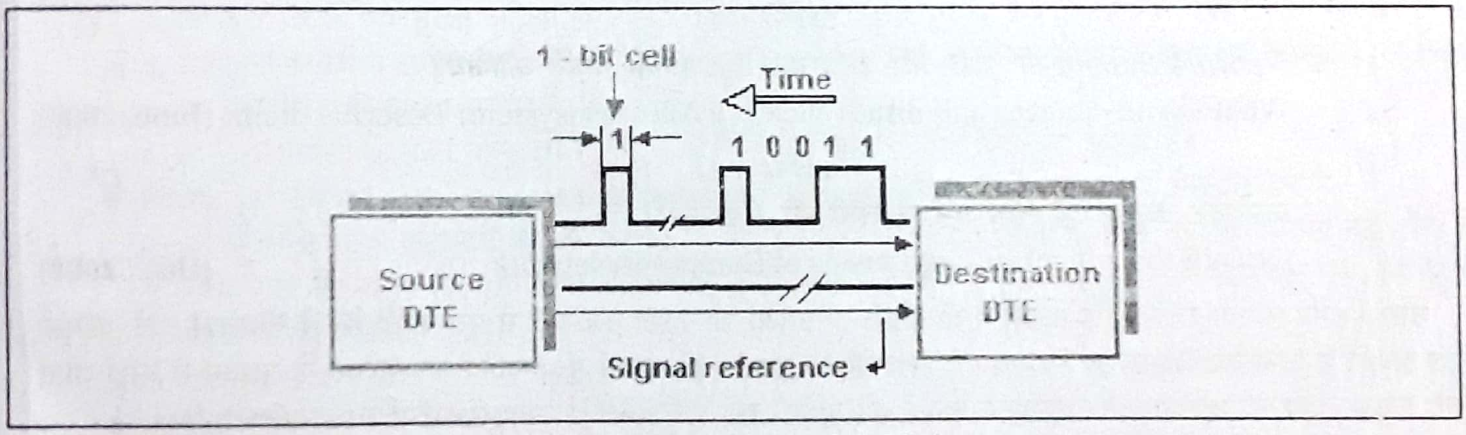


Fig. : Serial Transmission Mode

Serial Transmission, Parallel Transmission की तुलना में सस्ता होता है, परन्तु इसकी गति कम होती है।

Serial Transmission भी दो प्रकार से सम्भव है—

(i) Asynchronous Transmission

(ii) Synchronous Transmission

(i) Asynchronous Transmission—Asynchronous डाटा ट्रान्समिशन में डाटा Byte के साथ एक Stop Bit और एक Start Bit लगा दी जाती है। Start तथा Stop Bit का उद्देश्य Receiver को प्रत्येक Byte के आरम्भ और समाप्त होने की सूचना देना होता है। इसमें Data Transfer Byte के रूप में होता है।

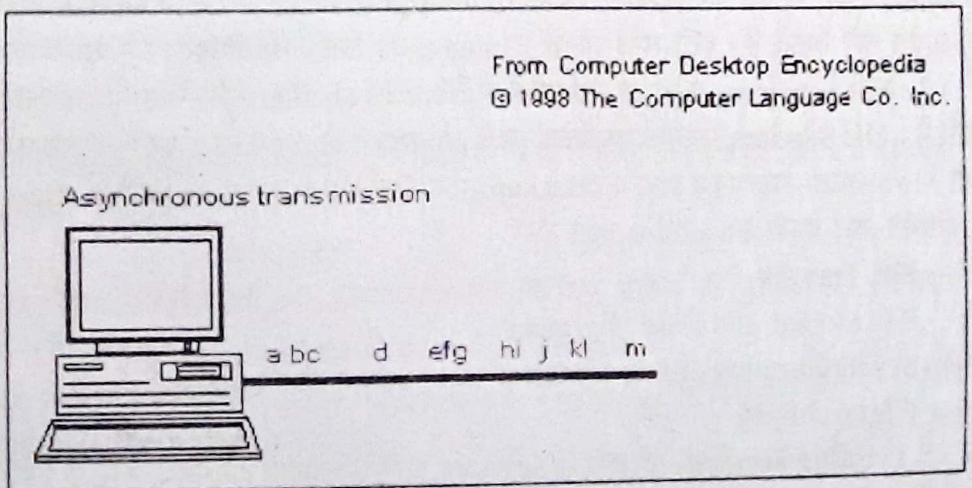


Fig. : Asynchronous Transmission

(ii) Synchronous Transmission—Synchronous Transmission में डाटा फ्रेम के रूप में होता है जो कि विभिन्न Bytes के समूहों से बना होता है। Receiver इस फ्रेम से Bytes को अलग कर लेता है। Synchronous Transmission निम्न प्रकार से होता है–

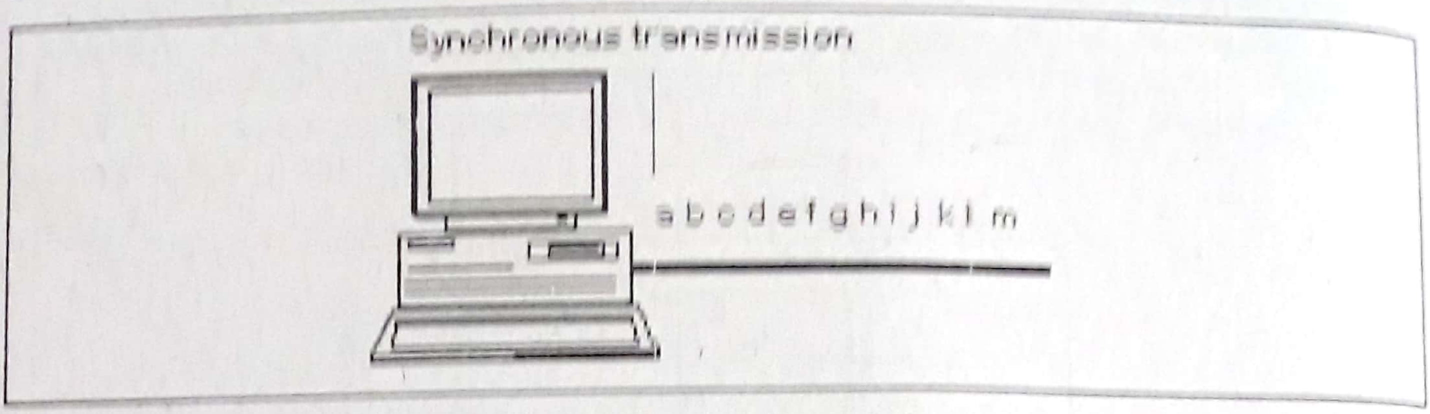


Fig. : Synchronous Transmission

❑

प्रश्न 4 – *कम्प्यूटरों को नेटवर्किंग करने की क्या आवश्यकता है? इसके क्या-क्या लाभ हैं?*

What is the requirement of Computer Networking? What are the advantages of Computer Networking? **(Jan., 2004; June, 2002; June, 2003; Dec., 2002)**

अथवा (Or)

***Network System* के लाभ और हानि क्या हैं? उनका वर्णन कीजिये।**

What are advantages and disadvatages of Network system? Describe them. **(June, 2004)**

अथवा (Or)

कम्प्यूटर नेटवर्क के लाभ एवं जरूरतों को समझाइये।

Explain the advantages and needs of Computer Network. **(Dec., 2008)**

उत्तर–कम्प्यूटर एक इलैक्ट्रॉनिक मशीन है जो हमारी समस्याओं को काफी तेज गति से पूरा करती है। ये समस्यायें आर्ट, कॉमर्स, साइंस इत्यादि से सम्बन्धित हो सकती हैं। जब एक से अधिक कम्प्यूटरों को आपस में कम्यूनिकेशन मीडिया के माध्यम से जोड़ा जाता है तब इसे कम्प्यूटर नेटवर्क कहते हैं। कम्प्यूटर नेटवर्क को संक्षिप्त रूप से निम्नलिखित रूप में परिभाषित कर सकते हैं–

"Group of Computers are linked together with a communication system is called Computer Network."

कम्प्यूटर नेटवर्क के प्रमुख लाभ निम्नलिखित हैं–

1. Resources Sharing–कम्प्यूटर नेटवर्क में जुड़े हुये सभी कम्प्यूटरों को आपस में जोड़ने का प्रमुख लाभ है। कि आप कम्प्यूटर Resources को Share कर सकते हैं। यदि 10 कम्प्यूटर्स के नेटवर्क में एक कम्प्यूटर से प्रिंटर जुड़ा है तो शेष 9 कम्प्यूटर भी इस प्रिंटर का प्रयोग कर सकते हैं। इसी तरह किसी Resource को किसी भी कम्प्यूटर पर प्रयोग किया जा सकता है।

2. File Services–कम्प्यूटर नेटवर्क में Resources Sharing की सुविधा नेटवर्क ऑपरेटिंग सिस्टम के माध्यम से उपलब्ध करायी जाती है। File Services, नेटवर्क एप्लीकेशन्स हैं जो फाइलों के रूप में डाटा को मैनीपुलेट करती हैं। इस Services में फाइलों को Copy तथा Move करना, महत्त्वपूर्ण डाटा को Backup करना तथा एक ही फाइल की विभिन्न drives को मैनेज करना इत्यादि है। File Services के अंतर्गत चार प्रमुख Functions आते हैं–

- File Transfer
- File Storage and Data Migration
- Synchronization of File Updates
- File Archiving

3. Printing Services–Printing Services, प्रिंटिंग डिवाइसों को मैनेज करने के लिये Allow करता है। प्रिंटिंग सर्विस का उद्देश्य व Printers तथा Fax Machines इत्यादि डिवाइसों को Share करना है; जो प्रिंटिंग कार्यों को आसानी से करती हैं।

Scanned by CamScanner

4. Mail Services—इस टाईप की Services के अंतर्गत स्टोरेज, इनफॉरमेशन का ट्रांसमिशन तथा प्रयोग आते हैं। इस तरह की इनफॉरमेशन मल्टीमीडिया डाटा, इम्बेडेड्ड ऑब्जेक्ट तकनीकियां होती हैं। इन फाइल सर्विस के अतिरिक्त Mail Services, यूजर्स के मध्य डॉयरेक्ट कम्यूनिकेशन या यूजर्स तथा एप्लीकेशनूस के मध्य कम्यूनिकेशन को मैनेज करती हैं। E-mail, Fax Services तथा इंटरनेट न्यूजग्रुप्स इत्यादि प्रमुख तीन Fundamental सेवायें इस Services में उपलब्ध हैं।

5. Application Services—एप्लीकेशन सर्विसेज प्रोसेसिंग पॉवर के अतिरिक्त डाटा शेयरिंग सर्विसेज भी उपलब्ध कराती हैं। ये Services, विभिन्न मशीनों के मध्य अधिक प्रभावशाली कार्यों को पूरा करती हैं; जैसे—यदि हम क्लाइंट के रूप में सर्वर से जुड़ते हैं तथा सर्वर पर एक प्रोग्राम के क्रियान्वयन की रिक्वेस्ट करते हैं और यदि सर्वर एक फाइल सर्वर है तो प्रोग्राम से सम्बन्धित फाइल नेटवर्क पर ट्रांसफर होती है और क्लाइंट मशीन पर मैमोरी में लोड होती है तथा क्लाइंट मशीन पर क्रियान्वित होती है। इसके विपरीत यदि सर्वर, एक एप्लीकेशन सर्वर है तो Peer-to-Peer कम्यूनिकेशन स्थापित होता है तथा मैसेजों का एक्सचेन्ज क्लाइंट तथा सर्वर के मध्य स्थापित होता है। क्लाइंट एक रिक्वेस्ट करता है तथा सर्वर से रेस्पांस का इंतजार करता है। क्लाइंट, प्रोग्राम के क्रियान्वयन के लिये रिक्वेस्ट करता है तत्पश्चात् प्रोग्राम सर्वर पर क्रियान्वित होता है तथा क्रियान्वयन का रिजल्ट क्लाइंट पर वापिस आता है। इस Case में सर्वर प्रोसेसर क्लाइंट के लिये कार्य करता है।

6. Database Services—Client/Server डाटा एप्लीकेशनूस में क्लाइंट रिक्वेस्ट करता है तथा रेस्पांस को प्रोसेस करता है। इसके सापेक्ष सर्वर, रिक्वेस्ट का विश्लेषण करता है तथा रिक्वेस्ट किये गये डाटा को सप्लाई करता है। इस रूप में सर्वर मशीन पर डाटा की फिजीकल लोकेशन को डाटा सिक्योरिटी के क्रम में चुना जा सकता है। कम्पनी लेवल पर केवल एक डाटाबेस Visible होता है। हालांकि फिजीकल लेवल पर डाटाबेस डिस्ट्रीब्यूटेड हो सकता है।

● **कम्प्यूटर नेटवर्क सिस्टम के लाभ**—कम्प्यूटर नेटवर्क सिस्टम के प्रमुख लाभ निम्नलिखित हैं—

1. कम्प्यूटरों का नेटवर्क बनाने से कम्प्यूटर पर कार्य करना आसान होता है।
2. कम्प्यूटर नेटवर्क से जुड़े हुये किसी भी कम्प्यूटर का डाटा किसी भी कम्प्यूटर पर देखा जा सकता है।
3. कम्प्यूटर नेटवर्क पर हार्डवेयर तथा सॉफ्टवेयर संसाधनों को Share कर सकते हैं, इससे लागत कम हो जाती है।
4. कम्प्यूटर नेटवर्क पर सुरक्षा अधिक होती है, इस तरह कोई Unauthorised User फाइलों में एक्सेस नहीं कर सकता है।
5. कम्प्यूटर नेटवर्क में सभी सॉफ्टवेयरों को एक कम्प्यूटर (सर्वर) पर लोड किया जा सकता है तथा शेष कम्प्यूटरों (Clients) पर इन्हें प्रयोग किया जा सकता है।
6. E-mail प्रणाली के तहत कम्प्यूटरों में आपस में मैसेज का आदान-प्रदान किया जा सकता है।

● **नेटवर्क की हानियां (Disadvantages of Network)**—कम्प्यूटर नेटवर्क की प्रमुख हानियां निम्नलिखित हैं—

1. कम्प्यूटर नेटवर्क में कम्प्यूटरों की संख्या बढ़ने पर यह काफी Complex हो जाता है, जिसे समझना आसान नहीं होता है।
2. नेटवर्क का रख-रखाव समय-समय पर करते रहना चाहिये अन्यथा नेटवर्क से जुड़े Resources के खराब होने पर पूरा नेटवर्क ध्वस्त हो जाता है।
3. Centralized नेटवर्क में सर्वर के खराब हो जाने पर फाइलों के डाटा के खो जाने की संभावना रहती है।

● **कम्प्यूटर नेटवर्क की आवश्यकता (Need of Computer Network)**—कम्प्यूटर नेटवर्क की जरूरत के प्रमुख कारण निम्नलिखित हैं—

1. यह यूजर्स तथा प्रोसेसर के मध्य आन्तरिक प्रक्रिया संवाद प्रदान करता है।
2. यह Resources को डिस्ट्रीब्यूट करता है।
3. यह कम Cost पर यूजर्स को अधिक सुविधा प्रदान करता है।
4. यह सॉफ्टवेयर्स तथा हार्डवेयर्स के मध्य अनुरूपता बनाता है।
5. यह Centralized मैनेजमेन्ट तथा नेटवर्क संसाधनों का आबंटन प्रदान करता है। ❑

प्रश्न 5 — ***Communication Channels से आप क्या समझते हैं? विभिन्न प्रकार के Communication Chanels को उनकी विशेषताओं के साथ बताइये।***

अथवा (Or)

डाटा ट्रांसमिशन में ट्रांसमिशन मीडिया की क्या उपयोगिता है? विभिन्न प्रकार के ट्रांसमिशन मीडिया को उनकी विशेषताओं के साथ बताइये।

What are the uses of transmission media in the data transmission? Explain various transmission media with their characteristics.

(Dec., 2006)

उत्तर—ट्रांसमिशन मीडिया (Transmission Media)—ट्रांसमिशन मीडिया का प्रयोग कम्प्यूटर नेटवर्क में जुड़े हुये कम्प्यूटरों में

Scanned by CamScanner

एक कम्प्यूटर से दूसरे कम्प्यूटर पर डाटा को ट्रांसमिट करने के लिये किया जाता है। कम्प्यूटर नेटवर्क में विभिन्न प्रकार के ट्रांसमिशन मीडिया का प्रयोग किया जाता है। इनमें से प्रमुख रूप से प्रयोग किये जाने वाले ट्रांसमिशन मीडिया निम्नलिखित हैं–

1. Twisted Pair Cables–Twisted Pair Cables का प्रयोग LAN में सबसे अधिक किया जाता है। यह Cable दो Insulated कॉपर की तारों से मिलकर बनी होती है। Unshielded Twisted Pair (UTP) तथा Shielded Twisted Pair (STP) दो प्रमुख तरह की Twisted Pair Cables का प्रयोग आवश्यकता के अनुसार किया जाता है। Twisted Pair Cables का प्रयोग करना आसान होता है क्योंकि यह Cables बाजार में आसानी से उपलब्ध हो जाती हैं तथा यह सबसे सस्ती Cables होती हैं।

2. Co-axial Cables–Twisted Pair Cables का मुख्य Drawback यह है कि इन्हें आसानी से तोड़ा जा सकता है; अर्थात् सुरक्षा की दृष्टि से यह कमजोर होती हैं क्योंकि इन्हें कोई भी हाथ से आसानी से तोड़ सकता है। इस तरह डाटा सही रूप में ट्रांसफर नहीं होता है। इस Drawback को दूर करने के लिये Co-axial Cables का प्रयोग किया जाता है। Co-axial Cable, Central Copper Conductor (Core) से मिलकर बनी होती है। यह Core, Second Conductor इन्सुलेशन से ढकी होती है जो पुनः प्लास्टिक की कवर से ढकी होती है।

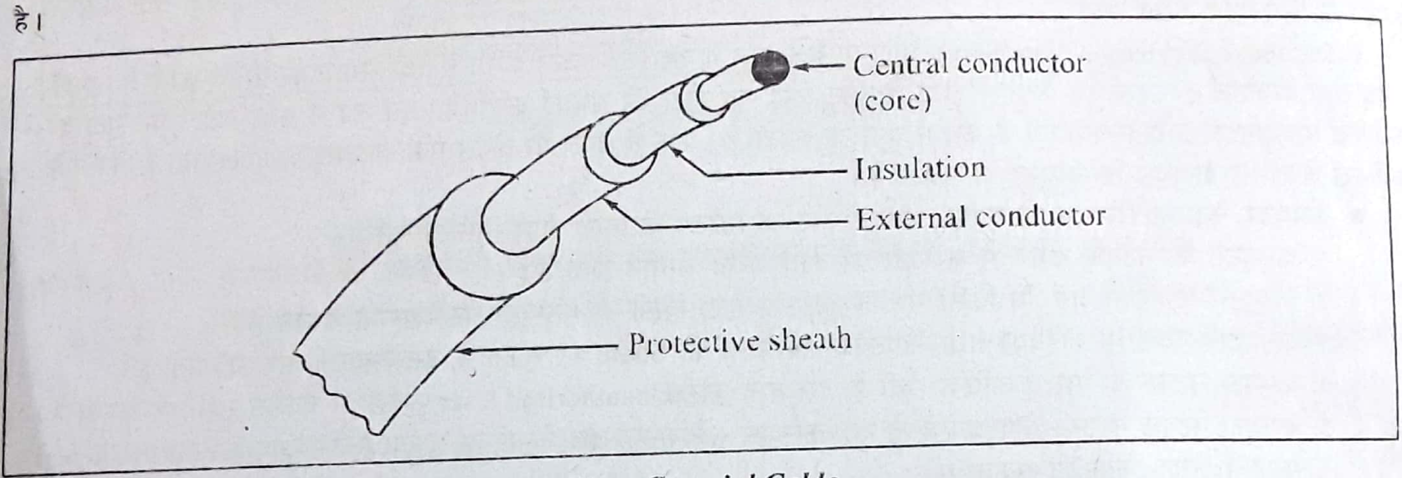


Fig. : Co-axial Cable

Co-axial Cable को इनके Impedance के अनुसार वर्गीकृत किया जाता है। 50 ohms डिजिटल ट्रांसमिशन तथा 75 ohms एनालॉग ट्रांसमिशन के रूप में Co-axial Cable को वर्गीकृत किया गया है। Twisted Pair Cables की तुलना में यह Cables अत्यन्त सुरक्षित होती हैं। इन्हें आसानी से तोड़ा नहीं जा सकता है। इनकी स्पीड Twisted Pair Cables की तुलना में तेज होती है। Co-axial Cables को लम्बी दूरी के नेटवर्क के लिये प्रयोग किया जाता है।

3. Fiber Optics–तीसरी प्रकार की प्रमुख Cable, Fiber Optics Cables होती है। Fiber Optics Cable, Fiber से मिलकर बनी होती है जो Light को Conduct करती है। यह Fiber ग्लास या प्लास्टिक के रूप में हो सकती है। Fiber Optics Cable में डाटा का ट्रांसमिशन काफी तेज होता है। यह Cables, सभी Cables की तुलना में मजबूत होती हैं।

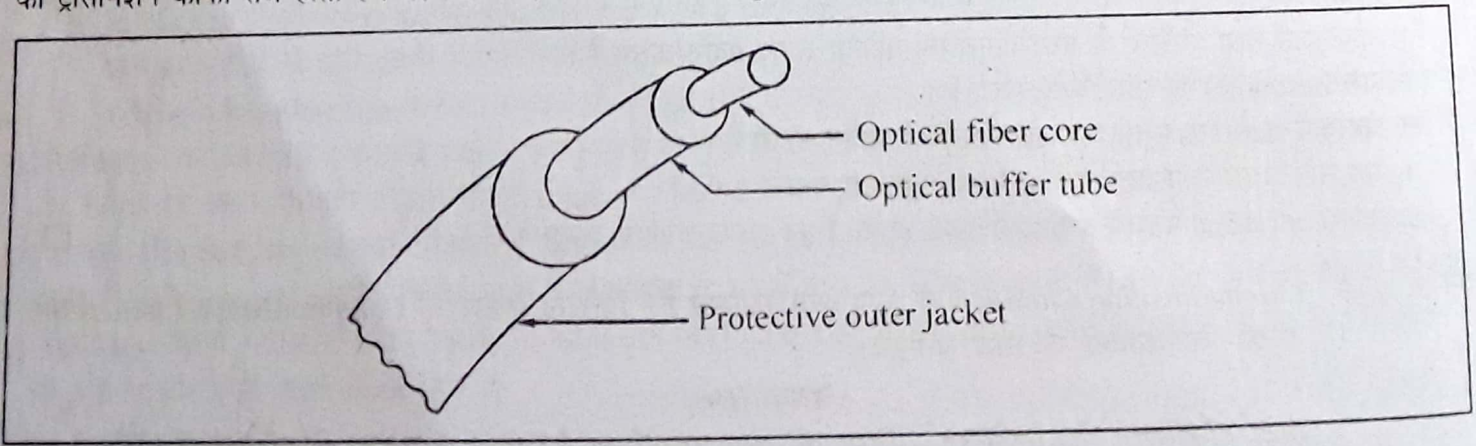


Fig. : Fiber Optics Cable

इस Cable में सबसे Inner Core, Optical fiber core होती है जो प्लास्टिक तथा कांच से मिलकर बनी होती है, जिसमें डाटा प्रकाश की स्पीड के समतुल्य ट्रांसफर होता है। यह Core, optical buffer tube से घिरी होती है। इसके ऊपर Protective outer jacket की लेयर होती है। यह Cabel सुरक्षा की दृष्टि से अधिक मजबूत होती है। इसे छोटी दूरी तथा लम्बी दूरी दोनों रूप में प्रयोग कर सकते हैं। ❑

Scanned by CamScanner

प्रश्न 6 – *कम्प्यूटर नेटवर्क में प्रयुक्त होने वाले विभिन्न प्रकार के संचार मीडिया (Transmission Media) का तुलनात्मक वर्णन कीजिये।*

Explain in different way of various types of Transmission Media which are used in Computer Network.

अथवा (Or)

नेटवर्क में Communication की उपयोगिता को समझाइये। विभिन्न प्रकार के Communication Media को विस्तार से लिखिये।

Explain uses of Communication in Network. Explain in detail about various types of Communication Media. **(June, 2004)**

अथवा (Or)

Bounded एवं Unbounded (Boundless) Media से आप क्या समझते हैं? प्रत्येक के उदाहरण लेकर समझाइये।

What do you understand by Bounded and Unbounded (Boundless) Media? Explain each with example. **(Jan., 2004)**

उत्तर–ट्रांसमीशन मीडिया एक सामान्य टर्म है जिसका प्रयोग Sender तथा Receiver के मध्य फिजीकल चैनल के रूप में डाटा पाथ का वर्णन करने के लिये किया जाता है। नेटवर्क में कम्यूनिकेशन का अर्थ है कि एक सिस्टम से दूसरे सिस्टम में डाटा का रूपान्तरण होना, यह डाटा Text, Audio, Video, Sound के रूप में हो सकता है। कम्प्यूटर नेटवर्क में विभिन्न प्रकार के फिजीकल चैनल्स या कम्यूनिकेशन मीडिया होते हैं, जिनके माध्यम से एक नोड से दूसरी नोड पर डाटा को ट्रांसमिट किया जा सकता है। सामान्यतः ट्रांसमीशन मीडिया को दो भागों में बांटा जा सकता है–

(i) Bounded or Guided Media.

(ii) Unbounded or Unguided Media.

(i) Bounded or Guided Media–Bounded or Guided Media को क्रमशः तीन भागों में विभाजित किया गया है–

(a) Twisted Pair Cable–Twisted Pair Cables दो Insulated कॉपर तारों से मिलकर बनी होती हैं। Twisted Pair Cables सबसे पुराना कम्यूनिकेशन मीडिया है जो डाटा ट्रांसमीशन के लिये प्रयोग किया जाता है। टेलीफोन सिस्टम में Twisted Pair Wires का प्रयोग करने से Signals बिना एम्प्लीफिकेशन के कई किलोमीटर तक Travel कर सकते हैं। Twisted Pair Cables का प्रयोग एनालॉग तथा डिजीटल डाटा ट्रांसमीशन के लिये कर सकते हैं। छोटी दूरी के लिये इस तरह का मीडिया सबसे सस्ता है। यदि Twisted Pair Cable का एक भाग खराब हो जाता है, तो पूरा नेटवर्क बन्द नहीं होता है

(b) Co-axial Cable–Co-axial Cable में एक स्टिक कॉपर तार कोर के रूप में बनी होती है जिसके चारों तरफ इन्सुलेटिंग मैटिरियल होता है। Signal, Inner कॉपर तार के द्वारा ट्रांसमिट होता है। Co-axial Cable में इलैक्ट्रोमैग्नेटिक इण्टरफेयरेन्स, Twisted Pair Cable की तुलना में कम होता है। इस मीडिया का प्रयोग भी एनालॉग तथा डिजिटल डाटा ट्रांसमीशन के लिये किया जा सकता है। एनालॉग डाटा ट्रांसमीशन में 75 ohm Broadband Coaxial का प्रयोग किया जाता है तथा डिजिटल डाटा ट्रांसमीशन के लिये 50-ohm Baseband केबल प्रयोग किया जाता है। Coaxial Cable, उच्च Bandwidth तथा एक्सीलेंट Noise Immunity को रखता है।

(c) Optical Fiber–Fiber Optic, Bounded Media का सबसे नया रूप है। यह मीडिया डाटा हैण्डलिंग तथा सिक्योरिटी में बढ़िया है। Fiber Optic Cable, इलैक्ट्रिक सिग्नल्स की अपेक्षाकृत लाइट सिग्नल्स को ट्रांसमिट करता है।

(ii) Unbounded or Unguided Media–Unguided Media वह ट्रांसमीशन मीडिया होता है, जिसमें Signals एक Solid मीडिया के माध्यम से निर्देशित नहीं होते हैं। यह मीडिया हब मीडिया के तौर पर प्रयोग होती है, जिसके माध्यम से इलैक्ट्रोमैग्नेटिक एनर्जी (Electromagnatic Energy) आसानी से फ्लो हो सकती है। Electromagnetic Energy को एक बिन्दु से दूसरे बिन्दु तक भेजने के लिये निम्नलिखित Methods होते हैं–

(a) Radio Wave Communication

(b) Satellite Links

(c) VSATs (Very Small Aperture Terminals)

(d) Infrared and Millimeter Waves

(a) Radio Wave Communication–Radio Waves को आसानी से जनरेट किया जाता है। ये लम्बी दूरी के लिये Travel कर सकती हैं। ये Building को भेद सकती हैं इसलिये इन्हें Indoors तथा Outdoors दोनों में प्रयोग किया जा सकता है।

Scanned by CamScanner

(b) Satellite Links—100 MHz के ऊपर Waves सीधी रेखा में Travel करती हैं। Microwave Transmission, Wireless कम्यूनिकेशन का उदाहरण है। Microwave, फाइबर ऑप्टिक सिस्टम की तुलना में सस्ती होती है। सैटेलाइट माइक्रोवेव सिस्टम Signals को Directional Paratbolic Antennas के मध्य में ट्रांसमिट करता है। सैटेलाइट सिस्टम तथा माइक्रोवेव सिस्टम के मध्य में मुख्य अन्तर यह है कि सैटेलाइट सिस्टम्स के Case में एक एन्टिना geo-synchronous orbit में सेटेलाइट लगभग 36,000 किलोमीटर ऊपर होता है। इसके कारण सैटेलाइट माइक्रोवेव सिस्टम Earth पर अधिकतर रिमोट स्थानों पर पहुंच सकता है।

(c) VSATs—VSATs को विस्तृत रूप में Very Small Aperture Terminals कहते हैं। यह Finy Terminals 1-मीटर चौड़े Antennas होते हैं तथा 1 Watt की पॉवर को रखते हैं। Uplink सामान्यतः 15.2 kbps तथा Downlink 512 kbps होता है।

(d) Infrared and Millimeter Waves—Infrared तथा Millimetre Waves का प्रयोग Short-range कम्यूनिकेशन के लिये किया जाता है। Television, VCRs तथा Stereos में रिमोट कंट्रोल का प्रयोग Infrared कम्यूनिकेशन होता है।

Guided तथा Unguided Media के मध्य मुख्य अन्तर निम्नलिखित है—

Guided Media	Unguided Media
1. Guided Media मुख्यतः Point to Point कम्यूनिकेशन के लिये प्रयोग होता है।	1. Unguided Media मुख्यतः प्रसारण के लिये प्रयोग प्रयोग होता है।
2. Guided Media में वोल्टेज Protons के रूप में होता है।	2. Unguided Media में Electromagnetic Waves के रूप में Signals Travel करते हैं।
3. Guided Media के उदाहरण हैं— • Twisted Pair Cable • Optical Fibre Cable	3. Unguided Media के उदाहरण हैं— • Microwave or Radiowaves • Satellite Link • VSATs • Infrared

❑

प्रश्न 7 – *LAN, MAN, WAN को समझाइये।*
Describe to LAN, MAN, WAN. (Jan., 2004)

अथवा (Or)

N/W को वर्गीकृत करने के लिये उपयोग में लाये जाने वाले Parameter के बारे में चर्चा कीजिये।
Discuss about parameters which are used in Network Classfication. (June, 2004)

उत्तर—LAN (Local Area Network)—LAN को विस्तृत रूप में Local Area Network कहते हैं। LAN, कम्प्यूटरों का एक समूह होता है, जिसे एक कमरे में एक छत के नीचे या एक बिल्डिंग में जो एक Single नेटवर्क से जुड़े होते हैं। LAN, यूजर्स के लिये स्टोरेज डिवाइसेस, प्रिंटर्स, एप्लीकेशन्स, डाटा तथा दूसरे नेटवर्क संसाधनों को Share करने की अनुमति प्रदान करता है। LAN एक Specified क्षेत्र में प्रयोग किया जाता है। सामान्यतः LAN का एरिया 2 Km. के Diameter में प्रयोग किया जाता है। LAN, के माध्यम से प्रिंटर्स, मास स्टोरेज डिवाइस इत्यादि को Share किया जा सकता है।

MAN (Metropolian Area Network)—MAN को विस्तृत रूप से Metropolian Area Network भी कहते हैं। MAN का प्रयोग LAN के एरिया से ज्यादा एरिया में कम्प्यूटरों को आपस में जोड़ने के लिये किया जाता है। सामान्यतः 2 Km. के Diameter एरिया से ज्यादा एरिया के अंतर्गत कम्प्यूटर नेटवर्क के लिये MAN को डिजाइन किया जाता है। सामान्यतः 10 Km. के Diameter को रेंज में कम्प्यूटरों को आपस में जोड़ने के नेटवर्क को MAN कहते हैं।

WAN (Wide Area Network)—आज के समय में MAN का प्रयोग कम ही किया जाता है। Short Distance के लिये LAN का प्रयोग किया जाता है। इसके पश्चात् WAN का प्रयोग किया जाता है। WAN को विस्तृत रूप में Wide Area Network कहते हैं। WAN के अंतर्गत एक प्रदेश, एक देश या फिर पूरी दुनिया में आपस जुड़े हुये कम्प्यूटर्स को सम्मिलित किया गया है। WAN के अंतर्गत कम्प्यूटरों को सैटेलाइट कम्यूनिकेशन लिंक (Satellite Communication Link) के माध्यम से जोड़ा जाता है। किसी मल्टीनेशनल कम्पनी, जैसे रिलायन्स इण्डस्ट्रीज की विभिन्न शाखाओं को आपस में जोड़ने के लिये तैयार किया गया नेटवर्क WAN का प्रमुख उदाहरण है। इन शाखाओं को माइक्रोवेव सैटेलाइट कम्यूनिकेशन सिस्टम या इंटरनेट कनेक्शन का प्रयोग करके जोड़ा जाता है। प्रत्येक शाखा अपने LAN Circuit को रखती है, लेकिन अलग-अलग शाखाओं में विभिन्न LANs, WAN लिंक का प्रयोग करके Head Office के साथ कम्यूनिकेट करते हैं। ❑

Scanned by CamScanner

प्रश्न 8 – *Network Topology से आप क्या समझते हैं? विभिन्न Topology के प्रकार बताइये।*
What do you mean by Network Topology? Explain various types of Topology.
(June, 2002, 2003, Jan., 2004)

अथवा (Or)

विभिन्न LAN टोपोलॉजी के नाम लिखिये व किन्हीं दो के बारे में वर्णन कीजिए।
Write the name of various Topology and describe any two. **(Dec., 2008)**

अथवा (Or)

कम्प्यूटर नेटवर्किंग में प्रयुक्त होने वाली विभिन्न Topologies की व्याख्या कीजिये। साथ ही प्रत्येक के फायदे व नुकसान की भी चर्चा कीजिये।
Explain various Topologies used in Computer Networking and also discuss advantages and disadvantages of them. **(Dec., 2008)**

उत्तर–नेटवर्क टोपोलॉजी एक मैथड है जिसमें Networks आपस में एक-दूसरे से फिजीकली कनेक्टेड होते हैं। संक्षिप्त रूप में टोपोलॉजी को इस तरह परिभाषित कर सकते हैं–

"Topology is a Physically layout of Network."

नेटवर्क से जुड़े हुये कम्प्यूटरों की Complexity को टोपोलॉजी द्वारा सुधारा जा सकता है तथा नेटवर्क केबल Installation की Cost में सुधार होता है। टोपोलॉजी, भविष्य के नेटवर्क के विस्तारण की रणनीति में भी सुधार करती हैं।

कम्प्यूटर नेटवर्क में प्रयोग की जाने वाली प्रमुख टोपोलॉजी निम्नलिखित हैं–

● **Bus Topology**–बस टोपोलॉजी में सभी कम्प्यूटर्स प्रत्येक end पर एक Terminator के साथ एक केबल के द्वारा जुड़े होते हैं। बस टोपोलॉजी, लोकल एरिया नेटवर्क डिजाइन में सबसे अधिक प्रयोग की जाने वाली साधारण टोपोलॉजी है। यह एक Passive टोपोलॉजी है जिसका अर्थ है कि एक समय में केवल एक कम्प्यूटर मैसेज को भेज सकता है। अतः Bus नेटवर्क से जुड़े हुये कम्प्यूटरों की संख्या नेटवर्क की स्पीड को प्रभावित करती है। निम्न Fig. में Bus Topology से जुड़े गये कम्प्यूटरों को दर्शाया गया है–

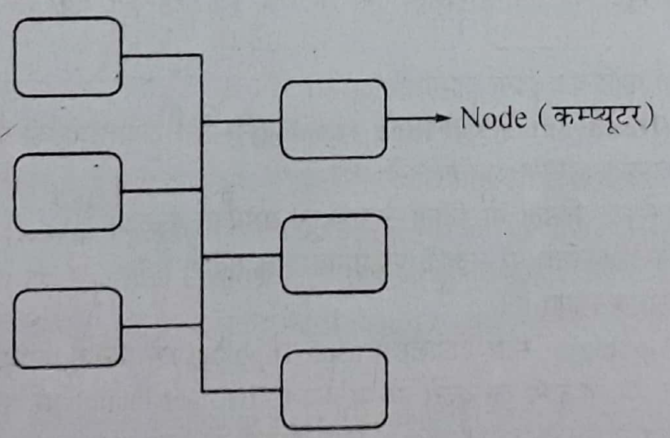


Fig. : Bus Topology

बस टोपोलॉजी के लाभ (The Advantages of Bus Topology)–Bus Topology के प्रमुख लाभ निम्नलिखित हैं–

1. Bus Topology साधारण, भरोसेमंद, प्रयोग में आसान तथा छोटे Size के लोकल एरिया नेटवर्क को आसानी से समझने वाली टोपोलॉजी है।
2. Bus नेटवर्क में कम्प्यूटर्स को आपस में जोड़ने के लिये कम केबल की जरूरत होती है। इसलिये दूसरे केबलिंग व्यवस्था की तुलना में यह कम खर्चीली है।
3. Bus नेटवर्क का विस्तार करना आसान है।

बस टोपोलॉजी की हानियां (Disadvantages of Bus Topology)–बस टोपोलॉजी की प्रमुख हानियां निम्नलिखित हैं–

1. ज्यादा नेटवर्क ट्रैफिक बस नेटवर्क को काफी हद तक धीमा कर सकता है।
2. बस नेटवर्क में यदि मध्य में कोई कम्प्यूटर खराब हो जाता है तो इससे आगे के कम्प्यूटरों का सम्बन्ध समाप्त हो जाता है।
3. बस नेटवर्क में एक नये कम्प्यूटर को जोड़ना आसान नहीं होता है।

Scanned by CamScanner

● **रिंग टोपोलॉजी (Ring Topology)**–इस टोपोलॉजी का Layout बस टोपोलॉजी की तरह होता है, लेकिन रिंग टोपोलॉजी में Nodes एक Circle के रूप में Cable segmant का प्रयोग करके जुड़ी होती हैं।

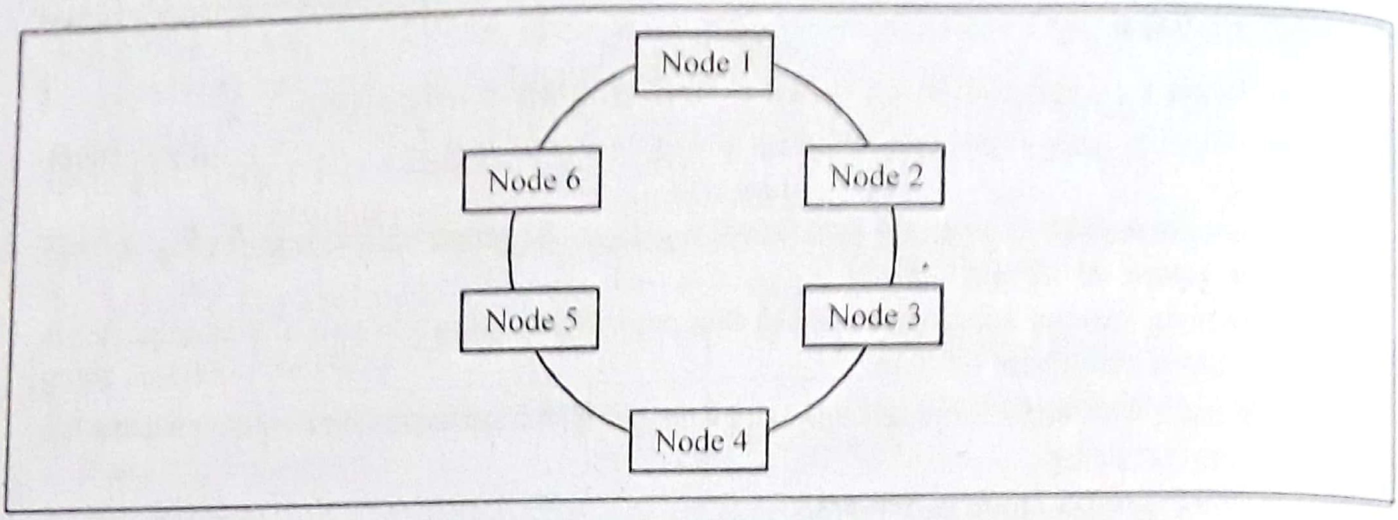


Fig. : Ring Network Topology

इस Layout में केवल दोनों नोड एक-दूसरे से फिजीकली कनेक्टेड होती हैं। प्रत्येक नोड अपनी अगली नोड को मैसेज पास करती है जब तक कि इस मैसेज का सही स्थान नहीं मिलता है। इस टाईप की टोपोलॉजी की स्पीड काफी तेज होती है क्योंकि केबलिंग सिस्टम का प्रत्येक भाग दो मशीनों के मध्य डाटा फ्लो को हैण्डल करता है। इस टाईप की टोपोलॉजी, Peer-to-Peer नेटवर्क में पायी जाती है जिसमें प्रत्येक मशीन डाटा फाइलों के प्रोसेसिंग तथा डिस्ट्रीब्यूशन दोनों को मैनेज करती है।

रिंग टोपोलॉजी के लाभ (Advantages of Ring Topology)–रिंग टोपोलॉजी के प्रमुख लाभ निम्नलिखित हैं–

1. रिंग टोपोलॉजी की स्पीड काफी तेज होती है।
2. रिंग टोपोलॉजी में प्रत्येक कम्प्यूटर को समान एक्सेस दिया जाता है, इस तरह कोई एक कम्प्यूटर नेटवर्क को Monopolize नहीं कर सकता है।
3. रिंग टोपोलॉजी में केबल की कमी को ढूंढना आसान होता है।

रिंग टोपोलॉजी की हानियां (Disadvantages of Ring Topology)–रिंग टोपोलॉजी की प्रमुख हानियां निम्नलिखित हैं–

1. रिंग नेटवर्क में एक नया कम्प्यूटर जोड़ना आसान नहीं होता है।
2. रिंग नेटवर्क में एक नया कम्प्यूटर जोड़ना या हटाना नेटवर्क को प्रभावित करता है।
3. रिंग नेटवर्क में एक नोड की असफलता पूरे नेटवर्क पर प्रभाव डाल सकती है।
4. रिंग नेटवर्क में केबल की कीमत ज्यादा है।

● **स्टार टोपोलॉजी (Star Topology)**–स्टार टोपोलॉजी (Star Topology) में प्रत्येक कम्प्यूटर एक Central Hub के साथ कम्यूनिकेट करता है जो मैसेज को पुनः या तो सभी कम्प्यूटरों पर या केवल इसके Destination पर भेजता है। ब्रॉडकास्ट स्टार नेटवर्क में Hub या तो Active या Passive हो सकता है। निम्न Fig. में स्टार नेटवर्क को प्रदर्शित किया गया है–

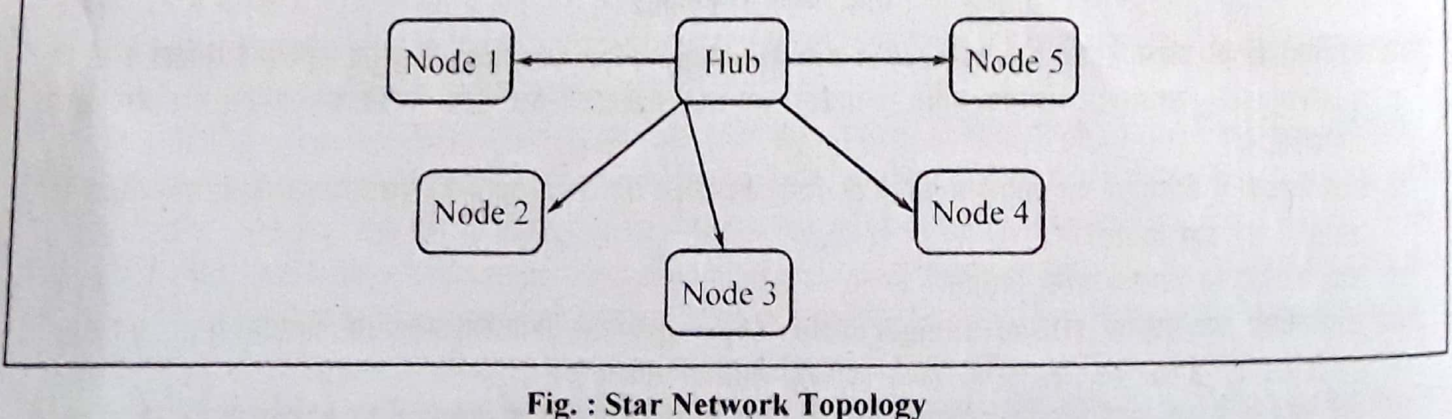


Fig. : Star Network Topology

स्टार नेटवर्क को इम्प्लीमेन्ट करने के लिये आप अलग-अलग तरह के केबल का प्रयोग कर सकते हैं।

Scanned by CamScanner

स्टार टोपोलॉजी के लाभ (Advantages of Star Topology)—स्टार टोपोलॉजी के लाभ निम्नलिखित हैं—

1. स्टार नेटवर्क में किसी नये कम्प्यूटर को जोड़ना आसान होता है।
2. स्टार नेटवर्क में किसी कम्प्यूटर को संशोधित करना आसान होता है। इससे शेष कम्प्यूटरों पर कोई फर्क नहीं पड़ता है।
3. स्टार नेटवर्क में दोष निवारण तकनीकी आसान है।
4. स्टार नेटवर्क में किसी एक नोड की असफलता पूरे नेटवर्क को प्रभावित नहीं करती है।

स्टार टोपोलॉजी की हानियां (Disadvantages of Star Topology)—स्टार टोपोलॉजी की प्रमुख हानियां निम्नलिखित हैं—

1. स्टार नेटवर्क में यदि Hub फेल हो जाता है तो पूरा नेटवर्क काम करना बंद कर देता है।
2. प्रत्येक Instrument को स्वयं के केबल Segment की आवश्यकता होती है।

- **ट्री टोपोलॉजी (Tree Topology)**—Tree टोपोलॉजी, स्टार टोपोलॉजी का ही रूपान्तरण है। Tree टोपोलॉजी में Nodes, केन्द्रीय Hub से जुड़ी होती हैं, जो ट्रेफिक को नियंत्रित करती हैं। निम्न Fig. में Tree Topology को प्रदर्शित किया गया है—

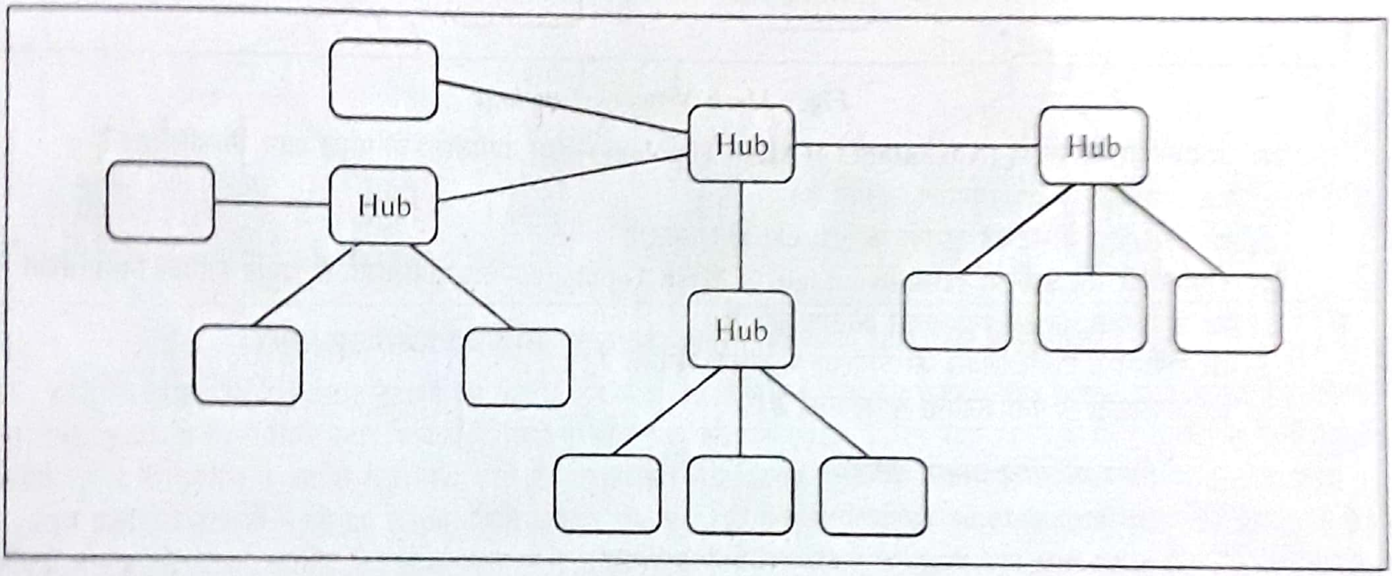


Fig. : Tree Topology

Tree टोपोलॉजी में Central Hub एक एक्टिव हब है जिसमें रिपोर्टर होता है। रिपोर्टर सिग्नल को बढ़ाता है।

ट्री टोपोलॉजी के लाभ (Advantages of Tree Topology)—Tree Topology के प्रमुख लाभ निम्नलिखित हैं—

1. यह टोपोलॉजी, एक ही हब में अधिक उपकरणों को जोड़ने की सुविधा प्रदान करती है।
2. यह नेटवर्क को विभिन्न कम्प्यूटर्स से प्राप्त संवाद को Isolate करने तथा संप्रेषणों की प्राथमिकता निर्धारित करने की अनुमति देती है।

ट्री टोपोलॉजी की हानियां (Disadvantages of Tree Topology)—Tree Topology की प्रमुख हानियां निम्नलिखित हैं—

1. यदि Central हब खराब हो जाता है तो पूरा सिस्टम रुक जाता है।
2. केबल लगाने की लागत ज्यादा होती है।

- **मैश टोपोलॉजी (Mesh Topology)**—मैश टोपोलॉजी में नेटवर्क के प्रत्येक उपकरण के बीच एक सम्बंध होता है। जब उपकरणों की संख्या बढ़ती है तो इसे स्थापित करना और भी कठिन हो जाता है। मैश नेटवर्क को दोषमुक्त करना आसान है। निम्न Fig. में मैश टोपोलॉजी नेटवर्क को प्रदर्शित किया गया है—

Scanned by CamScanner

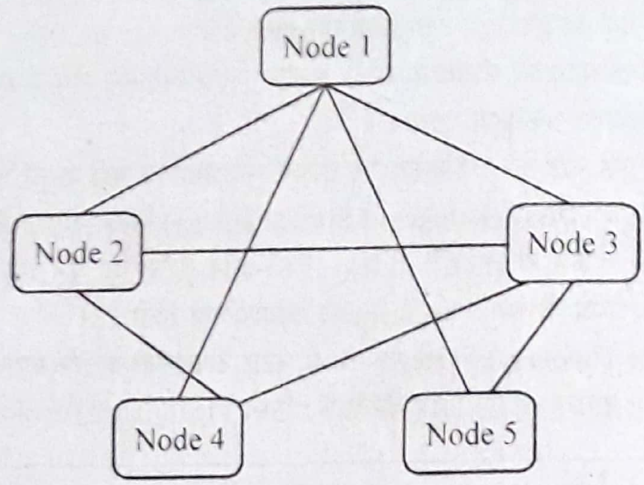


Fig. : Mesh Network Topology

मैश टोपोलॉजी के लाभ (Advantages of Mesh Topology)–मैश टोपोलॉजी के प्रमुख लाभ निम्नलिखित हैं–

1. मैश टोपोलॉजी में दोष निवारण आसान है।
2. मैश टोपोलॉजी में नेटवर्क खराबी की Checking आसान है।

मैश टोपोलॉजी की हानियां (Disadvantages of Mesh Topology)–मैश टोपोलॉजी की प्रमुख हानियां निम्नलिखित हैं–

1. मैश टोपोलॉजी की स्थापना करना आसान नहीं है।
2. मैश टोपोलॉजी दोहरी लिंक्स की व्यवस्था के कारण खर्चीला है।
3. मैश टोपोलॉजी में पुनः संरचना में कठिनाई है।

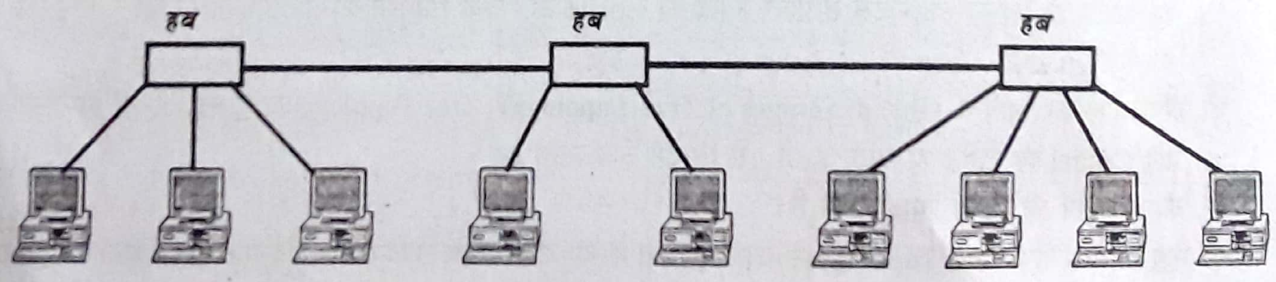
प्रश्न 9 – *निम्न के बीच अन्तर बताइये–*

Differentiate between following :

(i) Start-Bus topalogy and star-ring topology.

(ii) Digital signaling and Analog signaling.

उत्तर–स्टार-बस टोपोलॉजी (Star-bus topoloty)—जैसा कि इसके नाम से स्पष्ट है स्टार-बस टोपोलॉजी स्टार टोपोलॉजी और बस टोपोलॉजी का मिश्रित अर्थात् मिला-जुला रूप होता है। इस टोपोलॉजी में स्टार टोपोलॉजी वाले दो या अधिक नेटवर्कों के केन्द्रीय हब (Central hubs) एक दूसरे के साथ बस टोपोलॉजी की तकनीक से जुड़े रहते हैं, जैसा कि निम्न चित्र में दिखाया गया है–



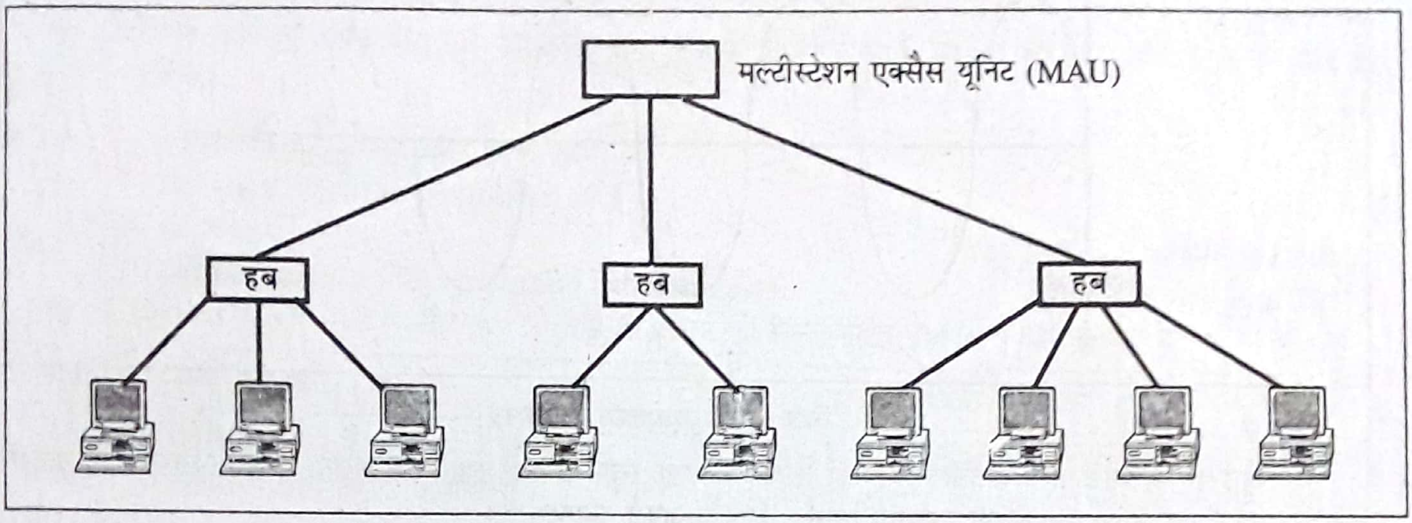
चित्र–स्टार बस टोपोलॉजी

यहां यह उल्लेखनीय है कि प्रत्येक हब एक स्टार नेटवर्क का केन्द्रीय हब होता है, जो उस नेटवर्क के अन्दर स्वतंत्र रूप से कार्य करता है। लेकिन इस टोपोलॉजी के दो भिन्न-भिन्न स्टार नेटवर्कों के नोडों के बीच डाटा का सम्प्रेषण या आदान-प्रदान करने के लिए उनके हब आपस में सम्पर्क करते हैं और इसमें बस टोपोलॉजी के नियमों का पालन किया जाता है।

इस प्रकार के नेटवर्कों में हब (Hub) सबसे अधिक महत्वपूर्ण होता है। यदि कोई एक स्टेशन खराब हो जाता है तो नेटवर्क पर अधिक प्रभाव नहीं पड़ता, क्योंकि शेष स्टेशन आपस में संचार करते रहते हैं। लेकिन यदि कोई हब खराब हो जाता है, तो उससे जुड़े हुए सभी स्टेशन भी नेटवर्क से कट जाते हैं और नेटवर्क की कार्यकुशलता पर भी बुरा प्रभाव पड़ता है।

Scanned by CamScanner

स्टार-रिंग टोपोलॉजी (Star-ring topology)—जैसा कि इसके नाम से स्पष्ट है स्टार-रिंग टोपोलॉजी स्टार टोपोलॉजी और रिंग टोपोलॉजी का मिश्रित अर्थात् मिला-जुला रूप होता है। इसे स्टार-वायर्ड रिंग (Star-Wired ring) टोपोलॉजी भी कहा जाता है। इस टोपोलॉजी में स्टार टोपोलॉजी वाले दो या अधिक नेटवर्कों के केन्द्रीय हब (Central hubs) एक-दूसरे के साथ रिंग टोपोलॉजी की तकनीक से जुड़े रहते हैं। वास्तव में वे सभी हब एक मल्टीस्टेशन एक्सैस यूनिट (Multistation Access Unit या MAU) को एक केन्द्रीय हब की तरह प्रयोग करके जुड़े रहते हैं। इससे वास्तव में तो वह रिंग नेटवर्क होता है, परन्तु देखने में स्टार नेटवर्क लगता है, जैसा कि निम्न चित्र में दिखाया गया है–

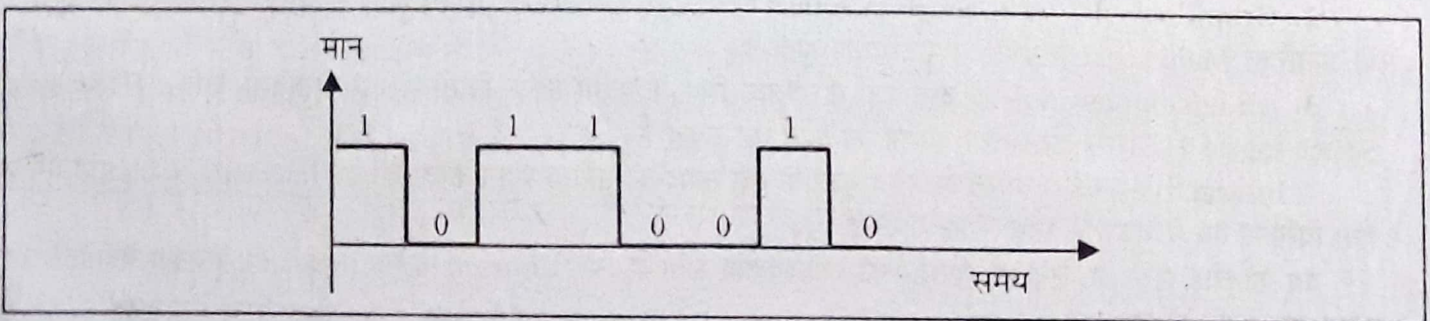


चित्र–मल्टीस्टेशन एक्सैस यूनिट के उपयोग के साथ स्टार रिंग टोपोलॉजी

इसमें भी प्रत्येक हब एक स्टार नेटवर्क का केन्द्रीय हब होता है, जो उस नेटवर्क के अन्दर स्वतंत्र रूप से कार्य करता है। लेकिन इस टोपोलॉजी के दो भिन्न-भिन्न स्टार नेटवर्कों के नोडों के बीच डाटा का सम्प्रेषण या आदान-प्रदान करने के लिए उनके हब मल्टीस्टेशन एक्सैस यूनिट के माध्यम से आपस में सम्पर्क करते हैं और इसमें रिंग टोपोलॉजी के नियमों का पालन किया जाता है।

इस प्रकार के नेटवर्कों में भी हब (Hub) सबसे अधिक महत्वपूर्ण होते हैं। यदि कोई एक स्टेशन खराब हो जाता है, तो नेटवर्क पर अधिक प्रभाव नहीं पड़ता, क्योंकि शेष स्टेशन आपस में संचार करते रहते हैं। लेकिन यदि कोई हब खराब हो जाता है, तो उससे जुड़े हुए सभी स्टेशन भी नेटवर्क से कट जाते हैं और नेटवर्क की कार्यकुशलता पर भी बुरा प्रभाव पड़ता है।

(ii) डिजिटल सिग्नल (Digital Signals)—डिजिटल सिग्नल आधुनिक कम्प्यूटरों के आधार हैं, क्योंकि किसी कम्प्यूटर द्वारा उत्पन्न किया गया डाटा डिजिटल होता है। इसीलिए उन्हें डिजिटल कम्प्यूटर (Digital computer) कहा जाता है। किसी डिजिटल सिग्नल में मानों की संख्या सीमित होती है और वह डिस्क्रीट (Discrete) भी होता है। इसके एक मान से दूसरे मान में बदलना तत्काल (Instaneous) होता है। वास्तव में डिजिटल सिग्नलों में केवल दो भिन्न-भिन्न मान या स्थितियाँ (States) होती हैं, जिन्हें क्रमशः 0 और 1 से दिखाया जाता है। इन दोनों स्थितियों को दो अलग-अलग वोल्टेज रेंजों (Voltage ranges) से व्यक्त किया जाता है, जैसा कि निम्न चित्र में दिखाया गया है–

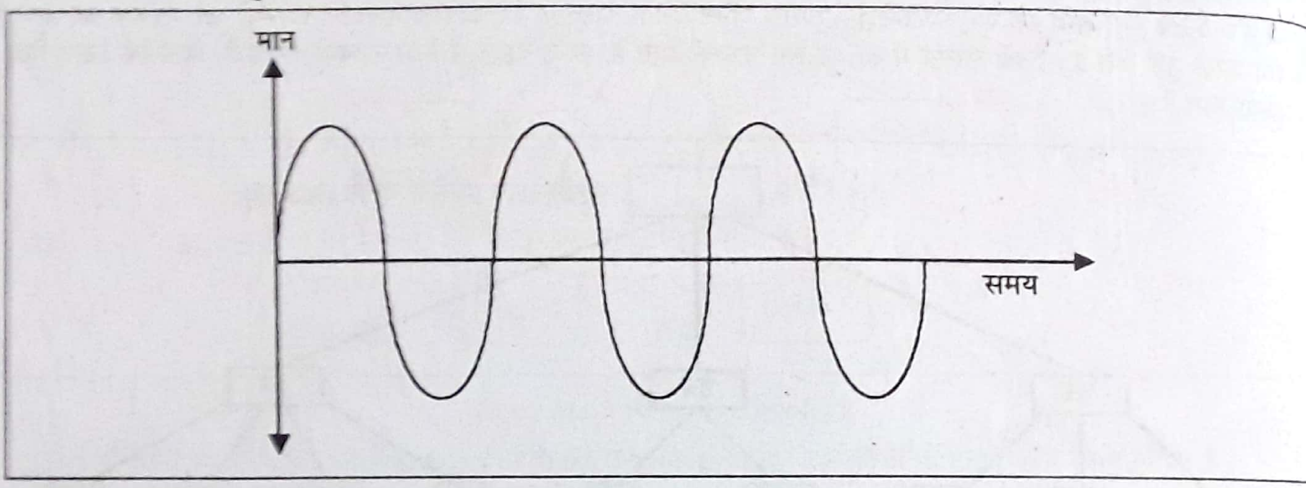


चित्र : एक डिटिजल सिग्नल

डिजिटल सिग्नलों के सम्बंध में हम प्रायः दो शब्दों (Terms) का उपयोग करते हैं–बिट रेट (Bit rate) और बिट अंतराल (Bit interval)। किसी एक बिट को भेजने में लगने वाले समय को **बिट अंतराल** कहा जाता है। उदाहरण के लिए, यदि हम एक सेकंड में 8 बिट डाटा सम्प्रेषित करते हैं, तो बिट अंतराल 1/8 अर्थात् 0.125 सेकंड होगा। एक सेकंड में भेजी जाने वाली बिटों की संख्या को **बिट रेट** कहा जाता है। यहाँ बिट रेट 8 बिट प्रति सेकंड (Bits per second) है, जिसे संक्षेप में इचे लिखा जाता है।

Scanned by CamScanner

एनालॉग सिग्नल (Analog Signals)—एनालॉग सिग्नल ऐसे सिग्नलों को कहा जाता है जो लगातार अर्थात् अनवरत (Continuous) होते हैं और जिनके अनन्त मान (Infinite values) हो सकते हैं। इनमें एक मान से दूसरे मान में बदलना धीरे-धीरे (Smoothly) होता है। निम्न चित्र में एक एनालॉग सिग्नल दिखाया गया है—



चित्र : एक एनालॉग सिग्नल

टेलीफोन पर की जाने वाली बातचीत में हमारी आवाज को एक स्थान से दूसरे स्थान तक भेजना एनालॉग सिग्नलों के माध्यम से होता है। साइन वेव (Sine wave) भी एनालॉग सिग्नल का एक अच्छा उदाहरण है।

एनालॉग सिग्नलों का डाटा कम्यूनिकेशन, डाटा ट्रांसमिशन और कम्प्यूटर नेटवर्कों के सम्बंध में बहुत महत्व है, क्योंकि लम्बी दूरी को डाटा का सम्प्रेषण एनालॉग सिग्नलों के माध्यम से ही किया जाता है।

प्रश्न 10 – *World Wide Web क्या है? इसके इतिहास को भी समझाइये।*
What is World Wide Web? Explain its history also.

उत्तर—World Wide Web—World Wide Web को संक्षिप्त रूप में WWW भी कहते हैं। World Wide Web, इंटरनेट पर आधारित एक ऐसी शृंखला है जो हाइपरटैक्स्ट के माध्यम से आपस में संयोजित होती है। World Wide Web संक्षिप्त रूप में इंटरनेट पर आधारित ग्लोबल इनफॉरमेशन है। हाइपरटैक्स्ट सूचना को प्रस्तुत करने का एक ऐसा तरीका है जिसमें आइटम Highlighted होते हैं। इस Highlighted text को क्लिक करने पर हमें उस Text से सम्बन्धित जानकारी प्राप्त होती हैं। ये Highlighted items आपस में लिंक होते हैं जो हमें एक डॉक्यूमेन्ट से दूसरे डॉक्यूमेन्ट में जाने में सहायता करते हैं। वेब हमें URL (Uniform Resource Locator) की विशेषता प्रदान करता है, जिसके माध्यम से हम विश्व में कहीं भी कहीं से किसी भी वेब पेज को एक्सेस कर सकते हैं।

World Wide Web की निम्नलिखित विशेषतायें होती हैं—

1. **Non-Linear**—यह Non-Linear सूचनाओं से मिश्रित होता है। इसमें Linear सूचनायें भी होती हैं।

2. **Graphical**—वेब पेजों में Graphical format में बटन, चित्र इत्यादि की सूचना होती हैं, जो Linked होती हैं। इसमें Text के अतिरिक्त Multimedia के गुणों का भी मिश्रण होता है।

3. **All-encompassing**—वेब दस्तावेजों में उपलब्ध लिंक के प्रयोग से हम विभिन्न अन्य दस्तावेजों; जैसे FTP Session तथा Search engine को प्रारम्भ करने तथा खोलने का कार्य कर सकते हैं।

4. **Interactive**—वेब आधारित दस्तावेज यूजर के रूल संवाद की सुविधा प्रदान करता है। यह Interactive tools डायलॉग बॉक्स तथा विभिन्न रूप में यूजर के साथ संवाद करते हैं।

वेब को लोड करने के लिये हमें ब्राउजर की आवश्यकता होती है। यह Browser, मोज़ेक (Mosaic), नेटस्केप नेवीगेटर, इंटरनेट एक्सप्लोरर आदि हो सकते हैं।

प्रश्न 11 – *इन्टरनेट सर्विस प्रोवाइडर से आप क्या समझते हैं? समझाइये।*
What do you mean by Internet Service Provider? Explain it.

उत्तर—इंटरनेट के उपयोग को सभी इच्छुक व्यक्तियों तक पहुंचाने के लिए कई कम्पनियां अपने सर्वरों की सेवाएं प्रदान करती हैं उनके सर्वर इंटरनेट से सीधे जुड़े होते हैं। वे अपने सर्वर के माध्यम से अन्य उपयोगकर्त्ताओं को इंटरनेट का उपयोग करने की सुविधा

Scanned by CamScanner

देती हैं। ऐसी कम्पनियों को इंटरनेट सेवा प्रदाता (Internet Service Provider) कहा जाता है। यदि हम अपने कम्प्यूटर को इंटरनेट से जोड़ना चाहते हैं तो हमें उसके लिए किसी इंटरनेट सेवा प्रदाता कम्पनी से कनेक्शन लेना पड़ता है। यह ठीक वैसे ही जैसे हम टेलीफोन एक्सचेंज से टेलीफोन कनेक्शन लेते हैं या किसी गैस कम्पनी से गैस का कनेक्शन लेते हैं। इस कनेक्शन के लिए हमें कुछ शुल्क देना पड़ता है।

भारत में ISP (ISP in India)—भारत में कुछ प्रमुख इंटरनेट सेवा प्रदाता कम्पनियों के नाम हैं—भारत संचार निगम लि०, महानगर टेलीफोन निगम लि०, मंत्र ऑनलाइन, सत्यम् ऑनलाइन, नेटफॉरयू, डिशनेट, डीएसएल, ग्लाइड, नेटक्रैकर, रिलायंस, सिफी, भारती आदि। इन कम्पनियों द्वारा इंटरनेट का उपयोग करने के लिए अलग-अलग शुल्क लिये जाते हैं। कुछ कम्पनियाँ एक निश्चित मासिक शुल्क लगाती हैं, तो कुछ इंटरनेट से जुड़ने की समयावधि, डाटा डाउनलोड तथा अपलोड करने की मात्रा, उपयोग का समय (दिन या रात) आदि के अनुसार शुल्क लेती है। ❑

प्रश्न 12 — निम्नलिखित के मध्य अंतर स्पष्ट करें।

Differentiate between following :

(i) LAN and WAN **(Dec., 2012/Jan., 2013)**

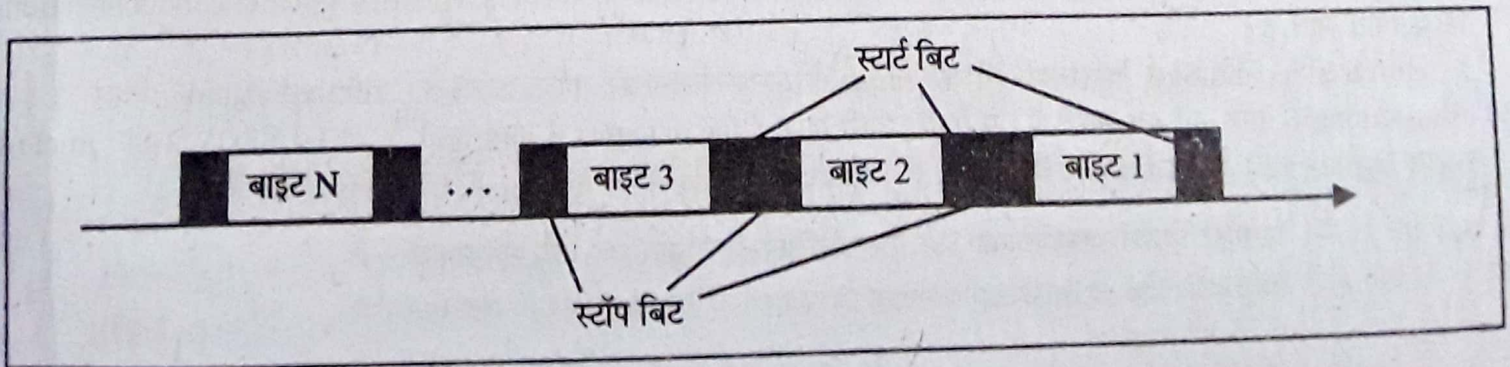
(ii) Synchronous and Asynchronous transmission **(Dec., 2012/Jan., 2013)**

उत्तर—**LAN and WAN**—LAN और WAN के प्रमुख अन्तर को निम्नलिखित Table में दर्शाया गया है—

लोकल एरिया नेटवर्क (LAN)	वाइड एरिया नेटवर्क (WAN)
1. LAN सीमित भौगोलिक क्षेत्र में कार्य करता है।	1. WAN भौगोलिक दृष्टि से विस्तृत क्षेत्र में कार्य करता है।
2. कम्प्यूटरों को आपस में तारों अथवा केबिलों से जोड़ा जाता है।	2. WAN में विभिन्न कम्प्यूटरों को भौतिक लिंक से जोड़ने की आवश्यकता नहीं होती है।
3. LAN को स्थापित करने अथवा प्रयोग करने की लागत बहुत अधिक होती है।	3. WAN को स्थापित अथवा प्रयोग करने की लागत बहुत अधिक होती है।
4. LAN किसी संस्था या संगठन विशेष से सम्बन्धित होते हैं।	4. WAN विश्वव्यापी होते हैं। उदाहरणतया—Internet.
5. LAN में आंकड़ों के संचार की गति 0.1 से 100 MB प्रति सैकेण्ड होती है।	5. WAN में आंकड़ों के संचार की गति 1,200-9,600 बिट् प्रति सैकेण्ड होती है।

(ii) असिंक्रोनस ट्रांसमिशन (Asynchronous Transmission)—असिंक्रोनस ट्रांसमिशन किसी कम्यूनिकेशन को तब असिंक्रोनस **(Asynchronous)** कहा जाता है जब प्रेषक (Sender) और प्राप्तकर्त्ता (Receiver) के बीच किसी डाटा को ट्रांसमिट करने से पहले किसी सम्पर्क या सूचना के आदान-प्रदान की आवश्यकता नहीं होती। इसका अर्थ है कि कोई प्रेषक अपना डाटा भेजने के लिए कितने भी समय तक प्रतीक्षा कर सकता है जब तक डाटा प्रेषण के लिए उपलब्ध न हो जाये और प्राप्तकर्त्ता को भेजा गया डाटा प्राप्त करने के लिए हमेशा तैयार रहना पड़ता है। इस प्रकार का कम्यूनिकेशन प्रायः ऐसे उपकरणों के लिए अधिक उपयोगी है जहाँ भेजा जाने वाला डाटा मानव के हस्तक्षेप से अथवा कोई बटन दबाने से उत्पन्न होता है; जैसे—कीबोर्ड, माउस, टेलीफोन आदि।

अधिक तकनीकी शब्दों में किसी कम्यूनिकेशन उपकरण को तब असिंक्रोनस श्रेणी में रखा जाता है जब उसके ट्रांसमिटर द्वारा भेजे गये इलैक्ट्रीकल सिग्नलों में प्राप्तकर्त्ता उपकरण के लिए ऐसी सूचनाएँ नहीं होतीं जिनसे पता चलता हो कि कोई बिट कहाँ से प्रारम्भ और कहाँ पर समाप्त हो रही है अर्थात् उसका बिट अंतराल कितना है। इसके बजाय प्राप्तकर्त्ता उपकरण को इस प्रकार बनाया जाता है कि वह प्राप्त हुए सिग्नलों को स्वीकार करके स्वयं उनका अर्थ निकाल सके।



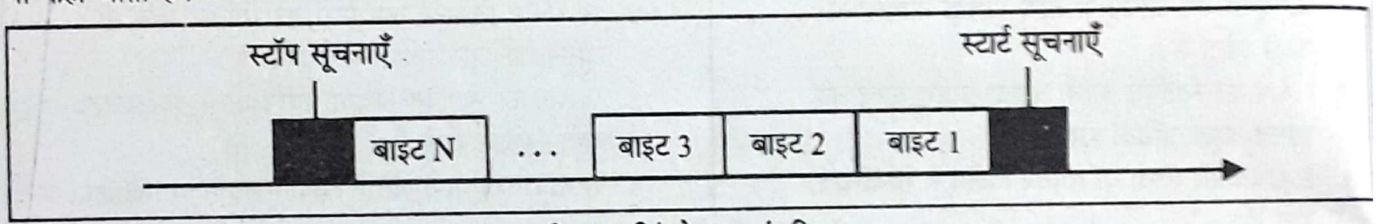
चित्र : असिंक्रोनस ट्रांसमिशन

Scanned by CamScanner

किसी प्रेषक (Sender) से प्राप्त किये गये सिग्नल को ठीक-ठीक समझने के लिए प्राप्तकर्त्ता (Receiver) के बिट अंतराल (Bit intervals) प्रेषक के बिट अंतरालों (Bit intervals) से पूरी तरह मैच करने चाहिए। यदि प्राप्तकर्त्ता की क्लॉक (Clock) तेज या धीमी है, तो बिट अंतराल पूरी तरह नहीं मिलते और प्राप्तकर्त्ता सिग्नलों को प्रेषक द्वारा भेजे गये सिग्नल से भिन्न रूप में समझ लेता है। इसलिए असिंक्रोनस कम्यूनिकेशन उपकरण विश्वसनीयता की दृष्टि से अधिक उपयोगी नहीं होते। अतः हम सिंक्रोनस कम्यूनिकेशन उपकरणों का अधिक उपयोग करते हैं।

सिंक्रोनस ट्रांसमिशन (Synchronous Transmission)—सिंक्रोनस ट्रांसमिशन (Synchronous Transmission) में डाटा को एक निश्चित गति से एक पूर्वनिर्धारित रूप में ट्रांसमिट किया जाता है, जिसमें डाटा के प्रारम्भ और समाप्त होने की सूचनाएँ भी होती हैं। इनके साथ ही उसमें समय को नियंत्रित करने की सूचनाएँ भी दी जाती हैं, जिनसे प्राप्तकर्त्ता को पता चलता है कि भेजे जाने वाले डाटा का बिट अंतराल क्या है, ताकि उसी के अनुसार वह अपनी क्लॉक को निर्धारित कर सके। सिंक्रोनस ट्रांसमिशन में डाटा की जाँच करने के लिए भी सूचनाएँ दी जाती हैं।

सामान्य रूप में हम असिंक्रोनस और सिंक्रोनस ट्रांसमिशन के अन्तर को चित्र द्वारा अच्छी तरह समझ सकते हैं। पिछले पृष्ठ पर दिये गये चित्र में असिंक्रोनस ट्रांसमिशन दिखाया गया है और निम्न चित्र में सिंक्रोनस ट्रांसमिशन दिखाया गया है। इससे स्पष्ट है कि किसी असिंक्रोनस ट्रांसमिशन में प्रत्येक डाटा बाइट से पहले एक प्रारम्भ बिट (Start bit) और एक समाप्ति बिट (Stop bit) लगायी जाती है, जिससे प्राप्तकर्त्ता को पता चलता है कि कोई बाइट कहाँ से प्रारम्भ होकर कहाँ समाप्त हो रही है। इसके विपरीत सिंक्रोनस ट्रांसमिशन में सभी बाइटों को एक साथ लगातार ट्रांसमिट किया जाता है और प्रारम्भ (Start) और समाप्ति सूचनाएँ (Stop informations) इन बाइटों की श्रृंखला से क्रमशः पहले और बाद में दी जाती हैं। इन सूचनाओं को सिंक्रोनाइजेशन सूचनाएँ (Synchronization informations) भी कहा जाता है।



चित्र : सिंक्रोनस ट्रांसमिशन

इस तुलना से स्पष्ट है कि सिंक्रोनस ट्रांसमिशन विश्वसनीयता और गति की दृष्टि से अधिक उपयोगी है। वैसे कोई उपकरण किस प्रकार का ट्रांसमिशन करेगा, यह इस बात पर निर्भर करता है कि वह किस प्रोटोकॉल (Protocol) का पालन कर रहा है। सम्बंधित प्रोटोकॉल द्वारा ही सिंक्रोनस अथवा असिंक्रोनस ट्रांसमिशन को सम्पन्न किया जाता है। सामान्यतया डिजिटल ट्रांसमिशन में उपकरणों के बीच सिंक्रोनस प्रोटोकॉल का उपयोग किया जाता है, जबकि एनालॉग ट्रांसमिशन में सामान्यतया असिंक्रोनस प्रोटोकॉल का उपयोग किया जाता है।

प्रश्न 13 – Infrared पर संक्षेप में नोटस लिखिए–
Write down the short notes on Infrared. **(Dec., 2012/Jan., 201**

उत्तर–**Infrared**—Infrared technology, computing devices को short range wireless signals को कम्यूनिकेट करने की अनुमति प्रदान करती है। Infrared के माध्यम से computers, files तथा दूसरे डिजीटल डाटा को bidirection रूप में ट्रांसफर कर सकते हैं। Infrared ट्रांसमीशन टैक्नौलॉजी, कम्प्यूटर्स में उसी तरह प्रयोग की जाती है, जिस तरह remote control units प्रोडक्ट्स में की जाती है। Computer infrared network adapters, एक डिवाइस के side या rear पर ports के माध्यम से डाटा को ट्रांसमिट या रिसीव करते हैं। Infrared adapters, बहुत सारे laptops में तथा handheld personal devices में install होते हैं। माइक्रोसॉफ्ट विण्डोज infrared connections को उसी मैथड् के माध्यम से क्रिएट किया जा सकता है, जिस तरह दूसरे network connections क्रिएट किये जाते हैं।

Infrared technology, बहुत कम दूरी की range के कम्यूनिकेशन को सपोर्ट करती है। Infrared signals, दीवार या obstructions को पार नहीं कर सकते हैं। ये केवल सीधी दिशा (line of sight) में कार्य करते हैं। जैसे TV, DVD को remote के माध्यम से play करते हैं, तो remote के माध्यम से infrared signals क्रिएट होते हैं, जो इन्हे ऑपरेट करते हैं।

प्रश्न 14 – क्लाइंट सर्वर आर्कीटेक्चर के निम्नलिखित डिजाइन इशू को समझाइये :
Explain the following design issue of client server architecture.
(i) Addressing
(ii) Blocking
(iii) Buffering **(Dec., 2012/Jan., 2**

Scanned by CamScanner

उत्तर–(i) **Addressing :** Client server architecture में client तथा server के मध्य कनेक्शन स्थापित करने के लिये system call की जाती है इसमें client तथा server दोनों के मध्य socket addressing को स्थापित किया जाता है। client side पर एक socket addressing को स्थापित करने के लिये निम्नलिखित steps सम्मिलित होते हैं–

(1) socket( ) system call के साथ एक socket क्रिएट करते हैं।

(2) connect( ) system call का प्रयोग करके server के address को socket से कनेक्ट करते हैं।

(3) इसके पश्चात् data को send तथा रिसीव करते हैं।

server side पर एक socket को स्थापित करने के लिये निम्नलिखित steps सम्मिलित होते हैं–

(1) socket( ) system call के साथ एक socket को क्रिएट करते हैं।

(2) bind( ) system call का प्रयोग करके address को socket से bind करते हैं।

नोट–इंटरनेट पर server socket के लिये address, host machine पर port number से मिलकर बना होता है।

(3) listen ( ) system call के साथ connection को listen करते हैं।

(4) accept ( ) system call का प्रयोग करके एक connection को accept करते हैं।

(5) read ( ) तथा write ( ) system call का प्रयोग करके data को send तथा receive करते हैं।

(ii) Blocking : client-server architectire में सामान्यतः तीन blocks होते है।

(a) client

(b) server

(c) middleware

(a) Client Block : यह एप्लीकेशन के client side पर run करता है। यह ऑपरेटिंग सिस्टम पर रन होता है जो GUI को उपलब्ध कराता है। client block, distributed system management (DSM) पर भी रन करता है। Thin client block को web browser की आवश्यकता होती है, जो demand के आधार पर java beans तथा applets को डाउनलोड करता है।

(b) Server Block : यह एप्लीकेशन के server part पर रन होता है। server OS, middlware के साथ इंटरफेस पर डिपेन्ड होता है। server भी DSM component पर रन होता है।

(c) Middleware Block : यह एप्लीकेशन के client तथा server दोनों sides पर रन होता है। यह भी DSM कम्पोनेन्ट को रखता है। यह पुनः तीन श्रेणियों में विभाजित होता है। (i) Transport stacks (ii) Network operating systems (iii) Service-specific middleware

(iii) Buffering : client-server architecture में server application में डाटा तथा इन्फॉरमेशन save रहती है, यह लोकेशन server पर Buffer log के नाम से होती है। client अपनी आवश्यकता के अनुसार इस Buffer log में एक्सेस करके डाटा को अपने सिस्टम पर रिट्रीव कर सकता है। जब client, डाटा के लिये server पर रिक्वेस्ट send करता है, तो server, रिक्वेस्ट किये गये डाटा को client पर भेज देता है तथा एक copy को buffer log में save कर देता है, जिससे कि इसे भविष्य में प्रयोग किया जा सके। इसे buffering कहते हैं।

❑

प्रश्न 15 – ***Optical Fibre के अन्दर Cladding का क्या मतलब है? विस्तार से समझाइये?***

What is the purpose of cladding in an optical fiber? Explain in detail.

उत्तर–Fiber optical cable के सामान्यतः तीन मूलभूत एलीमेन्ट्स होते हैं।

(i) Core–यह, fiber का light transmission area होता है। यह area या तो glass का होता है या plastic का होता है।

(ii) Cladding–Cladding का function, lower refractive index को उपलब्ध कराता है।

(iii) Coating–coating सामान्यतः plastic की multi-layers होती है, जो fiber strength की सुरक्षा के लिये apply की जाती है।

Scanned by CamScanner

निम्नलिखित Fig. में Optical Fiber को दिखाया गया है–

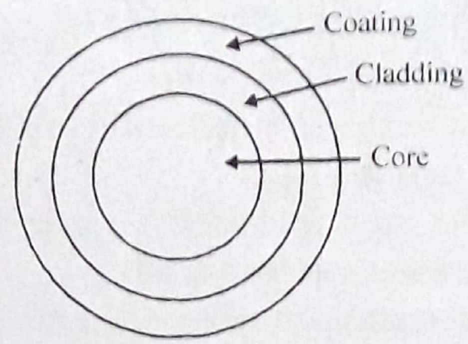


Fig. : Optial Fiber

Optical fiber की सामान्यतः दो layers होती हैं। प्रथम inner layer तथा द्वितीय Outer layer, Inner layer के माध्यम से travel होने वाला data, central hollow material से मिलकर बना होता है। यह glass से या plastic से मिलकर बना होता है। यह Core, एक less dense material के द्वारा cover होती है, जो cladding के नाम से जानी जाती है, जो glass या plastic से भी मिलकर बनी हो सकती है।

Core में light reflecting को रखना जरूरी होता है, क्योंकि हमें इसे source से destination को pass करने की जरूरत होती है। Fiber optical cable में डाटा optical fiber के रूप में travel करता है। इसलिये अधिक से अधिक light के reflection को रोकने की आवश्यकता होती है। जब light, core से cladding में enter करती है तो यह angle को बदलती है, तब यह core में light को वापिस reflect करती है, जिसे Cladding रोकती है। Cladding, less dense material से निर्मित होता है, इसलिये Cladding का प्रयोग optical fiber में किया जाता है। ❑

प्रश्न 16 – ***एक 5KHz bandwidth चैनल है। यदि हम डाटा को 150-kbps से भेजना चाहते हैं तो कम से कम $SNRd_B$ की जरूरत पड़ेगी। SNR क्या है?***

We have a channel with 5KHz bandwidth. If we want to send data to 150 Kbps, what is the minimum $SNRd_B$? What is SNR?

उत्तर–SNR––SNR, Signal-to-Noise Ratio का संक्षिप्त रूप है। SNR को db में मापा जाता है। SNR एक नेटवर्क चैनल पर एक audio signal या एक ट्रांसमीशन चैनल की क्वालिटी को मापता है। SNR, signal strength तथा कनेक्शन में उपस्थित Noise के बीच का ratio है। एक नेटवर्क के लिये जितना संभव हो सके उनते उच्च (high) SNR की जरूरत होती है।

According to question

Channel bandwidth = 5KHz

data transmission rate = 150kbps

To find SNR formulae is

data transmission rate = bandwidth$\cdot \log_2(1+\frac{S}{N})$ (bit persec) (b)

Putting the values in formulae

$$150\times1024\times8 = 5\log_2(1+\frac{S}{N})$$

$$\log_2(1+\frac{S}{N}) = 240 \times 1024$$

Taking Antilog both side, We get SNR

$$1+\frac{S}{N} = \infty \text{ (infinity)}$$

$$\therefore \frac{S}{N}(SNR) = \text{(infinity)}$$

❑

Scanned by CamScanner

प्रश्न 17 – निम्नलिखित पर संक्षिप्त टिप्पणी लिखिये :

Write the short notes on the following :

(a) Circuit Switching

(b) Message Switching

(c) Packet Switching

उत्तर–**(a) Circuit Switching**–Circuit Switching एक टेलीकम्युनिकेशन नेटवर्क को इम्पलीमेन्ट करने की मैथडोलॉजी है। एक मैथोडौलॉजी में दो network, nodes के माध्यम से एक dedicated कम्युनिकेशन चैनल को स्थापित करती है। इसके पश्चात् इनके मध्य में कम्यूनिकेशन संम्पन्न होता है। Analog telephone network, Circuit Switching तकनीकी का प्रयोग करके nodes के मध्य में कम्यूनिकेशन स्थापित करता है। जब एक कॉल एक टेलीफोन से दूसरे टेलीफोन के लिये की जाती है तो टेलीफोन एक्सचेंज में प्रयुक्त switches, दोनों Telephones के बीच में एक Continuous wire circuit को क्रिएट करते हैं। ये तब तक कनेक्ट रहते हैं, जब तक कि Call पूर्ण नहीं हो जाती है। अतः Circuit Switching में एक बार कॉल सेटअप हो जाती है तो दोनों ends के बीच में एक dedicate path exist करता है। यह path तब तक exist करता है जब तक कि call finish नहीं हो जाती है।

(b) Message Switching–टेलीकम्यूनिकेशन में Message switching, packet swtiching से पहले प्रयोग की जाती थी अर्थात् यह packet switching के packet या डाटा पर messages को एक बार में एक hop के रूप में route किया जाता था। आज के समय में message swtiching systems अधिकतर packet-switched या circuit-switched data network के ऊपर प्रयोग किये जाते हैं। Message Switching में source तथा destination के बीच में किसी फिजीकल कनेक्शन की आवश्यकता नहीं होती है। इस टाइप के नेटवर्क को store and forword network कहते हैं। इसमें message priority को स्थापित किया जा सकता है।

(c) Packet switching–Packet switching को Circuit switching के alternate के रूप में प्रयोग किया जाता है। Packet switching नेटवर्क तकनीक में डाटा को packets के रूप में ट्रांसमिट किया जाता है। पैकेट डाटा तथा कण्ट्रोल इनफॉरमेशन को रखता है। Packet switching नेटवर्क किसी भी host को किसी भी host के पास डाटा को भेजने की अनुमति देता है। इसमें किसी फिजीकल Circuit की आवश्यकता नहीं होती है। इसमें sender तथा receiver के बीच में multiple path के pair exist करते हैं। Source तथा destination के बीच में एक path को सलेक्ट किया जाता है। जब भी sender, डाटा को भेजता है, यह packets में convert हो जाता है। तथा इन्हें next computer या router के पास forword कर देता है। Router इन pakets को स्टोर करता है। तथा output line के free हो जाने पर इन्हें भेजता है। ❑

प्रश्न 18 – Circuit Switching तथा Packet switching के बीच में अन्तर बताइये।

Differentiate between circuit switching and packet switching.

उत्तर–Circuit Switching और Packtet Switching के मध्य अन्तर निम्नलिखित है–

Circuit Switching	Packet Switching
1. Circuit switching Connection-oriented data transmission है।	1. Packet Switching, Connetion-less data transmission है।
2. Circuit switching में data transmission के शुरू होने से पहले path अवश्य निर्धारित होना चाहिये।	2. Packet switching में transmission के शुरू होने से पहले path का निर्धारित होना आवश्यक नहीं है।
3. Circuit switching में fixed bandwidth circuit स्थापित होता है, तत्पश्चात् यूजर कम्यूनिकेशन कर सकता है।	3. Packet switching में Circuit के स्थापित होने की आवश्यकता नहीं है।
4. Circuit switching का प्रयोग phone calls में किया जाता है। टेलीफोन नेटवर्क इसका मुख्य उदाहरण है।	4. Packet Switching का प्रयोग data को हैण्डल या data communication में किया जाता है। कम्प्यूटर नेटवर्क इसका मुख्य उदाहरण है।

❑

प्रश्न 19 – Virtual Circuit से आप क्या समझते हैं? Virtual circuits को उपलब्ध कराने वाले प्रोटोकॉल कौन से होते हैं?

What do you understand by virtual circuit? Which Protocols are provided to virtual circuits?

Scanned by CamScanner

या

Virtual Circuit पर संक्षिप्त टिप्पणी लिखिये?

Write the short notes on virtual circuit.

उत्तर–टेलीकम्यूनिकेशन तथा कम्प्यूटर नेटवर्क में Virtual Circuit, Virtual channel तथा Virtual Connection का पर्यायवाची (Synonyms) के रूप में जाना जाता है। यह कनेक्शन ऑरिएन्टेड कम्यूनिकेशन सेवा को उपलब्ध कराता है। दो nodes के मध्य में virtual circuit के माध्यम से कनेक्शन स्थापित हो जाने के पश्चात् bit stream या byte stream nodes के बीच में डिलीवर हो सकती है। अतः virtual circuit, packed switched नेटवर्क पर दो end systems के बीच में लॉजिकल रूप में कनेक्शन ओरिएण्टेड नेटवर्क है। Packet switched से तात्पर्य है कि Virtual Circuit, packets के रूप में डाटा तथा इनफॉरमेशन को ट्रांसफर करने की अनुमति देता है। Virtual Circuit दो end systems के बीच में उपलब्ध path में से एक path को चुनता है। यद्यपि दो end systems के बीच में multiple paths उपलब्ध होते हैं किन्तु यह एक समय में केवल दो end systems को कनेक्ट करता है।

Virtual circuit को मुख्य रूप से ATM (Asynchronous Transfer mode), Frame Relay, GPRS (General Packet Radio Servie) IP इत्यादि नेटवर्क में प्रयोग किया जाता है।

Virtual Circuit को उपलब्ध कराने वाले प्रमुख प्रोटोकॉल्स TCP (Transmission Centrol Protocal), SCTP (Stream Control Transmission Protocol) है।

निम्नलिखित Fig में Virtual circuit network को दर्शाया गया है–

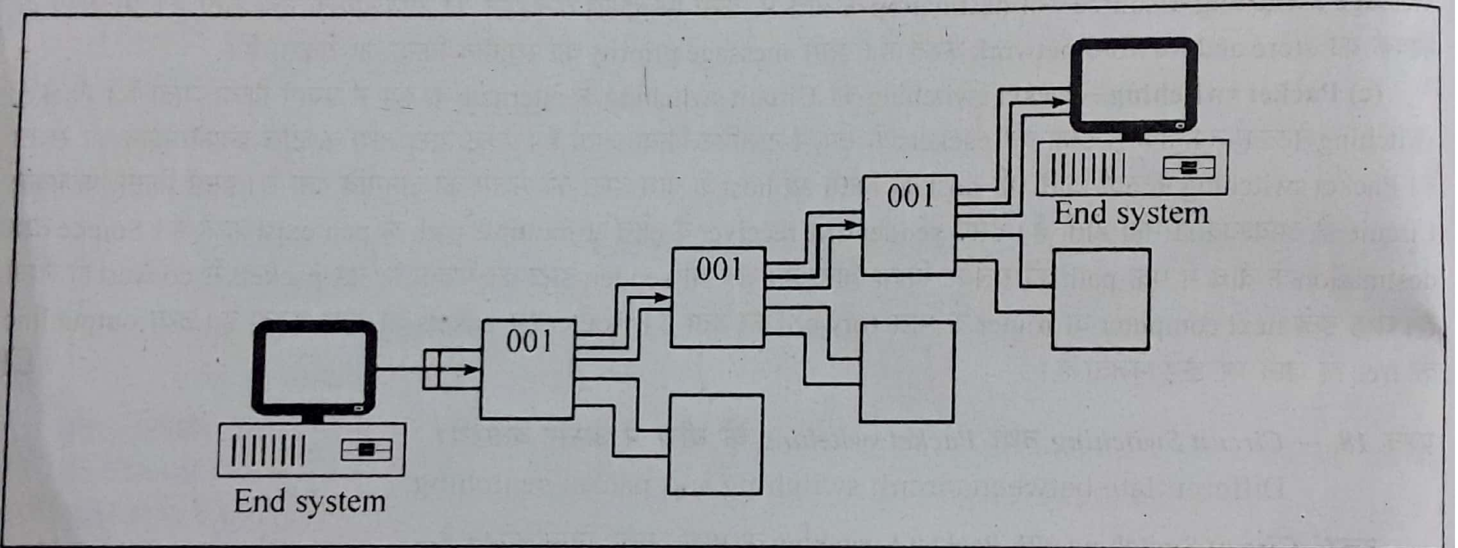


Fig : Virtual Circuits

Virtual Circuits को दो types में विभाजित किया जा सकता है–

1. Permanent virtual circuits (PVC)
2. Switched virtual circuits (SVC)

1. Permanent Virtual Circuits (PVC)–Permanent Virtual Circuits का प्रयोग permanent या dedicated path के लिये किया जाता है। यह path पूरे समय तक कनेक्ट रहता है। PVC's का प्रयोग मुख्य रूप से Frame Relay networks पर किया जाता है।

2. Switched Virtual Ciruits (SVC)–Switched Virtual Ciruits का प्रयोग तब किया जाता है, जब दो end systems के मध्य में temporary कनेक्शन की आवश्यकता होती है। इसमें डाटा ट्रांसफर के पूर्ण हो जाने पर कनेक्शन disconnect हो जाता है। ATM दोनों types के virtual कनेक्शन की सुविधा को उपलब्ध कराता है। □□

Scanned by CamScanner

UNIT-II

प्रश्न 1 – बेसबैंड तथा ब्रॉडबैंड ट्रांसमिशन में अंतर स्पष्ट कीजिये।

Explain the difference between baseband and broadband transmission. **(June, 2007)**

उत्तर–जब एक से अधिक कम्प्यूटरों को आपस में जोड़ते हैं तो इस तकनीक को कम्प्यूटर नेटवर्क कहते हैं। कम्प्यूटर नेटवर्क में जुड़े हुये कम्प्यूटरों में आपस में डाटा को ट्रांसफर कर सकते हैं। डाटा को ट्रांसफर करने के लिये ट्रांसमिशन मीडिया का प्रयोग करते हैं। भिन्न-भिन्न प्रकार के ट्रांसमिशन मीडिया बाजार में उपलब्ध हैं। अपनी आवश्यकता के अनुसार इच्छित मीडिया का प्रयोग करके एक कम्प्यूटर से दूसरे कम्प्यूटर पर डाटा को ट्रांसफर कर सकते हैं। ट्रांसमिशन मीडिया की क्षमता (Capacity) को एलोकेट करने के तरीके को बैंडविड्थ (Bandwidth) कहते हैं। सम्पूर्ण मीडिया क्षमता या Bandwidth को Channels में विभाजित किया जा सकता है। एक Channel, Bandwidth का एक भाग होता है जो डाटा को ट्रांसमिट करने के लिये प्रयोग किया जा सकता है। ट्रांसमिशन मीडिया की क्षमता को एलोकेट करने के लिये निम्नलिखित दो तरीके प्रयोग किये जाते हैं–

1. Baseband, 2. Broadband

Baseband तथा Broadband के मध्य मुख्य अन्तर निम्नलिखित है–

Baseband	Broadband
1. इस ट्रांसमिशन में सम्पूर्ण मीडिया Bandwidth को एक Single Channel में प्रयोग किया जाता है।	1. इस ट्रांसमिशन में संपूर्ण मीडिया Bandwidth को Multiple Channels में विभाजित कर दिया जाता है।
2. Baseband सामान्यतः Digital Signal के लिये प्रयोग किया जाता है। यद्यपि इसे Analog Signals के लिये भी प्रयोग कर सकते हैं।	2. प्रत्येक Channel विभिन्न Analog Signals या Digital Signal को Carry कर सकते हैं।
3. अधिकतर Local Area Networks, Baseband Signalling को प्रयोग करते हैं।	3. Broadband Network एक Single ट्रांसमिशन मीडिया के ऊपर एक से अधिक Conversations को सपोर्ट करता है।

❑

प्रश्न 2 – निम्नलिखित ट्रांसमिशन पर संक्षिप्त टिप्पणियां लिखिये–

Write short notes on following transmission media :

(i) Baseband coaxial cable

(ii) Broadband coaxial cable

उत्तर–**(i) Baseband coaxial cable**–Coaxial cable, स्टिफ कॉपर Wire से मिलकर बनी होती है। यह Wire कोर के रूप में Insulating material के द्वारा घिरी होती है। Insulator, एक Cylinder Conductor द्वारा घिरी होती है। बाह्य Conductor, एक प्लास्टिक Sheath के द्वारा घिरी होती है। Baseband coaxial cables प्रायः Baseband Networks में प्रयोग की जाती हैं। Baseband Networks वह Networks होते हैं, जहां Cable की पूरी Bandwidth एक single channel के रूप में प्रयोग की जाती है। सामान्यतः दो प्रकार की Coaxial cable का प्रयोग किया जाता है–

(a) 50-ohm cable

(b) 75-ohm cable

(a) 50-ohm cable–50-ohm cable सामान्यतः डिजीटल ट्रांसमीशन में प्रयोग की जाती है।

(b) 75-ohm cable–75-ohm cable सामान्यतः Cable TV ट्रांसमीशन में Analog ट्रांसमीशन के लिये प्रयोग की जाती है।

(ii) Broadband coaxial cable–Broadband coaxial cables प्रायः Broadband Networks में प्रयोग की जाती हैं। Broadband Networks वह Networks होते हैं, जहां Cable की पूरी bandwidth, multiple channel में विभाजित कर दी जाती है। सामान्यतः Broadband, frequency division multiplexed स्थिति होती है जहां Coaxial cable की bandwidth को subchannels में विभाजित कर दिया जाता है। ये subchannels या तो बराबर frequencies में होते हैं या Varying frequencies रेन्ज में होते हैं, जो अलग-अलग कम्यूनिकेशन मीडिया के रूप में treat किये जाते हैं। ❑

Scanned by CamScanner

प्रश्न 3 – *OSI नेटवर्क मॉडल को विस्तार से समझाइये।*
Explain in detail the OSI Network Model.

उत्तर–OSI नेटवर्क मॉडल–OSI को विस्तृत रूप में Open System Interconnection कहते हैं। OSI नेटवर्क मॉडल में सात लेयर होती हैं। जिसका चित्र नीचे दिया गया है–

Application Layer
Presentation Layer
Session Layer
Transport Layer
Network Layer
Data Link Layer
Physical Layer

OSI नेटवर्क मॉडल को प्रोसेसिंग सिस्टम्स के बीच में इनफॉरमेशन को बदलने के प्रोसीजर को स्टैण्डर्डराइज करने के लिये डेवलप किया गया था। OSI एक कम्यूनिकेशन रेफरेन्स मॉडल है जिसे ISO (International Standards Organization) के द्वारा परिभाषित किया गया है। OSI नेटवर्क मॉडल में सात लेयर (Seven Layers) होती हैं। प्रत्येक लेयर एक विशेष कार्य को पूरा करती है। OSI नेटवर्क मॉडल की सात प्रमुख लेयर्स निम्नलिखित हैं–

1. फिजीकल लेयर (Physical Layer)–फिजीकल लेयर इलैक्ट्रिकल, ऑप्टीकल या रेडियो सिग्नलस के साथ फिजीकल सर्किट को बनाती है। फिजीकल लेयर में पेसिव हब, एक्टिव हब, टर्मिनेटर्स, कपलर्स, केबल्स, कनेक्टर्स, रिपोटर्स, मल्टीप्लेक्सर्स, ट्रांसमीटर्स, रिसीवर्स तथा ट्रांस रिसीवर्स इत्यादि डिवाइसेस होती हैं।

2. डाटा लिंक लेयर (Data Link Layer)–डाटा लिंक लेयर नेटवर्क में एक्सेस करने के लिये जिम्मेदार होती है तथा डाटा के फिजीकल ब्लॉक को एक डिवाइस से दूसरी डिवाइस पर ट्रांसमिट करती है। इस लेयर में Error Checking सम्मिलित होती है।

3. नेटवर्क लेयर (Network Layer)–नेटवर्क लेयर Routing Decision लेती है तथा डिवाइसेस के लिये पैकेटों को आगे बढ़ाती है। Routers तथा Gateways नेटवर्क लेयर में ऑपरेट किये जाते हैं।

4. ट्रांसपोर्ट लेयर (Transport Layer)–ट्रांसपोर्ट लेयर मैसेज को नेटवर्क के ऊपर ट्रांसमीशन के लिये आवश्यक स्ट्रक्चर में कनवर्ट करने के लिये जिम्मेदार होती है। यह लेयर पैकेटों को Error Free, सीक्वेंस में तथा पैकेटों को खोये बिना भेजने के लिये सुनिश्चित करती है। ट्रांसपोर्ट लेयर बड़े मैसेजों को पैकेटों के रूप में ब्रेक करती है।

5. सैशन लेयर (Session Layer)–Session लेयर सैशन को स्थापित तथा टर्मिनेट करती है। यह लेयर एप्लीकेशनों को अलग-अलग कम्प्यूटरों पर कनेक्शन को शेयर करने के लिये अनुमति देती है। यह लेयर दो प्रोसेस के बीच डायलॉग को भी कंट्रोल करती है।

6. प्रजेन्टेशन लेयर (Presentation Layer)–प्रजेन्टेशन लेयर नेटवर्क की आवश्यकतानुसार प्रारूपों के बीच डाटा को ट्रांसलेट करने तथा जिस फॉर्मेट को कम्प्यूटर स्वीकार करता है, उस फॉर्मेट में ट्रांसलेट करती है। प्रजेन्टेशन लेयर, प्रोटोकॉल कनवर्जन, डाटा ट्रांसलेशन, कम्प्रेशन तथा इनक्रेप्शन, कैरेक्टर सेट कनवर्जन और ग्राफिक्स कमांडो के व्याख्यान को पूरा करती है।

7. एप्लीकेशन लेयर (Application Layer)–एप्लीकेशन लेयर, OSI मॉडल की Top Most लेयर है। यह यूजर एप्लीकेशनस; जैसे–डाटाबेस एक्सेस, ई-मेल तथा File Transfers को डायरेक्टली सपोर्ट करने की सेवा को उपलब्ध कराता है। यह लेयर दूसरे कम्प्यूटरों पर एप्लीकेशनस के साथ एप्लीकेशनस को कम्यूनिकेट करने के लिये भी Allow करती है। एप्लीकेशन लेयर अलग-अलग मशीनों पर एप्लीकेशन प्रोग्राम्स को कनेक्शन उपलब्ध कराती है। □

प्रश्न 4 – *IEEE 802 Standards से आप क्या समझते हैं? IEEE 802.3, 802.4 तथा 802.5 के बारे में बताइये।*
What do you understand by IEEE 802 Standards? Explain about IEEE 802.3, 802.4 and 802.5

उत्तर–आईईईई 802 मानक (IEEE 802 Standards)–इंस्टीट्यूट ऑफ इलैक्ट्रीकल एंड इलैक्ट्रॉनिक इंजीनियर्स (Institute of Electrical and Electronic Engineers), संक्षेप में IEEE, संसार में पेशेवरों का सबसे बड़ा संगठन है। अनेक जर्नल (Journals) प्रकाशित करने और प्रतिवर्ष सैकड़ों सम्मेलन आयोजित करने के अलावा IEEE में एक मानकीकरण समूह (Standardization group)

Scanned by CamScanner

है, जो इलैक्ट्रीकल इंजीनियरिंग और कम्प्यूटिंग के क्षेत्र में मानकों (Standards) का विकास करता है। सन् 1985 में IEEE की कम्प्यूटर सोसाइटी ने एक प्रोजेक्ट प्रारम्भ की, जिसका उद्देश्य विभिन्न प्रकार के निर्माताओं द्वारा बनाये गये उपकरणों के बीच परस्पर संचार (Intercommunication) को सम्भव बनाना था। इस प्रोजेक्ट का नाम प्रोजेक्ट 802 (Project 802) था। यहाँ 802 केवल एक क्रम संख्या है। प्रोजेक्ट 802 का उद्देश्य OSI मॉडल के किसी भाग को हटाकर उसके बदले कोई अन्य प्रोटोकॉल रखने का नहीं है, बल्कि अधिकांश लोकल एरिया नेटवर्कों में फिजीकल लेयर और डाटा लिंक लेयरों के कार्यों को परिभाषित करने की एक अन्य विधि बताना है।

प्रोजेक्ट 802 ने जो मानक निर्धरित किये उन्हें IEEE 802 मानक कहा जाता है। इन मानकों को अमेरिकन नेशनल स्टैंडर्ड्स इंस्टीट्यूट (American National Standards Institute या ANSI) द्वारा अंगीकार किया गया था। सन् 1987 में इंटरनेशनल स्टैंडर्ड्स ऑर्गनाइजेशन (International Standards Organization या ISO) ने इनको अन्तर्राष्ट्रीय मानकों के रूप में स्वीकार कर लिया।

IEEE 802 मानक OSI मॉडल के सबसे निचले दो लेयरों डाटा लिंक लेयर तथा फिजीकल लेयर की सेवाओं और प्रोटोकॉलों को परिभाषित करता है। वास्तव में, IEEE 802 मानक डाटा लिंक लेयर को दो सब-लेयरों (Sub-layers) में तोड़ता है, जिनके नाम हैं—लॉजिकल लिंक कंट्रोल (Logical Link Control या LLC) तथा मीडिया एक्सैस कंट्रोल (Media Access Control या MAC). इन सब-लेयरों का परिचय नीचे दिया गया है।

एलएलसी सब-लेयर (LLC Sub-layer)—यह सब-लेयर सभी प्रकार के लैन प्रोटोकॉलों (LAN protocols) में आपस में सम्पर्क करना सम्भव बनाता है। यदि दो लैनों के प्रोटोकॉलों का LLC सब-लेयर समान है, तो उन लैनों को एक दूसरे से जोड़ा जा सकता है। इसका अर्थ है कि LLC सब-लेयर उन लैनों के एक्सैस मैथड (Access method), एनकोडिंग (Encoding), सिग्नलिंग (Signaling) और सम्प्रेषण माध्यम (Transmission medium) को ऊपरी लेयरों के लिए पारदर्शी (Transparent) बना देता है। हालांकि कोई नेटवर्क LLC सब-लेयर की सेवाओं को लेने या न लेने के लिए स्वतंत्र है। यदि नेटवर्क अन्य किसी विश्वसनीय उच्च-स्तरीय प्रोटोकॉल; जैसे TCP, का उपयोग करता है, तो उसे LLC की सेवाओं की आवश्यकता नहीं है।

एमएसी सब-लेयर (MAC Sub-layer)—MAC सब-लेयर कई अलग-अलग मॉड्यूलों का समूह है, जिनमें से प्रत्येक किसी विशेष प्रकार के लैन (LAN) से सम्बंध रखता है। प्रत्येक मॉड्यूल अपने प्रकार के लैन के लिए साझा माध्यम (Shared media), सिंक्रोनाइजेशन (Synchronization), फ्लैग (Flag), फ्लो (Flow), त्रुटि नियंत्रण (Error control) आदि का विवरण निश्चित करता है, जिनका उपयोग सूचनाओं को एक स्थान से दूसरे स्थान तक ले जाने में किया जाता है। इसके साथ ही यह सब-लेयर अगले स्टेशन के फिजीकल पते (Physical address) का भी ध्यान रखता है।

MAC प्रोटोकॉल उनका उपयोग करने वाले लैनों (LANs) पर निर्भर करता है। इसलिए हर प्रकार के लैन के लिए विशेष IEEE 802 मानक निश्चित किया गया है। वास्तव में IEEE 802 मानकों का एक परिवार (Family) या कार्यकारी समूह (Working group) है, जिनका उपयोग विभिन्न प्रकार के लैनों जैसे ईथरनेट (Ethernet), टोकन रिंग (Token ring), वायरलैस लैन (Wireless LAN) आदि द्वारा किया जाता है।

यहाँ हम इनमें से उन मानकों की चर्चा करेंगे, जो अधिक महत्वपूर्ण हैं अथवा जिनका उपयोग प्रमुख रूप से किया जा रहा है।

● **आईईईई 802.3 (IEEE 802.3)**—यह आईईईई मानकों का ऐसा समूह है, जिसके द्वारा तार-सहित ईथरनेट (Wired Ethernet) नेटवर्कों के फिजीकल लेयर (Physical layer) तथा डाटा लिंक लेयर (Data link layer) के मीडिया एक्सैस कंट्रोल (MAC) सब-लेयर को परिभाषित किया गया है। सामान्यतया इसका उपयोग लोकल एरिया नेटवर्कों (LANs) में किया जाता है, परन्तु कुछ सीमा तक वाइड एरिया नेटवर्कों (WANs) में भी किया जा सकता है। इस प्रकार के नेटवर्कों में विभिन्न नोडों (Nodes) अथवा उपकरणों (Devices) के बीच भौतिक कनेक्शन बनाये जाते हैं।

802.3 एक ऐसी तकनीक है, जो 802.1 नेटवर्क आर्कीटैक्चर के साथ भी कार्य करती है।

इन मानकों में अधिकतम पैकेट साइज 1518 बाइट होता है। यदि ऊपरी लेयर का प्रोटोकॉल कोई डाटा यूनिट 64 बाइट से कम का देता है, तो 802.3 मानक उस डाटा फील्ड को न्यूनतम 64 बाइटों का बना लेता है। इस प्रकार न्यूनतम फ्रेम आकार 64 बाइटों का होता है।

इस समूह के अन्तर्गत अनेक मानक हैं, जिनका उपयोग विभिन्न प्रकार के ईथरनेट नेटवर्कों में किया जाता है।

● **आईईईई 802.4 (IEEE 802.4)**—यह आईईईई मानक टोकन बस नेटवर्कों (Token Bus networks) के डाटा लिंक लेयर के मीडिया एक्सैस कंट्रोल (MAC) सब-लेयर को परिभाषित करता है। यह ऐसे लेयरों में टोकन पास करने के सिस्टम (Token-passig mechanism) में उपयोग में लाया जाता है।

अब इस वर्किंग समूह (Working group) को समाप्त कर दिया गया है।

● **आईईईई 802.5 (IEEE 802.5)**—इस आईईईई मानक का उपयोग टोकन रिंग नेटवर्कों (Token ring networks) में किया जाता है। टोकन रिंग नेटवर्क ऐसे रिंग नेटवर्क होते हैं, जिनमें किसी निश्चित आकार (सामान्यतया 3 बाइट) के फ्रेम (Frame), जिसे टोकन (Token) कहा जाता है, को पूरे लूप में घुमाया जाता है। □

Scanned by CamScanner

प्रश्न 5 – *Modem पर संक्षिप्त टिप्पणी लिखिए।*
Write down shorts notes on Modem.

उत्तर–मॉडेम (Modem)–मॉड्यूलेशन (Modulation) तकनीक का उपयोग करते हुए डिजिटल संकेतो को एनालॉग माध्यम से एनालॉग संकेतों में बदला जाता है। इसके पश्चात् इन्हें टेलीफोन लाइन पर प्रेषित किया जाता है। यह क्रिया एक डिवाइस, जिसे मॉडेम कहा जाता है, के द्वारा सम्पन्न होती है। उदाहरणार्थ, कम्प्यूटर द्वारा भेजे गये डिजिटल संकेतों को मॉडल एनालॉग माध्यम (टेलीफोन लाइन) के लिए एनालॉग संकेतों में बदलता है, इसे मॉड्यूलेशन कहते हैं।

इसी प्रकार डी-मॉड्यूलेशन (De-modulation) तकनीक का उपयोग करते हुए एनालॉग संकेतों को डिजिटल माध्यम से डिजिटल संकेतों में परिवर्तित किया जाता है। यह क्रिया भी मॉडेम के द्वारा ही सम्पन्न होती है। उदाहरणार्थ, एनालॉग माध्यम (टेलीफोन लाइन) द्वारा प्रेषित किए गए एनालॉग संकेतों को मॉडेम डिजिटल माध्यम (कम्प्यूटर) के लिए डिजिटल संकेतों में बदलता है, इसे डी-माड्यूलेशन कहते हैं। माइक्रो-कम्प्यूटर के डाटा स्थानान्तरण की गति (Data Transfer Rate) 2,400 से 3,600 BPS (Bits Per Second) होती है।

मॉडेम एक सीरियल कम्यूनिकेटर डिवाइस है। मॉडेम के निम्न प्रकार होते हैं–

(1) एक्सटरनल मॉडेम–यह एक Cute Small Box की तरह उपलब्ध होता है। इसमें बहुत-सी LED होती हैं। इस मॉडेम में AC पॉवर सप्लाई से कुछ अल्प पॉवर सप्लाई की आवश्यकता होती है। इस मॉडेम में RJ11 फोन जैक होती हैं जिसका एक सिरा फोन लाइन से जुड़ा होता हैं और दूसरा सिरा फोन यंत्र से जुड़ा होता है।

(2) इन्टरनल मॉडेम–यह मॉडेम add-on Card Plugged फॉर्म में उपलब्ध होता है। इसका स्लॉट मदरबोर्ड में उपलब्ध होता है। आजकल नये मॉडेम USB इन्टरफेस का प्रयोग कर रहे हैं, क्योंकि सीरियल पोर्ट पर इंटरनेट की गति धीमी होती है।

(3) फैक्स मॉडेम (Fax Modem)–इस मॉडेम के प्रयोग द्वारा आप अपने पर्सनल कम्प्यूटर को Fax मशीन के रूप में भी उपयोग कर सकते हैं। इस तरह मॉडेम के प्रयोग से Fax का आदान-प्रदान आसानी से कर सकते हैं। इसका सबसे बड़ा फायदा यह है कि उपयुक्त Software का प्रयोग कर फैक्स को फाइलों में परिवर्तित कर उसमें आवश्यक संशोधन भी कर सकता है। ❑

प्रश्न 6 – *Wireless Transmission के संदर्भ में Transmission Technique को समझाइये–*
Explain Wireless Transmission with reference to Transmission Technique. **(Jan., 2004)**
(i) Microwave Transmission,
(ii) Radio Transmission,

उत्तर–(i) Microwave Transmission–100 MHz के ऊपर तरंगें सीधी दिशा (Straight lines) में गमन (Travel) करती हैं और इसलिये संकीर्ण (Narrowly) रूप से केन्द्रित की जा सकती है। पूरी ऊर्जा एक Parabolic एन्टिना का इस्तेमाल करके एक छोटी किरण के रूप में केन्द्रित करने से ध्वनि तथा शोर का एक उच्च अनुपात प्राप्त होता है। लेकिन भेजने वाले और प्राप्त करने वाले एन्टिना को पूरी तरह एक-दूसरे के साथ पंक्तिबद्ध होना चाहिये। कम्प्यूटर नेटवर्क में डाटा को ट्रांसमिट करने के लिये Twisted Pair Cable, Coaxial Cable तथा Fibre Optic Cable का प्रयोग किया जाता है। लोकल एरिया नेटवर्क के लिये सामान्यतः Twisted Pair Cable तथा Co-axial Cables का प्रयोग किया जाता है। लम्बी दूरी के नेटवर्क (MAN) जैसे एक शहर को दूसरे शहर से जोड़ने के लिये माइक्रोवेव स्टेशन (Microwave Station) का प्रयोग किया जाता है। इन स्टेशनों के माध्यम से किये गये ट्रांसमीशन को माइक्रोवेव ट्रांसमीशन (Microwave Transmission) कहते हैं। जब फाइबर ऑप्टिक की संरचना नहीं हुई थी तब माइक्रोवेवूस का प्रयोग लम्बी दूरी के टेलीफोन ट्रांसमीशन सिस्टम के लिये किया जाता था। निम्न Fig. में एक पॉइंट से दूसरे पॉइंट पर माइक्रोवेव कम्यूनिकेशन को प्रदर्शित किया गया है–

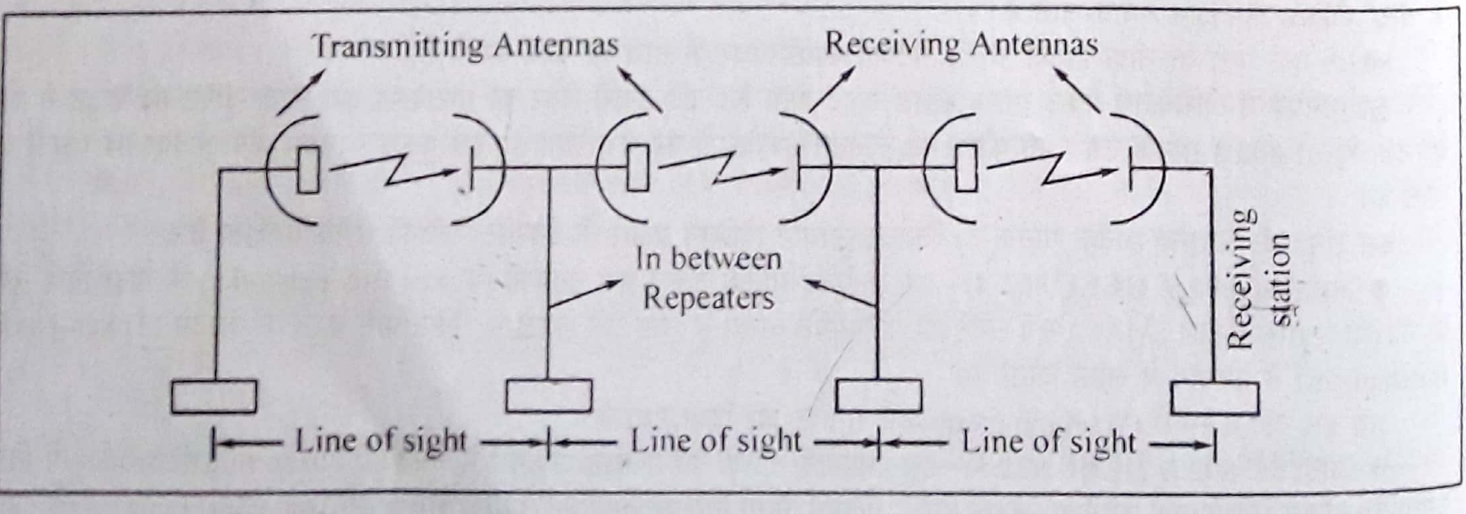


Fig. : Illustration of Microwave Communication from one point to another

Scanned by CamScanner

लम्बी दूरी के लिये कमजोर Signals के Power Amplifications तथा प्रकाश की संरचना से निपटने के लिये 25 से 30 किलोमीटर के अन्तर पर Transmitting तथा Receiving स्टेशनों के बीच में माइक्रोवेव सिस्टम्स Repeaters का प्रयोग करते हैं। प्रथम रिपीटर Transmitting स्टेशन पर तथा आखिरी रिपीटर Receiving स्टेशन पर स्थापित किया जाता है।

माइक्रोवेव ट्रांसमीशन मौसम (Weather) तथा आवृति (Frequency) पर निर्भर होते हैं। माइक्रोवेव ट्रांसमीशन का प्रयोग मुख्यतः लम्बी दूरी के टेलीफोन कम्यूनिकेशन, सेलुलर टेलीफोनूस, टेलीविजन इत्यादि के लिये किया जाता है। माइक्रोवेव, फाइबर ऑप्टिक सिस्टम की अपेक्षाकृत सस्ता होता है। माइक्रोवेव सिस्टम्स 16 Gigabits Per Second के Rate पर डाटा ट्रांसमीशन को परमिट करता है।

(ii) Radio Transmission–Radio Waves की आवृत्ति (Frequencies) 10 किलोहर्ट्ज (KHz) तथा 1 गीगाहर्ट्ज (GHz) के मध्य होती है। Radio Waves में निम्नलिखित Types की Waves सम्मिलित होती हैं–

(a) लघु तरंग (Short-Wave)

(b) बहुत ऊंची आवृत्ति (Very High Frequency—VHF) तथा FM रेडियो

(c) अल्ट्रा हाई फ्रीक्वेन्सी (Ultra High Frequency—UHF) रेडियो और टेलीविजन

Vacuum में सभी इलैक्ट्रोमैग्नेटिक तरंगें (Electromagnetic Waves) एक ही स्पीड पर Travel करती हैं, इससे कोई फर्क नहीं पड़ता है कि इनकी Frequency क्या है? इस स्पीड को सामान्यतः प्रकाश की स्पीड कहते हैं जो लगभग 3×10^8 प्रति सैकण्ड होती है। Radio Waves को आसानी से जनरेट किया जाता है। ये Waves लम्बी दूरी तक Travel कर सकती हैं। ये ठोस वस्तु जैसे Buildings को आसानी से भेद सकती हैं इसलिये इन्हें Indoors तथा Outdoors कम्यूनिकेशन के लिये अधिक मात्रा में प्रयोग किया जाता है।

Radio Waves, omnidirectional होती हैं; अर्थात् ये Source से किसी भी दिशा में Travel कर सकती हैं। ❑

प्रश्न 7 – निम्न पर संक्षिप्त टिप्पणी लिखिए–

Write short notes on the following :

(a) Wired Transmission

(b) Wireless Transmission

उत्तर–(a) वायर्ड ट्रांसमिशन (Wired Transmision)—इस प्रकार के ट्रांसमिशन में प्रेषक और प्राप्तकर्त्ता के बीच सूचना या प्रेषण किसी भौतिक तार (Physical wire) या केबल (Cable) के माध्यम से होता है। दूसरे शब्दों में, प्रेषक से प्राप्तकर्त्ता तक भेजे जाने वाले सिग्नल किसी तार या केबल में होकर यात्रा करते हैं। यह तार या केबल किसी भी प्रकार का हो सकता है; जैसे–

- ट्विस्टेड पेयर केबल (Twisted pair cable)
- बेसबैंड कोएक्सिल केबल (Baseband coaxial cable)
- ब्रॉडबैंड कोएक्सिल केबल (Broadband coaxial cable)
- फाइबर ऑप्टिक केबल (Fiber optic cable)

इन सभी भौतिक माध्यमों के अपने गुण-दोष होते हैं।

वायर्ड ट्रांसमिशन का उपयोग ऐसे ट्रांसमिशन के लिए किया जाता है जहां प्रेषक (Sender) और प्राप्तकर्त्ता (Receiver) दोनों ही एक निश्चित स्थान पर स्थिर हों। ऐसी स्थिति में उनके बीच भौतिक तार या केबल डाल दिया जाता है, जिसका उपयोग दोनों ओर से कभी भी किया जा सकता है। इस प्रकार के ट्रांसमिशन में प्रेषक और प्राप्तकर्त्ता के बीच की दूरी कुछ मीटर से लेकर हजारों किलोमीटर तक हो सकती है। यदि भौतिक दूरी कम है तो उनके बीच ट्रांसमिशन के लिए विशेष तार या केबल डाले जा सकते हैं और यदि दूरी बहुत अधिक है तो ट्रांसमिशन के लिए पहले से उपलब्ध तारों; जैसे–टेलीफोन लाइनों का भी उपयोग किया जा सकता है। यह भी आवश्यक नहीं है कि प्रेषक और प्राप्तकर्त्ता के बीच का ट्रांसमिशन माध्यम सारा एक ही तरह का हो। आवश्यकाता के अनुसार यह कई भागों में बंटा हुआ हो सकता है और हर भाग अलग तरह का हो सकता है। लेकिन यह आवश्यक है कि उनको किसी भी प्रकार आपस में जोड़कर एक लगातार माध्यम का रूप दिया जाये, ताकि भेजा जाने वाला डाटा बिना किसी बाधा के प्राप्तकर्त्ता तक पहुंच जाये। इसके लिए कुछ अन्य उपकरणों; जैसे–मोडेम (Modems) का प्रयोग भी आवश्यकता के अनुसार किया जा सकता है।

(b) वायरलैस ट्रांसमिशन (Wireless Transmission)—इस प्रकार के ट्रांसमिशन में प्रेषक से प्राप्तकर्त्ता तक कोई सूचना भेजने के लिए किसी भौतिक माध्यम का प्रयोग नहीं किया जाता बल्कि आकाश का उपयोग किया जाता है। ऐसा करना तब आवश्यक हो जाता है जब प्रेषक (Sender) अथवा प्राप्तकर्त्ता (Receiver) अथवा दोनों स्थिर न हों अर्थात् चलायमान (Mobile) हों। मोबाइल होने के कारण उनका कोई स्थान निश्चित नहीं होता, इसलिए उनके बीच कोई भौतिक ट्रांसमिशन माध्यम डालना सम्भव नहीं होता। अतः वायरलैस ट्रांसमिशन का उपयोग किया जाता है। कभी-कभी ऐसे मामलों में भी वारलैस ट्रांसमिशन का उपयोग किया जाता है जहां भौतिक केबल डालना सम्भव नहीं होता या बहुत कठिन होता है; जैसे–पहाड़ों पर, घने जंगलों में, समुद्र में, बर्फीले क्षेत्रों में आदि।

वायरलैस ट्रांसमिशन में सूचना को विद्युतचुम्बकीय तरंगों (Electromagnetic waves) में बदलकर किसी एंटीना (Antena) द्वारा आकाश में छोड़ दिया जाता है। उन तरंगों को प्राप्तकर्त्ता के रिसीवर द्वारा पकड़ा जाता है और उसे मूल सूचना में बदल लिया जाता है।

Scanned by CamScanner

रेडियो और टेलिविजन द्वारा वायरलैस ट्रांसमिशन का ही उपयोग किया जाता है। कई बार आर्थिक दृष्टि से भी वारलैस ट्रांसमिशन वायर्ड ट्रांसमिशन की तुलना में बहुत सस्ता पड़ता है और यह सरल भी है, इसलिए आजकल धीरे-धीरे वायरलैस ट्रांसमिशन का उपयोग बढ़ता जा रहा है।

वायरलैस उपकरण निम्न दो प्रकार के सिग्नलों द्वारा सूचना का संप्रेषण करते हैं–

1. रेडियो फ्रीक्वेंसी वेव (Radio Frequency Waves) इस प्रकार की तरंगों की फ्रीक्वेंसी 1 से 20 गीगाहर्ट्ज (GHz) होती है। इनका उपयोग वायरलैस लोकल एरिया नेटवर्कों (Wireless LANs) द्वारा विभिन्न स्टेशनों के बीच डाटा के ट्रांसमिशन में किया जाता है।

2. इन्फ्रारेड वेव (Infrared Waves) इस प्रकार की तरंगों की तरंगदैर्ध्य या वेवलेंग्थ (Wevelength) 800 से 900 नैनोमीटर (nm) होती है। इनका उपयोग भी वायरलैस लैनों द्वारा किया जाता है। रेडियो फ्रीक्वेंसी वेव की तुलना में इसमें कई विशेषताएं और कमियां भी होती हैं। यह चलायमान इकाइयों (Mobile units) के लिए उपयुक्त नहीं है। ❑

प्रश्न 8 – कम्यूनिकेशन के दौरान कनेक्शन बनाने के लिये OSI मॉडल की विभिन्न लेयर सूचना का आदान-प्रदान कैसे करती हैं? उपयुर्क्त उदाहरण की सहायता से वर्णन कीजिये।

During the communication, how various layers of OSI model exchange information to establish a connection? Describe with the help of suitable diagram.

(Dec., 2012/Jan., 2013)

उत्तर–यह मॉडल इंटरनेशनल स्टैंडर्ड्स ऑर्गनाइजेशन (International Standards Organization या OSI) द्वारा विकसित किये गये एक प्रस्ताव तथा विभिन्न लेयरों (Layers) में प्रयोग किये जाने वाले प्रोटोकॉलों (Protocols) के मानकीकरण पर आधारित है। ओएसआई (OSI) का पूरा रूप "Open System Interconnection" है। इसका यह नाम इसलिए पड़ा है कि इसके द्वारा अन्य सिस्टमों से सम्पर्क के लिए खुले हुए सिस्टमों को आपस में जोड़ा जाता है। हम इसे संक्षेप में OSI मॉडल कहते है।

OSI मॉडल में सात लेयर हैं। लेयरों की यह संख्या अग्रलिखित सिद्धान्तों के अनुसार तय की गई थी–

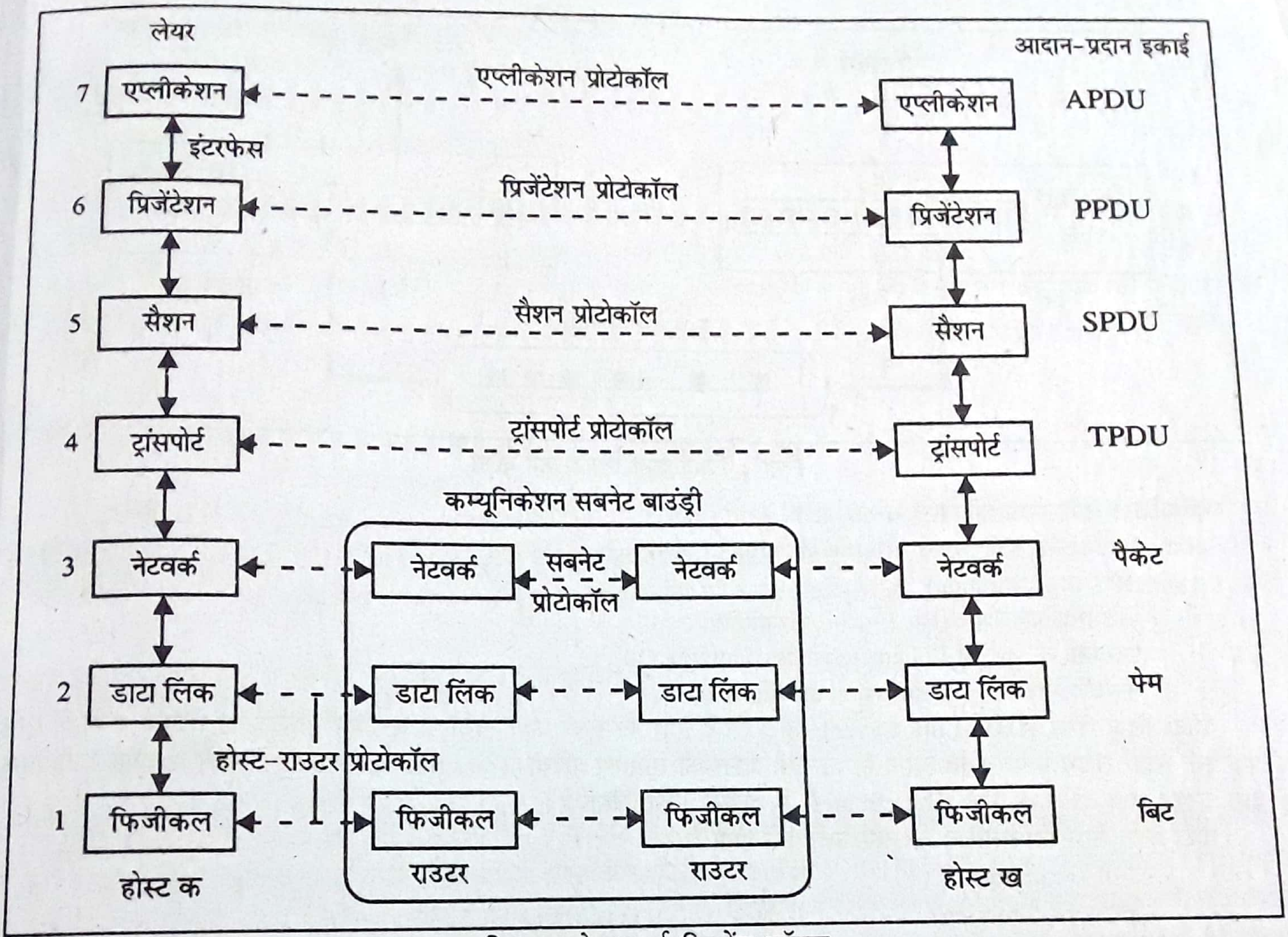
लेयर समूह	डाटा यूनिट	लेयर	कार्य (Functions)
होस्ट लेयर (Host Layers)	डाटा	7. एप्लीकेशन	एप्लीकेशन प्रोग्राम को नेटवर्क संसाधनों के उपयोग की सुविधा देना
		6. प्रिजेंटेशन	डाटा को प्रस्तुत, गूढ़लेखन (Encrypt) तथा कम्प्रैस करना
		5. सैशन	सैशन प्रारम्भ करना, प्रबंध करना और समापन करना
	सेगमेंट	4. ट्रांसपोर्ट	संदेशों को भेजने के लिए विश्वसनीय एंड-टू-एंड कनेक्शन बनाना
मीडिया लेयर (Media Layers)	पैकेट	3. नेटवर्क	पाथ तय करना, लॉजीकल पते बताना और पैकेट स्रोत से गंतव्य को भेजना
	फ्रेम	2. डाटा लिंक	फिजीकल पते बताना (MAC तथा LLC), बिटों को फ्रेम में बदलना
	बिट	1. फिजीकल	बिटों को किसी माध्यम पर भेजना और उसके लिए सभी विवरण बताना

सारणी : ओएसआई (OSI) मॉडल

OSI मॉडल के सभी लेयरों के कार्यों का सारांश उपर्युक्त सारणी में दिया गया है। निम्न चित्र में इस मॉडल की विस्तृत रूप रेखा दिखाई गई है। इसमें दो होस्ट क और ख माने गये हैं और उनके बीच पालन किये जाने वाले प्रोटोकॉलों का उल्लेख किया गया है।

यह बात ध्यान में रखना आवश्यक है कि OSI मॉडल स्वयं में कोई नेटवर्क आर्कीटैक्चर नहीं है, क्योंकि यह प्रत्येक लेयर में उपयोग किये जाने वाले प्रोटोकॉलों और सेवाओं को सही-सही परिभाषित नहीं करता। यह मॉडल केवल यह बताता है कि प्रत्येक लेयर में क्या-क्या कार्य किये जाने चाहिए। यद्यपि आईएसओ (ISO) ने प्रत्येक लेयर के लिए मानक निर्धारित किये हैं, फिर भी वे इस संदर्भ मॉडल के भाग नहीं हैं। वे सभी मानक अलग अन्तर्राष्ट्रीय मानकों (International standards) के रूप में प्रकाशित किये गये हैं।

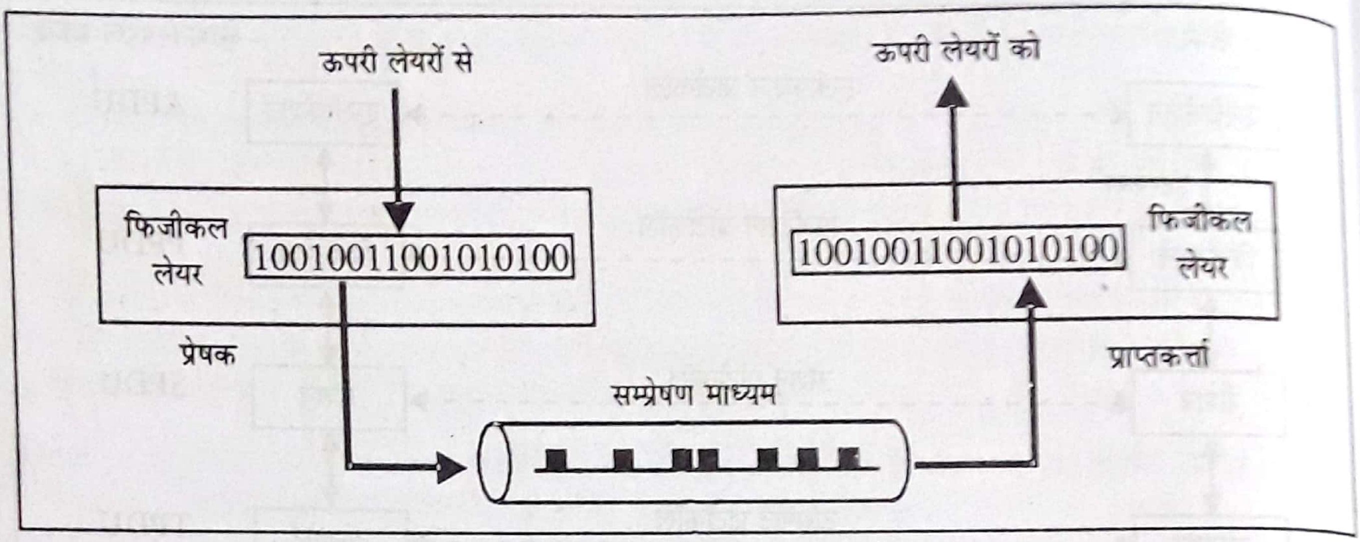
Scanned by CamScanner



चित्र : ओएसआई रिफरेंस मॉडल

फिजीकल लेयर (Physical Layer)—OSI मॉडल का सबसे पहला अर्थात् सबसे निचला लेयर फिजीकल लेयर है। यह लेयर प्रेषक (Sender) और प्राप्तकर्त्ता (Receiver) के बीच एक भौतिक सम्बंध (Physical connection) या बिट लिंक (Bit link) बनाने के कार्य के लिए उत्तरदायी है, जैसा कि निम्नांकित चित्र में दिखाया गया है। इस लेयर का मुख्य उद्देश्य यह सुनिश्चित करना है कि जब एक ओर से कोई 1 बिट भेजी जाती है, तो उसे दूसरी ओर 1 बिट के रूप में ही प्राप्त किया जाएगा, 0 बिट के रूप में नहीं। यहाँ ये साधारण प्रश्न उठते हैं कि कितने वोल्टेज को 1 बिट व्यक्त करने के लिए उपयोग किया जाएगा और कितने वोल्टेज को 0 बिट के लिए, कितने नैनोसेकंड तक किसी बिट को दिखाया जाएगा, क्या सम्प्रेषण दोनों दिशाओं में एक साथ होगा, प्रारम्भ में कनेक्शन किस प्रकार जोड़ा जाएगा और दोनों ओर से सम्प्रेषण समाप्त होने पर उसे किस तरह तोड़ा जाएगा, नेटवर्क कनेक्टर में कितनी पिनें (Pins) होंगी और प्रत्येक पिन का क्या उपयोग होगा आदि-आदि। ये सभी प्रश्न और उनके उत्तर इस लेयर के नीचे उपस्थित भौतिक सम्प्रेषण माध्यम (Physical transmission medium) और मैकेनिकल (Mecanical) तथा इलैक्ट्रीकल (Electrical) इंटरफेसों से सम्बंध रखते हैं।

Scanned by CamScanner



चित्र : फिजीकल लेयर का कार्य

फिजीकल लेयर निम्नलिखित से सम्वंध रखता है–

- बिटों को निरूपित करना (Representation of bits)
- डाटा रेट (Data Rate)
- बिट सिंक्रोनाइजेशन (Bit Synchronization)
- इटरकेसो के गुणधर्म (Characteristics of interface)
- सम्प्रेषण माध्यम (Transmission medium)

डाटा लिंक लेयर (Data Link Layer)–डाटा लिंक लेयर का मुख्य कार्य साधारण सम्प्रेषण सुविधा को नेटवर्क लेयर के लिए एक ऐसी संचार लाइन में परिवर्तित करना है, जो सभी प्रकार की सम्प्रेषण त्रुटियों (Transmission errors) से मुक्त हो। यह कार्य प्रेषक द्वारा इनपुट डाटा को डाटा फ्रेमों (Data frames) में तोड़कर किया जाता है।

डाटा लिंक लेयर निम्नलिखित के लिए उत्तरदायी होता है–

- फ्रेमिंग (Framing)
- एड्रेसिंग (Addressing)
- मीडियम एक्सैस कंट्रोल (Medium Access Control)
- फ्लो कंट्रोल (Flow Control)
- त्रुटि नियन्त्रण (Error Control)

नेटवर्क लेयर (Network Layer)–नेटवर्क लेयर नेटवर्क के एक भाग या सबनेट को नियंत्रित करता है। इसकी डिजायन बनाते समय मुख्य समस्या यह होती है कि पैकेटों को स्रोत (Source) से गंतव्य (Destination) तक किस रास्ते (Route) से भेजा जाये। यह रास्ता किसी निश्चित सारणी के आधार पर तय किया जाता है। यह रास्ता प्रत्येक वार्ता (Conversation) के शुरू होते समय भी तय किया जा सकता है। उदाहरण के लिए, किसी टर्मिनल से किसी दूरस्थ (Remote) कम्प्यूटर पर लॉगइन (Login) करना। किसी डायनामिक नेटवर्क में प्रत्येक पैकेट के लिए अलग रास्ता भी तय किया जा सकता है।

यदि किसी सबनेट में एक ही समय पर अनेक पैकेट भेजने के लिए उपस्थित हैं, तो वे एक दूसरे के रास्ते में आयेंगे, जिससे टकराव पैदा होगा। इस प्रकार की स्थितियों को नियंत्रित करना भी इस लेयर का कार्य है।

नेटवर्क लेयर निम्नलिखित कार्य के लिये जिम्मेदार होता हैं–

- लॉजीकल कनेक्शन बनाना (Creating a logical connection)
- निचले लेयरों के विवरण के छिपाना (Hiding details of the lower layers)
- एड्रेसिंग (Addressing)
- रूटिंग (Routing)

ट्रांसपोर्ट लेयर (Transport Layer)–ट्रांसपोर्ट लेयर का मौलिक कार्य ऊपरी लेयर अर्थात् सैशन लेयर से डाटा स्वीकार करना, आवश्यक होने पर उसे छोटे टुकड़ों या इकाइयों में तोड़ना, उनको नेटवर्क लेयर को भेजना तथा यह सुनिश्चित करना होता है कि सभी टुकड़े दूसरी ओर सही-सही प्राप्त हो चुके हैं। इससे भी महत्वपूर्ण बात यह है कि ये सभी कार्य बहुत दक्षता से किये जाने चाहिए, ताकि ऊपरी लेयरों को हार्डवेयर तकनीकों में होने वाले परिवर्तनों के प्रभावों से बचाये रखा जा सके।

Scanned by CamScanner

ट्रांसपोर्ट लेयर निम्नलिखित के लिये उत्तरदायित्व होता हैं–

- सर्विस-पॉवइंट एड्रेसिंग (Service Point addressing)
- सेगमेंटेशन (Segmentation)
- कनेक्शन कंट्रोल (Connection Control)
- फ्लो कंट्रोल (Flow Control)

सैशन लेयर (Session Layer)–सैशन लेयर में कम्प्यूटरों अर्थात् उनके उपयोगकर्त्ताओं के बीच कनेक्शन को नियंत्रित किया जाता है अर्थात् उनके बीच वार्ता के लिए सत्र (Session) तैयार किया जाता है। दोनों उपयोगकर्त्ताओं के कम्प्यूटर अलग-अलग प्रकार के हो सकते हैं। प्रत्येक सैशन में कई प्रकार की सेवाएँ हो सकती हैं, जैसे वार्ता पर नियंत्रण करना अर्थात् यह तय करना कि कब-कौन अपनी बात भेजेगा, टोकन प्रबंध (Token management) अर्थात् दोनों पक्षों को एक ही क्रिया एक साथ करने से रोकना, सिंक्रोनाइजेशन (Synchronization) अर्थात् लम्बे सम्प्रेषण में जहाँ से कनेक्शन टूटा था वहीं से आगे सम्प्रेषित करना आदि।

Session Layer निम्नलिखित कार्य के लिये उत्तरदायी होता है–

- हाफ या फुल, डुप्लैक्स सेवा (Half or Full-duplex Service)
- सिंक्रोनाइजेशन (Synchronization)

प्रिजेंटेशन लेयर (Presentation Layer)–प्रिजेंटेशन लेयर भेजी गयी सूचनाओं के व्याकरण (Syntax) और अर्थ (Semantics) से सम्बंध रखता है। भिन्न-भिन्न डाटा प्रस्तुतीकरण वाले कम्प्यूटरों के बीच संचार को सम्भव बनाने के लिए उनकी डाटा संरचनाओं को एक निश्चित सारांश रूप (Abstract form) में परिभाषित किया जाता है, ताकि उनका आदान-प्रदान या विनिमय (Exchange) किया जा सके।

प्रिजेंटेशन लेयर निम्नलिखित के लिये विशेष उत्तरदायी होता हैं–

- अनुवाद (Translation)
- गूढलेखन (Encryption)
- संकुचन (Compression)

एप्लीकेशन लेयर (Application Layer)–एप्लीकेशन लेयर उपयोगकर्त्ता के सबसे निकट होता है। इस लेयर में कई प्रकार के प्रोटोकॉल होते हैं, जिनकी आवश्यकता उपयोगकर्त्ताओं को होती है, जैसे टेलनेट (Telnet), हाइपरटैक्स्ट ट्रांसफर प्रोटोकॉल (HTTP), फाइल ट्रांसफर प्रोटोकॉल (FTP), सिम्पल मेल ट्रांसफर प्रोटोकॉल (SMTP) आदि। उदाहरण के लिए, जब कोई उपयोगकर्त्ता या ब्राउजर (Browser) किसी वेब पेज को खोलना चाहता है, तो वह उसका नाम अपने सर्वर को HTTP का प्रयोग करके भेजता है और सर्वर उसे वह बेव पेज भेज देता है। इस प्रकार एप्लीकेशन लेयर में विभिन्न सॉफ्टवेयर एप्लीकेशनों के साथ सीधे संवाद (Interact) किया जाता है।

एप्लीकेशन लेयर की सेवायें निम्नलिखित हैं–

- इलैक्ट्रॉनिक मेल (Electronic Mail)
- रिमोट फाइल एक्सैस और ट्रांसफर (Remote File Access and Transfer)
- शेयर्ड डाटाबेस मैनेजमेंट (Shared Database Management) ❑

प्रश्न 9 – Multiplexing/Multiplexer से आप क्या समझते हैं? विस्तार में वर्णन करें।

What do you understand by multiplexing/multiplexer? Explain in detail.

अथवा (Or)

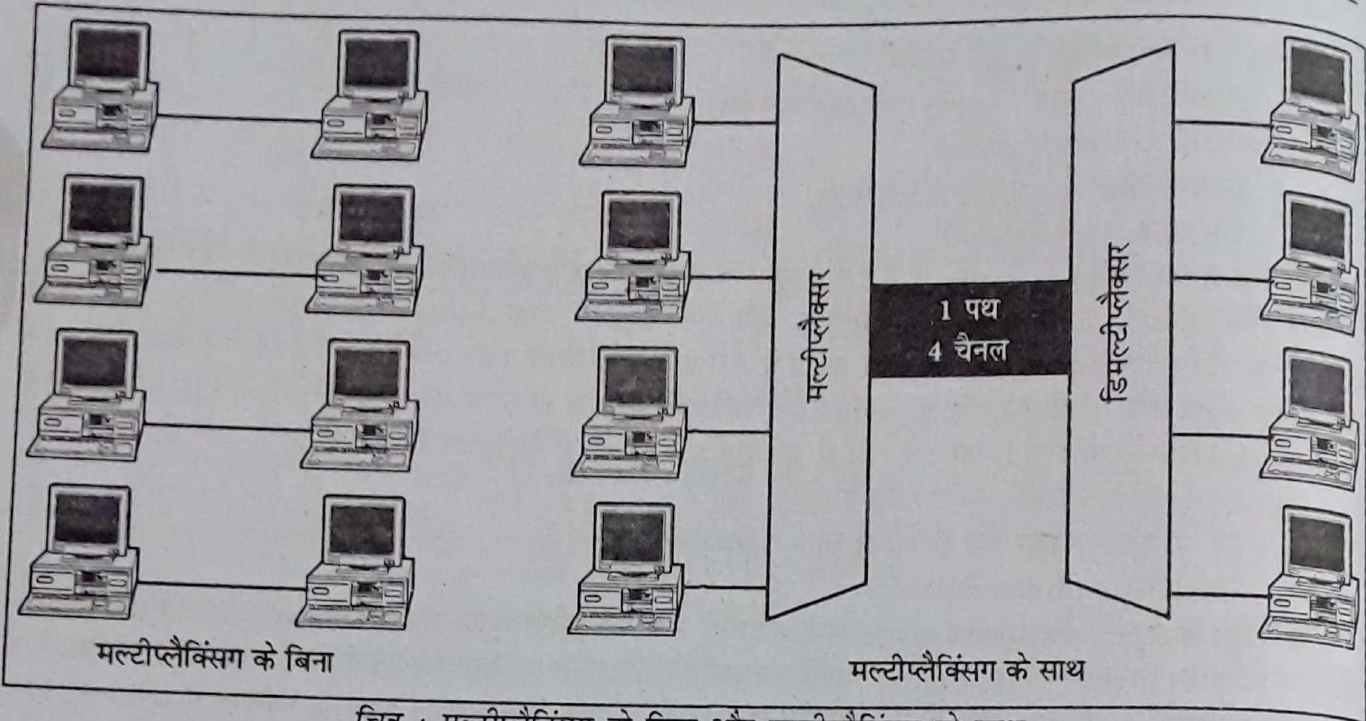
Multiplexing में FDM और TDM से आप क्या समझते हैं? बताइयें।

What do you understand by FDM and TDM in multiplexing? Explain.

उत्तर–मल्टीप्लैक्सिंग (Multiplexing)–मल्टीप्लैक्सिंग का तात्पर्य किसी सम्पर्क या लिंक (Link) की उपलब्ध बैंडविड्थ (Bandwidth) को कई उपयोगकर्त्ताओं में बाँटना होता है। इसे किसी लिंक को कई चैनलों में बाँटने के रूप में समझा जा सकता है।

उदाहरण के लिए, मान लीजिए कि दो-दो कम्प्यूटरों के चार जोड़े (Pairs) हैं। यदि हम प्रत्येक जोड़े के लिए अलग लिंक का उपयोग करते हैं, तो हमें चार लिंकों की आवश्यकता होगी। यदि किसी लिंक की कुल बैंडविड्थ का उपयोग नहीं किया जा रहा है, तो उसका एक भाग बेकार जा रहा है। ऐसी स्थिति में हम एक ही लिंक को मल्टीप्लैक्सिंग द्वारा चारों जोड़ों के बीच कार्य करने योग्य बना सकते हैं। इसका अर्थ है कि एक ही लिंक की बैंडविड्थ का चारों जोड़ों द्वारा साझा किया जाएगा। इसे निम्न चित्र में दिखाया गया है–

Scanned by CamScanner

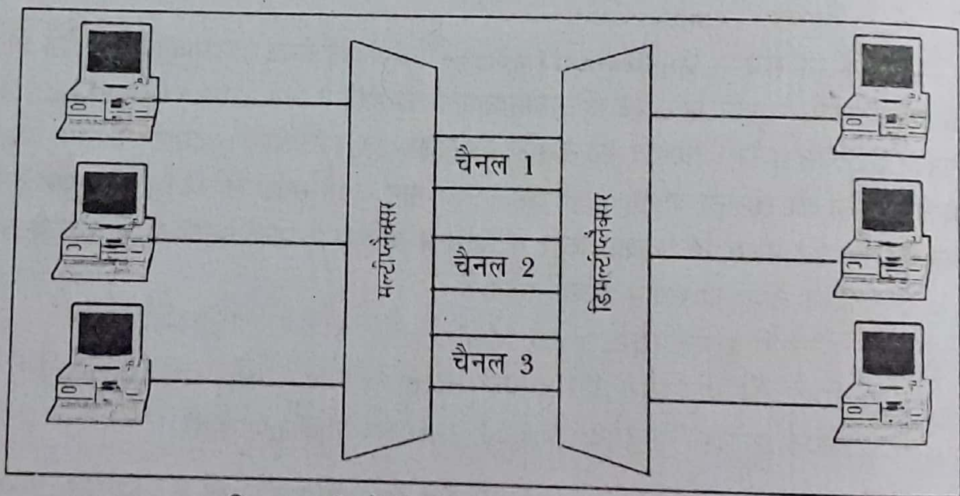


चित्र : मल्टीप्लैक्सिंग के बिना और मल्टीप्लैक्सिंग के साथ

मल्टीप्लैक्सिंग की दो प्रमुख तकनीकें होती हैं–

1. फ्रीक्वेंसी-डिवीजन मल्टीप्लैक्सिंग (Frequency Division Multiplexing)
2. टाइम-डिवीजन मल्टीप्लैक्सिंग (Time Division Multiplexing)

1. फ्रीक्वेंसी-डिवीजन मल्टीप्लैक्सिंग (Frequency Division Multiplexing)–फ्रीक्वेंसी-डिवीजन मल्टीप्लैक्सिंग (FDM) एक ऐसी एनालॉग तकनीक है, जिसका उपयोग तब किया जा सकता है, जब किसी लिंक की बैंडविड्थ (हर्ट्ज में) उसमें होकर ट्रांसमिट किये जाने वाले सिग्नलों की संयुक्त बैंडविड्थ से अधिक होती है। FDM में प्रत्येक प्रेषक उपकरण द्वारा उत्पन्न किये जाने वाले सिग्नल विभिन्न कैरियर बारम्बारताओं (Carrier frequencies) को मॉडुलेट करते हैं। मॉडुलेट किये गये इन सिग्नलों को मिलाकर एक अकेले संयुक्त सिग्नल (Composite signal) में बदल दिया जाता है, जिसे उस लिंक में होकर ट्रांसमिट किया जा सकता है। मॉडुलेट किये गये सिग्नलों को स्थान देने के लिए कैरियर बारम्बारताओं को पर्याप्त बैंडविड्थ द्वारा अलग-अलग किया जाता है। सिग्नलों को एक-दूसरे से टकराने अर्थात् ओवरलैप (Overlap) होने से बचाने के लिए उपयोग न की जाने वाली बैंडविड्थ (Unused bandwidth) पट्टियों, जिन्हें गार्ड बैंड (Guard Bands) कहा जाता है, द्वारा अलग-अलग किया जाता है।



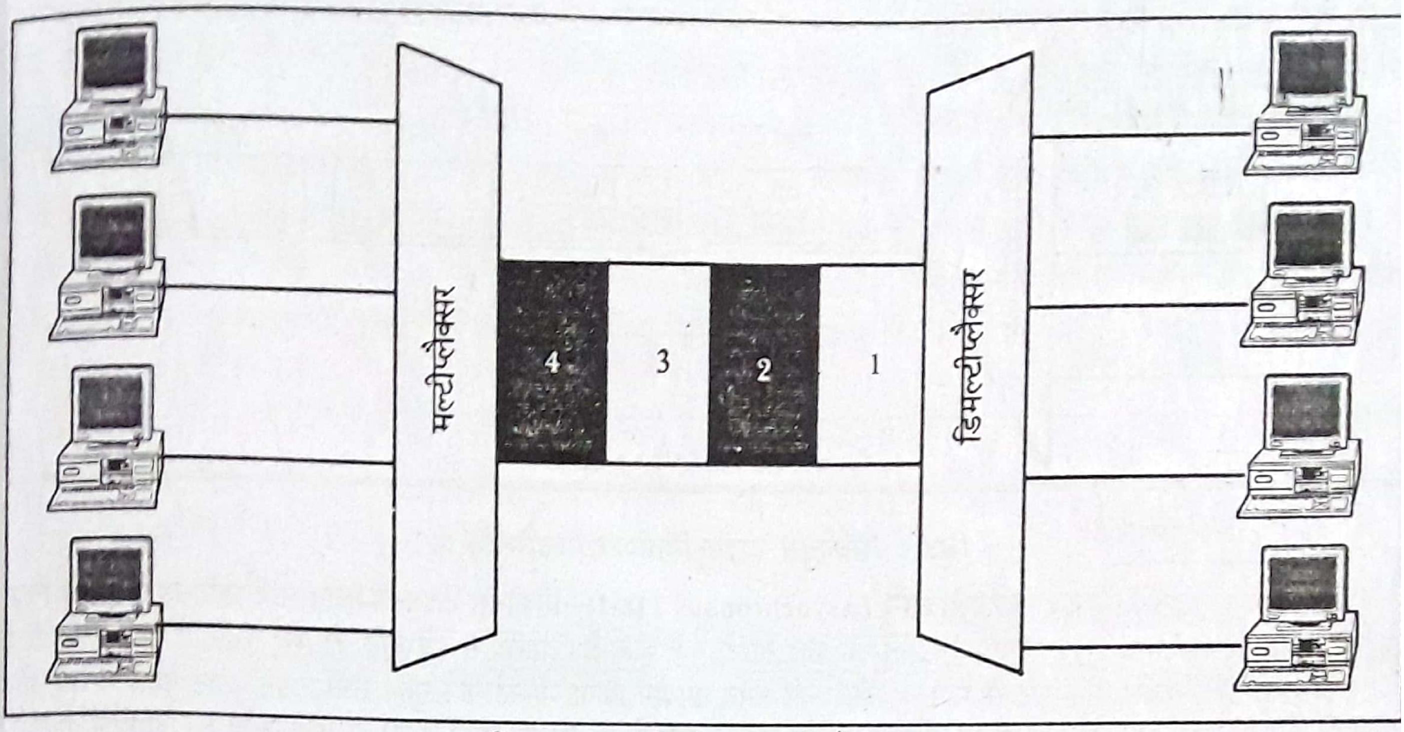
चित्र : फ्रीक्वेंसी-डिवीजन मल्टीप्लैक्सिंग

संलग्न चित्र में फ्रीक्वेंसी डिवीजन मल्टीप्लैक्सिंग के विचार की रूपरेखा दी गयी है। इसमें ट्रांसमिशन पाथ को तीन भागों में बाँटा गया है, जिनमें से प्रत्येक भाग एक चैनल की तरह सिग्नलों के सम्प्रेषण (Transmission) का कार्य करता है।

2. टाइम-डिवीजन मल्टीप्लैक्सिंग (Time Division Multiplexing)–टाइम-डिवीजन मल्टीप्लैक्सिंग (TDM) एक ऐसी डिजिटल प्रक्रिया या तकनीक है, जिसका उपयोग तब किया जा सकता है, जब किसी लिंक की बैंडविड्थ (बिट प्रति सेकंड में) प्रेषक (Sending) और प्राप्तकर्त्ता (Receiver) द्वारा आवश्यक बैंडविड्थ से अधिक होती है।

निम्न चित्र में टाइम-डिवीजन मल्टीप्लैक्सिंग के विचार की रूपरेखा दी गयी है। इसमें लिंक वही है जो फ्रीक्वेंसी-डिवीजन मल्टीप्लैक्सिंग में प्रयोग किया जाता है, लेकिन इसे फ्रीक्वेंसी के बजाय समय के अनुसार कई क्रमानुसार भागों में बाँटा गया है, जिनमें से प्रत्येक भाग किसी एक सिग्नल के एक अंश का सम्प्रेषण (Transmission) करता है।

Scanned by CamScanner



चित्र : टाइम-डिवीजन मल्टीप्लैक्सिंग

प्रश्न 10 – TDM का उपयोग किस प्रकार से किया जाता है? बताइये।

How to use of TDM? Explain.

अथवा (Or)

सिंक्रोनस TDM और असिंक्रोनस TDM से आप क्या समझते हैं? बताइयें।

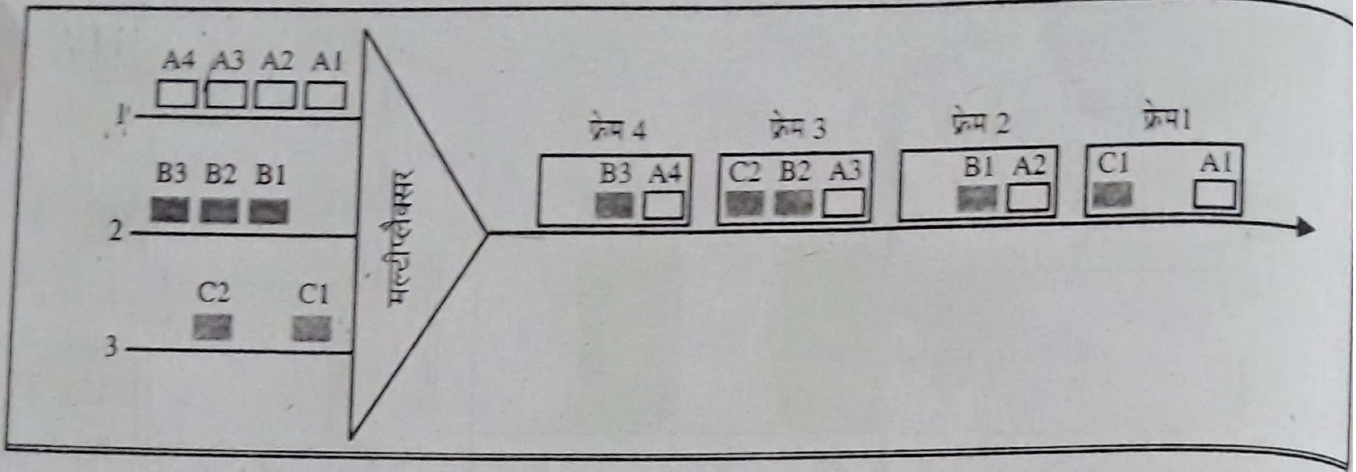
What do you understand by synchronous TDM and Asynchronous TDM? Explain.

उत्तर–टाइम-डिवीजन मल्टीप्लैक्सिंग का उपयोग दो प्रकार से किया जा सकता है–सिंक्रोनस टाइम-डिवीजन मल्टीप्लैक्सिंग (Synchronous TDM) और असिंक्रोनस टाइम-डिवीजन मल्टीप्लैक्सिंग (Asynchronous TDM)।

सिंक्रोनस टाइम-डिवीजन मल्टीप्लैक्सिंग (Synchronous TDM)–टाइम-डिवीजन मल्टीप्लैक्सिंग में सिंक्रोनस का अर्थ है कि मल्टीप्लैक्सर (Multiplexer) प्रत्येक उपकरण को हर बार समान कालावधि या टाइम स्लॉट (Time slot) आवंटित करता है, भले ही उस उपकरण के पास सम्प्रेषण करने के लिए कुछ भी न हो। इसका अर्थ है कि कोई टाइम स्लॉट A, उपकरण A के उपयोग के लिए ही रहेगा, कोई दूसरा उपकरण उस टाइम स्लॉट का उपयोग नहीं कर सकता। इस स्थिति में हर बार जब भी किसी उपकरण का टाइम स्लॉट आता है, तो उस उपकरण के पास अपने डाटा के एक भाग को प्रेषित करने का अवसर होता है। यदि उपकरण कुछ भी प्रेषित करने में असफल रहता है या उसके पास भेजने के लिए कोई डाटा नहीं होता, तो वह टाइम स्लॉट खाली रहता है।

इसमें टाइम स्लॉटों को फ्रेमों में समूहबद्ध किया जाता है। कोई फ्रेम (Frame) टाइम स्लॉटों के एक पूर्ण चक्र (Complete cycle) के बराबर होता है, जिसमें प्रत्येक प्रेषक उपकरण के लिए एक या अधिक टाइम स्लॉट होता है। इसे अग्र चित्र में दिखाया गया है। यदि किसी सिस्टम में n इनपुट लाइनें हैं, तो प्रत्येक फ्रेम में कम से कम n टाइम स्लॉट होंगे, जिनमें से प्रत्येक स्लॉट एक विशेष इनपुट लाइन का डाटा ले जाने के लिए आवंटित होगा। वह स्लॉट खाली भी रह सकता है।

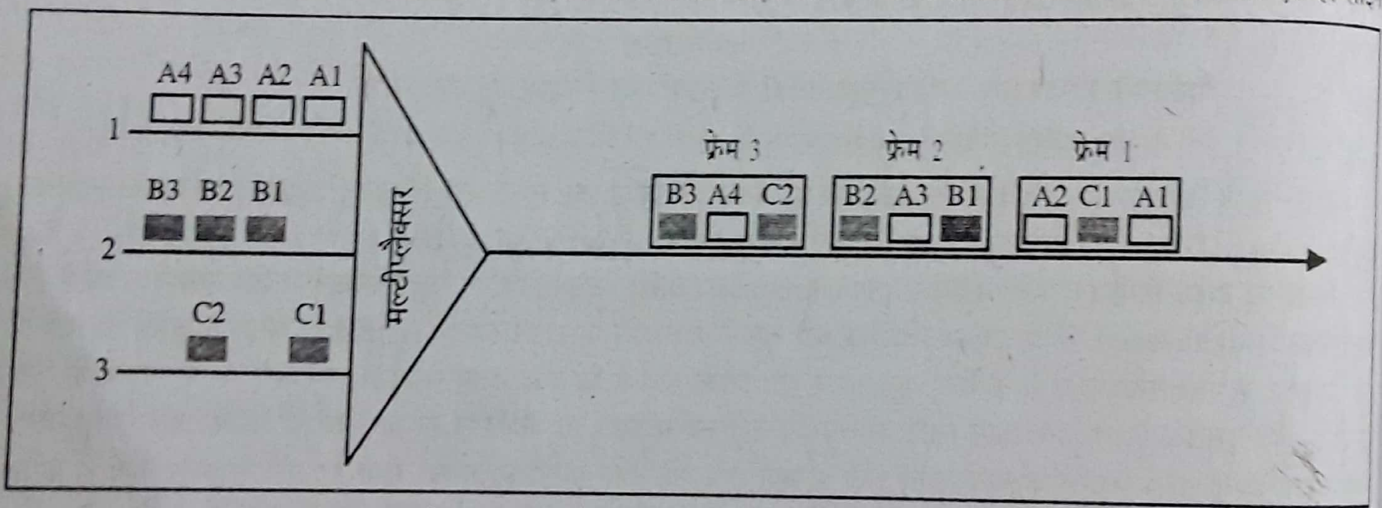
Scanned by CamScanner



चित्र : सिंक्रोनस टाइम-डिवीजन मल्टीप्लैक्सिंग

असिंक्रोनस टाइम-डिवीजन मल्टीप्लैक्सिंग (Asynchronous TDM)—सिंक्रोनस टाइम-डिवीजन मल्टीप्लैक्सिंग से किसी लिंक की पूर्ण क्षमता (Full capacity) का उपयोग होने की कोई गारंटी नहीं होता है। वास्तव में इस बात की पूरी संभावना होती है कि दिये गये टाइम स्लॉटों के केवल एक छोटे से भाग का ही किसी समय उपयोग किया जा रहा है। चूँकि सभी टाइम स्लॉट पहले से तय और आवंटित हैं, अतः यदि कोई उपकरण अपने टाइम स्लॉट का उपयोग नहीं करता, तो वह समय बेकार ही चला जाता है। उदाहरण के लिए यदि हम एक ही लाइन पर 20 कम्प्यूटरों के आउटपुट को मल्टीप्लैक्स करते हैं और एक समय में केवल 10 कम्प्यूटर ही चालू रहते हैं तो लगभग आधा समय हमेशा बेकार होता रहेगा अर्थात् उस लाइन की आधी क्षमता व्यर्थ जायेगी।

इस प्रकार की बरबादी को रोकने के लिए असिंक्रोनस टाइम-डिवीजन मल्टीप्लैक्सिंग अथवा सांख्यिकीय टाइम-डिवीजन मल्टीप्लैक्सिंग (Statistical TDM) की डिजायन बनायी गयी है। इसमें भी सिंक्रोनस टाइम-डिवीजन मल्टीप्लैक्सिंग की तरह उच्च-गति की एक ही लाइन



चित्र : असिंक्रोनस टाइम-डिवीजन मल्टीप्लैक्सिंग

पर कम गति की अनेक इनपुट लाइनों की मल्टीप्लैक्सिंग की जाती है, लेकिन उसके विपरीत इसमें इनपुट लाइनों की कुल गति (Total speed) पाथ की क्षमता से अधिक हो सकती है। सिंक्रोनस TDM में यदि n इनपुट लाइनें हैं, तो एक फ्रेम में कम से कम n ही टाइम स्लॉट होंगे, जबकि असिंक्रोनस TDM में यदि n इनपुट लाइनें हैं, तो प्रत्येक फ्रेम में टाइम स्लॉटों की संख्या m से अधिक नहीं होगी, जहाँ m का मान n से कम होगा। इस प्रकार से असिंक्रोनस TDM में सिंक्रोनस जितनी ही इनपुट लाइनों का कार्य कम क्षमता की लिंक लाइन से किया जा सकता है। इसका तात्पर्य यह भी है कि इसमें हम उसी क्षमता की लिंक लाइन से अधिक इनपुट लाइनों का कार्य कर सकते हैं। □

प्रश्न 11 — Data Communication में Modulation की उपयोगिता लिखिए। ये कितने प्रकार के होते हैं? प्रत्येक को विस्तार से समझाइये।

Write utility of modulation in data communication. Write types of modulation and explain each in detail.

Scanned by CamScanner

उत्तर–Modulation in Data Communication–Data को एक स्थान से दूसरे स्थान पर भेजने की प्रक्रिया को Data Communication कहते हैं; जैसे–हम इंटरनेट पर अपने सिस्टम से किसी फाइल या Text मैसेज को किसी दूसरे सिस्टम पर भेजते हैं, इसे Data Communication कहते हैं। हमारे सिस्टम में डाटा डिजिटल रूप में होता है; जबकि इसका ट्रांसमीशन एनालॉग (Analog) रूप में किया जाता है, तो Data को एक फॉर्मेट से दूसरे फॉर्मेट में रूपान्तरित करने की आवश्यकता होती है, इसे Modulation कहते हैं; जैसे–जब हम इंटरनेट के माध्यम से एक सिस्टम से दूसरे सिस्टम में किसी मैसेज को send करते हैं तो यह मैसेज डिजिटल रूप में होता है, जबकि इसका ट्रांसमीशन Analog रूप में होता है तो इसके लिये हम अपने सिस्टम में Modem का प्रयोग करते हैं। यह Modem source data Analog format में बदलता है तथा destination end पर पुनः digital format में बदलता है। जैसा कि निम्नांकित Fig. से स्पष्ट है–

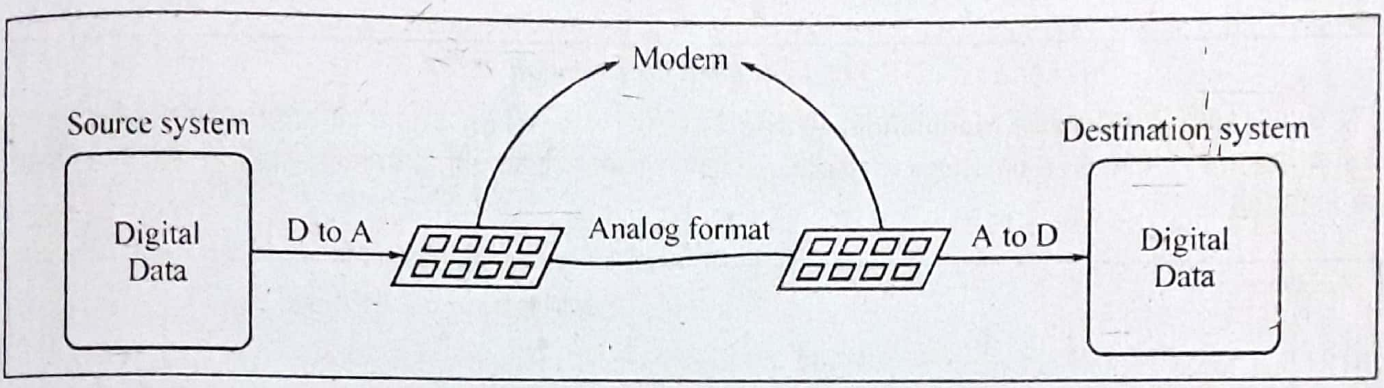


Fig. : Modulation Process

Modulation सामान्यतः तीन प्रकार का होता है–

1. Amplitude Modulation
2. Frequency Modulation
3. Phase Modulation

1. एम्प्लीट्यूड मॉड्यूलेशन (Amplitude Modulation-AM)–किसी Signal dk Amplitude किसी बिन्दु पर मान टंसनम होता है। इसको हम दूसरे शब्दों में इस प्रकार परिभाषित कर सकते हैं कि तरंग के किसी बिन्दु से क्षैतिज अक्ष तक की ऊधर्वाधर दूरी को Amplitude कहते हैं। सिग्नल के प्रकार के आधार पर Amplitude को वोल्ट एम्पीयर या वाट में मापा जाता है।

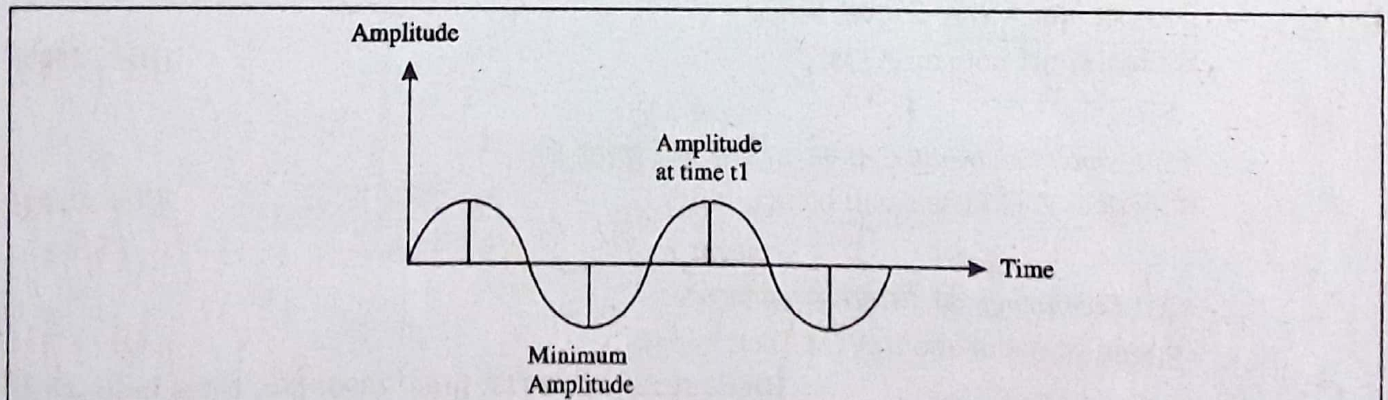


Fig. : Amplitude Modulation

ध्वनि के लिए प्रयुक्त सिग्नल में इसी प्रकार की तकनीकी का प्रयोग किया जाता है।

2. फ्रीक्वेंसी मॉड्यूलेशन (Frequency Modulation-FM)–Frequency से तात्पर्य एक सेकेण्ड में पूरे हुए पीरियडों से है। किसी सिग्नल की Frequency को हम No. of Cycles/Sec. के रूप में व्यक्त करते हैं।

दूसरे शब्दों में इस मॉड्यूलेशन में डिजिटल आंकड़ों को भिन्न आवृत्तियों (Frequencies) में व्यक्त किया जाता है। इस सिग्नल में Amplitude एवम् Phase को स्थिर रखा जाता है। इस प्रकार के सिग्नल निर्माण में सरल एवं कोलाहलयुक्त ध्वनियों से कम प्रभावित होने वाले होते हैं।

Scanned by CamScanner

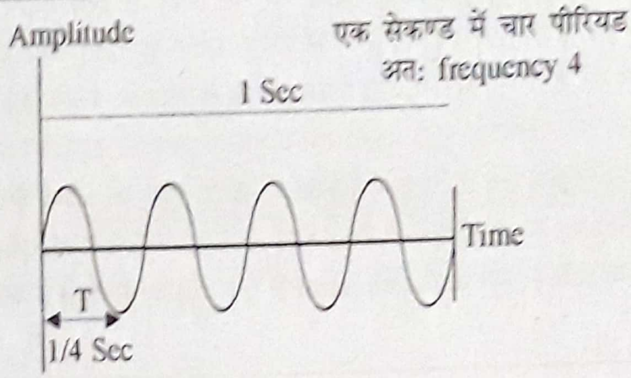


Fig. : Frequency Modulation

3. **फेज मॉड्यूलेशन (Phase Modulation)**—Phase किसी तरंग (Wave Form) के समय को सापेक्ष स्थिति में दर्शाती है। इसे डिग्री या Radian में मापते हैं। (360 degree = π Radian)। यदि हम किसी तरंग को बायें या दायें खिसकाते हैं तो Phase उस Shift को बताता है।

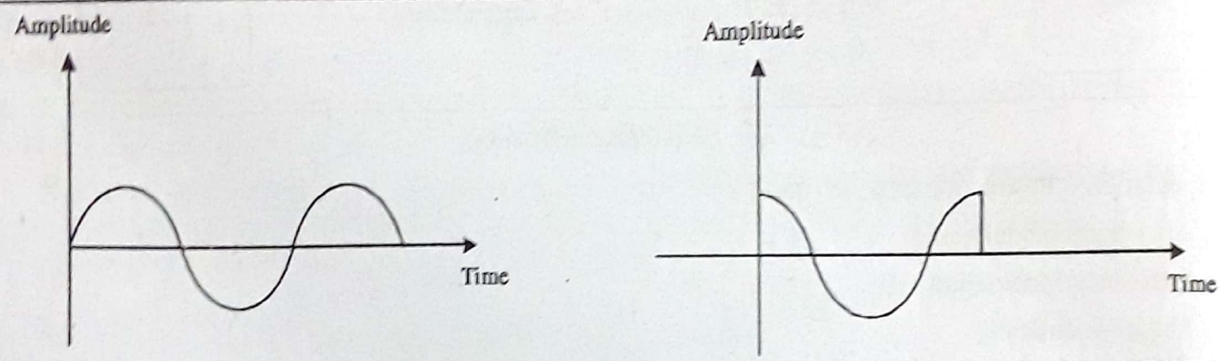


Fig. : Phase Modulation

❑

प्रश्न 12 – *ATM पर एक संक्षिप्त टिप्पणी लिखिये।*

Write a short note on ATM. **(Dec., 2008)**

अथवा (Or)

ATM, small bandwidth Cell का उपयोग क्यों करता है?

Why does ATM use small band width? **(Jan., 2005)**

अथवा (Or)

ATM Technology को विस्तार से समझाइये।

Explain in detail about ATM Technology.

(Dec., 2012/Jan., 2013; June, 2005; Jan, 2004; June, 2003)

उत्तर–ATM–ATM को विस्तृत रूप से Asynchronous Transmission Mode कहते हैं। ATM एक कनेक्शन ओरियेन्टेड प्रोटोकॉल है जो या तो PVCs (Permanent Virtual Circuits) या SVCs (Switched Virtual Circutis) के साथ कार्य कर सकता है। ATM नेटवर्क अधिकतम Bandwidth का प्रयोग करता है जबकि यह QOS (Quality Of Service) को Maintain करता है।

ATM के दो प्रमुख निम्नलिखित फायदे हैं–

(a) उच्च ट्रांसमीशन स्पीड (High Transmission Speed)

(b) Flexible bandwidth-on-demand Capability

ATM डिवाइसेस, Fixed Speeds पर इनफॉरमेशन को Send तथा रिसीव नहीं करती हैं लेकिन हार्डवेयर तथा इनफॉरमेशन फ्लो रिलायेबिलिटी पर आधारित ट्रांसमीशन स्पीड को गतिशील समायोजित करती हैं।

Scanned by CamScanner

ATM, पैकेजिंग इनफॉरमेशन के लिये Fixed-size Cells का प्रयोग करता है। Cells के Fixed-size की वजह से ATM कनेक्शनूस, पूर्वअनुमानित हैं तथा आसानी से मैनेज हो सकते हैं।

ATM टैक्नोलॉजी OSI रेफरेन्स मॉडल के डाटा लिंक लेयर पर कार्य करती है।

ATM, WAN पर VCs (Virtual Channels) तथा VPs (Virtual Paths) का प्रयोग करके डिवाइसेस को कनेक्ट करती है।

Virtual Channels, रिमोट स्टेशनों के मध्य डाटा को ट्रांसमिट करने के लिये एक या अधिक फिजीकल ATM Links की एक श्रेणी से मिलकर बनी होती है। एक दिये गये ATM ट्रांसमीशन में सभी Cells, एकजैसे VC को Fallow करते हैं जो भरोसेमंद डाटा ट्रांसमीशन को सुनिश्चित करता है।

Virtual Channel केवल उतनी देर के लिये Exist करता है जितनी देर तक इस पर डाटा ट्रांसमिट होता है।

Virtual Path, VCs (Virtual Circuits) का कलेक्शन है जो Same Source तथा Destination Points को रखता है। VP को दिये गये Destination सभी Traffic के ग्रुप को प्रयोग कर सकता है तथा इसे VP पर भेजता है। ATM Cells, 53 bytes Size के होते हैं जिसमें 48 bytes का Payload डाटा तथा 5 bytes का कंट्रोल और Routing इनफॉरमेशन है। Payload Fields उस डाटा को रखता है जिसमें साधारण Text, Images Voice या Video डाटा होता है।

ATM, डायनामिकली Bandwidth को एलोकेट करता है। ❑

प्रश्न 13 – *एटी०एम० लेयर के नाम और उनके फंक्शन बताओ।*

Name the ATM layers and their functions.

उत्तर–ATM Layer–ATM Asynchronous Transfer Mode है। यह एक Cell Relay प्रोटोकॉल है, जिसको ATM फोरम द्वारा 1990 के बाद के दशक के प्रारम्भ में डिजायन किया गया था। मूल रूप में यह तकनीकी Wide Area Networks के लिये डिजायन की गयी थी, परन्तु आजकल इसका उपयोग WAN तथा LAN दोनों के लिये किया जाता है। इसकी विशेषता यह है कि यह उच्च गति वाले सम्प्रेषण माध्यम की क्षमताओं का अधिकतम उपयोग करता है। दूसरी ओर सभी प्रकार के विद्यमान नेटवर्कों के साथ इंटरफेण्स भी उपलब्ध कराता है। इसको डिजायन करने वालों की एक महत्वाकांक्षा यह भी थी कि सभी प्रकार की नेटवर्किंग आवश्यकताओं या तत्वों; जैसे–ध्वनि, डाटा, Cable टेलीविजन, टेलेक्स, टेलीग्राम आदि को एक ही नेटवर्क से पूरा करना सम्भव हो। इसका उपयोग मुख्यतः टेलीफोन सिस्टमों द्वारा अपने आंतरिक यातायात के लिये किया जाता है।

ATM के फिजीकल स्ट्रक्चर को निम्न Fig. में प्रदर्शित किया गया है–

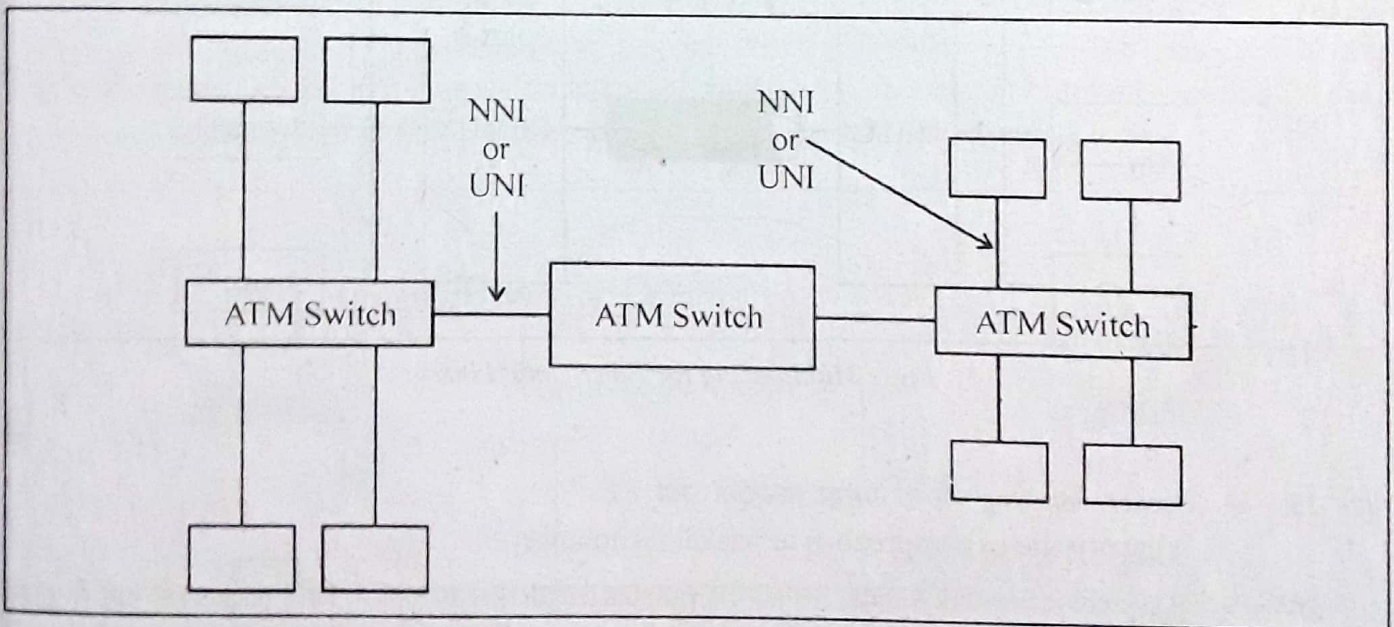


Fig. : ATM Physical Structure

ATM तथा पैकट प्रोटोकॉल्स के मध्य एक प्रोटोकॉल लेयर होती है, जिसे ATM Adaptation Layer (AAL) कहते हैं। AAL (ATM Adaptation Layer) header आवश्यक इनफॉरमेशन को रखता है, जो ऑरिजनल पैकट में Cells से सम्बन्धित है। AAL में Pass किये गये पैकट के साथ header तथा trailer भी जुड़ा होता है।

Packet header में निम्नलिखित Fields होते हैं–

(a) 8 bit Common Part Indicator (CPI)

Scanned by CamScanner

(b) 8 bit Beginning tag (B tag)

(c) 16 bit Buffer Allocation size (BA size)

Packet trailer में निम्नलिखित Fields होते हैं–

(a) Pad Field

(b) 8 bit End tag (E tag)

(c) 16 bit Len

प्रश्न 14 – *Fiber optic link में किस तरह की multiplexing तकनीकि उपयोग की जाती है और क्यों?*

Which type of multiplexing tecchnique is common or applicable for fiber optic link? Explain the reason.

उत्तर–Fiber optic communication, optical fiber के माध्यम से light की pulses के द्वारा एक स्थान से दूसरे स्थान पर Information को ट्रांसमिट करने का एक मैथड् है। इसमें light, electromagnetic carrier wave के रूप में होती है, जो information को carry करने के लिये modulate की जाती है। Multiplexing एक मैथड है, जिसके द्वारा multiple analogue मैसेज signals व digital data streams को एक signal में combine करके एक medium में शेयर किया जाता है। Fiber optic link में frequency division multiplexing (FDM) तकनीकि का प्रयोग किया जाता है। इस तकनीकि में several signals को एक medium में combine करके, single medium में ट्रांसमिट किया जाता है। इस Type की multiplexing के प्रयोग करने से कई सारे signals (channels) को एक साथ ट्रांसमिट किया जा सकता है। इसमें proper operation के लिये transmitter तथा receiver के बीच में synchronization की जरूरत नहीं होती है। इस type की multiplexing के प्रयोग करने से demodulation आसान होता है। इसमें main channel के साथ प्रत्येक signal को भिन्न-भिन्न frequency assign की जाती है। निम्नलिखित Fig. में fiber optic link के लिये multiplexing को चित्रित किया गया है–

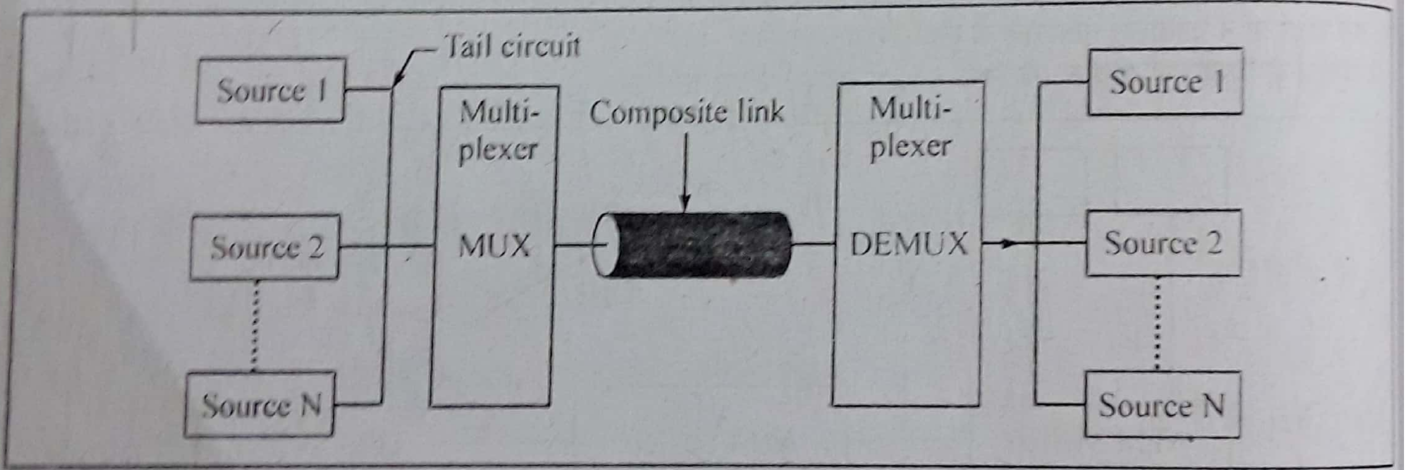


Fig. : Multiplexing for Fiber Optic Link

प्रश्न 15 – *Packet switching की दो प्रमुख तकनीकें क्या हैं?*

What are the two approahes to packet switching?

उत्तर–Packet switching network में data, अलग-अलग variable length में भेजा जाता है, जिन्हें packets के नाम से पुकारा जाता है। Packet, डाटा तथा Control information को रखता है। Packet switched network, किसी एक होस्ट से दूसरे होस्ट के तरह बिना reserve circuit के भेजने के लिये अनुमति प्रदान करता है।

Source तथा destination के बीच में एक path सलेक्ट हो जाता है। जब भी sender, डाटा को sent करता है तो डाटा packets में convert हो जाता है तथा अगले कम्प्यूटर या router के पास forward हो जाता है। Router इस पैकेट को तब तक स्टोर करता है जब तक कि output line free नहीं हो जाती है। इसके पश्चात् यह packet अगले कम्प्यूटर या router के पास transfer हो जाता है। packet का route, network layer protocols के द्वारा निर्धारित होता है।

Scanned by CamScanner

Packet switching की निम्नलिखित दो techniques हैं–

(i) Virtual Circuit Packet Switching

(ii) Datagram Packet Switching

(i) Virtual Circuit Packet Switching–Virtual Circuit packet switching में sender तथा receiver के बीच में single route को चुना जाता है तथा सभी packets को इस route के माध्यम से भेजा जाता है। प्रत्येक packet virtual circuit number को रखता है। वास्तविक ट्रांसमिशन से पहले virtual circuit की कॉल सेटअप की जरूरत होती है। निम्नलिखित Fig. में virtual circuit packet switching के data transfer phase को चित्रित किया गया है–

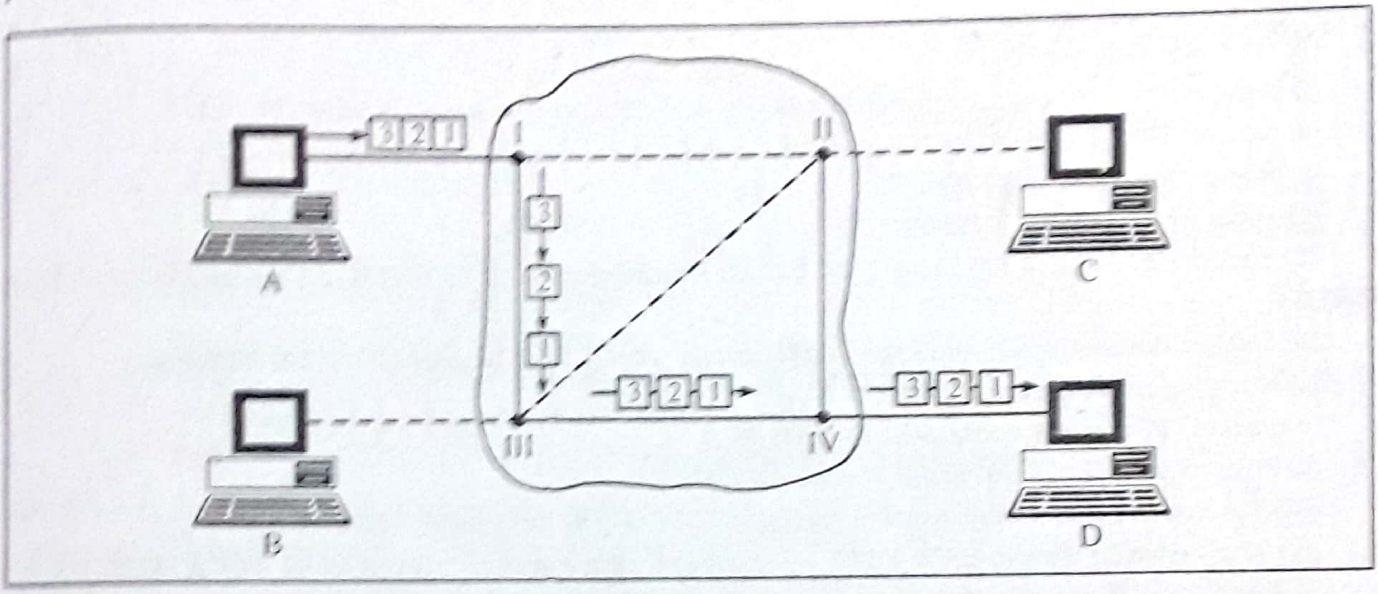


Fig. : Phases in Virtual circuit packet switching

(ii) Datagram Packet Switching–Datagram packet switching में प्रत्येक packet को दूसरे packets के पास बिना किसी regard के ट्रांसमिट किया जाता है। प्रत्येक packet, source तथा destination के पूर्ण information को रखता है। प्रत्येक packet को individual तथा independent transmission की तरह treat किया जाता है। इस तकनीकि में packets को datagrams के नाम से पुकारा जाता है। Datagram switching नेटवर्क लेयर पर होती है। निम्नलिखित Fig. में दर्शाया गया है कि कैसे 4 packets को A station से D station पर डिलीवर करने के लिये datagram switching तकनीकि का प्रयोग किया जाता है–

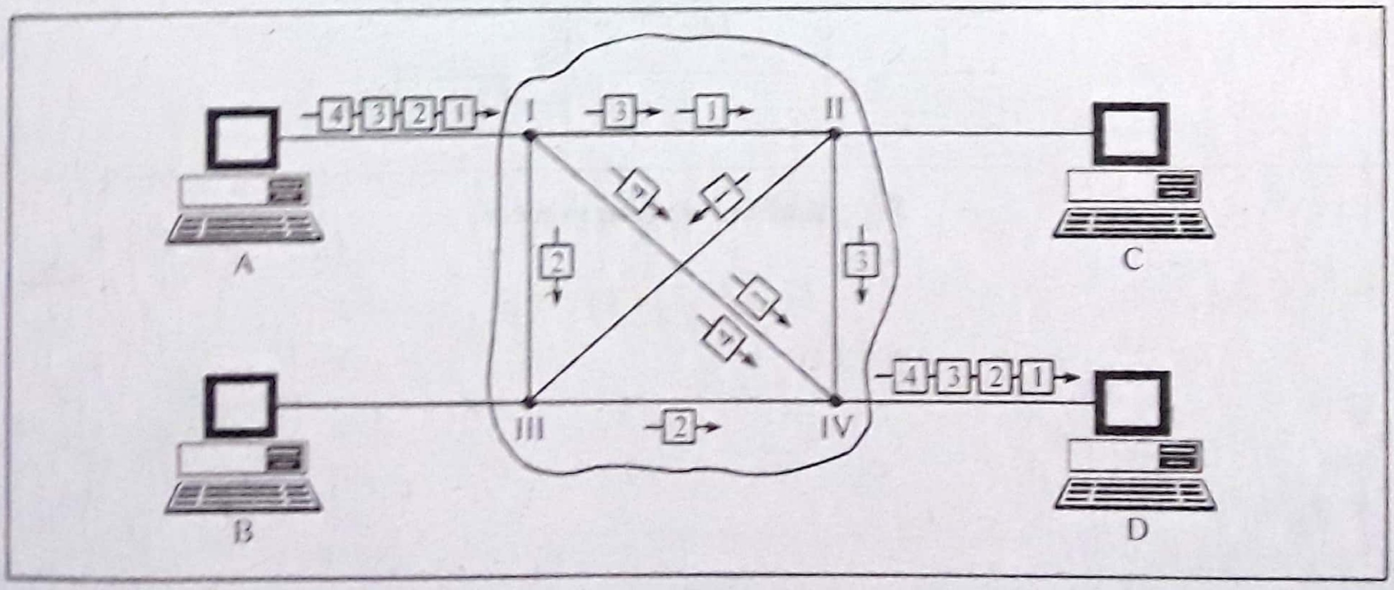


Fig. : Datagram packet switching

Scanned by CamScanner

प्रश्न 16 – *Packet switch के चार प्रमुख घटकों तथा उनके कार्यों का वर्णन कीजिए।*

List four major components of a packets switch and their functions.

उत्तर–Packet switch नेटवर्क एक Digital कम्यूनिकेशनूस नेटवर्क है जो ट्रांसमिट किये जाने वाले डाटा को सामूहिक रूप में रखता है। Packet switching सामान्यतः switches तथा routers पर भरोसा करती है अर्थात् switches तथा routers का प्रयोग packet transfer के लिये करती है। चार प्रमुख घटक निम्नलिखित हैं–

(i) Input Ports

(ii) Output Ports

(iii) The routing Processor

(iv) The switching Fabric

(i) Input Ports–Input port, packet switch का physical तथा data link functions को परफॉर्म करता है–

(a) receive किये गये signal से bits को construct करता है।

(b) frame से packet को रिमूव करता है।

(c) errors को डिटेक्ट करके करेक्ट करता है।

अब packet, नेटवर्क लेयर के द्वारा route के लिये तैयार है। Switching fabric को इसे भेजने से पहले buffers, packet को hold रखता है।

(ii) Output Ports–Output port, input port के reverse order में same functions को परफॉर्म करता है–

(a) Outgoing packets, queue में रखे जाते हैं।

(b) Packet, एक frame में encapsulate किये जाते हैं।

(c) Physical layer functions, frame पर apply किये जाते हैं।

(iii) The routing Processor–Routing processor नेटवर्क लेयर के fuctions को परफॉर्म करता है।

(iv) The switching Fabric–इसके अंतर्गत, Input queue से output queue में packets को मूव करने के प्रक्रिया होती है। निम्नलिखित Fig. में packet switch के components के स्ट्रक्चर को स्पष्ट रूप से दर्शाया गया है–

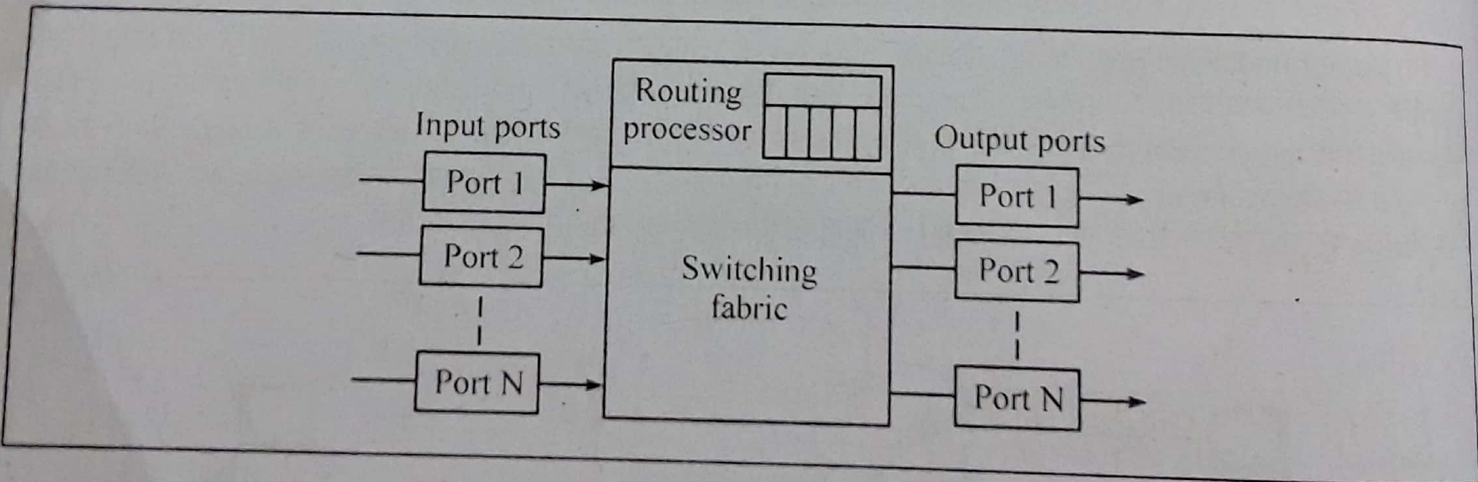


Fig. : Structure of packet switches

□□

UNIT-III

प्रश्न 1 – *Fast Ethernet पर संक्षिप्त टिप्पणी लिखिये।*
Write a short note an Fast Ethernet. **(June, 2009)**

उत्तर–1994 से, Fast Ethernet ने Ethernet का विकल्प बहुत अच्छा उपलब्ध कराया है। इसके प्रमुख कारण निम्नलिखित हैं–

1. यह 10 Base T की अपेक्षाकृत Ten times band width ऑफर करता है।
2. आप Existing 10 Base Ethernet नेटवर्क में Fast Ethernet switching को इंटीग्रेट कर सकते हैं।
3. Fast Ethernet स्टार टोपोलॉजी तथा CSMA/CD को इम्प्लीमेन्ट करता है।

- **100 Base T4–**100 Base T4 चार Unshielded Twisted Pair (UTP) Cables का प्रयोग करती है। कनेक्टर्स भी 10 Base T के अनुरूप हैं। 100 Base T4 साधारणतः दो Extra Pairs का प्रयोग करता है। 100 BaseT4 8B/6T Encoding टाइप को इम्प्लीमेन्ट करता है।
- **100 Base Tx–**यह Fast Ethernet Standards का सबसे Common प्रयोग है। यह दो Unshielded Twisted Pairs (UTP) को प्रयोग करता है, जो Category 5 को इंगित करता है या Category 1 की दो Shielded Twisted Pairs (STP) का प्रयोग करता है। 100 Base Tx कनेक्टर्स 10 BaseT कनेक्टर्स के अनुरूप होते हैं। यह 4B/5T तथा MLT3 (3-Level Multiline Transmission) Type की Encoding का प्रयोग करता है।
- **100 Base Fx–**100 Base Fx एक Fiber Optics के इम्प्लीमेन्टेशन को Specify करता है। ❑

प्रश्न 2 – *FDDI से आप क्या समझते हैं? बताइये।*
What do you understand by FDDI? Explain. **(Dec., 2012/Jan., 2013)**

उत्तर–FDDI को विस्तृत रूप से Fiber Distributed Data Interface कहते हैं। FDDI दूसरे टाईप का रिंग पर आधारित नेटवर्क है। FDDI नेटवर्क कॉपर केबलिंग के स्थान पर ऑप्टिक फाइबर केबल पर रन करता है। यह बहुत तेज, भरोसेमन्द नेटवर्क को फाइवर ऑप्टिक केबल पर इम्प्लीमेन्ट करता है। FDDI, 802.5 मैथड के ऑपरेशन को भी प्रयोग करता है। FDDI एक उच्च परफॉरमेन्स फाइवर ऑप्टिक टोकन रिंग LAN है जो 200 km. तक की दूरी पर 100 mbps की स्पीड से 1,000 स्टेशनों को जोड़ता है।

FDDI को दूसरे LAN की तरह ही प्रयोग किया जा सकता है।

FDDI, Multimode Fibers का प्रयोग करता है। यह Lasers की अपेक्षाकृत LED का प्रयोग भी करता है।

निम्न Fig. में FDDI नेटवर्क को प्रदर्शित किया गया है–

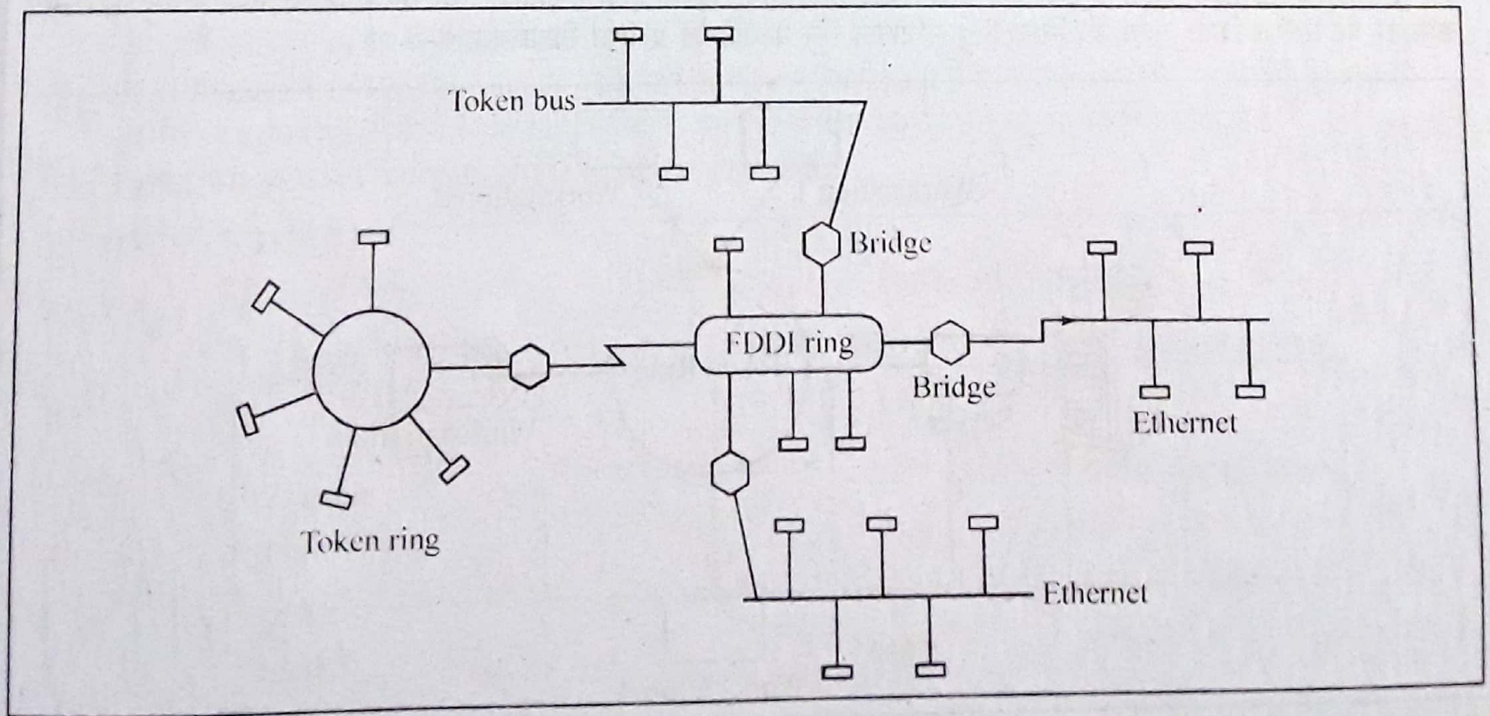


Fig. : FDDI ring being used as a backbone to connect LANs and Computers

Scanned by CamScanner

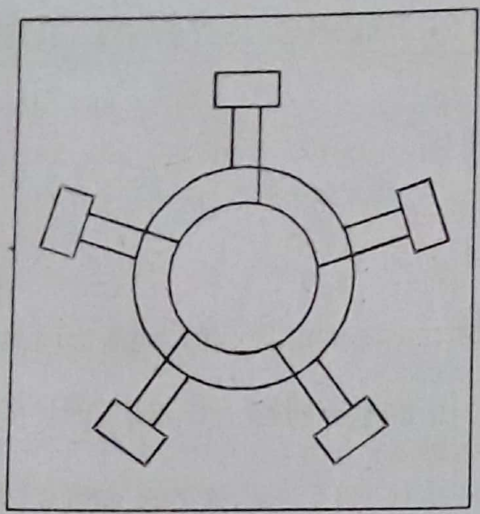
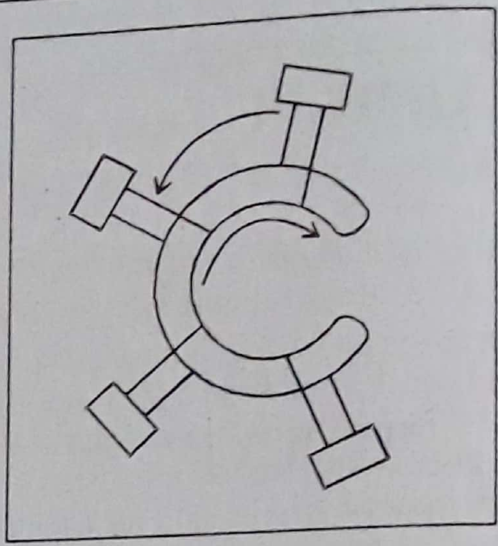


Fig. : (a) FDDI Consisting of two rings



(b) Two rings joined together counter rotating rings

FDDI केबलिंग दो Fiber rings से मिलकर बनी होती है, एक Transmitting Clockwise तथा दूसरी Transmitting Counter Clockewise होती है जैसा कि उपरोक्त Fig. (a) में प्रदर्शित किया गया है। यदि इनमें से कोई एक Break होती है तो दूसरी बैकअप के रूप में प्रयोग की जा सकती है। यदि एक ही Point पर Fire या किसी और वजह से Break हो जाती है तो दोनों Ring एक Single Ring में Join हो सकती हैं, जैसा कि Fig. (b) में प्रदर्शित किया गया है।

FDDI काफी Fast है, यद्यपि यह महंगा है। ❑

प्रश्न 3 – टोकन रिंग को विस्तारपूर्वक चित्र सहित समझाइये।

Explain token ring in detail with neat diagram. (Dec., 2008)

अथवा

Token Ring के कार्य करने के सिद्धान्त को समझाइये।

Explain the working principle of token Ring. (June, 2004)

उत्तर–टोकन रिंग, रिंग टैक्नोलॉजी पर आधारित नेटवर्क है। टोकन रिंग Ethernet नेटवर्क से कॉफी भिन्न रूप में कार्य करती है। Ethernet में वह कम्प्यूटर जो डाटा को रखता है वह डाटा ट्रांसमिट कर सकता है, जब तक कि यह दूसरे कम्प्यूटर के Collision को Sense नहीं करता है। टोकन रिंग नेटवर्क में, एक Single विशेष पैकट को टोकन कहते हैं। यह टोकन नेटवर्क के Around Pass किया जाता है। जब एक कम्प्यूटर को डाटा ट्रांसमिट करना है तो यह तब तक इंतजार करता है जब तक कि टोकन उपलब्ध नहीं होता है। इसे संभालकर होल्ड किया जाता है तथा एक डाटा पैकट को ट्रांसमिट किया जाता है जबकि उसी समय पर लाइन में टोकन को अगले कम्प्यूटर पर रिलीज किया जाता है। निम्न Fig. में टोकन रिंग नेटवर्क को प्रदर्शित किया गया है–

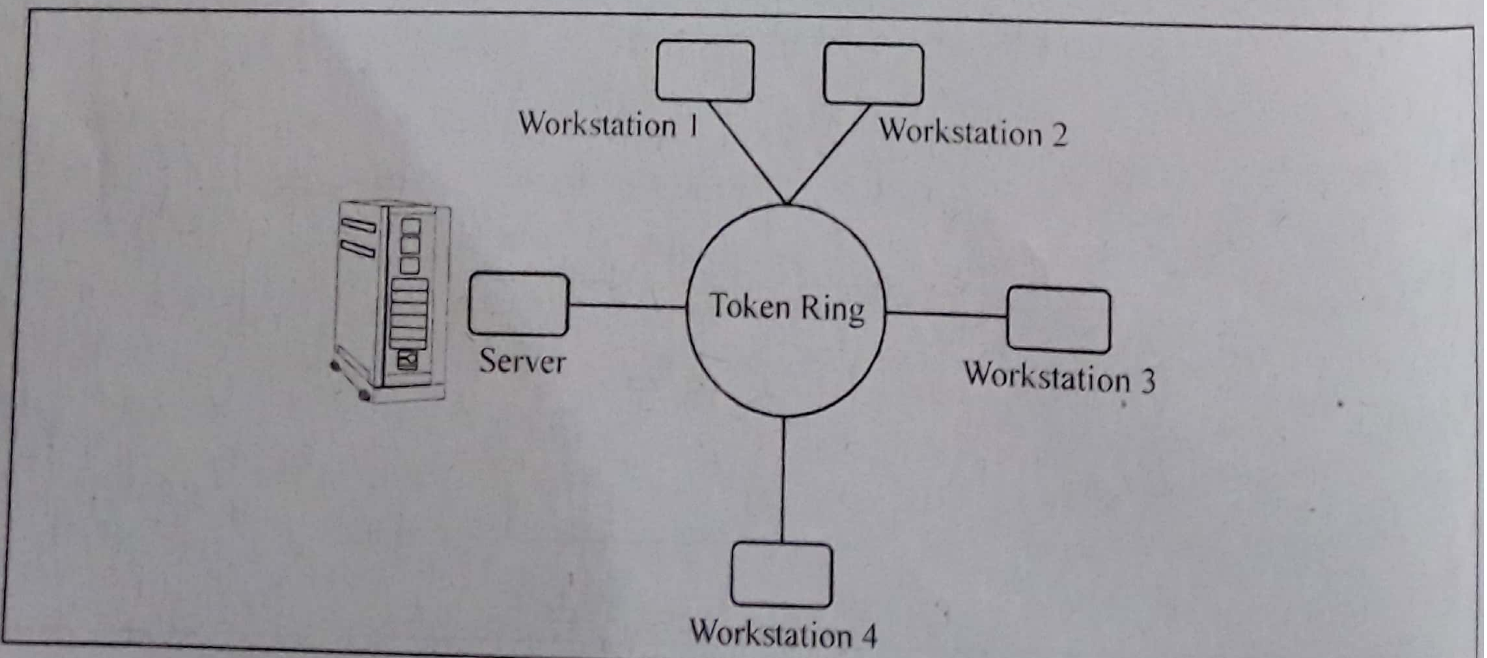


Fig. : Token Ring Network

Scanned by CamScanner

जब एक से अधिक स्टेशनों पर डाटा को भेजने की प्रक्रिया की जाती है तब यह लॉजिकल टोपोलॉजी Collisions को नहीं रखती है।

टोकन रिंग में एक शॉर्ट मैसेज जिसे टोकन कहते हैं इसे पूरे रिंग में Pass किया जाता है जब तक कि एक कम्प्यूटर किसी दूसरे कम्प्यूटर पर इनफॉरमेशन को नहीं भेजता है। कम्प्यूटर टोकन को संशोधित करता है, इलैक्ट्रॉनिक एड्रेस तथा डाटा को Add करता है तथा इसे रिंग के Around भेजता है। क्रम में जुड़ा हुआ प्रत्येक कम्प्यूटर टोकन को रिसीव करता है तथा Pass की गयी इनफॉरमेशन को अगले कम्प्यूटर पर Pass करता है, यह प्रक्रिया तब तक चलती रहती है जब तक कि एक कम्प्यूटर का एड्रेस इसके इलैक्ट्रॉनिक एड्रेस से नहीं मिलता है या टोकन इसके Originator के पास रिटर्न नहीं होती है। टोकन को प्राप्त करने वाला कम्प्यूटर एक मैसेज को Originator के पास रिटर्न करता है जो यह दर्शाता है कि इसे भेजा गया मैसेज प्राप्त हो चुका है। इसके पश्चात् मैसेज भेजने वाला कम्प्यूटर दूसरी टोकन को क्रिएट करता है तथा इसे नेटवर्क पर स्थापित करता है।

टोकन रिंग मैथड को IEEE 802.5 Standard ने परिभाषित किया है। UTP में इम्प्लीमेंट की गयी टोकन रिंग 4 mbps की स्पीड से 260 मशीनों को सम्मिलित कर सकती है।

इसमें Wiring तथा फिजीकल व्यवस्था रिंग नेटवर्क की तरह ही होती है। रिंग नेटवर्क में MAU (Multistation Access Unit) एक डिवाइस होती है जो रिंग नेटवर्क में Center में स्थापित होती है। MAU उसी तरह कार्य करता है; जैसे Hub कार्य करता है लेकिन यह Ethernet नेटवर्क के स्थान पर टोकन रिंग नेटवर्क के साथ कार्य करता है तथा कम्प्यूटरों के मध्य कम्यूनिकेशन को हैण्डल करता है। ❑

प्रश्न 4 – *इथरनेट से आप क्या समझते हो?*
What do you mean by ethernet.

(Dec. 2008)

उत्तर–इथरनेट (Ethernet) को 1973 में Bob Metcalfe ने विकसित किया। इथरनेट, IEEE (Institute of Electronic and Electric Engineers) 802.3 स्टैण्डर्ड पर आधारित नेटवर्क है, इसे 802.3 CSMA/CD भी कहते हैं। नेटवर्किंग में, Collision तब घटित होता है जब दो कम्प्यूटर एक ही समय पर एक ही नेटवर्क Wire पर भेजे गये डाटा को चुनते हैं। यह Conflict (कलह) को क्रिएट करता है। दोनों कम्प्यूटर Collision को Sense करते हैं, ट्रांसमीटिंग को रोकते हैं तथा पुनः ट्रांसमीटिंग के समय का इंतजार करते हैं।

Collision domain, कम्प्यूटरों का ग्रुप है जो Single नेटवर्क Wire पर कम्यूनिकेट करते हैं। Collision domain में प्रत्येक कम्प्यूटर, Collision domain में प्रत्येक दूसरे कम्प्यूटर को सुनता है। प्रत्येक कम्प्यूटर डाटा को केवल तभी ट्रांसमिट कर सकता है जब कोई दूसरा कम्प्यूटर उस समय पर डाटा को ट्रांसमिट नहीं कर रहा है। Ethernet की Nuclear Family के प्रमुख सदस्य निम्नलिखित हैं–

1. **10 Base 2 या Coaxial Cable Networking–**10 Base 2 की अधिकतम Segment लम्बाई 185 मीटर है।
2. **10 Base 5 या Thicknet–**Thicknet को AUI (Attached User Interface) भी कहते हैं। AUI नेटवर्क 10 Base 2 तथा 10 Base T के मध्य का Step है।
3. **10 Base T–**10 Base T में hub से वर्कस्टेशन तक की अधिकतम Cable लम्बाई 100 Meters है।
4. **100 Base T–**इसे Fast इथरनेट भी कहते हैं। यह UTP Wires की दो Pairs पर 100 Megabits Per Second के डाटा रेट को सपोर्ट करती है।
5. **100 Base Fx–**यह Optical Fibers पर रन करती है।
6. **100 Base T4–**100 Base T4 की अधिकतम लम्बाई Concentrator तथा Workstation के मध्य 20 Meters है।

इथरनेट, एक हार्डवेयर सिस्टम है जो OSI मॉडल के डाटा लिंक तथा फिजीकल लेयर में उपलब्ध होता है।

इथरनेट फ्रेम के फॉर्मेट को अग्रांकित Fig. में प्रदर्शित किया गया है–

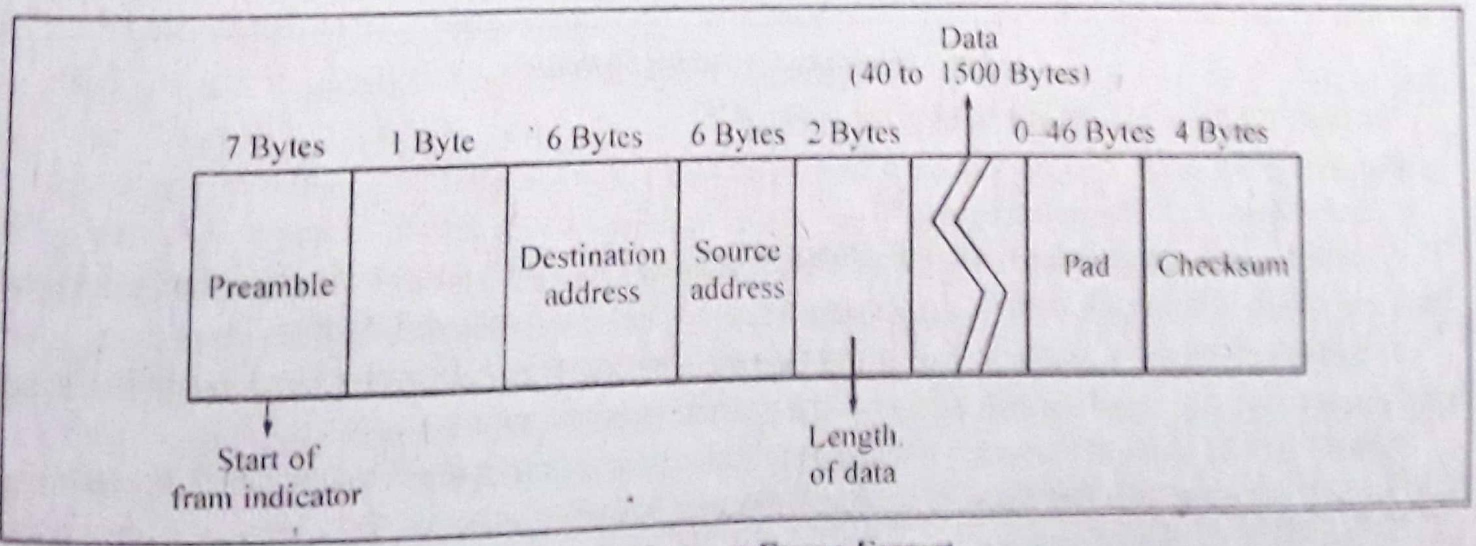


Fig. : Ethernet Frame Format

Scanned by CamScanner

इथरनेट डाटा के रूप में IP Datagrams को रखता है। इथरनेट फ्रेम में Source तथा Destination address, फिजीकल एड्रेस है। फिजीकल एड्रेस, एक नोड का एड्रेस होता है जो LAN तथा WAN के द्वारा परिभाषित होता है। फिजीकल एड्रेस का Size तथा फॉर्मेट नेटवर्क पर निर्भर करता है; जैसे–इथरनेट 6-byte (48 bit) एड्रेस तथा Local Talk 1 byte डायनामिक एड्रेस को प्रयोग करता है। इथरनेट 48 bit एड्रेस स्कीम का प्रयोग करता है। ❑

प्रश्न 5 – *राउटर (Router) की कम्प्यूटर नेटवर्क में क्या भूमिका है?*
What is the role of Router in Computer Network? **(Dec., 2008)**

उत्तर–राउटर (Router)–Routers डिवाइसेस सॉफ्टवेयर को रखती है जो उपलब्ध Paths में से Best Path को चुनते हैं, जिसके माध्यम से विशिष्ट ट्रांसमीशन किया जाता है। ये हार्डवेयर तथा सॉफ्टवेयर का मिश्रण होते हैं।

हार्डवेयर, इंटरनेटवर्क में विभिन्न नेटवर्कों के फिजीकल इंटरफेसों को सम्मिलित करते हैं। Router में सॉफ्टवेयर के दो मुख्य भाग ऑपरेटिंग सिस्टम तथा Routing प्रोटोकॉल होते हैं।

Routers का प्रयोग दो या दो से अधिक लॉजिकली अलग नेटवर्कों के लॉजिकल तथा फिजीकल एड्रेसिंग के लिये होता है। ये इस कनेक्शन को बड़े नेटवर्क को लॉजिकल नेटवर्क Segments या Subnetworks में Organise करके पूरा करते हैं। इन Subnetworks में प्रत्येक को एक लॉजिकल एड्रेस दिया जाता है। यह नेटवर्कों को अलग-अलग Allow करते हैं लेकिन प्रत्येक एक्सेस करते हैं तथा जब आवश्यक हो डाटा को एक्सचेन्ज करते हैं। डाटा पैकेटों के रूप में या Blocks के रूप में Grouped होते हैं। प्रत्येक पैकेट, एक फिजीकल डिवाइस एड्रेस, एक लॉजिकल नेटवर्क एड्रेस को रखता है। निम्न Fig. में Routers का प्रयोग करके नेटवर्क को दर्शाया गया है–

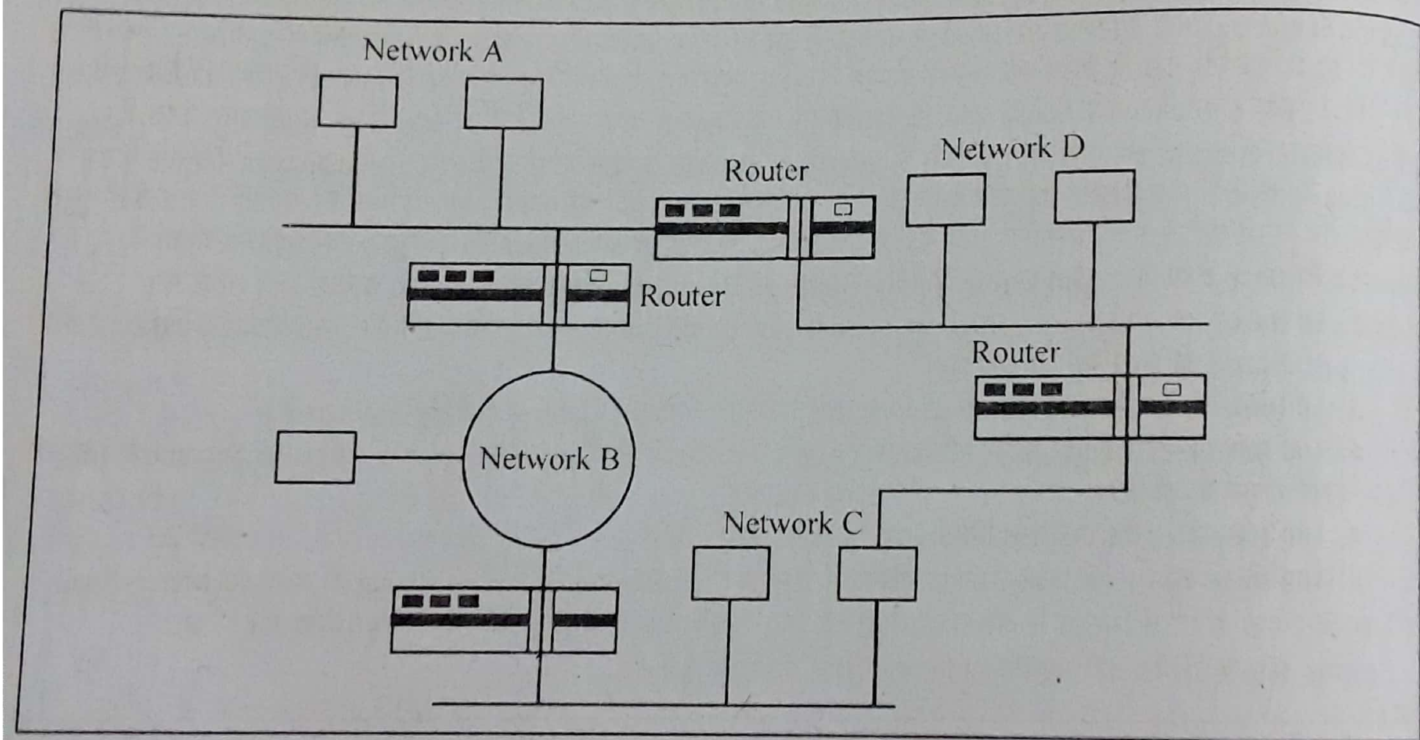


Fig. : Networks Connected by Routers

Routers केवल Routable प्रोटोकॉल के साथ कार्य कर सकते हैं।

Router दो प्रकार के होते हैं–

1. Static Routers, 2. Dynamic Routers

1. Static Routers–Static Routers में नेटवर्क एडमिनिस्ट्रेटर, Routing Table को Manually रूप से इनिशियलाइज करते हैं। इसमें संभव Paths पहले से परिभाषित होते हैं तथा Intermediatery Routers, Routing Decisions नहीं लेते हैं।

2. Dynamic Routers–Dynamic Routers के साथ First Route को अक्सर Manually रूप से Configure करते हैं। तत्पश्चात प्रत्येक Intermediatery Router, Best Path को चुनते हैं जब यह डाटा को ट्रांसफर करता है।

Routers का प्रयोग Identical Network तथा नेटवर्क को विभिन्न टाईप के हार्डवेयर के साथ इंटरकनेक्ट करने के लिये किया जाता है। दो LAN के मध्य एक Router दोनों नेटवर्कों से मैसेजों को रिसीव करता है, इनके Destinations को Check करता है तथा आवश्यक LAN के पास मैसेजों को ट्रांसमिट करता है।

Scanned by CamScanner

वास्तविक रूप में Routers, एक नेटवर्क को Split करते हैं, नेटवर्क पर प्रत्येक पैकेट को पढ़ते हैं तथा दूसरे नेटवर्क पर इंटरनेटवर्क ट्रैफिक को Pass करते हैं।

Routers के माध्यम से LAN को कनेक्ट करने के निम्नलिखित प्रमुख फायदे हैं–

1. इसका सबसे बड़ा फायदा Security है। LAN, एक ब्रॉडकास्ट मोड में ऑपरेट करता है।
2. Router का दूसरा फायदा Reliability है। यदि एक नेटवर्क बन्द हो जाता है तो दूसरे नेटवर्क को Serve करने वाला Router प्रभावित नहीं होता है।
3. Router का तीसरा फायदा Performance Enhancement है।
4. Router का चौथा फायदा Networking Range है। ❑

प्रश्न 6 (a) – Bridge पर संक्षिप्त टिप्पणी लिखिए–

Write short notes on Bridge. **(Dec., 2008)**

उत्तर–Bridges–Bridges, डिवाइसेस होती है जो दो असमान LANs के बीच में डाटा को ट्रांसमिट कर सकती हैं। Bridges, एक बड़े नेटवर्क को छोटे-छोटे Segments में विभाजित करती हैं। ये डाटा को फिल्टर भी करती हैं तथा प्रत्येक Segment के लिये ट्रैफिक को अलग रखती हैं।

जब एक पैकट, एक ब्रिज में Enter करता है, यह फ्रेम में से एड्रेस को पढ़ता है तथा उस एड्रेस की एक टेबल में स्टोर एड्रेस से तुलना करता है। टेबल में दोनों Segments में सभी Nodes का एड्रेस स्टोर होता है। जब Bridge को एक मैच मिल जाता है, यह Destination Segment पर पैकेट को भेज देता है। जैसा कि निम्न Fig. से स्पष्ट है–

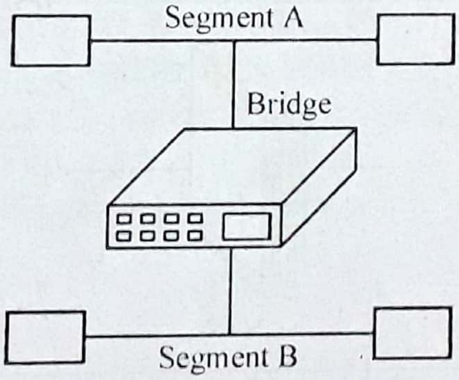


Fig. : The Bridge connecting two segements of PCs

एक ब्रिज निम्नलिखित रूप में ऑपरेट करता है–

(a) एक ब्रिज, दोनों Segments A तथा B से सभी Signals को रिसीव करता है जैसा कि उपर्युक्त Fig. में दर्शाया गया है।

(b) ब्रिज एड्रेस को पढ़ता है तथा Segment A में से सभी Signals को Discard करता है जो Segment A को एड्रेस करते हैं, क्योंकि इन्हें ब्रिज को Cross करने की आवश्यकता नहीं होती है।

(c) Segment A से Signals को Segment B के कम्प्यूटर से Address करने के पश्चात् Segment B पर पुनः ट्रांसमिट किया जाता है।

(d) Segment B के Signals को Similar Way में Treat किया जाता है। केवल जो Signals Segment A के लिये Meant होते हैं उन्हें पुनः ट्रांसमिट किया जाता है।

ब्रिज निम्नलिखित तीन प्रकार के होते हैं–

1. Transparent Bridge–इससे वह अपना नाम पाता है। नेटवर्क पर उपकरण अपनी उपस्थिति से अनजान होते हैं। एक Transparent ब्रिज MAC एड्रेस पर आधारित डाटा को Forward करने या Stop करने के अतिरिक्त कुछ नहीं करता है।

2. Source Routing Bridge–यह ब्रिज Token Ring नेटवर्क में इस्तेमाल किया जाता है। नेटवर्क में पैकेट को गुजारने वाला पूर्ण मार्ग पैकेट में ही होता है, इसी कारण इसका नाम यह रखा गया है।

3. Translational Bridge–इस ब्रिज का प्रयोग नेटवर्किंग डाटा प्रारूप को दूसरे प्रारूप में बदलने में प्रयोग होता है। ❑

Scanned by CamScanner

प्रश्न 6 (b) – रिपीटर से आप क्या समझते हैं? चित्र द्वारा समझाइयें।

What do you understand by Repeater? Explain by figure.

उत्तर–रिपीटर (Repeater)–सभी ट्रांसमीशन मीडिया, इलैक्ट्रॉनिक मैग्नेटिक Waves को कमजोर करते हैं जो मीडिया के माध्यम से Travel करते हैं, इसे Attenuation कहते हैं। Attenuation, किसी मीडियम के डाटा को Carry करने की दूरी की सीमा बनाता है। एक डिवाइस को Add करने पर जो Signals Amplify करती है, इसे आगे के लिये नेटवर्क के Size को बढ़ाकर Travel करने के लिये Allow करती है, यह डिवाइस रिपीटर कहलाती है।

जैसे–यदि Ethernet Cable के माध्यम से 100 कम्प्यूटर्स से ज्यादा को जोड़ा गया है तो इसमें एक डिवाइस की जरूरत होती है जो ट्रांसमीशन को सुनिश्चित करने के लिये Signals को Amplify करती है। जो डिवाइस इस तरह से Signals को Amplify करती है, रिपीटर कहलाती है। रिपीटर को दो श्रेणियों में विभाजित किया गया है–

(a) Amplifiers

(b) Signal-regenerating Devices (Repeaters)

(a) Amplifiers– Amplifiers, आने वाले सभी Signals को Amplify करते हैं; अर्थात् Signal तथा Noise दोनों को Amplify करते हैं। ये केवल Analog Type के Signal को Improve करते हैं।

(b) Signal-regenerating Devices (Repeaters)– Signal-regenerating Repeaters, आने वाले डाटा के Exact डुप्लीकेट को तैयार करते हैं, इसे reconstruct करते हैं तथा केवल इच्छित इनफॉरमेशन को Pass करते हैं। इस तरीके में ऑरिजनल Signal, डुप्लीकेट्ड होते हैं, इनकी ऑरिजनल Strength को बूस्ट करते हैं तथा भेजते हैं।

निम्न Fig. में Repeater के प्रयोग को दर्शाया गया है–

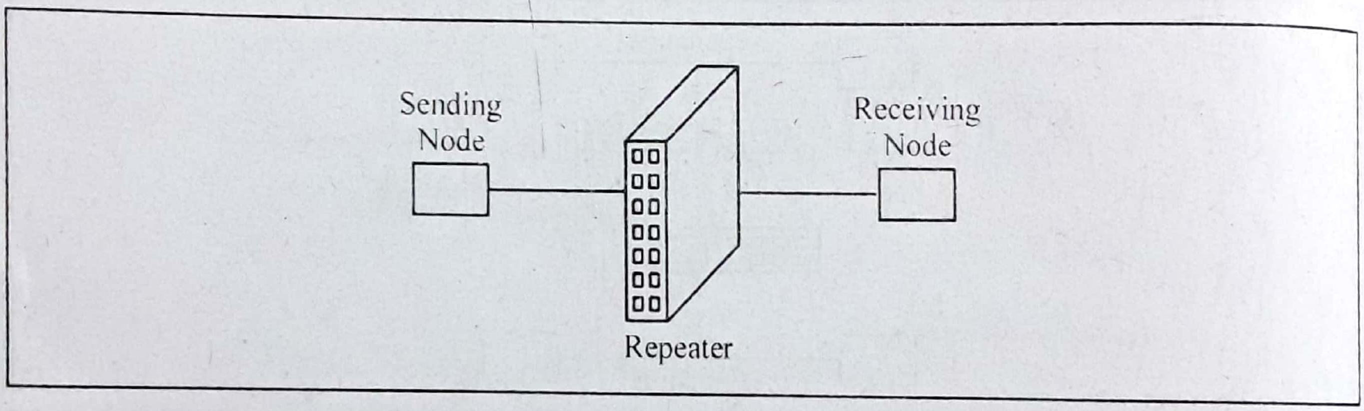


Fig. : Repeater Connecting two computers and regenerating digital signal

Repeaters, एक Single नेटवर्क की दूरी को बढ़ाते हैं। इसलिये यदि आप Ethernet LAN का प्रयोग कर रहे हैं लेकिन, सामान्यतः दूरी से आगे तक के लिये नेटवर्क को बढ़ाना चाहते हैं तो आप एक रिपीटर को Install कर सकते हैं। जब एक रिपीटर को Install किया जाता है, यह केबल में फिजीकल ब्रेक को क्रिएट करता है। Signal रिपीटर के एक साइड में रिसीव किये जाते हैं, इन्हें पुनः जनरेट करके केबल के अगले सैक्शन में Pass किया जाता है।

एक रिपीटर वास्तव में दो LANs को कनेक्ट नहीं करता है, यह एक ही तरह के LAN के दो Segement को कनेक्ट करता है। निम्न Fig. में एक LAN के दो Segments को एक रिपीटर के द्वारा जोड़ा गया है–

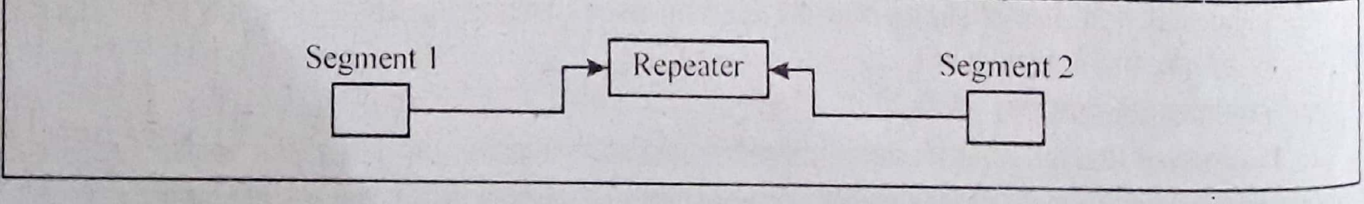


Fig. : A repeater connecting two segments of a LAN

एक रिपीटर, एक LAN के Segments को कनेक्ट करता है। एक रिपीटर प्रत्येक फ्रेम को Forward करता है, यह कोई फिल्टरिंग Capability को नहीं रखता है। एक रिपीटर, एक रिजनरेटर है न कि एक एम्प्लीफायर है। □

Scanned by CamScanner

प्रश्न 7 – निम्न पर संक्षिप्त टिप्पणियां लिखिये–

Write short notes on the following : **(June, 2009)**

(i) UDP And ARP Protocols.

(ii) Domain name Address Schemes.

(iii) Active and Passive Hubs.

(iv) Static and Dynamic Routers.

उत्तर–**(i) UDP and ARP Protocols**–UDP को विस्तृत रूप से User Datagram Protocal कहते हैं। UDP एक कनेक्शनविहीन (Connectionless) प्रोटोकॉल है जो ट्रांसपोर्ट लेयर पर कार्य करता है। UDP, Datagrams को ट्रांसपोर्ट करता है लेकिन इसके रिसीव होने का Acknowledge को नहीं करता है। UDP भी डाटाग्राम डिलीवरी को एचीव करने के लिये Port एड्रेस का प्रयोग करता है लेकिन यह Port एड्रेस एक पॉइन्टर होता है जो प्रोसेस को Point करता है न कि कनेक्शन आइडेंटिफायर होता है, जैसे कि TCP के साथ होता है।

UDP, Flow Control या Acknowledge को उपलब्ध नहीं कराता है। डाटाग्राम को ट्रांसमिट करते समय यदि UDP किसी Error को पकड़ता है तो यह डाटाग्राम को Drop कर देता है तथा Sender को इसके बारे में कोई सूचना नहीं देता है।

ARP Protocols को विस्तृत रूप से Advance Research Protocol कहते हैं। ARP, एक नोड के MAC (Medium Access Control) एड्रेस को उपलब्ध करता है। यह एक ARP रिक्वेस्ट को ब्रॉडकास्टिंग के द्वारा किया जाता है जो इससे सम्बन्धित नोड के IP एड्रेस को रखता है। यह तकनीकी आपको एक लोकल IP नेटवर्क पर Peripheral को एक फ्रेम को भेजने के लिये Allow करता है।

(ii) Domain Name Address Scheme–DNS (Domain Name System) एक डिस्ट्रीब्यूटेड डाटाबेस सिस्टम है जो ट्रांसपोर्ट लेयर पर कार्य करता है तथा क्लाइंट एप्लीकेशनूस के लिये name-to-address मैपिंग को उपलब्ध कराता है। DNS Servers, डाटाबेस को मैनटेन (Maintain) करता है जो डिवाइस आइडेन्टिफिकेशन के लिये लॉजिकल नामों को प्रयोग करने के क्रम में विभिन Domains के Hierarchical नेम स्ट्रक्चर्स से मिलकर बना होता है। इस टाइप के एड्रेस/नेम रिजॉल्यूशन को सर्वर प्रोवाइडर इनिशियेटेड कहते हैं। DNS का सबसे ज्यादा प्रयोग इंटरनेट में करते हैं।

इंटरनेट में डोमेन नेम स्पेस को तीन विभिन्न सैक्शनों में विभाजित किया जाता है–

1. Generic Domains
2. Country Domains
3. Invers Domains

1. Generic Domains–Generic Domains, रजिस्टर्ड Hosts को इनके Generic व्यवहार के अनुसार परिभाषित होते हैं। Tree में प्रत्येक नोड एक डोमेन को परिभाषित करती है, जिसका एक इंडेक्स, डोमेन नेम स्पेस डाटाबेस में होता है।

2. Country Domains–Country Domain सैक्शन, Generic Domains की तरह ही Same फॉर्मेट को Follow करता है लेकिन दो कैरेक्टर Country abbreviations का प्रयोग करता है; जैसे United States के लिये "US".

3. Inverse Domain–Inverse Domain का प्रयोग नेम के एड्रेस को मैप करने के लिये किया जाता है।

(iii) Active and Passive Hubs–Hub एक डिवाइस है जहां डाटा एक या एक से अधिक Nodes (Computers in a Network) से आता है तथा एक या एक से अधिक दूसरी Nodes के पास Forward किया जाता है। सामान्यतः Hubs 4 to 24 RJ-45 Ports को Twisted-Pair केबलिंग के लिये रखते हैं तथा एक या एक से अधिक Uplink Ports, एक Hub से दूसरे Hub को कनेक्ट करने के लिये किया जाता है। Hubs Port-link Status, Collisions इत्यादि के Status के लिये Indicator lights को Indicate करते हैं।

Hubs, प्रत्येक स्टेशन (नोड) से Signals को रिसीव करते हैं तथा Signals को सभी स्टेशनों पर रिपीट करते हैं जो Hub से कनेक्टेड होते हैं। कुछ Hubs को Active Hubs कहते हैं, जो दूसरी Nodes के पास Signals को ट्रांसमिट करने से पहले Amplity भी करते हैं। यह मल्टीपोर्ट रिपोर्टर की तरह होता है।

(iv) Static and Dynamic Routers–Static Routers में नेटवर्क एडमिनिस्ट्रेटर रूटिंग (Routing) टेबल को Manually रूप से इनिशियलाइज करता है। इसमें संभव Paths पहले से परिभाषित होते हैं तथा Routers, Routing निर्णय नहीं लेते हैं।

Dynamic Routers में First Route अक्सर Manually रूप से Configure होता है। प्रत्येक Intermediatery Router सबसे अच्छा Path चुनते हैं जब यह डाटा को ट्रांसफर करते हैं। ❑

Scanned by CamScanner

प्रश्न 8 – *TCP/IP मॉडल का विस्तार से वर्णन कीजिये तथा प्रत्येक लेयर पर प्रयुक्त प्रोटोकॉल बताइये।*

Explain in detail the TCP/IP model with its protocol on each layer. (June, 2009)

उत्तर–TCP/IP को विस्तृत रूप से Transmission Control Protocol/ Internet Protocol कहते हैं। TCP/IP को 1980 में US के Defense Department (DOD) ने डेवलप किया था। TCP/IP एक रूटेबल (Routable) प्रोटोकॉल है जो भिन्न-भिन्न नेटवर्क्स (जैसे–Microsoft Windows तथा Unix) को कनेक्ट करने के लिये सक्षम है। TCP/IP प्रोटोकॉल को प्रमुख रूप से WAN के लिए डेवलप किया गया था, परन्तु आजकल इसे किसी भी तरह के नेटवर्क में प्रयोग कर सकते हैं। TCP/IP मॉडल में चार लेयर्स होती हैं जो निम्नलिखित हैं–

1. नेटवर्क लेयर (Network Layer)
2. इंटरनेट लेयर (Internet Layer)
3. होस्ट टू होस्ट लेयर (Host to Host Layer)
4. एप्लीकेशन लेयर (Application Layer)

1. नेटवर्क लेयर (Network Layer)–TCP/IP मॉडल में नेटवर्क एक्सेस लेयर, OSI मॉडल की फिजीकल तथा डाटा लिंक लेयर के समतुल्य है।

2. इंटरनेट लेयर (Internet Layer)–TCP/IP मॉडल में इंटरनेट लेयर, OSI मॉडल की नेटवर्क लेयर के समतुल्य है। इस लेयर में प्रोटोकॉल्स, इंटरनेटवर्क के माध्यम से ट्रांसपोर्टिंग पैकेटों से सम्बन्धित होते हैं। IP, मुख्य इंटरनेट लेयर प्रोटोकॉल है।

3. होस्ट-टू-होस्ट लेयर (Host-to-Host Layer)–Host-to-Host लेयर, OSI मॉडल की Transport लेयर के समतुल्य होती है। इस लेयर में प्रोटोकॉल्स, दूसरी नेटवर्क डिवाइसेस के साथ कम्यूनिकेट करते हैं। TCP, Host प्रोटोकॉल का उदाहरण है।

4. एप्लीकेशन लेयर (Application Layer)–एप्लीकेशन लेयर, OSI मॉडल की Session, Presentation तथा Application लेयर के समतुल्य है। इस लेयर में प्रोटोकॉल्स, नेटवर्क पर एप्लीकेशन सेवायें उपलब्ध कराते हैं। Telnet, FTP इत्यादि इस लेयर के प्रोटोकॉल्स के उदाहरण हैं।

निम्न Fig. में OSI Model तथा TCP/IP मॉडल के अन्तर को दर्शाया गया है–

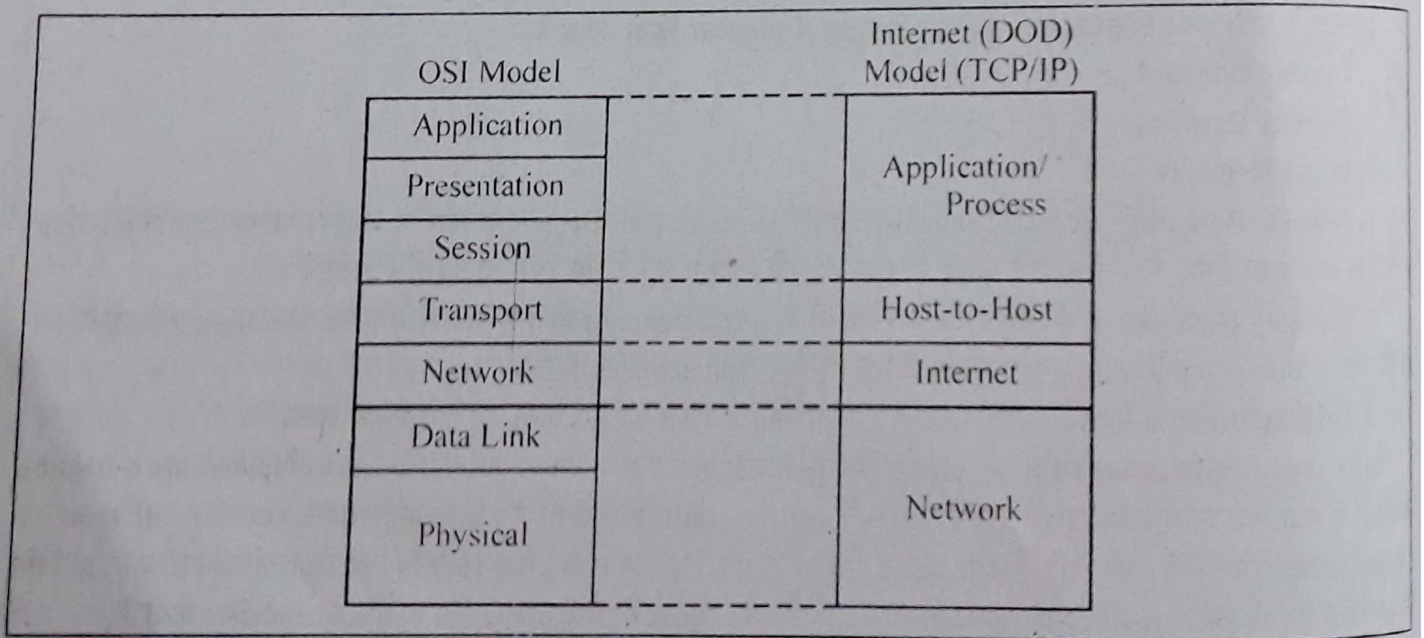


Fig. : Internet Model (TCP/IP) Mapped with OSI Model

प्रश्न 9 – *हब, स्विच और ब्रिज में अंतर बताओ।*

Differentiate between Hubs, Switches and Bridges.

उत्तर–हब, स्विच तथा ब्रिज के मध्य मुख्य अंतर निम्नलिखित है–

Scanned by CamScanner

हब (Hubs)	स्विच (Switches)	ब्रिज (Bridges)
1. हब एक ऐसा उपकरण है, जो कई Twisted pair cable या Fiber optic cable साधनों को आपस में जोड़ता है तथा उनका एक नेटवर्क के रूप में कार्य करना सम्भव बनाता है।	1. स्विच एक ऐसा उपकरण है, जो अधिक दक्षता के साथ दो नेटवर्कों के बीच Bridge सुविधा को उपलब्ध कराता है।	1. ब्रिज OSI Model के फिजीकल और डाटा लिंक दोनों लेयरों पर कार्य करते हैं।
2. हब को एक, कई पोर्ट वाले रिपीटर के रूप में समझा जा सकता है, इसलिये इनको रिपीटर हब भी कहते हैं।	2. कोई स्विच किसी लोकल एरिया नेटवर्क के विभिन्न Segments के बीच एक मल्टीपोर्ट ब्रिज की तरह कार्य कर सकता है। किसी स्विच को जब कोई फ्रेम या पैकट प्राप्त होता है, तो वह उसको प्राप्तकर्त्ता; अर्थात् आने वाली लिंक के बफर में स्टोर कर देता है और जाने वाली लिंक का पता लगाने के लिये उसके गंतव्य का ऐड्रेस देखता है।	2. ब्रिज मूलतः दो भिन्न प्रकार के Segments में फ्रेमों को रिले भी कर सकते हैं।
3. हब OSI Model के फिजीकल लेयर पर कार्य करते हैं।	3. स्विचों के डिजायन उनके कार्य करने के आधार पर दो प्रकार के होते हैं—(i) Store and forward, (ii) Cut through.	3. ब्रिज किसी पैकट के ढांचे या सामग्री में कोई परिवर्तन या सुधार नहीं करते और इसलिये उनका प्रयोग एक ही प्रोटोकॉल का उपयोग करने वाले Segments के बीच भी किया जा सकता है।
4. वास्तविक रूप से कोई हब केवल आने वाले पैकटों को प्राप्त करता है, आवश्यक होने पर विद्युत सिग्नलों की तीव्रता बढ़ा देता है और उन पैकटों को नेटवर्क के सभी साधनों को प्रसारित कर देता है, जिनमें प्रेषित करने वाला साधन भी शामिल होता है।	4. स्विच सामान्यतः हमेशा ही Full duplex mode में कार्य करते हैं।	4. कोई ब्रिज डाटा लिंक लेयर पर कार्य करता है और उसको स्वयं से जुड़े हुए सभी स्टेशनों को फिजीकल पता उपलब्ध कराता है।

□

प्रश्न 10 – निम्न पर संक्षिप्त टिप्पणी लिखिये–

Write short notes on the following :

(i) DNS **(Jan., 2005; June, 2003; June., 2009)**

(ii) Brouters and Gateways

(iii) Network scaling and its basics

(iv) Subnet and Subnet mask

उत्तर–(i) DNS–DNS को विस्तृत रूप में Domain Name System कहते हैं। कम्प्यूटर नेटवर्क से जुड़े रहते हैं। यह कम्यूनिकेशन मीडिया Twisted Pair Cable, Co-axial Cable, Fiber Optic Cable इत्यादि हो सकते हैं। कम्प्यूटरों को आपस में दो तरह से नेटवर्किंग के माध्यम से जोड़ सकते हैं। एक विधि में सभी कम्प्यूटर्स को आपस में जोड़ दिया जाता है इसे Peer-to-Peer नेटवर्क कहते हैं। इसमें कोई कम्प्यूटर सर्वर नहीं होता है। सभी आपस में एक-दूसरे का डाटा शेयर कर सकते हैं। दूसरी विधि में एक कम्प्यूटर को मुख्य कम्प्यूटर की तरह मानते हैं तथा शेष कम्प्यूटरों को इस मुख्य कम्प्यूटर से कनेक्ट करते हैं। मुख्य कम्प्यूटर को सर्वर कहते हैं, शेष कम्प्यूटरों को क्लाइंट कम्प्यूटर कहते हैं, इस नेटवर्किंग को Client Server Networking कहते हैं। इस नेटवर्किंग में Server को एक नाम दिया जाता है इसे Domain कहते हैं तथा इस सिस्टम को DNS (Domain Name System) कहते हैं जैसे; www.yahoo.com में yahoo, Domain name है जिसे इंटरनेट से जुड़े किसी भी क्लाइंट सिस्टम के माध्यम से yahoo डोमेन सर्वर में एक्सेस किया जाता है।

(ii) Brouters and Gateways–Brouters, नेटवर्क डिवाइस में होती है जिसमें सॉफ्टवेयर उपलब्ध होते हैं जो ट्रांसमीशन के लिये उपलब्ध Paths में से सबसे अच्छा Path (Host Path) को चुनने में सहायता करते हैं। ये हार्डवेयर तथा सॉफ्टवेयर से मिलकर बने होते हैं। हार्डवेयर में, इंटरनेटवर्क में विभिन्न नेटवर्कों के फिजीकल इंटरफेस सम्मिलित होते हैं।

Scanned by CamScanner

Brouters, दो या दो से अधिक लॉजिकली अलग-अलग नेटवर्कों को कनेक्ट करने के लिये लॉजिकल तथा फिजीकल एड्रेसिंग को प्रयोग करते हैं। दो LANs के मध्य एक Brouter, दोनों नेटवर्कों से मैसेजों को रिसीव करते हैं, इनके Destinations को Check करते हैं तथा आवश्यक LAN के पास मैसेजों को ट्रांसमिट करते हैं।

Gateway एक डिवाइस है जिसका प्रयोग पूर्ण रूप से भिन्न नेटवर्कों (Dissimilar Networks) को कनेक्ट करने के लिये किया जाता है। Gateways, OSI मॉडल की सभी लेयरों (Seven Layers) के लिये प्रोटोकॉल कनवर्जन को पूरा करते हैं। एक Gateway, e-mail मैसेजों को एक फॉर्मेट में रिकवर कर सकते हैं तथा इन्हें दूसरे फॉर्मेट में कनवर्ट कर सकते हैं। आप सिस्टम्स को विभिन्न कम्यूनिकेशन प्रोटोकॉल, लेंग्वेजों तथा आर्किटेक्चर को Gateway का प्रयोग करके कनेक्ट कर सकते हैं।

(iii) Network Scaling and its basics–जब एक से अधिक तत्वों को आपस में जोड़ दिया जाता है तो इसे नेटवर्क कहते हैं। इसी तरह जब एक से अधिक कम्प्यूटरों को आपस में जोड़ दिया जाता है तो इसे कम्प्यूटर नेटवर्क कहते हैं। कम्प्यूटर नेटवर्क में कम्प्यूटरों को आपस में कम्यूनिकेशन मीडिया के माध्यम से जोड़ा जाता है। ये कम्यूनिकेशन मीडिया Twisted Pair Cable, Co-axial Cables, Fiber Optic Cables इत्यादि के रूप में होते हैं। कम्प्यूटर नेटवर्क के माध्यम से हम नेटवर्क से जुड़े हुये किसी भी कम्प्यूटर के हार्डवेयर, सॉफ्टवेयर इत्यादि को Share कर सकते हैं। इसके अतिरिक्त एक कम्प्यूटर का डाटा किसी दूसरे कम्प्यूटर पर भेज सकते हैं। यह डाटा Text, Audio, Video, Image, Graphics इत्यादि के रूप में हो सकता है।

कम्प्यूटर नेटवर्किंग में Server, Workstations, कम्यूनिकेशन मीडिया, Network Interface Card इत्यादि घटक के रूप में होते हैं।

(iv) Subnet and Subnet mask–कम्प्यूटर नेटवर्क में जुड़े हुये सभी कम्प्यूटरों को एक Unique एड्रेस उपलब्ध कराया जाता है। जब कम्प्यूटर नेटवर्क में किसी नये कम्प्यूटर को जोड़ा जाता है तब इस नये कम्प्यूटर को एक Unique एड्रेस दिया जाता है, इस एड्रेस को IP एड्रेस कहते हैं। इसी तरह एक से अधिक भिन्न-भिन्न नेटवर्कों को मिलाकर एक नेटवर्क डिजाइन किया जाता है, इस नेटवर्क को इंटरनेट कहते हैं। इंटरनेट को नेटवर्कों का नेटवर्क कहते हैं।

प्रत्येक नेटवर्क से जुड़े हुये सभी कम्प्यूटरों को एक Unique IP एड्रेस दिया जाता है। प्रत्येक नेटवर्क के सर्वर को मिलाकर जब एक नेटवर्क बनाया जाता है तो इसे Subnet कहते हैं तथा इसकी id को व्यवस्थित करने के तरीके को Subnet mask कहते हैं। निम्न Fig. में Subnet को प्रदर्शित किया गया है–

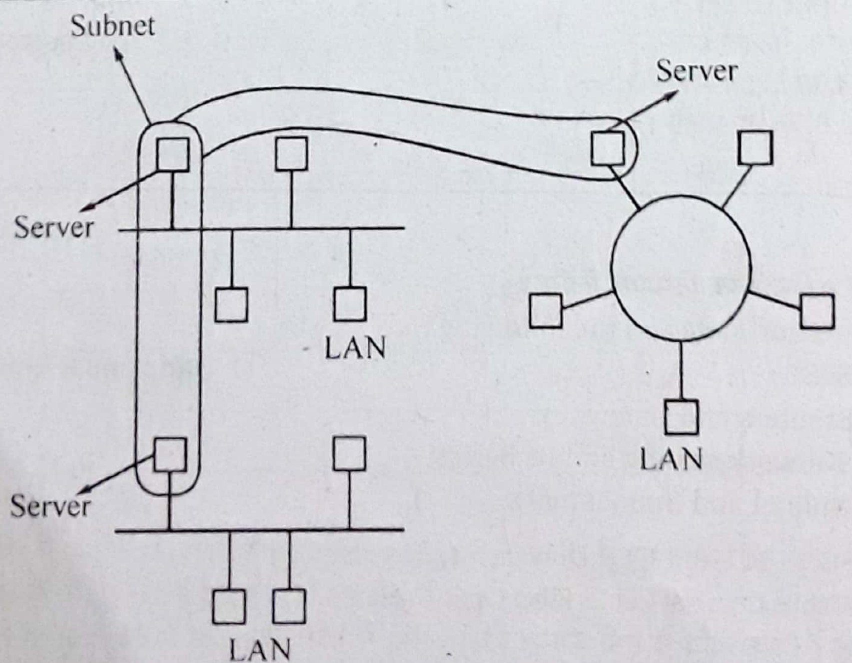


Fig. : Subnet

इस Fig. में प्रत्येक LAN के Server को मिलाकर एक Subnet बनाया गया है। इंटरनेट की लेयर में यह कार्य Subnet-work Layer के द्वारा उपलब्ध कराया जाता है। □

प्रश्न 11 – Gateways से आप क्या समझते हैं? समझाइये।

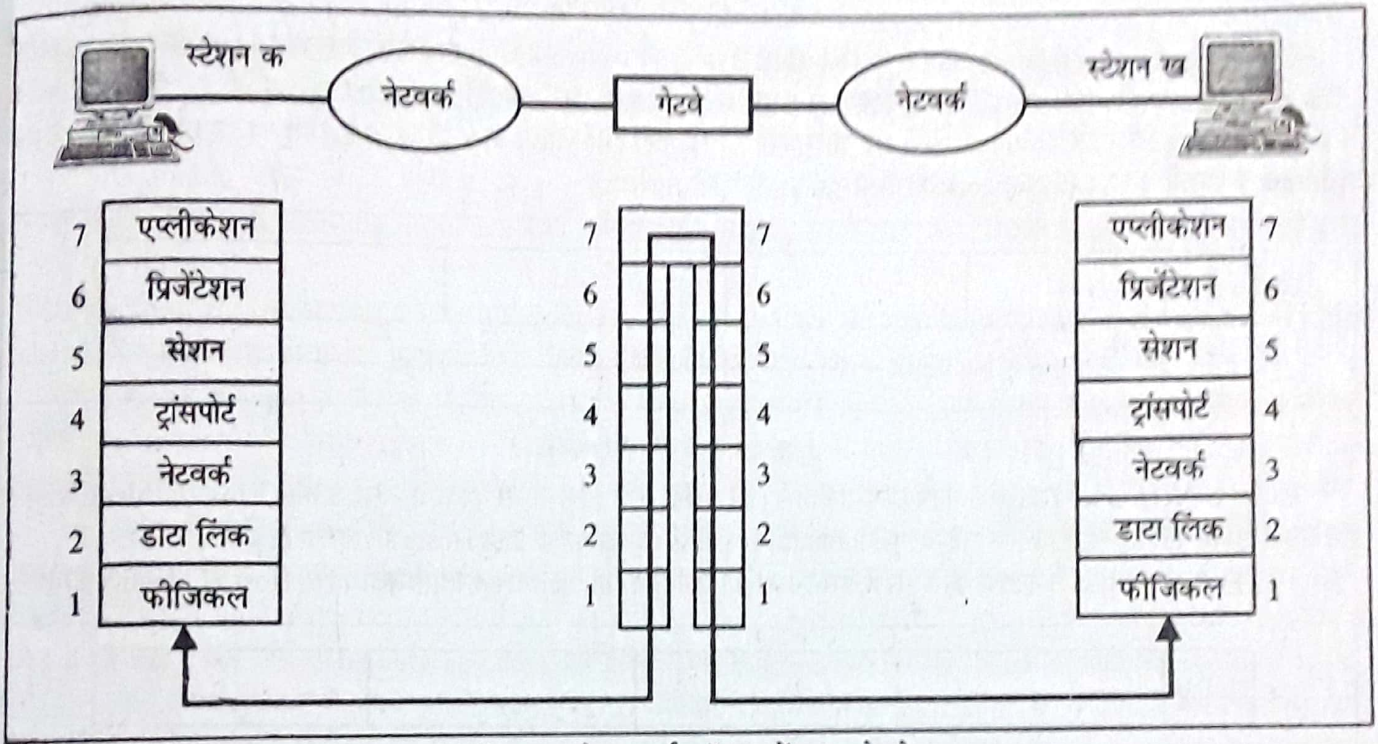
What do you understand by gateways? Explain.

उत्तर–गेटवे ऐसे उपकरण हैं जो ओएसआई मॉडल (OSI model) के सभी सात लेयरों पर कार्य करते हैं, जैसा कि अगले पृष्ठ पर दिये गये चित्र में दिखाया गया है।

Scanned by CamScanner

गेटवे को प्रोटोकॉल कन्वर्टर (Protocol Converter) भी कहा जाता है। यह एक प्रोटोकॉल (जैसे एपलटॉक) के अनुसार तैयार किये गये किसी पैकेट को स्वीकार कर सकता है और भेजने से पहले उसे किसी अन्य प्रोटोकॉल (जैसे टीसीपी/आईपी) के अनुसार तैयार किये गये पैकेट में बदल देता है। गेटवे का कार्य किसी राउटर या स्विच की तुलना में अधिक जटिल होता है।

सामान्यतया गेटवे एक सॉफ्टवेयर होता है, जो किसी राउटर में स्थापित किया जाता है। गेटवे उस राउटर से जोड़े गये प्रत्येक नेटवर्क के प्रोटोकॉल को समझता है और इसीलिए एक प्रोटोकॉल से दूसरे प्रोटोकॉल में अनुवाद करने की क्षमता रखता है। कुछ मामलों में उसे पैकेट की केवल हेडर (Header) और ट्रेलर (Trailer) सूचनाओं में सुधार करना पड़ता है। अन्य मामलों में गेटवे को पैकेट का आकार, फॉर्मेट और डाटा रेट (Data rate) भी बदलना पड़ता है।



चित्र : ओएसआई मॉडल में एक गेटवे

प्रश्न 12 – ***IP एड्रेस क्या है? क्लास A, B तथा C IP एड्रेस से आप क्या समझते हैं? किसी LAN का IP एड्रेस किस श्रेणी का होता है?***

What is IP address? What do you mean by Class A, B and C IP address? An address of a LAN belongs to which IP address class?

उत्तर–IP एड्रेस (IP Address)–IP पैकेट डिलीवरी तथा कनेक्शन विहीन सर्विस को उपलब्ध कराता है। इसके माध्यम से भेजे गये पैकेटों की कोई गारण्टी नहीं होती है। इसका प्रमुख Drawback यह है कि इसे एक Explicit एड्रेसिंग सिस्टम की आवश्यकता होती है। नेटवर्क से जुड़ी हुई प्रत्येक नोड को एक IP एड्रेस अवश्य मिलना चाहिये। यह एड्रेस दो भागों से मिलकर बना होता है–एक लॉजिकल नेटवर्क नम्बर तथा दूसरा होस्ट एड्रेस, जो इस लॉजिकल नेटवर्क के साथ होता है।

जब TCP/IP प्रोटोकॉल का प्रयोग किया जाता है, एडमिनिस्ट्रेटर को प्रत्येक Peripheral को एक लॉजिकल एड्रेस एलोकेट स्कीम के द्वारा स्टेटिक एड्रेसिंग स्कीम अवश्य परिभाषित करना चाहिये।

IP Version 4 के साथ, एक एड्रेस 4 Bytes का होता है। प्रत्येक Byte, एक Decimal Point के द्वारा अलग होती है; जैसे–131.147.65.2 First Byte की वैल्यू, IP एड्रेस क्लास को दर्शाने के लिये प्रयोग की जाती है।

भिन्न-भिन्न IP Address क्लासेस, नेटवर्क नम्बर के लिये भिन्न-भिन्न Bytes की संख्या को प्रयोग करती है। तीन IP Addresses Classes, एक होस्ट को Uniquely Identify करने के लिये परिभाषित की गयी हैं, जो निम्नलिखित हैं–

Class A Network–Class A, एड्रेस स्कीम में First Byte का प्रयोग Network Number के लिये प्रयोग किया जाता है तथा शेष तीन Bytes (24 bits) Host को Identify करने के लिये प्रयोग की जाती है। First Byte, 1 से 126 तक की Value को रखती हैं। Class A नेटवर्क में अधिकतम 6 Million Hosts (2^{24} - 2 Combinations) रखे जा सकते हैं।

Scanned by CamScanner

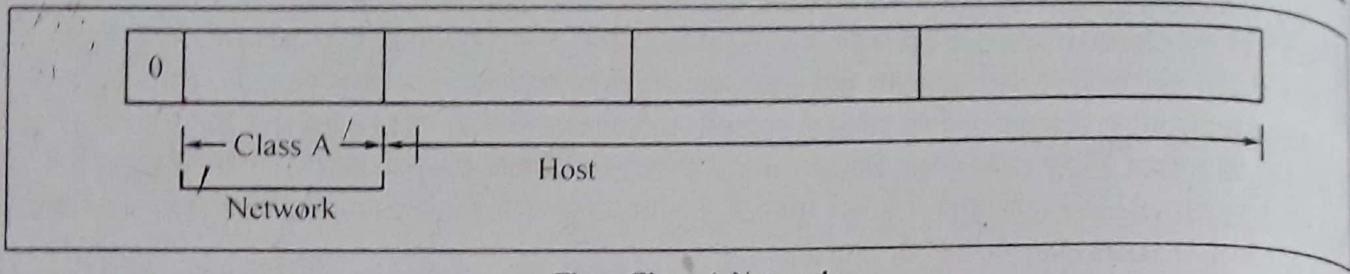


Fig. : Class A Network

Class B Network–Class B नेटवर्क में 16 bits (2 Bytes) का Network Number होता है तथा 16 bits होस्ट को Identify करने के लिये प्रयोग की जाती है। Class B नेटवर्क में प्रथम Byte 128 से 191 तक की Value को रख सकती है। Class B नेटवर्क में 65634 hosts (2^{16} – 2 Combinations) रखे जा सकते हैं। By default Mask 255.255.0.0 है; जैसे–132.147.66.2 Class B Address है जिसमें 132.147 Network को तथा 66.2 होस्ट को दर्शाता है–

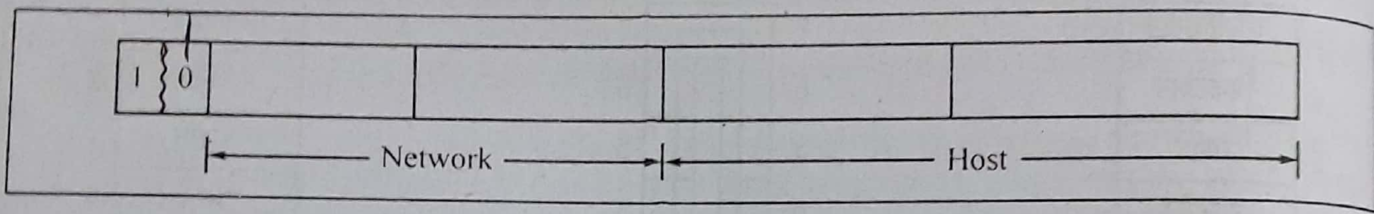


Fig. : Class B Network

Class C Network–Class C नेटवर्क में 24 bits (3 Bytes) में नेटवर्क नम्बर होता है तथा 8 bits, Host को Identify करते हैं। First Byte में 192 से 223 तक की वैल्यू हो सकती हैं। Class C नेटवर्क में 254 Hosts हो सकते हैं; जैसे–

193.11.2.116 Class B नेटवर्क का एड्रेस है, इसमें 193.11.2 नेटवर्क को Identify करता है तथा 116, Host को Identify करता है–

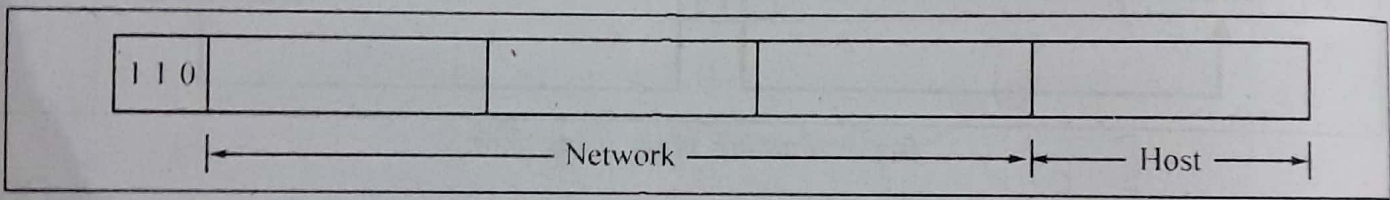


Fig. : Class C Network

सभी Classes में, एक Subnet Mask का प्रयोग किया जाता है जो Specify करता है कि कैसे IP Address को Network Part तथा Host Part में बांटता है? जब इसे Binary Notation में दर्शाया जाता है तथा Mask की Leading Bits को '1' से तथा दूसरी Bits को '0' से Mark करते हैं; जैसे–

132.148.67.2 को Binary Notation में निम्नलिखित रूप में लिख सकते हैं–

(1000010010010100.01000011.00000010)

यह Class B एड्रेस है क्योंकि इसमें First byte 132 है। ☐

प्रश्न 13 – लूप बैक एड्रेस क्या है? इनका उपयोग कब होता?

What is a loop back address? When it is used? **(Dec., 2012/Jan., 2013)**

उत्तर–**Loop back address :** Loop-back electronic signals, digital data streams या items back के flows के routing को रेफर करता है। loop back address एक विशेष IP number (127.0.0.1) होता है, जो एक मशीन के software loopback interface के लिये दिया जाता है। Loop-back इंटरफेस इससे एसोसिएट हार्डवेयर को नहीं रखता है तथा यह एक नेटवर्क से फिर्जीकल रूप में कनेक्ट नहीं होता है।

Loopback, केवल एक endpoint के साथ एक कम्यूनिकेशन चैनल है। TCP/IP नेटवर्क एक loopback को specify करता है जो same computer पर सर्वर सॉफ्टवेयर के साथ client software को कम्यूनिकेट करने की अनुमति देता है। users, loopback के लिये एक IP address (127.0.0.1) specify कर सकते हैं। Loopback address, नेटवर्क एडमिनिस्ट्रेटर को local machine को treat करने की अनुमति देता है। ☐

Scanned by CamScanner

प्रश्न 14 – *किन अवस्थाओं में राउटर निम्नलिखित ICMP मैसेजों को उत्पन्न करता है।*

Under what circumstances a router generates the following ICMP messages.

(i) Source Quench

(ii) Redirect

(iii) Destination Unreachable. **(Dec., 2012/Jan., 2013)**

उत्तर–**(i) Source Quench :** ICMP (Internet control message protocol), Internet Protocol Suite के core protocols में से एक प्रोटोकॉल है। इसे नेटवर्क से जुड़े कम्प्यूटर्स के ऑपरेटिंग सिस्टम्स के द्वारा error messages indications को भेजने के लिये प्रयोग किया जाता है। जैसे "a requested service is not available" या "a host or router could not be reached" ICMP का प्रयोग query messages को relay करने के लिये भी किया जा सकता है। इसे protocol number एसाइन किया जाता है।

जब एक router, आने वाले packets के volume को संभालने में सक्षम नहीं होता है, तब ICMP source quench मैसेज को डिजाइन किया जाता है। ICMP source quench मैसेज, इंटरनेट destination पर भेजे गये डाटा मैसेजों के traffic rate को कम करने के लिये एक रिक्वेस्ट है।

Source Quench, रिक्वेस्ट करता है कि एक router या एक होस्ट को भेजे गये messages के rate को कम किया जाये। यदि router या host, रिक्वेस्ट को प्रोसेस करने के लिये पर्याप्त बफर स्पेस को नहीं रखता है, तब यह मैसेज generate होता है।

एक particular router या नेटवर्क पर एक ही समय पर एक होस्ट से कई hosts पर काफी high speed से डाटा भेजा जाता है। यद्यपि एक router पर्याप्त क्षमता को रखता है। buffering, एक specific range के साथ सीमित होती है। Router, सीमित buffering space की क्षमता की अपेक्षाकृत ज्यादा डाटा को queue में नहीं रख सकता है। इस तरह यदि queue, पूर्ण हो जाता है तो आने वाला डाटा (Incoming data) discard हो जाता है। लेकिन नेटवर्क लेयर में acknowledgement विधि उपस्थित नहीं होती है, इसलिये क्लाइंट नहीं जान पाता है कि डाटा, destination पर पहुंच गया है या नहीं? अतः नेटवर्क लेयर को इस तरह की स्थिति को दूर करने के लिये यह तकनीकी source quench के नाम से रेफर की गयी है। source quench विधि में, router देखता है कि आने वाला डाटा, (Incoming data) जाने वाले डाटा (outgoing data) की दर से काफी तेज स्पीड से है तो एक ICMP मैसेज clients के पास भेजता है, जो यह सूचित करता है कि उन्हें अपने डाटा ट्रांसफर स्पीड को कम करना चाहिये या अधिक डाटा को भेजने से पहले समय का इन्तजार करना चाहिये। जब client इस मैसेज को प्राप्त करता है, तो यह ऑटोमेटिक रूप से जाने वाले डाटा दर (outgoing data rare) को कम कर देगा या एक पर्याप्त समय का इन्तजार करेगा जो router queue को खाली करने के लिये सक्षम बनायेगा। इस तरह source quench ICMP मैसेज नेटवर्क लेयर में flow contol की तरह कार्य करता है।

(ii) Redirect : Redirect, data packets को एक alternative route पर भेजने की request करता है। ICMP Redirect, routers के लिये routing information को hosts पर पहुँचाने (convey) के लिये एक mechanism है। Message, एक host को इसकी routing information को अपडेट करने के लिये सूचना देता है। यदि एक host, router R1 के माध्यम से डाटा को भेजने की कोशिश करता है तथा R1 डाटा को दूसरे router R2 पर भेजता है तथा एक direct path R2 से उपलब्ध है। (अर्थात host तथा R2, एक ही ethernet segment पर हैं) तो R1 एक redirect message भेजता है जो host को inform करता है कि destination के लिये best route, R2 के माध्यम (via) से है। तत्पश्चात् host को destination के लिये सीधे तौर R2 को packets भेजने चाहिये।

(iii) Destination unrechable : Destination unreachable, host या इसके अंतर्गत gateway के द्वारा जनरेट किया जाता है। यह client को इनफॉर्म करता है कि destination, कुछ कारणों से unreachable है। Destination unreahable, TCP, UDP या दूसरे ICMP ट्रांसमीशन के रिजल्ट के रूप में जनरेट किया जा सकता है।

Destination unreachable message यह indicate करता है कि एक frame, discard हो गया था क्योंकि यह इसके ultimate destination पर नहीं पहुँच सका। Destination unreachable message के निम्नलिखित कारण हो सकते हैं–

(i) Network unreachable

(ii) Host unreachable

(iii) Port unreachable

(iv) Protocol unreachable

(v) Fragmentation needed and 'Don't fragment' bit set

(vi) Source route failed

❑

Scanned by CamScanner

प्रश्न 15 – *FTP के विभिन्न ट्रांसफर मोड क्या हैं? संक्षेप में समझाइये।*

What are the various transmission modes of FTP? Explain briefly.

(Dec., 2012/Jan., 2013)

उत्तर–FTP में transmission mode निम्नलिखित हैं–

(i) Stream Mode : इस मोड में डाटा, bytes की stream के रूप में भेजा जाता है। Sending device साधारणतः डाटा को TCP पर रिसीवर के पास push करती है। इसमें distinct header fields के साथ कोई मैसेज फॉर्मेट का प्रयोग नहीं किया जाता है।

(ii) Block Mode : यह अत्यधिक Convential डाटा ट्रांसमीशन मोड है। इसमें डाटा, blocks के रूप में विभाजित किया जाता है तथा व्यक्तिगत FTP blocks या records के रूप में encapsulate करके ट्रांसमिट किया जाता है। प्रत्येक रिकॉर्ड 3-byte हैडर को रखता है जो इसकी length को indicate करता है तथा भेजे जाने वाले data blocks के बारे में इनफॉरमेशन को रखता है।

(iii) Compressed Mode : इस मोड में डाटा को compress करके भेजा जाता है। इस मोड में पहले डाटा को compress किया जाता है, इसके पश्चात् block Mode की तरह ट्रांसमिट किया जाता है। ❑

प्रश्न 16 – *802.11 wireless communication protocol को समझाइये।*

Explain 802.11 wireless communiation protocol.

उत्तर–IEEE 802.11 protocol, wireless stations तथा wired networking infrastructures के बीच में कनेक्टिविटी उपलब्ध कराने के लिये नेटवर्क एक्सेस टैक्नोलॉजी है। 802.11 लॉजिकल आर्किटेक्चर कई महत्वपूर्ण कम्पोनेन्ट्स जैसे–Station (STA), Wireless Access Point (AP), Independent Basic Service Set (IBSS), Basic Service Set (BSS), Distribution System (DS) तथा Extended service set (ESS) को रखता है। 802.11 लॉजिकल आर्किटेक्चर कुछ कम्पोनेंन्ट्स सीधे तौर पर हार्डवेयर डिवाइस जैसे–STA तथा Wireless APs से map करते हैं। wireless STA, एक adapter card, PC Card या एक embedded device wireless कनेक्टिविटी उपलब्ध कराने के लिये रखता है। wireless AP Functions, नेटवर्क एक्सेस के लिये wireless STAs तथा existing Network bakbone के बीच में एक bridge के रूप में कार्य करता है।

IBSS एक wireless network है, जो कम से कम दो STAs का प्रयोग करता है। इसे adhoc wireless network के नाम से भी जाना जाता है।

BSS एक wireless network है, जो एक single wireless AP से मिलकर बना होता है। यह एक या एक से अधिक wireless clients को सपोर्ट करता है। BSS को Infrastructure wireless नेटवर्क के नाम से भी जाना जाता है। BSS में सभी STAs, AP के माध्यम से कम्यूनिकेट करते हैं।

ESS, दो या दो से अधिक wireless APs का सेट होता है, जो same wired network से कनेक्ट होता है तथा यह एक single logical network को परिभाषित करता है। निम्नलिखित Fig. में 802.11 wireless architecture को चित्रित किया गया है–

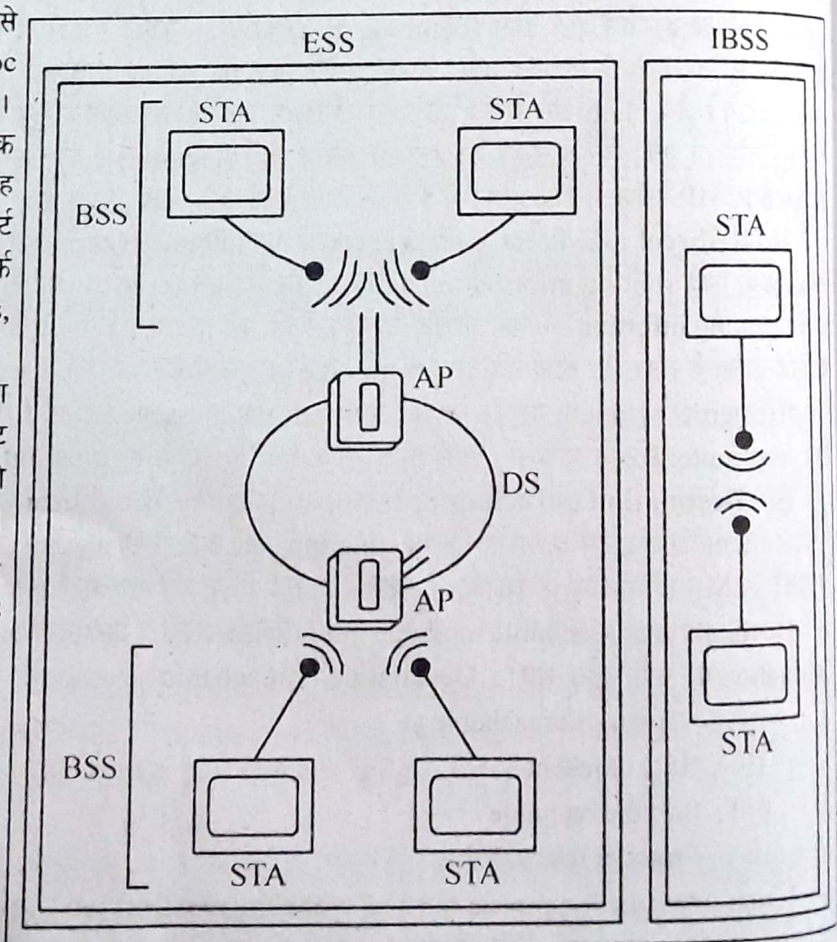


Fig : 802.11 Wireless architecture

IEEE 802.11 निम्नलिखित operating modes को परिभाषित करता है–

- Infrastructure mode
- Adhoc mode

दोनों operating modes में एक service set identities (SSID), Wireless network को identify करता है, इसे wireless network name से भी जाना जाता है।

Infrastructure mode में कम से कम एक wireless AP तथा एक wireless client होता है।

Wireless client, एक traditional network के resources को एक्सेस करने के लिये wireless AP का प्रयोग करता है। Traditional wired network, एक ऑर्गेनाइजेशन intranet या internet हो सकती है।

Adhoc mode में wireless clients, wireless AP के बिना एक दूसरे के साथ directly कम्यूनिकेट कर सकते हैं। ❑

प्रश्न 17 – *IPV4 Addressing क्या होता है? इसे कैसे denote किया जाता है? कैसे Binary notation से dotted notation में convert किया जाता है?*

What is IP-Addressing? How it is denoted? How to convert Binary notation to dotted notations?

उत्तर–IPV4 addressing–एक IP address एक identifier होता है, जो एक Interface या Interface के सेट को इंटरनेट लेयर पर assign किया जाता है। प्रत्येक IP address, IP Packets के source या destination को identify कर सकता है। IPV4 के लिये एक नेटवर्क पर प्रत्येक नोड एक या एक से अधिक interfaces को रखती है तथा हम प्रत्येक interface को TCP/IP enable कर सकते हैं। जब हम एक interface पर TCP/IP enable करते हैं, तो हम एक या एक से अधिक logical IPV4 addresses को assign करते हैं। ये addresses, automatically या manually assign किये जा सकते हैं। IPV4 एक logical address है, क्योंकि यह इंटरनेट लेयर पर assign किया जाता है। तथा उन addresses से relation नहीं रखता है, जो network interface layer पर प्रयोग किये जाते हैं। IPV4 addresses 32 bits के होते हैं। यदि IPV4 addresses को binary notation का प्रयोग करके express करते हैं तो प्रत्येक address, 1 तथा 0 की 32 digit string में प्रकट होगा।

क्योंकि binary strings में address को express करना तथा याद रखना कठिन होता है इसलिये इसे dotted decimal में express करते हैं।

जैसे–

11000000 10101000 00000011 00011000 का IPV4 address, 192.168.3.24 dotted decimal notation में express होता है।

Dotted decimal notation में four decimal numbers (0 to 255) को dots (periods) से अलग किया जाता है। प्रत्येक decimal number, एक octet के नाम से जाना जाता है तथा 32-bit address को 8 bits (1 byte) को रिप्रजेन्ट करता है।

IPV4 address को binary notation से dotted decimal notation में convert करने के लिये निम्नलिखित steps को follow करते हैं।

Step 1 : 8-bit blocks में इसे segment करते हैं।

11000000 10101000 00000011 00011000

Step 2 : प्रत्येक block को decimal में convert करते हैं।

192 168 3 24

Step 3 : Blocks को periods (dots) से separate करते हैं।

192.168.3.24

जब IPV4 address को रेफर करते हैं, तब w.x.y.z notation का प्रयोग कर सकते हैं। निम्नलिखित Fig. में IPV4 address structure को दर्शाया गया है–

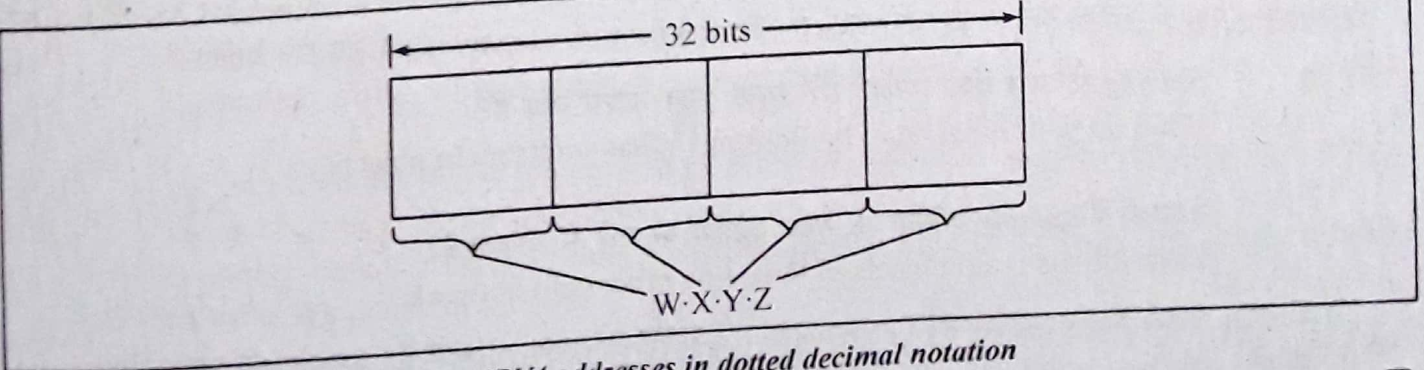


Fig : IPV4 addresses in dotted decimal notation ❑

प्रश्न 18 – *Wireless LAN के लाभ तथा हानियाँ क्या हैं? स्पष्ट कीजिये।*

What are the advantages and disadvantages of wireless LAN? Clarify.

उत्तर–Wireless LAN के लाभ (Advantages of Wireless LAN)–Wireless LAN के प्रमुख लाभ निम्नलिखित हैं–

1. Wireless LAN में व्यक्ति जहां से चाहता है, वहां से एक्सेस कर सकता है, इसमें Cable की लम्बाई की किसी सीमा की आवश्यकता नहीं होती है।

2. Wireless LAN's के माध्यम से व्यक्ति अपने कार्यस्थल क्षेत्र से बाहर के इंटरनेट में एक्सेस कर सकता है। अधिकतर organizations, shopping complexes इत्यादि wi-fi की सुविधा को उपलब्ध कराते हैं यदि कोई व्यक्ति shopping complex में shopping करते-करते अपने mobile में इंटरनेट से कनेक्ट होना चाहता है तो वह एक्सेस कर सकता है इसके लिये उस shopping complex में wi-fi की सुविधा होनी चाहिये तथा mobile में भी यह सुविधा होनी चाहिये।

3. Wireless LAN को एक बॉक्स के द्वारा setup कर सकते हैं। इस बॉक्स को Access Point कहते हैं। यह बॉक्स एक समय में कई कनेक्शनस् को हैण्डल कर सकता है।

4. Access points, कई Computers को यह सुविधा serve कर सकते हैं।

Wireless LAN की हानियाँ (Disadvantages of Wireless LAN)–Wireless LAN की प्रमुख हानियाँ निम्नलिखित हैं–

1. Wireless LAN's कम्यूनिकेशन के लिये radio waves का प्रयोग करते हैं। इसलिये Encrypt इनफॉरमेशन को संभालने के लिये ज्यादा care की जरूरत होती है।

2. इसमें signal ज्यादा खराब हो जाते हैं तथा error connection के लिये अधिक bandwidth को खर्च करने की जरूरत होती है।

3. Range को बढ़ाने के लिये अधिक access points की जरूरत होती है।

4. Wireless LANs, Wired LANs की अपेक्षाकृत slow होते हैं। ❑

प्रश्न 19 – *Wireless LAN पर संक्षिप्त टिप्पणी लिखिये।*

Write short notes on the wireless LAN.

या

Wireless Lan की क्रियाविधि को समझाइये।

Explain the process of wireless LAN.

उत्तर–Wireless LAN–Wireless LAN, radio signlas या infrared signals का प्रयोग करके short distances में जुड़े हुये nodes के ऊपर कम्यूनिकेशन को उपलब्ध कराने की तकनीक है। इसे wi-fi के नाम से भी जाना जाता है। Wireless LANs को access point डिवाइस के माध्यम से तैयार किया जाता है। Wireless LAN का उद्देश्य भी wired LAN की तरह ही सेवाओं को उपलब्ध कराना है। Wireless LAN में कीमती wiring की आवश्यकता नहीं होती है। सामान्यतः इसे setup करना सस्ता तथा आसान होता है। Wireless LAN को radio frequency (RF) टैक्नोलॉजी का प्रयोग करके ऑपरेट किया जाता है। जब RF current को एक एन्टिना को supply किया जाता है तो एक eletromagnetic field को क्रिएट होता है तब यह space के माध्यम से propagate करने में सक्षम होता है।

Wireless LAN में एक डिवाइस का प्रयोग किया जाता है, जिसे Access Point (AP) कहते हैं। इस डिवाइस प्रारम्भिक कार्य wireless सिग्नल को broadcast करना है, जिन्हें कम्प्यूटर्स डिटेक्ट करते हैं तथा ग्रहण करके इम्पलीमेन्ट करते हैं। Wireless LAN को Join करने तथा Access Point से कनेक्ट होने के लिये कम्प्यूटर्स से Wireless network adapters अवश्य जुड़े होने चाहिये। ❑

प्रश्न 20 – *Routing से आप क्या समझते हैं? इसके मुख्य उद्देश्य क्या हैं?*

What do you understand by Routing? What are its main objects?

या

नेटवर्क में Routing प्रक्रिया के मुख्य उद्देश्यों के बारे में समझाइये।

Describe the main objects of Rounting process in network.

उत्तर–एक नेटवर्क में एक packet को forward करने की प्रक्रिया को routing कहते हैं। Routing के प्रमुख उद्देश्य (goals) निम्नलिखित हैं।

(i) Correctness–Routing, proper तथा correct होनी चाहिये ताकि packets अपने proper destination पर पहुंच सके।

Scanned by CamScanner

2. Simpliity–Routing एक साधारण तरीके से होनी चाहिए ताकि overhead उतना कम हो जितना संभव हो। Routing algorithms की complexity के बढ़ने के साथ ही overhead भी बढ़ जाता है।

3. Robustness–एक बार major network ऑपरेटिव हो जाता है, तो इससे काफी सालों तक बिना किसी faliures के लगातार (Continiously) run करने की आशा की जा सकती है। Routing के लिये डिजाइन किये गये algorithms, robust होने चाहिये।

4. Stability–Routing algorithms सभी संभव परिस्थितियों में stable होने चाहिये।

5. Fairness–नेटवर्क से जुड़ी हुई प्रत्येक नोड अपने packets को ट्रांसमिट करने के लिये fair chance को प्राप्त करनी चाहिये। साधारणतयः यह first come first serve आधार पर होता है।

6. Optimality–Routing algorithms, packet delay minimizing तथा throughput के term में optimal होने चाहिये। ❑

प्रश्न 21 – *Routing Algorithm के वर्गीकरण को समझाइये।*
State the classification of routing algorithm.

या

Routing Algorithm को किन-किन रूपों में इम्पलीमेन्ट किया जा सकता है।
In which forms the routing algorithm can be implemented?

उत्तर–Routing Algorithm को निम्नलिखित रूपों में विभाजित किया जाता हैं

1. Adaptive Routing Algorithm
2. Non-Adaptive Routing Algorithm

1. Adaptive Routing Algorithm–ये algorithms अपने routing decisions के बदलाव को topology में reflet करते हैं। ये अपनी routing information को adjacent routers से प्राप्त करते हैं। इन्हें पुनः निम्नलिखित types में वर्गीकृत किया जा सकता है।

(a) Centralized–इस type के algorithm में नेटवर्क में कुछ Central node, नेटवर्क टॉपोलॉजी के बारे में संपूर्ण इनफॉरमेशन प्राप्त करते हैं। इसके पश्चात् यह इनफॉरमेशन routers को ट्रांसमिट की जाती है।

(b) Isolated–इस मैथड में node, दूसरी nodes से इनफॉरमेशन को प्राप्त किये बिना route का निर्णय लेती है। इसका लाभ यह है कि इनफॉरमेशन को रखने के लिये केवल एक node की आवश्यकता होती है।

2. Non-Adaptive Routing Algorithm–ये algorithms, current traffic तथा टॉपोलॉजी के estimate तथा measurement पर अपने routing decisions के base को नहीं रखते हैं। इसे static routing भी कहते हैं। इसे पुनः निम्नलिखित types में वर्गीकृत किया जा सकता है।

(a) Flooding–इस तकनीकि में प्रत्येक incoming packet को प्रत्येक outgoing line पर भेजा जाता है। इसमें उस node को छोड़ दिया जाता है, जिस node पर इसका आगमन होता है।

(b) Random Walk–इस मैथड में एक packet को node के द्वारा अपने पड़ोसी node के पास randomly भेजा जाता है। यह algorithm, highly robust है। ❑

प्रश्न 22 – *Shortest Path Routhing Algortilım को समझाइये। Dijkstra algorithm का प्रयोग करके nodes के बीच में shortest path को उदाहरण सहित समझाइये।*
Describe the shortest path routing algorithm. Describe the shortest path in nodes using dijkstra algorithm with example.

या

एक graph में nodes के मध्य shortest path को ज्ञात करने के लिये Diskstra Algorithm का प्रयोग करके shortest path algorithm को समझाइये।
Describe shortest path algorithm using dijkstra algorithm for knowing the shortest path between the nodes in a graph.

उत्तर–Shortest path routing algorithm एक साधारण routing algorithm है। इस तकनीकि को समझना आसान है। इस तकनीकि में subnet का एक graph बनाते हैं, इसमें graph की प्रत्येक नोड एक router को रिप्रजेन्ट करती है तथा प्रत्येक arc एक कम्यूनिकेशन लाइन या लिंक को रिप्रजेन्ट करती है। Routers के pair के बीच में route को find करने के लिये, algorithm shortest path को find

Scanned by CamScanner

करता है। एक graph के दो nodes के बीच में shortest path को कम्प्यूट करने के लिये कई प्रकार के algorithms हैं इसमें से सबसे अधिक प्रयोग किया जाने वाले algorithm, Dijkstra algorithm है।

इस algorithm में प्रत्येक node एक label रखती है जो source node से इसकी distance को रखती है। इन labels के आधार पर algorithm node को दो sets tentative तथा permanent में विभाजित करता है। शुरुआत में कोई किसी path के बारे में जानकारी नहीं होती है, इसलिये सभी labels tentative होते हैं। यह algorithm निम्नलिखित steps के अनुसार कार्य करता है।

Step 1 : Current node (T-node) के रूप में soure node को mark करते हैं।

Step 2 : T-node के सभी neighbours को find करते हैं तथा इन्हें tentative बनाते हैं।

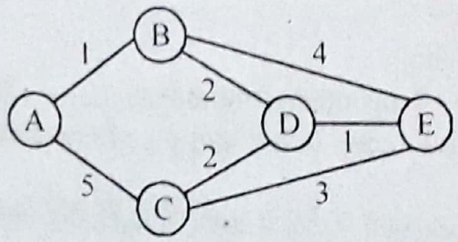
Step 3 : अब सभी neighbour को examine करते हैं।

Step 4 : इन सभी node के बीच में एक node को permanent के रूप में label करते हैं तथा इसे T-node mark करते हैं। permanent node वह node होती है, जिसका weight सबसे कम होता है।

Step 5 : यदि destination node पर पहुंच जाते हैं या tentative list empty है तो stop हो जाते हैं अन्यथा पुनः step 2 से follow करना शुरू करते हैं।

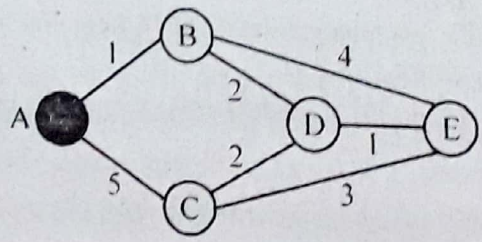
निम्नलिखित उदाहरण में Dijkstra routing algorithm को स्पष्ट रूप से समझाया गया है।

उदाहरण :

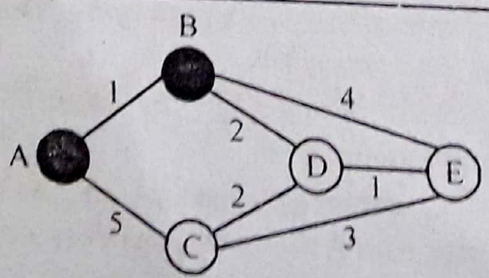


इसमें node A से node E के बीच में shortest path को find करना चाहते हैं, इसके लिये निम्नलिखित steps को follow करते हैं।

Step 1 : यहां पर soure node (A) को T-node के रूप में चुनते हैं, इसका label permanent है। जैसा कि निम्नलिखित fig में दर्शाया गया है।

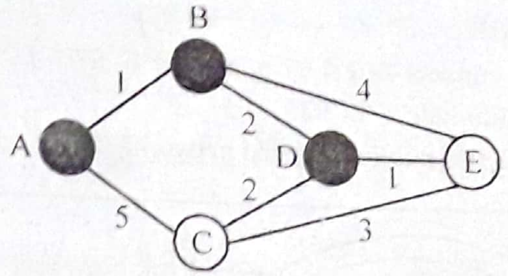


Step 2 : इस step में B तथा C Tentative nodes जो सीधे तौर पर T-node (A) से लिंक हैं। इन nodes में B node का weight कम है अतः इसे T-node चुनते हैं तथा इसका label, permanent के रूप में change करते हैं।

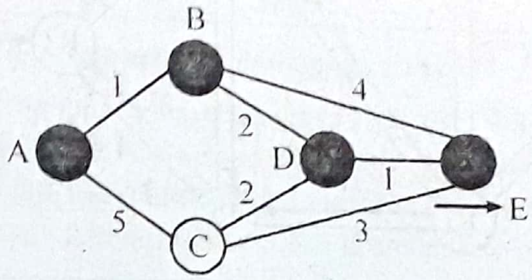


Scanned by CamScanner

Step 3 : इस step में D तथा E nodes tentative nodes हैं, जो सीधे तौर पर T-node (B) से लिंक है। इन nodes के बीच में D node का weight कम है, अतः इसे T-node चुनते हैं तथा इसका label, permanent के रूप में बदल जाता है।



Step 4 : इस Step में C,E tentative nodes हैं, जो directly T-node (D) से लिंक है। इस nodes में E node का weight less है। अतः इसे T-node के रूप में चुनते हैं तथा इसका label permanent में Change करते हैं।



Step 5 : E, destination node है, अतः हम destination node पर हैं, इसलिये यह रुक जाते हैं।

Shortest path A → B → D → E है। ❑

प्रश्न 23 – *Distance vector Routing से आप क्या समझते हैं? उदाहरण सहित स्पष्ट कीजिये।*

What do you understand by Distance vector routing? Clarify with example.

Or

Distance Vector Routing Algorithm को उदाहरण सहित समझाइये।

Describe distance vector routing algorithm with example.

उत्तर–Distance Vector Routing–आज के समय में Computer networks सामान्यतः static routing algorithm की अपेक्षाकृत dynamic routing algorithm का प्रयोग करते हैं। Distance Vector routing, dynamic routing algorithm का इम्पलीमेन्टेशन है। इसे Belman-ford routing algorithm भी कहते हैं। इस algorithm में दी गयी source node से destination node तक shortest path को find करते हैं। इस algorithm का वर्णन निम्नलिखित हैं।

s=source node

w (i,s) = i, node से j node तक link cost

w(i,j) = ∞ ,यदि दो nodes directly connected नहीं है।

w(i, j) ≥ 0, यदि दो nodes directly connected हैं।

h = algorithm के current stage पर एक path में links की अधिकतम संख्या।

Lh(n) = s node से n node तक least cost path की cost

Step 1 : [Initialisation]

L0 (n) = ∞ , for all $n \neq s$

$Lh(s) = 0$ for all h

Scanned by CamScanner

Step 2 [update]

for each successive $h \geq 0$;

for each $n \neq s$; compute

$L_{h+1}(n) \min_j [lh(j) = w(j,n)]$

n को इसकी predecessor node j से connect करते हैं जो minimum को प्राप्त करती है तथा एक भिन्न predecessor node के साथ n के किसी भी connection को eliminate करती है।

निम्नलिखित table इस algorithm को एक public switched network पर s = 1 apply किये गये result को दर्शाती हैं।

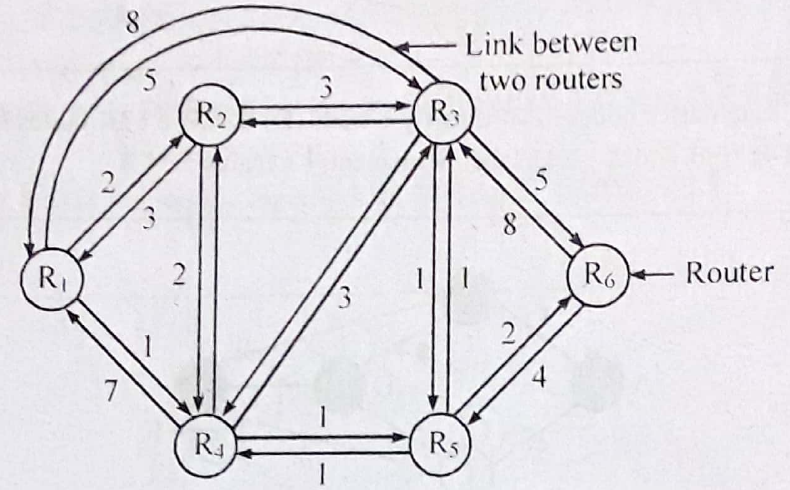


Fig : Public switched networks

प्रत्येक step पर links के अधिकतम संख्या के साथ least-cost paths, h से equal find हुये हैं। Find iteration के पश्चात् प्रत्येक node का least-cost path तथा उस path के cost को डेवलप किया गया है। Same procedure को node 2 के साथ source node के रूप में प्रयोग किया जा सकता है।

H	Ln(2)	Path	Ln(3)	Path	Ln(4)	path	Ln (5)	Path	Ln(6)	Path
0	∞	–	∞	–	∞	–	∞	–	∞	–
1	2	1–2	5	1–3	1	1–4	∞	–	∞	–
2	2	1–2	4	1–4–3	1	1–4	2	1–4–5	10	1–3–6
3	2	1–2	3	1–4–5–3	1	1–4	2	1–4–5	4	1–4–5–6
4	2	1–2	3	1–4–5–3	1	1–4	2	1–4–5	4	1–4–5–6

Table : Link Cost

❑

प्रश्न 24 – Multi cast Routing को उदाहरण सहित समझाइये।

Describe the Multi Cast Routing with example.

या

Multicast Routing का प्रयोग कहां और कैसे करते हैं?

Where does we use the multicast routing and how?

उत्तर–Multicast Routing–बहुत सारे cases में हमें same time पर multiple clients को डाटा send करने की जरूरत होती है। इस case में यदि हम unicasting routing का प्रयोग करते हैं तो server, इसके clients में से प्रत्येक Client को बार-बार connect करेगा लेकिन प्रत्येक बार यह प्रत्येक client के पास एक identical data stream को भेजेगा। यह server तथा network दोनों की capacity की wasting है। यदि इस case में हम bradcasting routing का प्रयोग करते हैं तो यह inefficient होगा क्योंकि कभी-कभी receivers, message में interested नहीं होते हैं ये इन्हें अनावश्यक रूप में रिसीव करते हैं लेकिन देखने के लिये बाध्य नहीं होते हैं।

Scanned by CamScanner

इस तरह के case में अर्थात् एक मैसेज को users (clients) के groups को भेजने के लिये हम दूसरी techniques का प्रयोग करते हैं। इस technique को multicasting कहते हैं तथा multicasting के लिये प्रयोग किये जाने वाले routing algoritum को multicost routing कहते हैं।

Multicasting की क्रियाविधि (working) को स्पष्ट रूप से समझने के लिये एक उदाहरण लेते हैं। निम्नलिखित fig में एक उदाहरण को दर्शाया गया है।

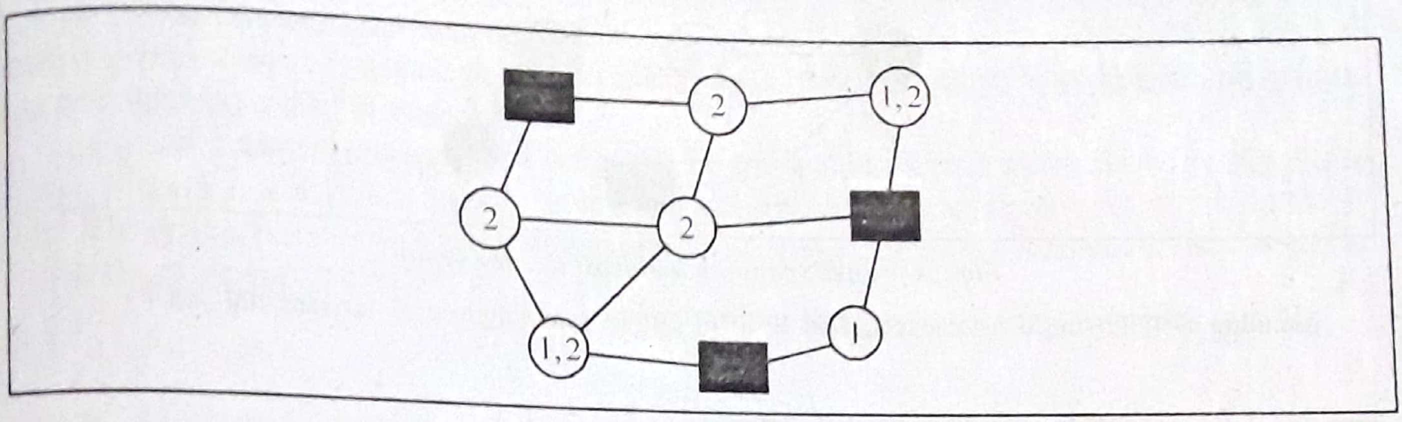


Fig : Network Containing two groups (1, 2)

इसमें हमने एक नेटवर्क लिया है जो दो groups (group1 तथा group 2) को रखता है। यहां हमने कुछ routers को hosts के लिये attach किया है जो इन groups में से केवल एक के साथ belong करता है तथा कुछ routers hosts से attach है जो इन groups के दोनों से belong करते हैं। Multicast routing के लिये सर्वप्रथम प्रत्येक routers दूसरे सभी routers के लिये एक spanning tree covering को compute करता है। जैसे निम्नलिखित fig leftmost router के लिये spanning tree को दर्शाती है।

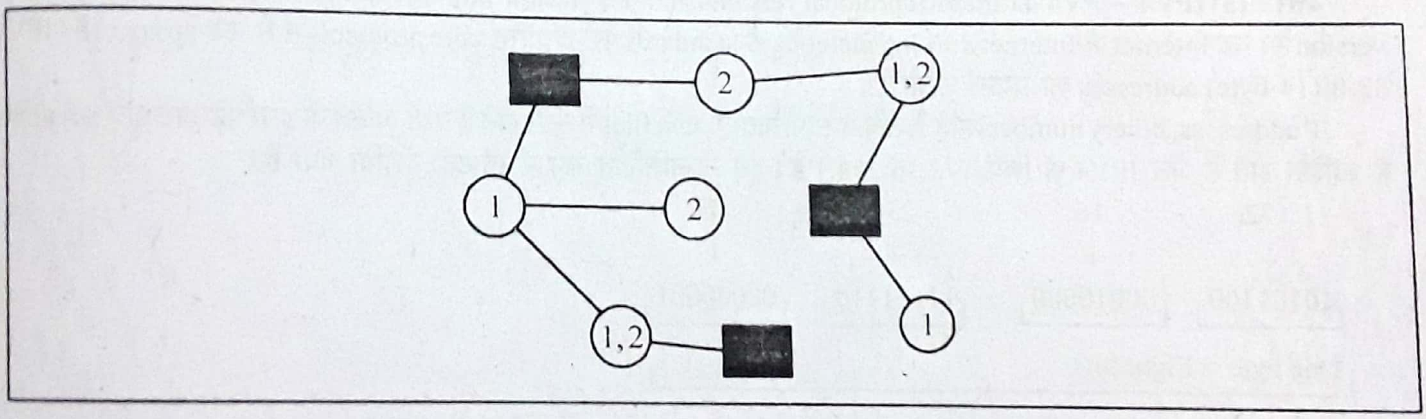


Fig : Spanning tree for left most router

अब, जब एक प्रोसेस, एक group को एक multicast packet भेजता है, तो प्रथम router इसके spanning tree को examine करता है तथा prunes करता है। Pruning, सभी lines को रिमूव करने की प्रक्रिया है जो उन hosts को read नहीं करती है, जो group के members हैं। निम्नलिखित fig group 1 के लिये pruned spanning tree को दर्शाती है।

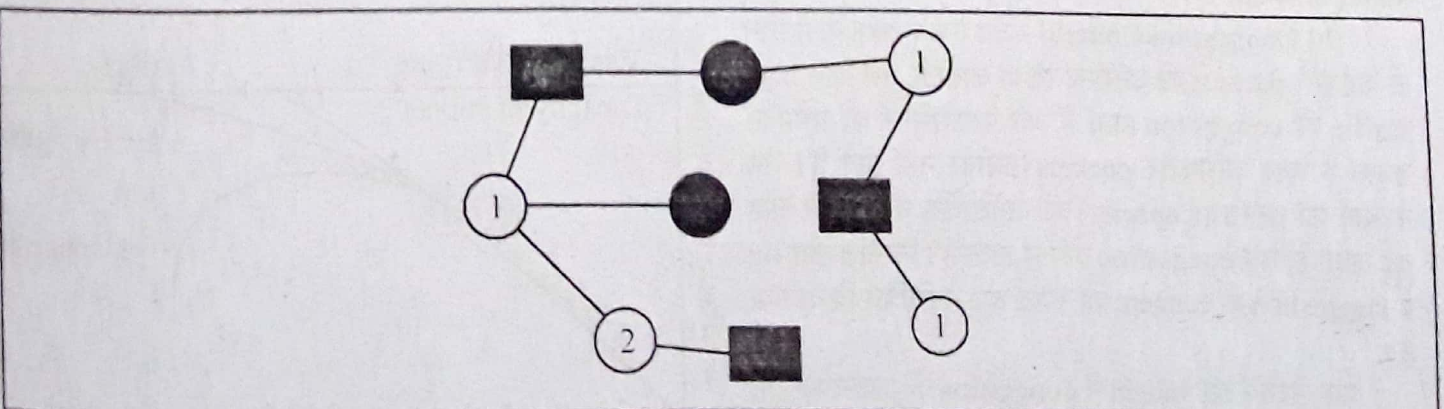


Fig : A pruned spanning multicast tree for group 1

Scanned by CamScanner

निम्नलिखित group 2 के लिये pruned spanning tree को दर्शाती है।

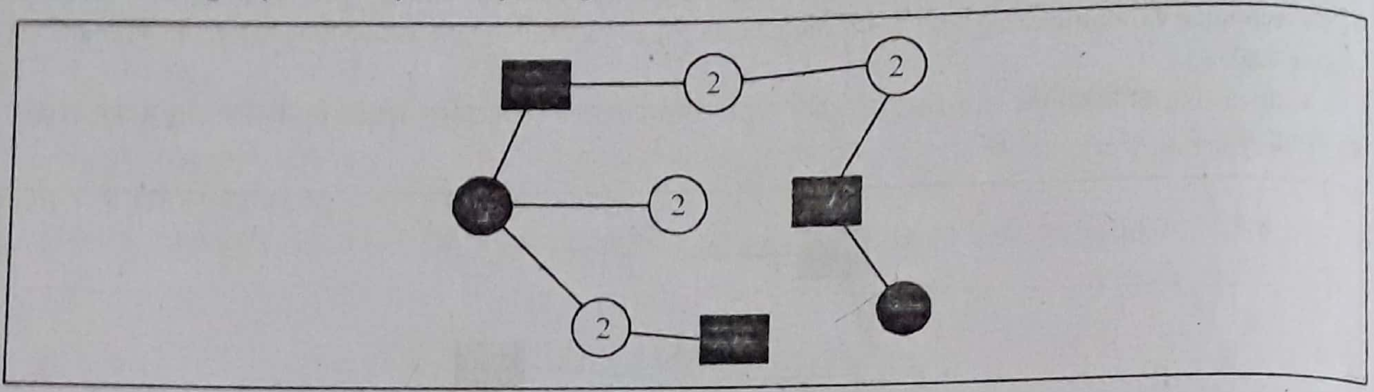


Fig : A pruned spanning multicast tree for group 2

prunning के पश्चात् multicast packets, केवल सम्बन्धित उपर्युक्त spanning tree को forward किये जाते हैं।

प्रश्न 25 – *निम्नलिखित पर संक्षिप्त टिप्पणी लिखिये।*

Write the brief note on the following :

(a) IPV4

(b) Congestion Control

(c) Traffic Shaping

उत्तर–(a) IPV4–IPV4 को Internet protocal version4 के नाम से भी जाना जाता है। यह Internet protocal (IP) का fourth version है। यह Internet के Internetworking methods के standards पर आधारित core protocols में से एक protocol है। IPV4 32-bit (4-byte) addresses का प्रयोग करता है।

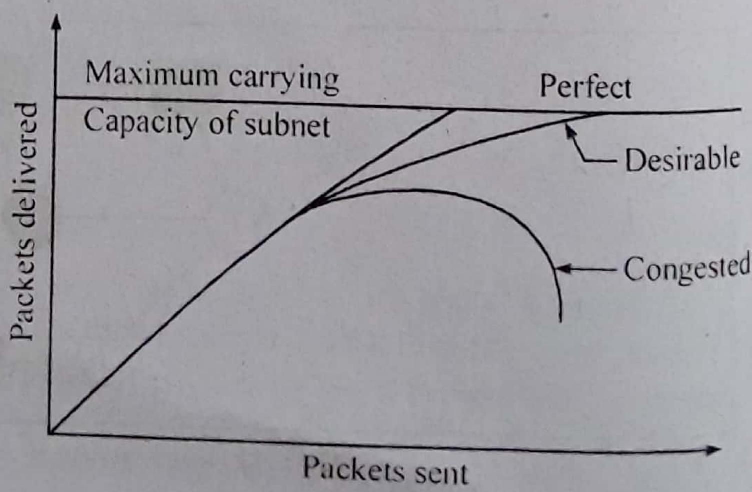
IP addresses, binary numbers होते हैं लेकिन सामान्यतः ये text files में स्टोर होते हैं तथा व्यक्ति के द्वारा पढ़े जाने वाले notations में प्रदर्शित होते हैं जैसे IPV4 के लिये 172.16.254.1 है। इसे निम्नलिखित रूप में स्पष्टतः दर्शाया गया है।

```
   172    .    16    .    254    .    1
    ↓          ↓           ↓          ↓
10101100 . 00010000 . 11111110 . 00000001
One byte = Eight bits
```

Thirty-two bits (4×8) या 4 bytes

IPV4 addresses को dot decimal notation में रिप्रजेन्ट किया जाता है, जो चार decimal numbers से मिलकर बना होता है। प्रत्येक की range 0 to 255 होती है। तथा इन्हें dots (.) से अलग किया जाता है। जैसे–172.16.254.1 प्रत्येक part address के 8 bits के एक group को रिप्रजेन्ट करता है। कुछ cases में IPV4 addresses को hexadecimal, octal या binary representations में रिप्रजेन्ट किया जा सकता है।

(b) Congestion Control–जब एक नेटवर्क के माध्यम से कई सारे packets को ट्रांसमिट किया जाता है, तब बहुत high traffic पर congestion होता है, जो परफॉरमेन्स को प्रभावित करता है तथा अधिकतर packets डिलीवर नहीं होते हैं। जब नेटवर्क की क्षमता (Capacity) की अपेक्षाकृत नेटवर्क पर लोड बढ़ जाता है, तब congestion उत्पन्न होता है। निम्नलिखित fig में congestion के concept को स्पष्ट रूप से चित्रित किया गया है।



एक नेटवर्क या subnet में congestion के उत्पन्न होने के प्रमुख कारण निम्नलिखित हैं।

Scanned by CamScanner

1. Output lines की क्षमता (Capacity) से अधिक Input rate traffic बढ़ जाता है।
2. Routers इतने slow होते हैं कि tasks को परफॉर्म करने में ज्यादा समय लेते हैं।
3. Routers के buffer सीमित हैं।
4. Slow links के द्वारा भी congestion उत्पन्न होता है।

(C) Trafic Shaping—Traffic shaping, एक नेटवर्क पर परफॉरमेन्स को optimize तथा traffic को मैनेज करने की एक strategy है। क्योंकि अधिकतर networks, bandwidth की एक सीमित मात्रा को रखते हैं इसलिये एक प्रभावी रणनीति की जरूरत होती है जो नेटवर्क को ओवरलोड न होने की सुनिश्चितता को दर्शाती है। कम्प्यूटर नेटवर्क ट्रेफिक कभी-कभी एक नेटवर्क को इतना व्यस्त कर सकता है कि इसकी परफॉरमेन्स प्रभावित हो सकती है।

Networks पर इनफॉरमेशन packets के रूप में भेजी जाती है, यह डाटा के blocks के रूप में प्रारूपित होती है। इन data packets को भिन्न-भिन्न priority level दिया जा सकता है, जो परफॉरमेन्स को optimize करने के क्रम में एक नेटवर्क पर निर्धारित होता है। Traffic shaping को packet shaping के नाम से भी जाना जाता है। अतः Trafic shaping, दी गयी priority के आधार पर packets की परफॉरमेन्स को बढ़ाने की एक तकनीकि है। ☐☐

Scanned by CamScanner

UNIT-IV

प्रश्न 1 – *निम्न पर संक्षिप्त टिप्पणी लिखिए–*

Write short notes on the following :

(a) SMTP

(b) TELNET

(c) FTP **(Dec., 2012/Jan., 2013)**

उत्तर (a) SMTP : SMTP का पूरा नाम Simple Mail Transfer Protocol है। प्रोटोकॉल एक सॉफ्टवेयर है जिसके अन्दर कुछ नियमों का समूह होता है जो इंटरनेट या नेटवर्क पर एक सिस्टम से दूसरे सिस्टम पर Data को ट्रांसफर करता है। सिस्टम में E-mail सुविधा को क्रियान्वित करने के लिये प्रयोग किया जाने वाला यह मुख्य प्रोटोकॉल है। इस प्रोटोकॉल की सहायता से Mail एक सिस्टम से दूसरे सिस्टम तक पहुँचती है। यह प्रोटोकॉल TCP/IP प्रोटोकॉल Stock का एक सदस्य है। SMTP E-mail में ASCII Character set का उपयोग करता है। एक सिस्टम से दूसरे सिस्टम तक Mail को पहुँचाने का विवरण इस प्रोटोकॉल की सहायता से पूरा किया जाता है।

(b) Telnet : इंटरनेट तथा इसके TCP/IP प्रोटोकॉल का मुख्य कार्य यूजर्स के लिये सुविधायें उपलब्ध कराना है; जैसे–यूजर्स, रिमोट साइट पर विभिन्न एप्लीकेशन प्रोग्रामों को रन करना चाहते हैं तथा रिजल्ट को जनरेट करता है जिसे इनके लोकल साइट पर ट्रांसफर किया जा सकता है। Telnet का प्रयोग रिमोट टर्मिनल इम्यूलेशन के लिये किया जाता है। यह यूजर के लिये होस्ट पर आधारित एप्लीकेशन्स के लिये यूजर को एक्सेस करने की क्षमता प्रदान करता है। Telnet, dissimilar ऑपरेटिंग सिस्टम के मध्य कनेक्टिविटी को उपलब्ध कराता है। OSI मॉडल की top तीन लेवलों के telnet functions निम्नलिखित होते हैं–

1. Session leyar पर यह half-duplex method का प्रयोग करके डायलॉग कन्ट्रोल को उपलब्ध कराता है। यह session administration, handling connection establishment, file transfer तथा relasing connection को भी उपलब्ध कराता है।
2. Presentation layer पर telnet, byter order तथा Character codes का प्रयोग करके ट्रांसलेशन की सुविधा को उपलब्ध कराता है।
3. Application layer पर, यह प्रोटोकॉल रिमोट ऑपरेशन के लिये function का प्रयोग करके सेवायें Supply करता है।

(c) FTP : FTP को File Transfer Protocol कहते हैं। जैसा कि इसके नाम से प्रतीत होता है कि इस प्रोटोकॉल का प्रयोग इंटरनेट पर फाइलों को लोड करने के लिये किया जाता है। इंटरनेट का सबसे लोकप्रिय तथा मुख्य उपयोग फाइलों को डाऊनलोड करना है, अर्थात् इंटरनेट पर एक कम्प्यूटर से दूसरे कम्प्यूटर पर फाइलों को Transfer करना है। हजारों फाइलें प्रत्येक दिन इंटरनेट पर एक कम्प्यूटर से दूसरे कम्प्यूटर पर Transfer होती हैं। इनमें से अधिकतर फाइलें इंटरनेट के फाइल ट्रांसफर प्रोटोकॉल के माध्यम से ट्रांसफर होती हैं। FTP का प्रयोग इंटरनेट पर फाइलों को अपलोड करने के लिये भी किया जाता है। Web Server की भाँति इंटरनेट FTP Servers की Installation करता है। बहुत-सी Organizations फाइलों को वितरित करने के लिये FTP Servers का प्रयोग करते हैं। FTP प्रोटोकॉल Text Files तथा Binary Files का आदान-प्रदान करता है। FTP सॉफ्टवेयर के मुख्य कार्य निम्नलिखित हैं–

1. यह Remote तथा Web host पर फाइलों को अपलोड करता है।
2. यह Remote तथा Web host से फाइलों को डाऊनलोड करता है।
3. यह Anonymous तथा Non-anonymous FTP Server के रूप में दो भागों में विभाजित होता है।
4. Anonymous FTP Server में Access करने के लिये FTP User को Password की आवश्यकता नहीं होती है।
5. Non-anonymous FTP Server में एक्सेस करने के लिये FTP User को Password की आवश्यकता होती है। □

प्रश्न 2 – *OSI तथा TCP/IP रिफरेंस मॉडलों की तुलना करें।*

Compare between OSI and TCP/IP Reference Models.

उत्तर–जैसा कि आप पढ़ चुके हैं, OSI तथा TCP/IP दोनों मॉडलों में बहुत कुछ समान है। दोनों ही मॉडल स्वतंत्र प्रोटोकॉलों की स्टैक (Stack) जैसी अवधारणा पर आधारित हैं, जिन्हें लेयर (Layer) कहा जाता है। दोनों मॉडलों में सभी लेयरों के कार्य लगभग समान हैं। उदाहरण के लिए, दोनों मॉडलों में निम्नतम स्तर से ट्रांसपोर्ट लेयर तक लगभग एक जैसे लेयर हैं। फिर दोनों मॉडलों में ट्रांसपोर्ट लेयर से ऊपर के मॉडल उपयोगों (एप्लीकेशनों) पर आधरित हैं।

Scanned by CamScanner

इन मौलिक समानताओं के बाद भी दोनों मॉडलों में बहुत-सी असमानताएँ भी हैं। यहाँ हम इनमें असमानताओं की चर्चा करेंगे। OSI मॉडल में तीन अवधारणाएँ (Concepts) केन्द्रीय हैं–

1. सेवाएँ (Services)
2. इंटरफेस (Interfaces)
3. प्रोटोकॉल (Protocols)

OSI मॉडल का शायद सबसे बड़ा योगदान यह है कि इसमें इन तीनों अवधारणाओं को स्पष्ट रूप से अलग-अलग किया गया है। प्रत्येक लेयर अपने से ऊपर के लेयर के लिए कुछ सेवाएँ प्रदान करता है। इन सेवाओं की परिभाषा स्पष्ट कर देती है कि किस लेयर में क्या किया जाता है, उसे पड़ोसी लेयरों से क्या सूचना प्राप्त होती है और उस सूचना का क्या किया जाता है आदि। इस प्रकार सेवाएँ किसी लेयर के अस्तित्व को परिभाषित करती हैं।

किसी लेयर का इंटरफेस अपने से ऊपर के प्रोसेसों को बताता है कि इसका उपयोग किस प्रकार करना है। यह बताता है कि किसी सूचना के पैरामीटर (Parameters) क्या हैं और उनका क्या परिणाम (Result) अपेक्षित है। लेकिन इंटरफेस भी यह नहीं बताता कि लेयर भीतर कैसे कार्य करते हैं।

अन्त में, किसी लेयर का प्रोटोकॉल ही उसके कार्य को ठीक-ठीक करता है। प्रोटोकॉल प्रत्येक लेयर का आन्तरिक मामला है। यह अपनी आवश्यकता के अनुसार कोई भी प्रोटोकॉल चुन सकता है ताकि उसका कार्य सही-सही हो जाये। आवश्यकता पड़ने पर वह प्रोटोकॉल को अपनी इच्छा के अनुसार बदल भी सकता है, वह भी बिना ऊपरी लेयरों के सॉफ्टवेयर को प्रभावित किये।

इस प्रकार OSI मॉडल में सेवाओं, इंटरफेसों और प्रोटोकॉलों को स्पष्टतः अलग-अलग कर दिया गया है।

इसके विपरीत TCP/IP मॉडल सेवाओं, इंटरफेसों और प्रोटोकॉलों में मूलतः स्पष्ट अन्तर नहीं करता। हालांकि लोगों ने इसे OSI जैसा बनाने के लिए इसे सुधारने की कोशिशें की हैं। उदाहरण के लिए, इंटरनेटवर्क लेयर (Internetwork layer) द्वारा दी जाने वाली दो वास्तविक सेवाएं SEND IP PACKET और RECEIVE IP PACKET हैं।

इसके परिणामस्वरूप OSI मॉडल में प्रोटोकॉल TCP/IP मॉडल की तुलना में भली भाँति छिपे रहते हैं और उनको तकनीकी परिवर्तन होने पर सरलता से बदला जा सकता है। लेयर आधारित प्रोटोकॉल बनाने का मुख्य उद्देश्य ही यह है कि उनको तकनीक के साथ बदला जा सके।

वास्तव में OSI मॉडल प्रोटोकॉलों के आविष्कार से पहले तैयार किया गया था। इसलिए यह मॉडल किसी विशेष प्रोटोकॉल की ओर झुका हुआ नहीं है। इसका एक कारण यह भी है कि इसे डिजायन करने वालों को विषय का पूरा अनुभव नहीं था और वे ठीक-ठीक नहीं जानते थे कि किस लेयर में वास्तव में क्या-क्या करना है। उदाहरण के लिए, डाटा लिंक लेयर मूलतः पॉइंट-टू-पॉइंट नेटवर्क के लिए था। इसलिए जब ब्रोडकास्ट नेटवर्क आये, तो इसके लिए एक नया सब-लेयर जोड़ना पड़ा। इसके अलावा, उन्होंने विभिन्न प्रकार के नेटवर्कों को आपस में जोड़ने अर्थात् इंटरनेटवर्किंग (Internetworking) के बारे में कुछ नहीं सोचा था।

इसके विपरीत TCP/IP मॉडल में प्रोटोकॉल पहले आये और मॉडल वास्तव में इन प्रोटोकॉलों का विवरण मात्र था। इसलिए प्रोटोकॉलों को मॉडल में फिट करने में कोई समस्या नहीं थी। लेकिन समस्या केवल यह थी कि वह मॉडल किसी अन्य प्रोटोकॉल स्टैक में फिट नहीं होता था। इसके परिणामस्वरूप यह अन्य नॉन-टीसीपी/आईपी नेटवर्कों को समझाने में समर्थ नहीं था।

OSI और TCP/IP दोनों मॉडलों में मुख्य अन्तर यह है कि OSI मॉडल में सात लेयर हैं, जबकि TCP/IP में केवल चार लेयर हैं। दोनों मॉडलों में (इंटर) नेटवर्क, ट्रांसपोर्ट और एप्लीकेशन लेयर हैं, लेकिन अन्य लेयरों में अन्तर है।

दूसरा अन्तर यह है कि OSI मॉडल अपने नेटवर्क लेयर में कनेक्शनरहित (Connectionless) और कनेक्शन-अभिमुखी (Connection-oriented) दोनों प्रकार के संचार (Communication) की सुविधा देता है, परन्तु ट्रांसपोर्ट लेयर में केवल कनेक्शन-अभिमुखी संचार उपलब्ध कराता है। इसकी तुलना में TCP/IP मॉडल के इंटरनेटवर्क लेयर में केवल एक मोड (कनेक्शनलेस) है, परन्तु ट्रांसपोर्ट लेयर में दोनों मोडों की सुविधा देता है। ❑

प्रश्न 3 – *URL से आप क्या समझते हैं? बताइये।*

What do you understand by URL? Explain.

उत्तर–यूआरएल (URL)–इंटरनेट से जुड़े हुए और संसार भर में फैले हुए कम्प्यूटरों पर विभिन्न प्रकार की सूचनाएँ दस्तावेजों के रूप में उपलब्ध करायी जाती हैं। इन दस्तावेजों को वेब पेज (Web page) कहा जाता है। प्रत्येक वेब पेज में संसार भर के किसी भी अन्य वेब पेज के लिंक (Links) या पॉइंटर (Pointers) हो सकते हैं। उपयोगकर्ता उन लिंकों का उपयोग करके उन वेब पेजों को खोल सकते हैं। वेब पेजों को पहचानने के लिए उनका एक नाम रखा जाता है। यह नाम ऐसा होना चाहिए, जो उस वेब पेज के लोकेशन को ठीक-ठीक व्यक्त कर सके। इस नाम को यूनीफॉर्म रिसोर्स लोकेटर (Uniform Resource Locator) या संक्षेप में यूआरएल (URL) कहा जाता है।

Scanned by CamScanner

किसी वेब पेज के यूआरएल में तीन भाग होते हैं– प्रोटोकॉल (Protocol), उस कम्प्यूटर का डोमेन नाम (Domain name) जिस पर वह वेब पेज स्टोर किया गया है, तथा उस फाइल का नाम (File name) जिसमें वह वेब पेज स्टोर है। उदाहरण के लिए, निम्नलिखित यूआरएल पर ध्यान दीजिए–

http://www.abcd.com/products/html

यहाँ http प्रोटोकॉल का नाम है, www.abcd.com होस्ट कम्प्यूटर का डोमेन नाम है तथा products.html उस वेब पेज की फाइल का नाम है। इन तीनों भागों को स्लैश द्वारा अलग-अलग किया जाता है। वैसे फाइल नाम फोल्डर के नाम के साथ भी हो सकते हैं। इससे स्लैश द्वारा अलग-अलग किये गये भागों की संख्या बढ़ जाती है, परन्तु इससे यूआरएल की संरचना पर कोई प्रभाव नहीं पड़ता।

जब किसी ब्राउजर प्रोग्राम द्वारा किसी यूआरएल वाले वेब पेज को खोलने की कोशिश की जाती है, तो ब्राउजर सबसे पहले उस होस्ट कम्प्यूटर का पता लगाता है, जहाँ वह वेब पेज स्टोर किया गया है। इसके लिए यूआरएल के दूसरे भाग अर्थात् डोमेन नाम का उपयोग किया जाता है। डोमेन नाम से होस्ट का आईपी एड्रेस (IP address) ज्ञात किया जाता है और फिर ब्राउजर उस होस्ट के साथ टीसीपी (TCP) कनेक्शन जोड़ता है। कनेक्शन जुड़ जाने पर वह उस कनेक्शन में होकर वेब पेज की फाइल का नाम उसके प्रोटोकॉल का उपयोग करके भेजता है। शीघ्र ही वह वेब पेज ब्राउजर के कम्प्यूटर पर आ जाता है। इस प्रकार यूआरएल द्वारा संसार भर के किसी भी वेब पेज को खोला जा सकता है, यदि वह इंटरनेट पर उपलब्ध हो।

यहाँ http प्रोटोकॉल वेब पेजों की मौलिक भाषा है, जो वेब सर्वरों द्वारा उपयोग की जाती है। इसका पूरा नाम हाइपर टैक्स्ट ट्रांसफर प्रोटोकॉल (Hyper Text Transfer Protocol) है। इसी तरह और भी कई प्रोटोकॉल होते हैं, जिनमें से कुछ के नाम निम्नलिखित हैं–

ftp	फाइल ट्रांसफर प्रोटोकॉल
file	लोकल फाइल
news	न्यूजग्रुप (Newsgroup)
gopher	गोफर
mailto	ई-मेल भेजना
telnet	रिमोट लॉगइन

यूआरएल में इनमें से आवश्यकता के अनुसार किसी भी प्रोटोकॉल का नाम हो सकता है। ❑

प्रश्न 4 – *हाइपर टर्मिनल पर संक्षेप में टिप्पणी लिखिये–*

Write down the short notes on hyper terminal.

उत्तर–हाइपर टर्मिनल (Hyper terminal)–विण्डोज के अन्दर कम्यूनिकेशन Tools में उपलब्ध विभिन्न Tools में से Hyper terminal एक प्रमुख Tool है। हमारे पास ऑफिस में एक कम्प्यूटर है तथा दूसरा कम्प्यूटर कहीं दूसरी जगह ऑफिस में है, हम चाहते हैं कि हमारे पास ऑफिस के कम्प्यूटर को हम दूसरी जगह के ऑफिस के कम्प्यूटर से जोड़ दें जिससे कि इन दोनों कम्प्यूटरों का डाटा आदान-प्रदान हो सके। विण्डोज में यह संभव है। विण्डोज में दूरस्थ कम्प्यूटर से अपने कम्प्यूटर को जोड़ने के लिये Communication Tool के अन्दर Hyper terminal Tool है। इस Tool का प्रयोग हम दूरस्थ के कम्प्यूटर से जोड़ने के लिये करते हैं। इस Tool का प्रयोग हम अपने सिस्टम की फाइलों को दूरस्थ के सिस्टम में भेजने के लिये तथा वहां से प्राप्त करने के लिये करते हैं।

Hyper terminal का प्रयोग करने के लिये निम्नलिखित Steps को Follow करते हैं–

Step 1 : start button पर click करते हैं।

Step 2 : इसके अंतर्गत Programs के अंतर्गत Accessories पर click करते हैं।

Step 3 : Accessories के अंतर्गत Communications पर click करते हैं।

Step 4 : Communications के अन्दर प्रदर्शित Tools में से Hyper terminal tool को select करते हैं तथा click करते हैं।

Step 5 : Hyper terminal Dialog box प्रदर्शित होता है। इसमें अपनी आवश्यकतानुसार तथा इच्छानुसार options को set करते हैं। ❑

प्रश्न 5 – *पिंग कमाण्ड के द्वारा Connectivity को कैसे जांचेंगे?*

How would you test the connectivity through ping command?

उत्तर–नेटवर्क से जुड़े हुये कम्प्यूटर, router तथा Internet कनेक्टिविटी को test करने के लिये ping कमाण्ड अत्यन्त उपयोगी है। इस कमाण्ड को command prompt पर रन करते हैं। ping कमाण्ड के माध्यम से कनेक्टिविटी को test करने के लिये निम्नलिखित steps को follow करते हैं–

Scanned by CamScanner

Step1 : Start बटन के अंतर्गत run ऑपशन को क्लिक करते हैं।

Step2 : प्रदर्शित run विण्डो में cmd type करते है तथा OK बटन पर क्लिक करते हैं। स्क्रीन पर एक black and white कमाण्ड लाइन प्रदर्शित होती है।

Step3 : प्रदर्शित prompt पर ping type करते हैं, तथा इसके साथ ही एक IP address या DNS address को भी type करते हैं। यह address वह address होता है, जिसके साथ current system की कनेक्टिविटी को test करना है।

Step4 : यदि कनेक्टिविटी में कोई समस्या नहीं होती है तो स्क्रीन पर reply प्रदर्शित होता है। जैसे–निम्नलिखित कमाण्ड 110.172.172.129 ip address के साथ कनेक्टिविटी को test करती है।

```
ping 110.172.172.129 ↵
     IP address
Reply from 110.172.172.129 : bytes = 32 time = 69ms
                                    TTL = 64
```

यह reply लगातार प्रदर्शित होता है, जो दर्शाता है कि 110.172.172.129 IP address के साथ कनेक्टिविटी सफल है। यदि कनेक्टिविटी fail होती है तो "request time out" या "host unreachable" मैसेज प्रदर्शित होता है। ❑

प्रश्न 6 – DNS समस्या का Network समस्या से आप कैसे फर्क करेंगे?

How do you distinguish a DNS problem from a network problem.

(Dec., 2012/Jan., 2013)

उत्तर–DNS Problems और Network Problems में निम्नलिखित अंतर है–

DNS Problems	**Network Problems**
1. यदि ब्राउजर, एक सर्वर को find नहीं करता है, तो यह problem, DNS problem है।	1. यदि एक सर्वर आपके कनेक्शन को रिफ्यूज करता है, तो यह problem नेटवर्क की है।
2. यदि domain name के साथ ping कमाण्ड का प्रयोग करते हैं लेकिन कोई reply नहीं मिलता है तो यह DNS की problem है।	2. यदि नेटवर्क से जुड़े कम्प्यूटर के IP Address के साथ ping कमाण्ड का प्रयोग करते हैं, लेकिन कोई reply नहीं मिलता है, तो यह Network की problem है।
3. DNS server से कनेक्ट किये गये router या switch, सफलतापूर्वक ping करते हैं, लेकिन DNS, ping नहीं करता है, तो निश्चित रूप से यह DNS server की problem है।	3. यदि नेटवर्क से जुड़े हुये कम्प्यूटर्स, server के साथ ping करते हैं, लेकिन server इनके साथ ping नहीं करता है, और सभी के Network card सही हैं, तो निश्चित रूप से यह नेटवर्क problem है।
4. यदि ping कमाण्ड के साथ DNS server का नाम type करते हैं, और "host unreachable" प्रदर्शित होता है तो यह DNS problem है।	4. यदि किसी कम्प्यूटर के IP address के साथ ping कमाण्ड को उसी कम्प्यूटर पर प्रयोग करते हैं और ."Network Not found" मैसेज प्रदर्शित होता है, तो यह नेटवर्क problem है।

❑

प्रश्न 7 – TCP/IP प्रोटोकॉल को Configure करने के लिये चरणों को लिखिये।

Write steps for configuring TCP/IP Protocol. **(Dec., 2012/Jan., 2013)**

उत्तर–TCP/IP Protocol को configure करने के लिये निम्नलिखित steps को follow करते हैं–

Step1 : Window में Start button पर क्लिक करते हैं। इसके अंतर्गत control panel ऑपशन को क्लिक करते हैं।

Step2 : प्रदर्शित control panel विण्डो में Network and Internet connections पर क्लिक करते हैं तत्पश्चात् Network connections पर क्लिक करते हैं।

Step3 : उस Network connection पर right click करते है, जिसे हम configure करना चाहते हैं तत्पश्चात् properties पर क्लिक करते हैं।

Scanned by CamScanner

Step4 : लोकल एरिया कनेक्शन के लिये General tab पर या सभी दूसरे connections के लिये Networking tab को सलेक्ट करते हैं तथा Internet Protocol (TCP/IP) पर क्लिक करते हैं। इसके पश्चात् Properties पर क्लिक करते हैं।

Step5 : यदि हम DHCP server से DNS server addresses को प्राप्त करना चाहते हैं तो obtain DNS server address automatically option पर क्लिक करते हैं।

Step6 : यदि हम DNS server addresses को manually configure करना चाहते हैं, तो use the following DNS server addresses ऑप्शन पर क्लिक करते हैं।

Step7 : इसके पश्चात् prefer किये गये DNS server तथा alternate DNS server IP address को preferred DNS server तथा Alternate DNS server boxes में type करते हैं।

Step8 : इसके पश्चात् OK बटन पर क्लिक करते हैं।

❑

प्रश्न 8 – *Nestat कमाण्ड की उपयोगिता को समझाइये।*

Explain the utilities of netstat command.

उत्तर–Netstat command, active TCP connections को प्रदर्शित करती हैं। इसका प्रारूप निम्नलिखित रूप में होता है।

प्रारूप:

```
netstat [–a] [–e] [–n] [–o] [–p] [–r] [–s]
```

- **–a :** यह parameter सभी active TCP connections को प्रदर्शित करता है, तथा TCP और UDP ports को प्रदर्शित करता है।
- **–e :** यह parameter, ethernet statistics को प्रदर्शित करता है, जैसे कितनी bytes की संख्या तथा packets को भेजा गया है तथा receive किया गया है।

इस parameter को –r के साथ combine रूप में प्रयोग किया जा सकता है।

- **–n :** यह parameter, active TCP connections को प्रदर्शित करता है। हांलाकि addresses तथा port numbers, numerically express किये जाते हैं।
- **–o :** यह parameter, active TCP connections को प्रदर्शित करता है, जिसमें process ID (PID) सम्मिलित होती है। इस parameter को –a, –n, –p के साथ combine रूप में प्रयोग किया जा सकता है।
- **–p :** यह parameter, specify किये गये protocol के लिये connections को दर्शाता है।
- **–s :** यह parameter, protocol के द्वारा statistics को प्रदर्शित करता है।
- **–r :** यह parameter, IP routing table के contents को प्रदर्शित करता है। ❑

प्रश्न 9 – *डोमेन एवं वर्कस्टेशन की भूमिका को विंडोज में समझाइये।*

Explain the role of domain and workstation in windows.

उत्तर–Domain, computers तथा users का एक ग्रुप है, जो computers तथा user accounts को एडमिनिस्ट्रेट करने में एडमिनिस्ट्रेटर की सहायता करता है। Windows में domain के क्रिएट करने की आवश्यकता तब होती है, जब इससे जुड़े हुये workstations को नियंत्रित करने की आवश्यकता होती है। Workstaions, कम्प्यूटर्स का एक ग्रुप होता है, जो domain से कनेक्ट होता है। जब दो या दो से अधिक कम्प्यूटर्स को आपस में एक नेटवर्क के माध्यम से कनेक्ट कर दिया जाता है, इसे कम्प्यूटर नेटवर्किंग कहते हैं। इस नेटवर्क में किसी एक कम्प्यूटर को server बना देते हैं, इस सिस्टम पर windows का server version, ऑपरेटिंग सिस्टम के रूप में install किया जाता है, इसे domain या domain server के नाम से भी जाना जाता है। शेष कम्प्यूटर्स पर windows का workstation version ऑपरेटिंग सिस्टम के रूप में install किया जाता है, इनको workstations कहते हैं। Domain के माध्यम से user accounts क्रिएट किये जाते हैं तथा इन्हें rights दिये जाते है। केवल authorised users ही workstation पर कार्य कर सकते हैं। Workstations, domains, windows network के heart होते हैं। विण्डोज एडमिनिस्ट्रेटर के रूप में, प्रारम्भिक जिम्मेदारियां, इन resources को मैनेज करना है। Windows administrator, system administration के निम्नलिखित tasks को handle करता है।

(i) Managing user sessions and connections

(ii) Managing file, directory and share usage

(iii) Setting administrative alerts

Scanned by CamScanner

(iv) Replicating directories and files to other systems in the domain.

(v) Creating and managing user accounts

(vi) Synchronizing and promoting domain controllers.

निम्नलिखित Fig. में Domain workstations रिलेशनशिप को स्पष्ट रूप से चित्रित किया गया है–

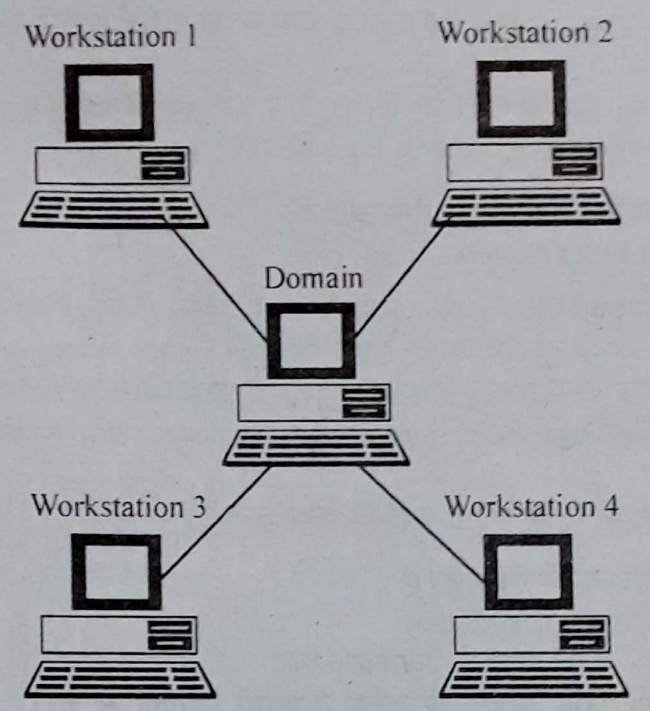


Fig. : Domain-Workstation Relationship

उपरोक्त Fig. में एक domain, तथा चार workstations को चित्रित किया गया है। ये चारों, workstations, domain से कनेक्टेड हैं।

❑

प्रश्न 10 – हाइपर टर्मिनल की उपयोगिता की चर्चा कीजिये।

Discuss the utilities of Hyperterminal.

उत्तर–Hyperterminal एक प्रोग्राम है, जिसे हम दूसरे computers, telnet sites, bulletin board systems इत्यादि से कनेक्ट करने के लिये प्रयोग कर सकते हैं। Hyperterminal connections, modem, null modem cable या ethernet connection का प्रयोग करके बनाये जाते हैं।

Hyperterminal, serial port का प्रयोग करके बड़ी फाइलों को एक कम्प्यूटर से हमारे portable computer पर ट्रांसफर कर सकता है। इसके लिये नेटवर्क पर हमें अपने portable computer को setup करने की आवश्यकता नहीं होती है। यह रिमोट टर्मिनल से सोर्स कोड को डिबग् करने में सहायता करता है। यह पुराने character-based computers के साथ कम्यूनिकेट करने में भी सहायता करता है। Hyperterminal के साथ रिमोट कम्प्यूटर में एक्सेस करने के लिये निम्नलिखित steps को follow करते हैं–

step1 : windows में start के अंतर्गत All Programs में Accessories में Communications में Hyperterminal ऑप्शन पर क्लिक करते हैं। स्क्रीन पर Hyperterminal का set-up डॉयलॉग बॉक्स प्रदर्शित होता है।

step2 : इस बॉक्स में "area code" बॉक्स में अपने area या city का कोड enter करते हैं।

step3 : यदि जरूरत हो तो "carrier code" बॉक्स में carrier code enter करते हैं। इसके पश्चात् phone system के access code को enter करते हैं।

step4 : इसके पश्चात् "tone dialing" या "pulse dialing" ऑप्शन को सलेक्ट करके OK बटन पर क्लिक करते हैं तथा अपने area code को confirm करने के लिये OK बटन पर क्लिक करते हैं।

Scanned by CamScanner

step5 : "connection description" डॉयलॉग बॉक्स पर "Name" हैडिंग में remote computer के नाम को enter करते हैं। इसके पश्चात् remote computer को रिप्रजेन्ट करने के लिये एक icon को सलेक्ट करते हैं तथा OK बटन पर क्लिक करते है, ऐसा करने पर स्क्रीन पर "connect to" डॉयलॉग बॉक्स ओपन हो जायेगा।

step6 : जिस रिमोट कम्प्यूटर में एक्सेस कर रहे है, उसका area code, country code तथा phone number, enter करते हैं। यदि कम्प्यूटर में modem नहीं है, तो remote computer के host address को "host address" बॉक्स में enter करते हैं तथा "port number" बॉक्स में computer के port number को enter करते हैं। इसके पश्चात् "TCP/IP" को "connect using" बॉक्स में सलेक्ट करते हैं तथा OK बटन पर क्लिक करते हैं।

step7 : Remote computer की access स्क्रीन पर assign किये गये user name तथा password को enter करते हैं। authorisation की पुष्टि हो जाने पर remote computer में login हो जाते हैं। ❑

प्रश्न 11 – OSI तथा ISO आपस में किस तरह सम्बन्धित हैं?

How are OSI and ISO related to each other.

उत्तर—ISO (International Standard Organization) एक स्टैण्डर्ड है, जिसने नेटवर्क मॉडल को सत्यापित है, अर्थात् यह एक standard है, जो networking protocol को सत्यापित करता है। OSI (Open System Interconnection) नेटवर्क प्रोटोकॉल मॉडल है, जिसका प्रयोग नेटवर्क से जुड़े हुये एक कम्प्यूटर से दूसरे कम्प्यूटर पर डाटा कम्यूनिकेशन के लिये किया जाता है। अतः इसका पूरा नाम ISO/OSI (International Standard Organizations/open system Interconnection) Network Model है। इसमें सात layers होती हैं, जो निम्नलिखित हैं–

[नोट—इसके उत्तर के लिए पृष्ठ 24 पर प्रश्न-3 के उत्तर का अध्ययन करें।] ❑

प्रश्न 12 – TCP/IP रेफरेंस मॉडल को समझाइये।

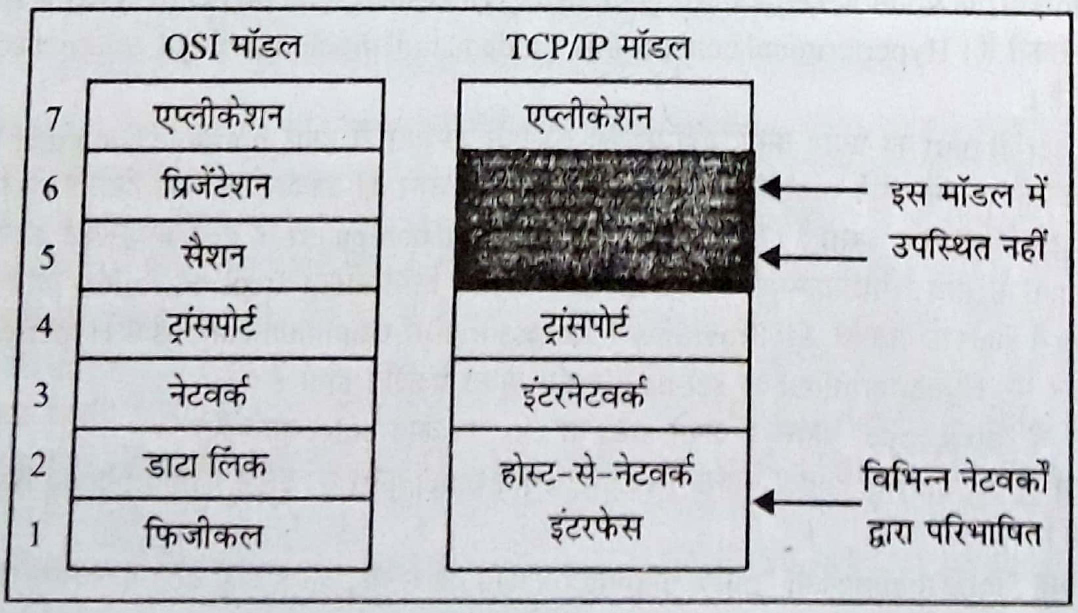
Explain TCP/IP Reference Model.

अथवा (Or)

OSI और TCP/IP रेफरेंस मॉडल की तुलना चित्र की सहायता से करें।

Compare OSI and TCP/IP Reference Model with the help of figure.

उत्तर—टीसीपी/आईपी रिफरेंस मॉडल (TCP/IP Reference Model)—सभी कम्प्यूटर नेटवर्कों का दादा (Grandparent) अर्पानेट (ARPANET) नामक नेटवर्क को माना जाता है। इंटरनेट इसी का वंशज या उत्तराधिकारी (Successor) है। अर्पानेट मूलतः अमेरिका के सुरक्षा विभाग (Defence Deptt.) द्वारा विभिन्न विश्वविद्यालयों और सरकारी संस्थानों को लीज टेलीफोन लाइनों के माध्यम से जोड़ने वाला एक रिसर्च नेटवर्क था। जब सैटेलाइट और रेडियो नेटवर्कों को इसमें जोड़ा गया, तो पुराने प्रोटोकॉलों की जगह नये प्रोटोकॉल लाने की आवश्यकता हुई। इस प्रोटोकॉल को इस प्रकार डिजायन किया गया कि एक से अधिक नेटवर्कों को आपस में जोड़ा जा सके अर्थात् इंटरनेटवर्किंग (Internetworking) की जा सके। यही डिजायन आगे चलकर टीसीपी/आईपी रिफरेंस मॉडल (TCP/IP Reference Model) अथवा टीसीपी/आईपी प्रोटोकॉल सुइट (TCP/IP Protocol Suite) के नाम से जानी गयी। यही आज के इंटरनेट का आधार है।



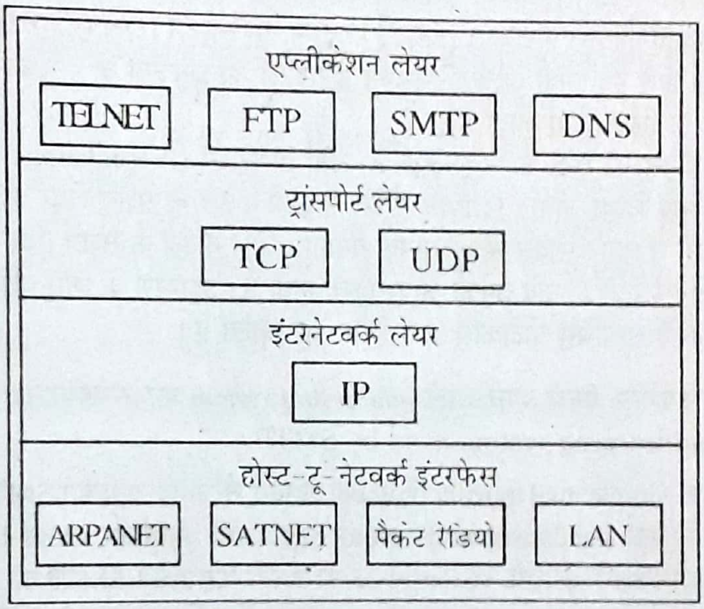
चित्र : OSI बनाम TCP/IP मॉडल

Scanned by CamScanner

क्योंकि टीसीपी/आईपी मॉडल ओएसआई मॉडल (OSI Model) से पहले विकसित किया गया था, इसलिए इस मॉडल के लेयर OSI मॉडल के लेयरों से पूरी तरह मैच नहीं करते। TCP/IP मॉडल तीन लेयरों से मिलकर बनता है– नेटवर्क, ट्रांसपोर्ट और एप्लीकेशन। इनमें से नेटवर्क और ट्रांसपोर्ट लेयर क्रमशः इंटरनेटवर्किंग और ट्रांसपोर्ट कार्यों को सँभालते हैं। लेकिन OSI मॉडल के तीन ऊपरी लेयरों के बदले TCP/IP में केवल एक लेयर है एप्लीकेशन लेयर, जैसा कि उपर्युक्त चित्र में दिखाया गया है।

TCP/IP कई परस्पर वार्तालापी मॉड्यूलों (Interactive modules) से बना हुआ एक वंशक्रमिक (Heirarchical) प्रोटोकॉल है, जिनमें से प्रत्येक विशेष कार्य करता है, परन्तु एक दूसरे पर निर्भर नहीं हैं। जहाँ OSI मॉडल अपने प्रत्येक लेयर के कार्यों (Functions) को ठीक-ठीक बताता है, वहीं TCP/IP मॉडल अपेक्षाकृत स्वतंत्र प्रोटोकॉलों से बना है, जिनको किसी सिस्टम की आवश्यकता के अनुसार आपस में मिलाया जा सकता है। इसमें 'वंशक्रमिक' शब्द का अर्थ है कि प्रत्येक ऊपरी लेयर अपने से नीचे के एक या अधिक लेयरों द्वारा समर्थित (Supported) है। इसे आगे चित्र में स्पष्ट किया गया है।

ट्रांसपोर्ट लेयर में, TCP/IP दो प्रोटोकॉलों को परिभाषित करता है–ट्रांसमिशन कंट्रोल प्रोटोकॉल (Transmission Control Protocol या TCP) और यूजर डाटाग्राम प्रोटोकॉल (User Datagram Protocol या UDP). इंटरनेटवर्क लेयर में केवल एक प्रोटोकॉल परिभाषित है–इंटरनेटवर्किंग प्रोटोकॉल (Internetworking Protocol या IP), हालांकि इस लेयर में डाटा के आवागमन में सहायता करने वाले कुछ अन्य प्रोटोकॉल होते हैं। अब हम इस मॉडल के सभी लेयरों की नीचे से ऊपर के क्रम में चर्चा करेंगे।



चित्र : TCP/IP मॉडल का वंशक्रमिक रूप

इंटरनेटवर्क लेयर (Internetwork Layer)–इसे इंटरनेट लेयर (Internet layer) या नेटवर्क लेयर (Network layer) भी कहा जाता है। यह OSI मॉडल के नेटवर्क लेयर की तरह है। इसमें कुछ प्रोटोकॉल होते हैं, जिनमें से मुख्य प्रोटोकॉल को इंटरनेटवर्किंग प्रोटोकॉल (Internetworking Protocol या IP) कहा जाता है। यह प्रोटोकॉल नेटवर्क-लेयर पैकेट, जिन्हें आईपी पैकेट (IP Packets) या आईपी डाटाग्राम (IP datagrams) कहा जाता है, बनाने और उन्हें उनके गंतव्य (Destination) तक भेजने के लिए उत्तरदायी है। डाटाग्राम नेटवर्क से नेटवर्क में यात्रा करते हैं और अपने गंतव्य पर किसी भी क्रम में पहुँचते हैं। इससे ऊपर के लेयर उन पैकेटों को प्राप्त करने और सही क्रम में लगाने के लिए उत्तरदायी हैं।

गंतव्य तक पहुँचने के लिए पैकेटों को कई Intermediate nodes से होकर गुजरना पड़ सकता है, जो किसी भी नेटवर्क लैन (LAN) या वैन (WAN) से जुड़े हो सकते हैं। वे नोड उन पैकेटों को सबसे उचित रास्ते से गंतव्य तक भेजने के लिए उत्तरदायी हैं। इस प्रक्रिया में उन्हें पैकेटों के डाटा भाग को बदलने का अधिकार नहीं होता। वे केवल उन पर अपना लेबल लगा सकते हैं।

ट्रांसपोर्ट लेयर (Transport Layer)–TCP/IP मॉडल के ट्रांसपोर्ट लेयर में दो प्रोटोकॉल होते हैं–ट्रांसमिशन कंट्रोल प्रोटोकॉल (Transmission Control Protocol या TCP) तथा यूजर डाटाग्राम प्रोटोकॉल (User Datagram Protocol या UDP). इनमें से पहला अर्थात् TCP प्रोटोकॉल एक विश्वसनीय प्रोटोकॉल है, जो दो एप्लीकेशन लेयरों को आपस में वार्तालाप करने की अनुमति देता है। यह प्रोटोकॉल चिन्हों की किसी धारा (Stream) को किसी स्रोत (Source) से ले जाकर किसी गंतव्य को सौंप देता है और उसका विपरीत भी करता है। इस प्रकार यह फुल-डुप्लेक्स संचार (Full-duplex communication) की सुविधा देता है। स्रोत मशीन पर यह बाइटों की धारा को उचित आकार के सेगमेंटों (Segments) में तोड़ देता है और उनमें आवश्यक हैडर (Header) लगाने के बाद उन्हें भेजने के लिए

Scanned by CamScanner

इंटरनेटवर्क लेयर को दे देता है। गंतव्य मशीन पर यह प्राप्त किये हुए सेगमेंटों को फिर से सही क्रम में लगाकर बाइटों की मूल धारा बना लेता है और उसे एप्लीकेशन लेयर के उपयोग के लिए सौंप देता है। TCP प्रोटोकॉल का निष्पादन OSI मॉडल के ट्रांसपोर्ट लेयर के प्रोटोकॉल से कहीं आगे है, क्योंकि यह OSI मॉडल के सैशन लेयर के कुछ कार्यों को भी करता है। वास्तव में यह दो एप्लीकेशन लेयरों के बीच एक पूर्ण-डुप्लैक्स सम्पर्क बनाता है। यह प्रोटोकॉल यह भी सुनिश्चित करता है कि कोई तेज प्रेषक किसी धीमें प्राप्तकर्ता को ढेरसारा डाटा एक साथ न भेज दे।

इस लेयर का दूसरा प्रोटोकॉल अर्थात् UDP प्रोटोकॉल एक बहुत साधारण ट्रांसपोर्ट लेयर प्रोटोकॉल है, जो कई बार OSI मॉडल के ट्रांसपोर्ट लेयर के सभी कार्यों को भी नहीं करता। यह एक अविश्वसनीय (Unreliable) प्रोटोकॉल है, जो ऐसे एप्लीकेशनों द्वारा उपयोग में लाया जाता है, जिनको डाटा पैकेट तेजी से भेजने या प्राप्त करने की आवश्यकता होती है, बिना गलतियों की चिन्ता किये। लेकिन कई बार ट्रांसपोर्ट-लेयर के रूप में UDP प्रोटोकॉल का उपयोग करना अच्छा रहता है, क्योंकि इसके द्वारा मल्टीकास्टिंग (Multicasting), अर्थात् एक संदेश कई प्राप्तकर्त्ताओं को भेजना तथा ब्रोडकास्टिंग (Broadcasting), अर्थात् एक संदेश सभी को भेजना आदि क्रियाएँ अच्छी तरह की जा सकती हैं। इसलिए इस प्रोटोकॉल का उपयोग सामान्यतया क्लाइंट-सर्वर (Client-Server) प्रकार के सम्पर्कों में अधिक किया जाता है, क्योंकि उसमें सही डिलीवरी से तेज डिलीवरी का अधिक महत्व होता है।

एप्लीकेशन लेयर (Application Layer)—TCP/IP प्रोटोकॉल का एप्लीकेशन लेयर कई प्रोटोकॉलों से मिलकर बनता है, जिनका प्रयोग उपयोगकर्त्ताओं तथा प्रोग्रामों द्वारा दूरस्थ सिस्टमों के संसाधनों का उपयोग करने के लिए किया जाता है। टेलनेट (TELNET), फाइल ट्रांसफर प्रोटोकॉल (FTP), इलैक्ट्रॉनिक मेल प्रोटोकॉल (SMTP), डोमेन नेम सिस्टम (DNS), एचटीटीपी (HTTP) आदि ऐसे कुछ प्रोटोकॉल हैं, जो इस लेयर में शामिल होते हैं। इनके अलावा और भी प्रोटोकॉल आवश्यकता के अनुसार जोड़े जाते हैं। इन प्रोटोकॉलों का उपयोग विभिन्न प्रकार के कार्यों के लिए किया जाता है।

टीसीपी/आईपी मॉडल में OSI मॉडल की तरह सैशन (Session) तथा प्रिजेंटेशन (Presentation) लेयर नहीं होते, क्योंकि इनका उपयोग अधिकांश एप्लीकेशनों द्वारा नहीं किया जाता। TCP/IP मॉडल में OSI मॉडल के सैशन लेयर के कुछ कार्य ट्रांसपोर्ट लेयर द्वारा किये जाते हैं, जैसे दो एप्लीकेशन लेयरों में फुल-डुप्लैक्स संचार सम्पर्क बनाना। OSI मॉडल के सैशन तथा प्रिजेंटेशन लेयरों के अन्य कार्य एप्लीकेशन लेयर के प्रोटोकॉलों में शामिल रहते हैं, यदि उनकी आवश्यकता होती है। उदाहरण के लिए, यदि किसी एप्लीकेशन को फॉर्मेट बदलने की आवश्यकता है, तो यह कार्य सम्बंधित प्रोटोकॉल द्वारा किया जा सकता है।

प्रश्न 13 – SMTP के द्वारा उपयोग किये जाने वाले addressing system को समझाइये।
Describe the addressing system used by SMTP.

उत्तर–SMTP को विस्तृत रूप से simple mail transfer protocol के नाम से जाना जाता है। SMTP, इंटरनेट पर email server को messages ट्रांसमिट करने के लिये एक standard network protocol है। सभी आधुनिक email client programs, SMTP को सपोर्ट करते हैं। SMTP, स्टैण्डर्ड कम्यूनिकेशन के लिये TCP port 25 का प्रयोग करता है। SMTP को सुधारने के लिये तथा इंटरनेट पर spam help के लिये standard group ने TCP port 587 को डिजाइन किया है, जो प्रोटोकॉल के निश्चित aspects को सपोर्ट करता है।

SMTP module को configure करने के लिये निम्नलिखित steps को follow करते हैं–

Step 1 : Web Admin Interface का प्रयोग करके setting में mail pages को open करके SMTP pages को खोलते हैं।

Step 2 : Server Log में किस प्रकार की इनफॉरमेशन को SMTP module को रखना चाहिये, इसे specify करने के लिये Log setting का प्रयोग करते हैं।

Step 3 : यदि हम इंटरनेट से प्राप्त किये गये messages को स्वयं के mail server में रखना चाहते हैं, तो इसके लिये अपने domain name को रजिस्टर करना चाहिये।

Step 4 : इसके पश्चात् setting से exit करते हैं।

☐☐

Scanned by CamScanner

UNIT-V

प्रश्न 1 – ***नेटवर्क सिक्यूरिटी क्या है? नेटवर्क सिक्यूरिटी का ऑफिशियल लेवल कम्प्यूटर सिक्यूरिटी से कैसे सम्बद्ध है? समझाइए।***

What is a network security? How is network security related to official level of computer security ? Explain.

उत्तर–नेटवर्क सिक्योरिटी (Network Security)–नेटवर्क सुरक्षा से हमारा तात्पर्य किसी कम्प्यूटर नेटवर्क से जुड़े कम्प्यूटरों और अन्य उपकरणों तथा उनमें स्टोर किये गये डाटा या सूचना की भौतिक (Physical) और तार्किक (Logical) सुरक्षा से है। किसी नेटवर्क के सम्बंध में सुरक्षा बहुत महत्वपूर्ण होती है। पहले जब नेटवर्क नहीं थे, तो कम्प्यूटर की भौतिक और तार्किक सुरक्षा करना सरल था। आप अपना कार्य समाप्त करने के बाद केवल अपने कम्प्यूटर कक्ष के दरवाजे को ताला लगा सकते थे और चैन से सो सकते थे, क्योंकि कम्प्यूटर तक पहुंचने के लिए शरारती तत्वों या चोरों को ताला या दरवाजा तोड़ना पड़ता।

कम्प्यूटर नेटवर्क बन जाने के पहले कुछ दशकों में ऐसे नेटवर्क्स केवल विश्वविद्यालय के शोध छात्रों द्वारा ई-मेल भेजने के लिए और बड़ी-बड़ी कम्पनियों के कर्मचारियों द्वारा प्रिंटरों का साझा करने के लिए ही उपयोग में लाये जाते थे। इन परिस्थितियों में भी केवल भौतिक सुरक्षा पर जोर दिया जाता था और तार्किक सुरक्षा पर बहुत अधिक ध्यान नहीं दिया जाता था।

परन्तु नेटवर्क सार्वजनिक बन जाने मुख्यतः इंटरनेट के विस्तार के बाद यह दृश्य बदल गया है। अब नेटवर्क सुरक्षा एक विकराल समस्या हो गयी है। अब कोई भी व्यक्ति जो नेटवर्क के किसी भी कम्प्यूटर तक पहुंच सकता है, नेटवर्क में घुसकर आपकी फाइलों को चुरा सकता है। इसलिए न केवल आपको अपने कम्प्यूटर को तालाबन्द करके भौतिक रूप से सुरक्षित करना पड़ता है, बल्कि यह भी पक्का करना पड़ता है कि नेटवर्क से जुड़े अन्य कम्प्यूटर भी इसी प्रकार सुरक्षित कर दिये गये हैं। इसके साथ ही ऐसा वातावरण भी बनाना या बनाये रखना पड़ता है कि नेटवर्क सुचारु रूप से कार्य कर सके।

कम्प्यूटर सुरक्षा के आधिकारिक स्तर (Official Levels of Computer Security)

किसी सुरक्षा तंत्र को विकसित करने में हमें सुरक्षा के कई स्तर निर्धारित करने पड़ते हैं। कई सूचनाएं हमारे लिए अधिक संवेदनशील (Sensitive) होती हैं और कई कम संवेदनशील होती हैं। किसी सरकारी कार्यालय में सूचनाओं को उनकी संवेदनशीलता के अनुसार कई वर्गों में वर्गीकृत (Classified) किया जाता है, जैसे साधरण या अवर्गीकृत (Unclassified), गोपनीय (Confidential) अति गोपनीय (Secret) पूर्ण गोपनीय (Top secret)। सूचनाओं के वर्गीकरण के अनुसार ही उन्हें किसी अधिकारी या कर्मचारी के लिए उपलब्ध (Available) या अनुपलब्ध (Non-available) कराया जाता है।

कम्प्यूटर सुरक्षा के मामले में भी लगभग इसी प्रणाली का पालन किया जाता है। हम प्रत्येक फाइल या फोल्डर को तो इस प्रकार वर्गीकृत कर नहीं सकते। इसलिए हम कम्प्यूटर उपयोगकर्त्ताओं को उनके महत्व के अनुसार वर्गीकृत करते हैं। फिर उन्हें उनके वर्ग के अनुसार फाइलों तक पहुंचने तथा बहुत-से कार्य करने के अधिकार देते हैं। उदाहरण के लिए, विंडोज ऑपरेटिंग सिस्टम में उपयोगकर्त्ताओं के दो स्तर होते हैं–एडमिनिस्ट्रेटर (Administrator) और लिमिटेड (Limited) जिन्हें एकाउंट टाइप करते हैं। उपयोगकर्त्ताओं को उनके स्तर के अनुसार ही सेटिंगों को बदलने और फाइलों का उपयोग करने की अनुमति दी जाती है।

इसी प्रकार किसी कम्प्यूटरीकृत बैंकिंग तंत्र (Computerised banking system) में भी उपयोगकर्त्ताओं के कई स्तर निर्धारित किये जाते हैं, जैसे मुख्य प्रबंधक (Chief Manager), प्रबंधक (Manager), अधिकारी (Officer), ऑपरेटर (Operator) तथा अतिथि (Guest) । इन उपयोगकर्त्ताओं को उनके स्तर के अनुसार ही कुछ निर्धारित कार्य करने का अधिकार दिया जाता है। कोई भी उपयोगकर्त्ता अपने स्तर के निर्धारित कार्यों से इतर कोई कार्य नहीं कर सकता।

इस प्रकार प्रत्येक कम्प्यूटरीकृत सिस्टम में सुरक्षा के स्तरों का निर्धारण और पालन किया जाता है। इनको ही सुरक्षा स्तर (Security levels) कहा जाता है। ये सुरक्षा स्तर दो प्रकार से परिभाषित किये जाते हैं। सबसे पहले तो प्रत्येक कार्य या प्रोसेस (Process) को सुरक्षा स्तर आवंटित किया जाता है। यह स्तर या तो लेबलों; जैसे–A, B, C, आदि या संख्याओं; जैसे– 1, 2, 3, आदि के रूप में हो सकता है और उनका ऊपर से नीचे तक का क्रम भी निर्धारित किया जाता है इसी प्रकार उस तंत्र में कार्य करने वाले व्यक्तियों या उपयोगकर्त्ताओं तथा सूचनाओं (Informations) को भी उनके महत्व और अधिकार के अनुसार सुरक्षा स्तर आवंटित किया जाता है। कोई भी व्यक्ति अपने स्तर के अनुसार ही किसी प्रोसेस को चला सकता है या किसी सूचना तक पहुंच सकता है। इसके लिए नियम निर्धारित किये जाते हैं, जिन्हें सुरक्षा नियंत्रण कहा जाता है। ❑

Scanned by CamScanner

प्रश्न 2 – क्रिप्टोग्राफी क्या है? इसे क्यों प्रयुक्त किया जाता है? पब्लिक/प्राइवेट की एनक्रिप्शन विधि को उदाहरण सहित समझाइये।

What is Cryptography? Why is it used? Give the details of Public/Private Key encryption method with example. ***(Jan., 2006)***

उत्तर–क्रिप्टोग्राफी (Cryptography)–कम्प्यूटर नेटवर्क में दो या दो से अधिक कम्प्यूटर आपस में कम्यूनिकेशन मीडिया के माध्यम से जुड़े होते हैं। कम्प्यूटर नेटवर्क में कनेक्टेड कम्प्यूटरों में आपस में एक कम्प्यूटर से दूसरे कम्प्यूटर में डाटा ट्रांसमिट किया जाता है। इस दृष्टि से नेटवर्क सिक्योरिटी की आवश्यकता होती है। क्रिप्टोग्राफी के माध्यम से नेटवर्क सिक्योरिटी उपलब्ध करायी जाती है। क्रिप्टोग्राफी Abstract Algebra पर आधारित है।

क्रिप्टोगाफी (Cryptography) शब्द को ग्रीक भाषा से लिया गया है। इसका अर्थ है, "Secret Writing"। निम्नांकित Fig. में Cryptography के Components को दर्शाया गया है–

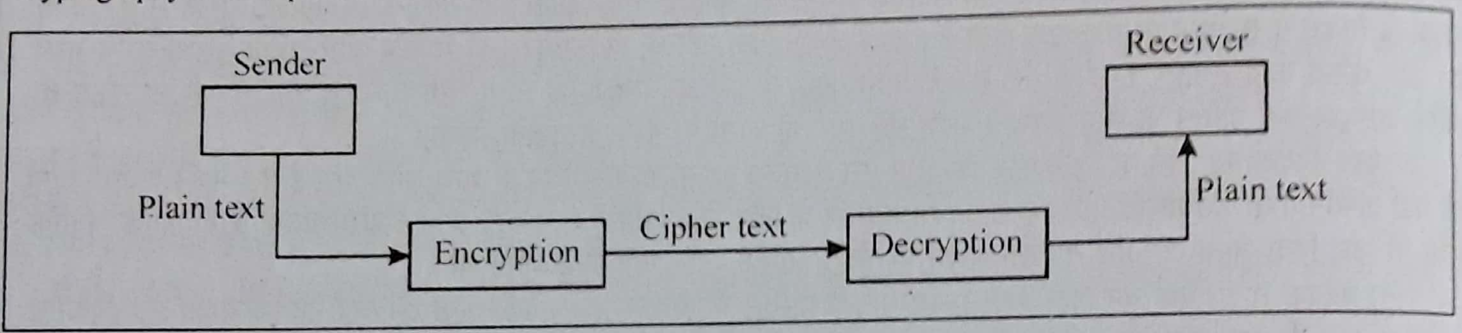


Fig. : Cryptography Components

जिस मैसेज को ट्रांसफर करना है वह Plain text कहलाता है। मैसेज को जब ट्रांसफर किया जाता है, इसे Cipher text कहते हैं। Encryption एक एल्गोरिथम् (Algorithm) है जो Plain text को Cipher text में Transfrom करता है। Decryption Algorithm, Cipher text को Plain text में Transform करता है। Sender, Encryption का प्रयोग करता है। तथा Receiver, decryption एल्गोरिथम् का प्रयोग करता है। Encryption तथा Decrytpion एल्गोरिथम् को Ciphers की तरह Refer करते हैं।

Key एक Number होता है जो Cipher पर एक एल्गोरिथम् की तरह ऑपरेट होती है।

हम पूरे क्रिप्टोग्राफी एल्गोरिथम्स को दो समूहों में विभाजित कर सकते हैं–1. Symmetric Key (इसे Secret Key भी कहते हैं) Cryptography Algorithms तथा (ii) Asymmetric (इसे Public Key भी कहते हैं) Key Cryptography Algorithms निम्न Fig. में दोनों कीज़ की Categroy को दर्शाया गया है–

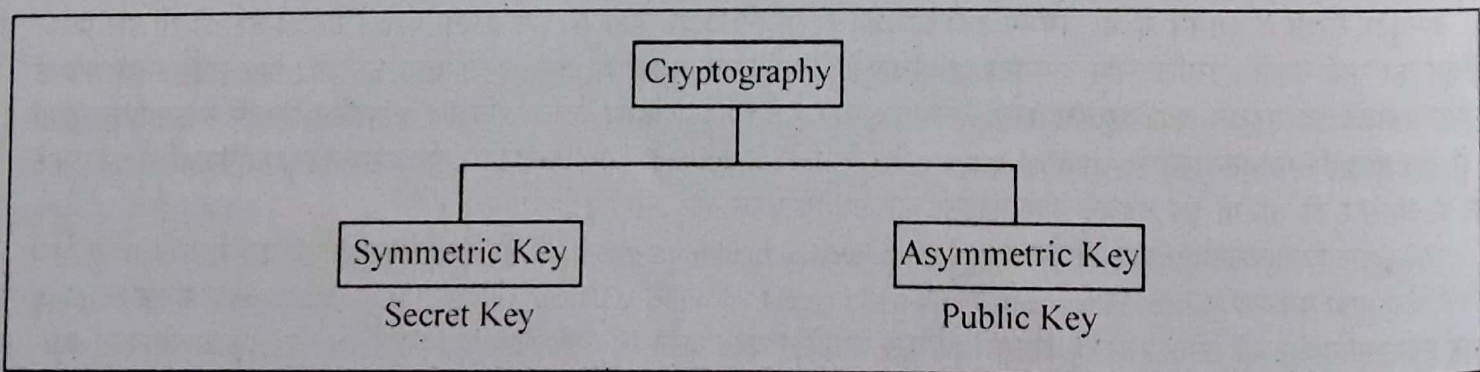


Fig. : Categories of Cryptography

1. Symmetric Key Cryptography–Symmetric Key Cryptography में दोनों Parties (Sender तथा Receiver) के द्वारा Same Key प्रयोग की जाती है। Sender इस Key को प्रयोग करता है तथा एक Encryption Algerithm डाटा को Encrypt करता है। Receiver, Same Key को प्रयोग करता है तथा इसके Corresponding, Decryption Algorithm डाटा को Decrypt करता है। अग्र Fig. में Symmetric Key Cryptography को प्रदर्शित किया गया है–

Scanned by CamScanner

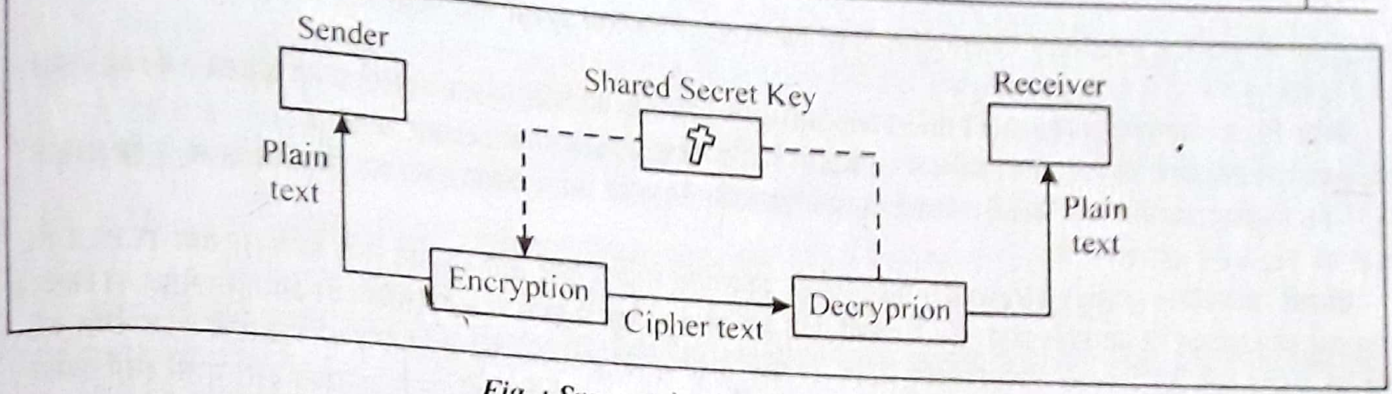


Fig. : Symmetric Key Cryptography

(ii) Asymmetric-Key Cryptography– Asymmetric या Public Key Cryptography में दो Keys होती हैं– (i) Private Key तथा (ii) Public Key. Private Key को रिसीवर (Receiver) के द्वारा रखा जाता है तथा Public Key को, Public को Announce किया जाता है। निम्न Fig. में Asymmetric Key Cryptography को प्रदर्शित किया गया है–

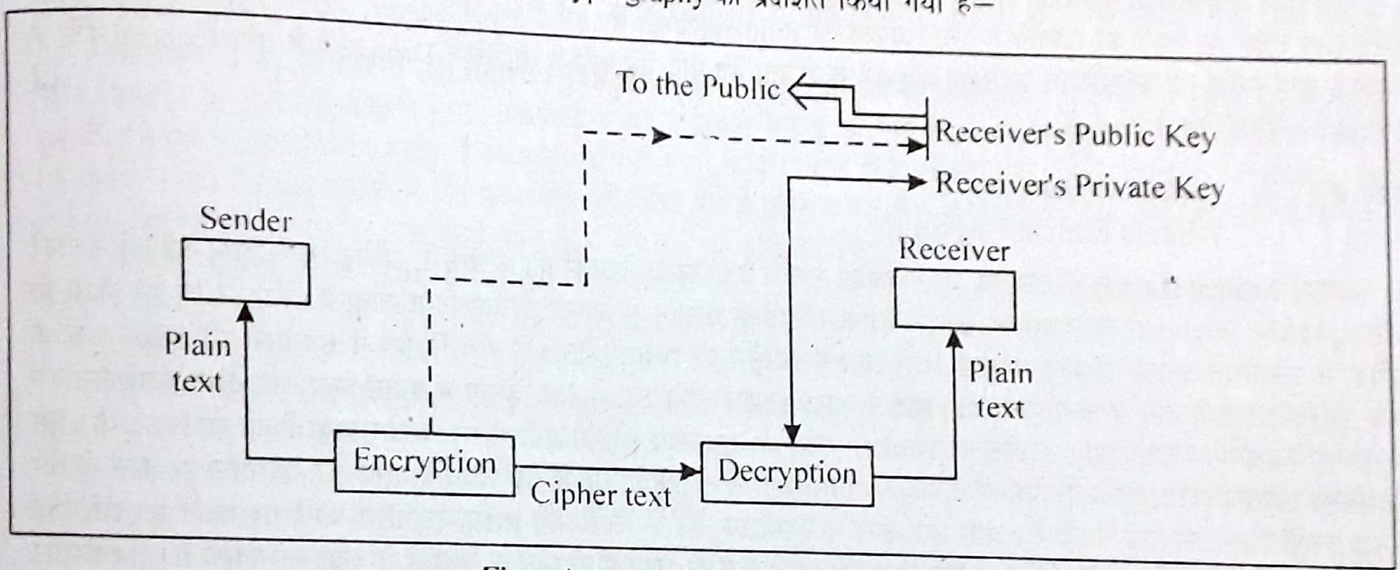


Fig. : Asymmetric Key Cryptography

Public Key Encryption/Decryption में Public Key का प्रयोग Encryption में Private Key (जिसे Decryption में प्रयोग किया जाता है) से अलग होता है। Public Key, Public को उपलब्ध होती है जबकि Private Key केवल Individual होती हैं।

❑

प्रश्न 3 – फायरवॉल क्या है? उदाहरण सहित समझाइये।

What is Firewall? Explain with examples. **(Jan., 2005)**

उत्तर–फायरवॉल (Firewall)–फायरवॉल एक डिवाइस होती है (सामान्यतः एक Router या एक कम्प्यूटर) जो एक ऑर्गेनाइजेशन के इंटरनल नेटवर्क तथा इसके अतिरिक्त इंटरनेट डिवाइसों के मध्य Install की जाती है। इसे कुछ पैकेटों को Forward तथा दूसरों को फिल्टर करने के लिये डिजाइन किया जाता है। अग्रांकित Fig. में Firewall को प्रदर्शित किया गया है–

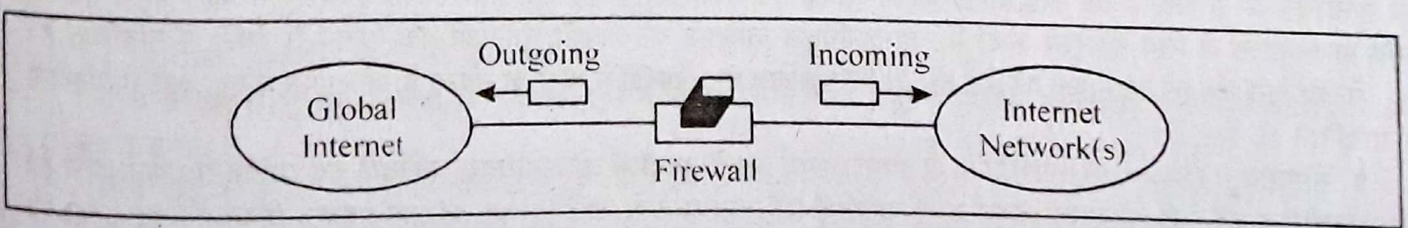


Fig. : Firewall

एक फायरवॉल सभी Incoming पैकेटों को एक Specific host या एक Specific Server जैसे HTTP के लिये भेजने के लिये फिल्टर कर सकता है। एक फायरवॉल ऑर्गेनाइजेशन में किसी Sepcific होस्ट या Specific सर्विस में एक्सेस करने के लिये Deny करने के लिये

Scanned by CamScanner

प्रयोग किया जा सकता है। फायरवॉल को सामान्यतः पैकेट फिल्टर फायरवॉल तथा प्रॉक्सी बेस्ड फायरवॉल के रूप में वर्गीकृत किया गया है।

पैकेट फिल्टर फायरवॉल (Packet Filter Firewall)—एक फायरवॉल को पैकेट फिल्टर की तरह प्रयोग कर सकते हैं। यह नेटवर्क लेयर तथा ट्रांसपोर्ट लेयर हैडर्स में इनफॉरमेशन पर आधारित पैकेटों को Forward या Block कर सकता है।

पैकेट फिल्टर फायरवॉल एक Router होता है जो एक फिल्टरिंग टेबल का प्रयोग करता है जो यह निर्धारित करती है कि कौन से पैकेटों को Forward नहीं करना है।

प्रॉक्सी फायरवॉल (Proxy Firewall)—पैकेट फिल्टर फायरवॉल, नेटवर्क लेयर तथा ट्रांसपोर्ट लेयर हैडर्स (IP तथा TCP/UDP) में उपलब्ध इनफॉरमेशन पर आधारित फायरवॉल है। कभी-कभी हमें मैसेज को खुद में उपलब्ध इनफॉरमेशन पर आधारित मैसेज को फिल्टर करने की जरूरत होती है। जैसे एक ऑर्गेनाइजेशन, अपने वेब पेजों से सम्बन्धित Policies को इम्प्लीमेन्ट करना चाहती है कि केवल वही इंटरनेट यूजर्स जो पहले से कम्पनी के साथ बिजनेस रिलेशन को रखते हैं। वही इसमें एक्सेस करें इनके अतिरिक्त दूसरे यूजर्स इसमें एक्सेस नहीं करें। इस Case में पैकेट फिल्टर फायरवॉल Feasible नहीं है। इस Case में Proxy कम्प्यूटर को Install करते हैं जो Customer कम्प्यूटर के बीच में होता है।

जब यूजर क्लाइंट एक मैसेज को भेजता है, Proxy Firewall रिक्वेस्ट को रिसीव करने के लिये सर्वर प्रोसेस को रन करता है। सर्वर एप्लीकेशन लेवल पर पैकेट को खोलता है तथा रिक्वेस्ट को Find out करता है। इस Case में Server, क्लाइंट प्रोसेस की तरह व्यवहार करता है तथा मैसेज को कॉरपोरेशन के Real Server पर भेजता है। यदि यह नहीं है तो मैसेज Drop होता है तथा External यूजर के पास Error मैसेज भेजता है। ❑

प्रश्न 4 – *Ethical Hacking क्या है?*

What is Ethical Hacking?

उत्तर–Ethical Hacking—इंटरनेट, सूचनाओं का भण्डार है। इंटरनेट नेटवर्कों का नेटवर्क है, अर्थात् भिन्न-भिन्न टाईप के नेटवर्कों (LAN, MAN, WAN) पर कम्प्यूटरों को कम्यूनिकेशन मीडिया के माध्यम से आपस में जोड़ दिया जाता है। इंटरनेट पर हम किसी भी टॉपिक से सम्बन्धित सूचना को देख सकते हैं। शुरूआत में इंटरनेट का विकास USA के रक्षा विभाग में सूचनाओं को Share करने के लिये ARPANET के नाम से किया गया था। बाद में ARPANET को USA में रक्षा विभाग में प्रयोग किया गया तथा कमर्शियल रूप से इंटरनेट का प्रयोग किया गया। इंटरनेट पर किसी भी तरह की सूचनाओं को आसानी से घर बैठकर प्राप्त किया जा सकता है। जैसे यदि किसी विश्वविद्यालय में किसी कोर्स में एडमीशन लेना चाहते हैं तो इसके बारे में उस विश्वविद्यालय की वेबसाइट पर कोर्स के बारे में पूरी इनफॉरमेशन को देख सकते हैं। तथा उस कोर्स में एडमीशन लेने के लिये ऑन-लाइन एडमिशन फॉर्म भर सकते हैं। इसी तरह किसी संख्या, प्रोडक्ट, आइटम इत्यादि के बारे में संपूर्ण जानकारी कुछ ही क्षणों में इंटरनेट के माध्यम से देखा जा सकती है। जब इंटरनेट का काफी प्रयोग किया जाने लगा तो इस पर किसी ऑर्गेनाइजेशन, संस्था आदि से सम्बन्धित इनफॉरमेशन को इंटरनेट यूजरों के माध्यम से चुराया जाने लगा जो कि अवैध है, इसे Hacking कहते हैं तथा इस प्रक्रिया को Ethical Hacking कहते हैं।

Hacking करने वाले यूजर को Hacker कहते हैं। Hacker वह यूजर होता है जो इंटरनेट पर किसी व्यक्तिगत या Secret सूचना को अवैध रूप से प्रयोग करता है। ❑

प्रश्न 5 – *नेटवर्क सिक्यूरिटी पाथवेज में क्या-क्या बाधाएं हैं? किन-किन बातों का आप ध्यान रखेंगे?*

What are the barriers in network security pathways? What are the issues to be considered in network security?

उत्तर—सिक्यूरिटी एक व्यापक विषय है और अनेक प्रकार के कार्यों को सम्मिलित करती है। अपने सरलतम रूप में, हमें इस बात को सुनिश्चित करना होता है कि कोई बाहरी व्यक्ति आपके उन संदेशों को न पढ़ सके तथा उनको गुप्त रूप से बदल भी न सके जो अन्य प्राप्तकर्त्ताओं के लिये हैं। दूसरे शब्दों में, यह अनधिकृत व्यक्तियों को आपकी सूचनाओं तक पहुंचने से रोकने से सम्बन्धित है।

नेटवर्क सुरक्षाओं की समस्याओं को मोटे तौर पर निम्नलिखित चार मापदंडों में बांटा जा सकता है, जो आपस में एक-दूसरे से घनिष्टता से सम्बन्धित भी हैं—

1. गोपनीयता (Secrecy)—गोपनीयता से हमारा तात्पर्य अपनी सूचनाओं को अनधिकृत व्यक्तियों तक पहुंचने से रोकना होता है। दूसरे शब्दों में हमारी कोई भी सूचना केवल उन्हीं व्यक्तियों को उपलब्ध होनी चाहिये, जिन तक हम पहुंचना चाहते हैं। यह सुरक्षा की सबसे अधिक मौलिक आवश्यकता होती है और नेटवर्क सुरक्षा की बात करते समय लोगों का ध्यान इसी पर सबसे पहले जाता है।

2. अधिप्रमाणन (Authentication)—अधिप्रमाणन से हमारा तात्पर्य कोई नाजुक सूचना देने या सौदा करने से पहले यह सुनिश्चित करना है कि हम सही व्यक्ति से ही संवाद कर रहे हैं।

Scanned by CamScanner

3. स्वीकृति (Non-repudiation)–इसका तात्पर्य है कि किसी विशेष दिन और समय पर कोई संदेश भेजे जाने का पक्का प्रमाण हमारे पास होना चाहिये, ताकि भेजने वाला उसके भेजे जाने से इंकार न कर सके।

4. सत्यनिष्ठा (Integrity)–इसका तात्पर्य यह सुनिश्चित करना है कि जो संदेश भेजा गया है वह बिना किसी परिवर्तन के ठीक वैसा ही प्राप्तकर्त्ता तक पहुंच जाये, अर्थात् बीच में ही कोई उसे शरारतपूर्ण ढंग से बदल न सके। ❑

प्रश्न 6 – *नेटवर्क लेवल एवं एप्लीकेशन लेवल फायरवाल में अंतर कीजिए।*
Differentiate between network level and application level firewall.

उत्तर–नेटवर्क-स्तरीय फायरवाल (Network-level Firewell)–नेटवर्क लेवल फायरवाल के अंतर्गत निम्नलिखित तकनीकियों का प्रयोग किया जाता है–

–पैकेट फिल्टरिंग (Packet Filtering)–कोई पैकेट फिल्टरिंग फायरवाल उसे पार करने वाले प्रत्येक पैकेट की जांच करता है और उसे आपके द्वारा निर्धारित नियमों की कसौटी पर कसता है। यह पैकेट उस परीक्षा में पास हो जाता है और यदि वह पास नहीं होता, तो उसे रद्द कर दिया जाता है। ऐसा प्रायः पैकेटों में शामिल IP header में दी गयी सूचनाओं अर्थात् IP addresses के आधार पर किया जाता है, इसलिये ऐसे फायरवाल को एड्रेस फिल्टरिंग भी कहा जाता है। एड्रेस फिल्टरिंग में ऐसे नोडों को सुरक्षित किया जा सकता है, जिनका बाहरी दुनिया से मतलब नहीं होता।

–स्टेटफुल पैकेट इंस्पेक्शन (Stateful Packet Inspection)–इस तकनीकी को संक्षेप में SPI कहा जाता है। यह साधारण पैकेट फिल्टरिंग के आगे की सीढ़ी है। SPI तकनीकी वाला फायरवाल पैकेटों को एक समूह के रूप में देखता है न कि अलग इकाई के रूप में। यह इस बात का विवरण रखता है कि कौन-कौन-से पैकेट फायरवाल से होकर निकल चुके हैं और इस प्रकार अनधिकृत उपयोग को पहचान सकते हैं। कुछ मामलों में ऐसे फायरवाल संदेहास्पद पैकेटों को तब तक रोके रखते हैं, जब तक उन्हें ऐसी अतिरिक्त सूचनायें न मिल जायें जिनके आधार पर उन्हें आगे जाने दिया जा सके या रद्द कर दिया जा सके।

–सर्किट-स्तरीय गेटवे (Circuit-level Gateway)–कोई सर्किट स्तरीय गेटवे फायरवाल किसी सर्वर और उसके क्लाइंट कम्प्यूटरों के बीच कनेक्शनों का प्रबंध करता है। जो TCP/IP पतों और पोर्ट नम्बरों पर आधारित होता है। जब उनमें कनेक्शन स्थापित हो जाता है, तो वह गेटवे या फायरवाल उन सिस्टम के बीच पैकेट के आदान-प्रदान में कोई बाधा नहीं डालता।

–एप्लीकेशन-स्तरीय फायरवाल (Application-level Firewall)–उपरोक्त तीनों प्रकार के फायरवाल-पैकेट फिल्टरिंग, स्टेट फुल पैकेट इंस्पेक्शन और सर्किट-स्तरीय फायरवाल केवल IP addresses और Root Numbers के आधार पर पैकेटों को फिल्टर करते हैं और सभी TCP/IP पैकेटों को एक ही प्रकार से संभालते हैं। इनको Network-level Firewall कहते हैं, परन्तु एप्लीकेशन-लेवल फायरवाल, नेटवर्क-लेवल फायरवालों से अधिक बुद्धिमान होते हैं।

· एप्लीकेशन लेवल फायरवाल, प्रॉक्सी सर्वरों की तरह भी कार्य करते हैं। कोई प्रॉक्सी सर्वर एक ऐसा कम्प्यूटर है जो किसी क्लाइंट कम्प्यूटर और किसी वास्तविक सर्वर के बीच बैठता है। वह वास्तविक सर्वर को भेजे गये प्रत्येक पैकेट को बीच में ही रोक लेता है और उसको प्रोसेस करता है। प्रॉक्सी सर्वर किसी पैकेट के अन्दर की सामग्री की जाँच कर सकता है और यह तय कर सकता है कि उसको वास्तविक सर्वर को जाने दिया जाये अथवा वहीं रद्द कर दिया जाये। आवश्यक होने पर वह वास्तविक सर्वर को शामिल किये बिना सीधे ही क्लाइंट कम्प्यूटर को उस पैकेट का उत्तर दे सकता है। ❑

प्रश्न 7 – *फायरवाल की विशेषताएं एवं सीमाओं को लिखिए।*
Write the features and limitations of firewalls.

उत्तर–फायरवाल, नेटवर्क वातावरण को सुरक्षित रखते हैं। फायरवॉल की प्रमुख विशेषतायें निम्नलिखित हैं–

1. फायरवाल "deny all services except those specifically permitted" डिजाइन पॉलिसी पर आधारित है।
2. फायरवाल, Flexible होते हैं। ये ऑर्गेनाईजेशन के अनुसार सिक्योरिटी पॉलिसी तथा नयी सेवाओं को उपलब्ध कराते हैं।
3. फायरवाल, authentication measures को रखते हैं।
4. फायरवाल फिल्टरिंग तकनीकी को रखते हैं।
5. फायरवाल FTP तथा Telnet के लिये Proxy सेवाओं का प्रयोग करते हैं ताकि एडवांस authentication measures को धारण किया जा सके।

फायरवाल की प्रमुख सीमायें निम्नलिखित हैं–

1. यद्यपि फायरवाल का प्रयोग नेटवर्क को पूर्ण सुरक्षा प्रदान करना होता है लेकिन यदि केवल हार्डवेयर फायरवाल का ही प्रयोग किया गया है तो सॉफ्टवेयर का प्रयोग करने से सिस्टम में Virus की संभावनायें बढ़ जाती हैं, जिससे सिस्टम में स्टोर किया गया डाटा खराब हो सकता है। इसलिये हार्डवेयर तथा सॉफ्टवेयर दोनों में फायरवाल को होना जरूरी है।

2. नेटवर्क पर सिस्टम में इंटरनेट का प्रयोग करते समय कुछ Sites को प्रयोग नहीं करना चाहिये क्योंकि इनकी वजह से सिस्टम में फाइलें करेप्ट हो जाती हैं। ❑

Scanned by CamScanner

प्रश्न 8 – डिक्रिप्शन से आप क्या समझते हैं?
What do you understand by Decryption? Explain.

उत्तर–Descryption : Decryption, encryption की विपरीत प्रक्रिया है। कम्प्यूटर नेटवर्किंग में जब डाटा एण्ड सिस्टम से दूसरे सिस्टम के रूप में होता है। अतः डाटा कम्युनिकेशन में डाटा को सुरक्षित रूप में पहुंचाने के लिये Cryptography तकनीक का प्रयोग किया जाता है। इस तकनीक के अनुसार डाटा को एक कोड में envelope करते है तथा इस प्रक्रिया को encryption कहते हैं तथा इसके विपरीत destination नोड पर इस envelope को खोलकर पुनः डाटा को पूर्ण अवस्था में लाया जाता हैं इसे decryption कहते हैं।

Decryption, डाटा को बदलने का विज्ञान है ताकि यह unauthorised व्यक्ति के लिये प्रयोग हीन तथा unrecognised रहे। Decryption, Encrypted डाटा को पुनः इसके वास्तविक रूप में बदलते हैं। निम्नलिखित Fig में इस प्रोसेस को स्पष्ट रूप से समझाया गया है।

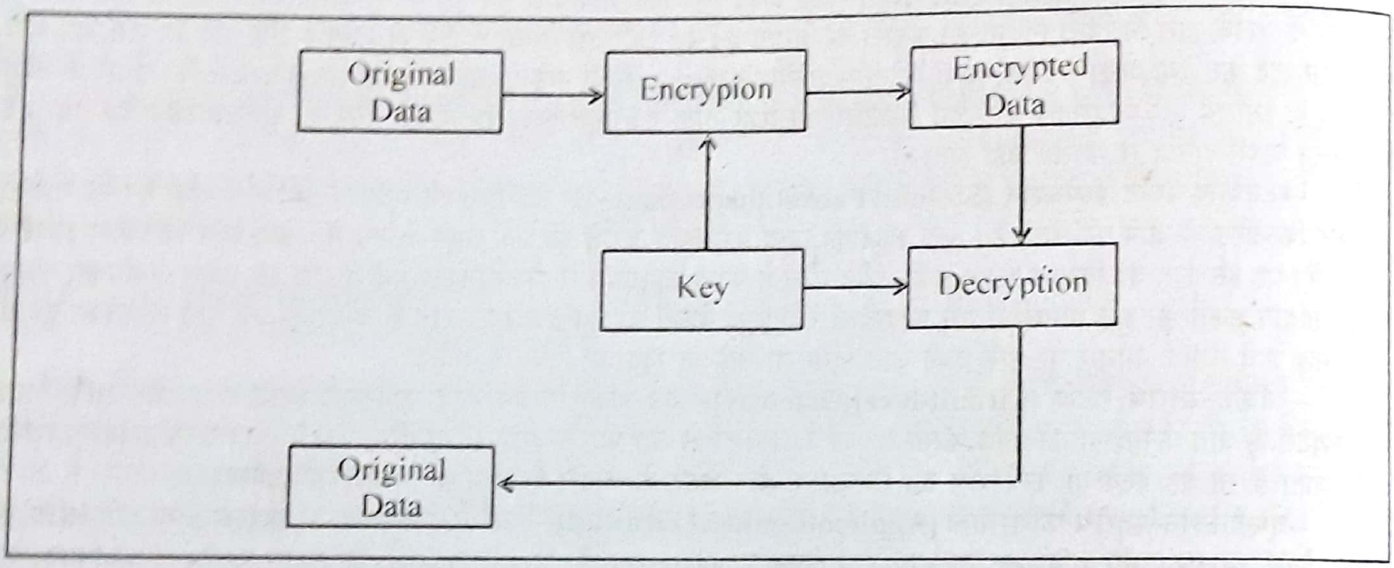


Fig. : Encryption- Decryption Process

❑

प्रश्न 9 – डिजिटल सिग्नेचर क्या है? इसकी उपयोगिता बताइये। इसे कैसे बनाया जाता है?
What is digital Signature? Explain the uses. How will you prepare this? (June, 2006)

उत्तर–डिजिटल सिग्नेचर (Digital Signature)–यद्यपि MAC मैसेज इंटीग्रिटी तथा मैसेज ऑथेन्टिकेशन को उपलब्ध करा सकता है लेकिन इसका एक Drawback है। इसे एक Symmetric Key की जरूरत होती है जो Sender तथा Receiver के मध्य अवश्य स्थापित होनी चाहिये। इसके सापेक्ष डिजिटल सिग्नेचर (Digital Signature) Asymmetric Keys के Pair को प्रयोग कर सकता है जिसमें एक Public तथा एक Private Key होती है।

सिग्नेचर के बारे में हम सभी अच्छी तरह जानते हैं। हम एक डॉक्यूमेण्ट को यह दिखाने के लिये Sign करते हैं। यह हमारे द्वारा सत्यापित किया गया है। सिग्नेचर, Recipient के लिये Proof होता है। जब एक कस्टमर (Customer) एक चैक को अपने द्वारा Sign करता है, बैंक को इस बात के Proof की आवश्यकता होती है यह चैक Customer के द्वारा ही Sign किया गया है किसी दूसरे के द्वारा Sign नहीं किया गया है। दूसरे शब्दों में हम यह कह सकते हैं कि एक डॉक्यूमेण्ट पर सिग्नेचर, Authentiation को Verify करते हैं। इसी तरह जब Sender, Receiver के पास एक मैसेज को भेजता है तो Receiver को Sender की Authenticity को Check करने की जरूरत होती है। उसे Receiver को यह सुनिश्चित करने की जरूरत होती है कि यह मैसेज Sender के पास से आया है किसी और के पास से नहीं आया है। Sender इस सिग्नेचर को इलैक्ट्रॉनिक रूप से भी कर सकता है। दूसरे शब्दों में हम यह भी कह सकते हैं कि इलैक्ट्रॉनिक सिग्नेचर Sender की Authenticity को सिद्ध करते हैं। इस टाईप के सिग्नेचर को डिजिटल सिग्नेचर (Digital Signature) कहते हैं।

पारम्परिक रूप से हम जो सिग्नेचर करते हैं वह डॉक्यूमेन्ट में सम्मिलित होते हैं, यह डॉक्यूमेण्ट का भाग होता है। जब हम एक चैक को लिखते हैं तो सिग्नेचर चैक पर होते हैं यह अलग डॉक्यूमेण्ट नहीं होता है। दूसरी तरफ जब हम डॉक्यूमेण्ट को डिजिटल रूप में Sign करते हैं तो हम सिग्नेचर (Signature) को अलग डॉक्यूमेन्ट के रूप में भेजते हैं। Sender दो डॉक्यूमेण्ट्स को भेजता है एक मैसेज तथा

Scanned by CamScanner

दूसरा सिग्नेचर (Signature). Receipent दोनों डॉक्यूमेण्ट्स को रिसीव करता है। उन्हें Verify करता है जिसमें सिग्नेचर Sender को इंगित करता है। यदि यह सिद्ध हो जाता है तो मैसेज रखा जाता है अन्यथा इसे रिजेक्ट कर दिया जाता है। डिजिटल सिग्नेचर का लाभ यह होता है कि इसमें Security अधिक होती है। कोई भी व्यक्ति इन सिग्नेचर को देख नहीं सकता है और Duplicate Sign नहीं कर सकता है, क्योंकि यह डिजिटली रूप में Save होते हैं जबकि साधारण सिग्नेचर की Duplicacy होने की संभावना होती है।

डिजिटल सिग्नेचर दो तरीके से बनाया जा सकता है–(i) डॉक्यूमेण्ट को Sign करके या (ii) डॉक्यूमेन्ट के एक Digest को Sign करके। प्रथम तरीका काफी आसान है, इसमें एक डॉक्यूमेन्ट को Sender Key Private Key के साथ Encrypt किया जाता है, Verify डॉक्यूमेन्ट को Sender के Public Key के साथ Decrypt किया जाता है। निम्न Fig. में दर्शाया गया है कि कैसे इसे Sign तथा Verify किया जाता है–

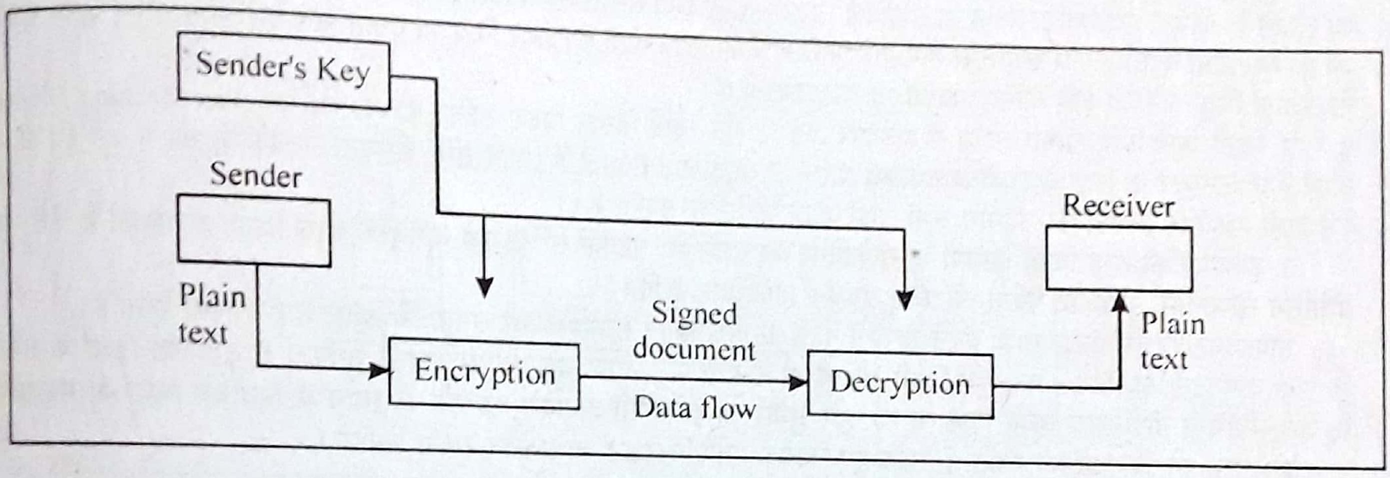


Fig. : Signing the Message itself in digital signature

दूसरे तरीके में डॉक्यूमेण्ट के Digest को Sign किया जाता है। इस तरीके का प्रयोग तब फायदेमंद होता है जब हम लम्बे मैसेज को Deal करते हैं। डिजिटल सिग्नेचर में मैसेज सामान्यतः लम्बा होता है। इसमें मैसेज को Sign करने के बजाय मैसेज के Digest को Sign करते हैं। Sender मैसेज Digest को Sign करता है तथा Receiver मैसेज Digest को Verify कर सकता है। अग्रांकित Fig. में डिजिटल सिग्नेचर में Digest Sign को दर्शाया गया है–

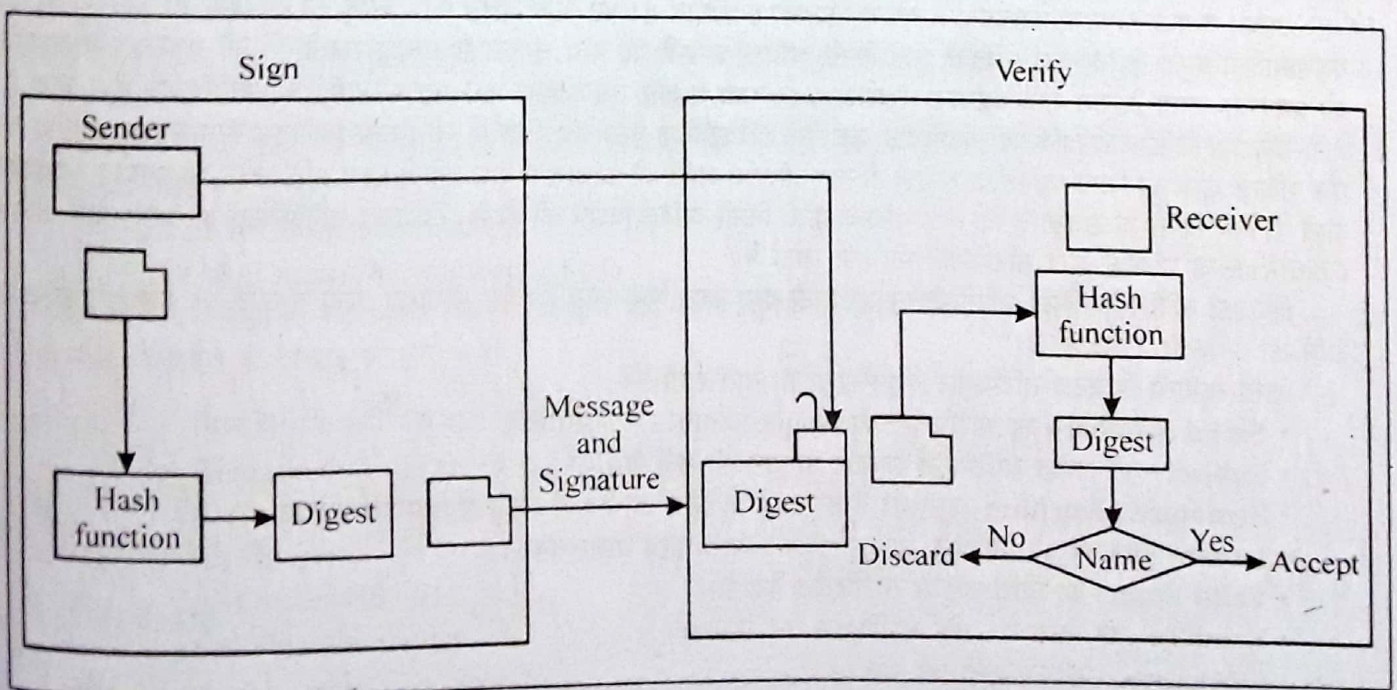


Fig. : Signing the digest in a digital system

Scanned by CamScanner

प्रश्न 10 – हमें नेटवर्क एडमिनिस्ट्रेशन का प्रबंधन कैसे करना चाहिए?
How should we manage networking administration?

उत्तर–एक से अधिक नोड के समूह को आपस में जोड़कर नेटवर्क को डिजायन किया जाता है। ये नोड आपस में किसी माध्यम से जुड़ी होती हैं। किसी नेटवर्क की नोड कोई कम्प्यूटर, प्रिंटर या अन्य उपकरण हो सकता है, जो नेटवर्क व अन्य नोडों द्वारा भेजा गया डाटा प्राप्त कर सके या उनको डाटा भेज सके। विभिन्न नोडों को जोड़ने वाले माध्यमों को प्रायः कम्यूनिकेशन चैनल कहा जाता है। दो या दो से अधिक कम्प्यूटरों को एक नेटवर्क के रूप में आपस में जोड़ने की क्रिया अथवा अवधारणा को नेटवर्किंग कहते हैं।

कम्प्यूटर नेटवर्क के एडमिनिस्ट्रेशन का प्रबंधन करते समय निम्नलिखित चार बिन्दुओं को ध्यान में रखना चाहिये–

1. नेटवर्क से जुड़े हुए किसी भी कम्प्यूटर पर स्टोर किया गया डाटा नेटवर्क के किसी भी अन्य कम्प्यूटर द्वारा सरलता से उपयोग में लाया जा सकता है–अथवा स्थानांतरित किया जा सकता है। इससे समस्त डाटा समस्त उपयोगकर्त्ताओं को हर समय उपलब्ध रहता है। इससे संगठन की कार्यकुशलता बढ़ती है और संचार पर होने वाले भारी खर्चे की बचत होती है। शेयर किये जा सकने वाले डाटा में साधारण पाठ्य फाइलों के अलावा चित्र, ऑडियो और वीडियो फाइलें भी हो सकती हैं।

2. किसी कम्पनी में सीमित संख्या में हार्डवेयर होते हैं; जैसे–हार्ड डिस्क, प्रिंटर, स्कैनर, DVD Drives, Fax Machine, Modem आदि। हर कम्प्यूटर के लिये ये हार्डवेयर उपलब्ध कराने से बहुत लागत आती है। यदि सभी कम्प्यूटर नेटवर्क के रूप में जुड़े हुए हों, तो ऐसे सभी हार्डवेयर साधनों का उपयोग सभी नोडों द्वारा किया जा सकता है।

3. हार्डवेयर की तरह किसी कम्पनी के सॉफ्टवेयर का साझा भी नेटवर्क से जुड़े हुये कम्प्यूटरों द्वारा किया जा सकता है; जैसे–वर्ड प्रोसेसिंग सॉफ्टवेयर, स्प्रैडशीट पैकेज, डाटाबेस प्रबंधन सॉफ्टवेयर आदि।

सॉफ्टवेयर का इस प्रकार साझा करने से सभी नोडों पर एक समान संस्करण और क्षमता का सॉफ्टवेयर उपलब्ध रहता है।

4. कम्प्यूटरों का नेटवर्क बनाने से किसी संगठन या कम्पनी के प्रशासन को एक ही नोड से सुगमता से संचालित किया जा सकता है; जैसे–विभिन्न नोडों द्वारा साझा किये जा रहे और सुधारे जा रहे किसी डाटाबेस को एक ही स्थान से नियंत्रित किया जा सकता है।

इस तरह इन बिन्दुओं को ध्यान में रखते हुए नेटवर्क एडमिनिस्ट्रेशन का प्रबंधन रखना चाहिये। ❑

प्रश्न 11 – डिजिटल सर्टिफिकेट टेक्नोलॉजी कहां उपयोग में लायी जाती है? यह कैसे काम करती है?
Where is digital certificate technology being used? How does it work?

उत्तर–पब्लिक कुंजियों को सुरक्षित रूप से वितरित करने के लिये एक ऐसे केन्द्र की कल्पना करते हैं, जो हर समय अर्थात् प्रतिदिन ऑन लाइन 24 घंटे मांग पर पब्लिक कुंजियां उपलब्ध कराने का कार्य करता हो। ऐसा केन्द्र शीघ्र ही कार्य के बोझ से दब जायेगा और इंटरनेट सुरक्षा जाम हो जायेगी।

इसका समाधान एक ऐसे संगठन के रूप में निकाला गया जिसे 24 घंटे ऑन लाइन कार्य करने की आवश्यकता नहीं है। वह केवल यह प्रमाणित करता है कि कोई पब्लिक कुंजी किसी व्यक्ति, कम्पनी या अन्य संगठन से सम्बंध रखती है। जो संगठन पब्लिक कुंजियों को प्रमाणित करता है, उसे सर्टिफिकेशन ऑथरिटी कहा जाता है और उसके द्वारा दिये गये डॉक्यूमेंट को सर्टिफिकेट कहा जाता है।

क्रिप्टोग्राफी में कोई डिजिटल सर्टिफिकेट एक ऐसा इलैक्ट्रॉनिक दस्तावेज होता है, जो किसी डिजिटल हस्ताक्षर का उपयोग करके एक पब्लिक कुंजी को किसी व्यक्ति या संगठन के नाम और पते आदि की पहचान से बांध देता है। इस सर्टिफिकेट का उपयोग यह प्रमाणित करने के लिये किया जा सकता है कि कोई पब्लिक कुंजी किसी व्यक्ति विशेष की ही है। डिजिटल सर्टिफिकेटों को कभी-कभी Identity Certificate या पब्लिक कुंजी सर्टिफिकेट भी कहा जाता है।

डिजिटल सर्टिफिकेट किसी सर्टिफिकेशन ऑथरिटी द्वारा जारी किये जाते हैं। वह ऑथरिटी अन्य संगठनों को ऐसे सर्टिफिकेट जारी करने का अधिकार दे सकती है।

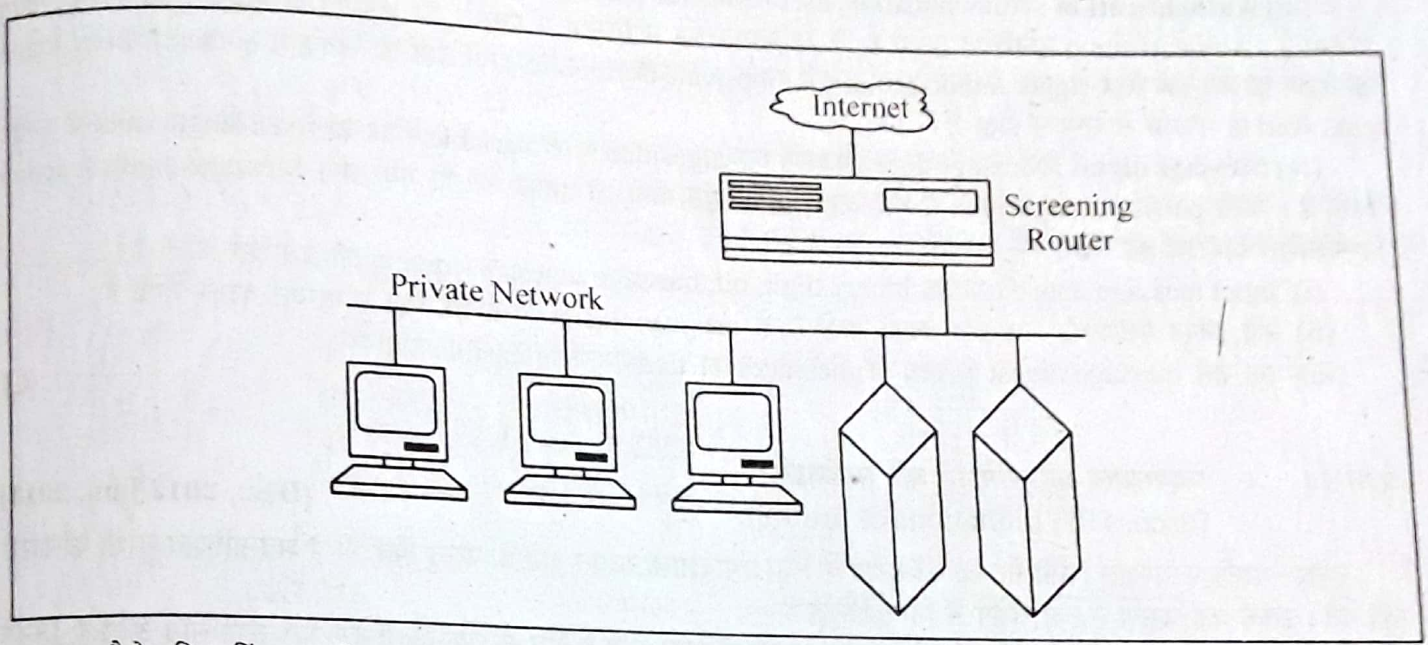
किसी सामान्य डिजिटल सर्टिफिकेट में निम्नलिखित बातें होती हैं–

- **Serial Number**–यह सर्टिफिकेट की unique पहचान संख्या होती है।
- **Subject**–वह व्यक्ति या संगठन जिसकी पहचान की गयी है।
- **Signature Algorithm**–हस्ताक्षर तैयार करने के लिये उपयोग में लाया गया एल्गोरिथम्।
- **Issuer**–सूचनाओं को प्रमाणित और सर्टिफिकेट जारी करने वाला संगठन।
- **Valid-From**–वह तिथि जब से सर्टिफिकेट वैध है।
- **Valid-To**–वह तिथि जब तक सर्टिफिकेट वैध रहेगा।
- **Key ussage**–पब्लिक कुंजी का उद्देश्य।
- **Public Key**–पब्लिक कुंजी।
- **Thumbprint Algorithm**–वह एल्गोरिथम् जो इस सर्टिफिकेट को हैश करने में प्रयोग किया जाता है।
- **Thumbprint**–हैश संख्या, यह प्रमाणित करने के लिये कि सर्टिफिकेट को बदला नहीं गया है। ❑

Scanned by CamScanner

प्रश्न 12 – ***IP Packet filter screening routers से आप क्या समझते हैं? बताइये।***
What do you under stand by IP Packet filter screening? Explain.

उत्तर–एक स्क्रीनिंग रूटर पैकेट फिल्टरिंग का कार्य करता है और एक फायरवॉल के रूप में प्रयोग किया जाता है। कुछ मामलों में एक स्क्रीनिंग रूटर आंतरिक नेटवर्क के लिए परिधि संरक्षण (Perameter protection) के रूप में या पूरे फायरवॉल समाधन के रूप में इस्तेमाल किया जा सकता है–



एक पैकेट फिल्टरिंग प्रणाली आंतरिक और बाहरी मेजबान (hosts) के बीच पैकेट को selectively रूट करता है। यह कार्य संगठन की नेटवर्क सुरक्षा नीति के अनुसार किया जाता है। पैकेट फिल्टरिंग एक रूटर में या एक bridge में या एक विशेष host में कार्य कर सकता है और नेटवर्क लेयर पर संचालित होता है।

जो रूटर, पैकेट फिल्टरिंग के लिए प्रयोग होता है, उसे **स्क्रीनिंग रूटर** कहा जाता है। इसे external network gateway में स्थापित किया जाता है। इसे नियमों से configure किया जाता है जिससे कि यह प्रोटोकॉल और एड्रेसस को ब्लॉक या फिल्टर कर सके। आंतरिक उपयोगकर्त्ताओं की आमतौर पर इंटरनेट पर सीधी पहुँच होती है, जबकि इंटरनेट से सभी या अधिकतर साइट प्रणालियों के लिए उपयोग अवरूद्ध है। हालांकि, रूटर नीति (policy) के आधार पर प्रणालियों और सेवाओं के लिए चयनात्मक पहुँच की अनुमति दे सकता है। खतरनाक सेवाएँ जैसे–कि NIS, NFS और X विंडोज को आमतौर पर अवरूद्ध किया जाता है।

एक स्क्रीनिंग रूटर पैकेट हेडर पर मौजूद जानकारी के आधार पर IP पैकेट को पास या खारिज कर देता है। स्क्रीनिंग रूटर निम्नलिखित जानकारी का मुख्य रूप से प्रयोग करता है–

(1) IP source और destination address

(2) TCP or UDP source और destination port

कुछ मामलों में स्क्रीनिंग रूटर पैकेट हेडर में जानकारी का प्रयोग ना करके, अपने रूटिंग निर्णय जानकारी जैसे–कि source और destination इंटरफेस के आधार पर लेता है। ❑

प्रश्न 13 – ***निम्नलिखित की परिभाषा दीजिये।***
Give the definitions of the following :
(i) Confidentiality
(ii) Integrity
(iii) Authentication
(iv) Message digest

उत्तर–**(i) Confidentiality :** Confidentiality, authorized users के लिये सीमित इनफॉरमेशन एक्सेस तथा disclousre को रेफर करती है तथा unauthorized users की एक्सेस को रोकती है।

Authentication methods जैसे user-IDs तथा passwords को unique रूप से identify किया जाता है। confidentiality के अंतर्गत डाटा सिस्टम के resources को नियन्त्रित करना तथा data system के users के द्वारा इनमें एक्सेस कराना है।

Scanned by CamScanner

confidentiality, विस्तृत रूप में data privacy के concept से सम्बन्धित है।

(ii) Integrity : Integrity, information resources के trustworthiness को रेफर करती है। इसमें data integrity का concept सम्मिलित होता है। यह inappropriate रूप में डाटा के बदलाव को रोकती है। Integrity, proper तथा स्पष्ट डाटा को सम्मिलित करती है। यह डाटा की puplicacy को रोकती है।

(iii) Authentication : Authentication, user name तथा password के आधार पर व्यक्तिगत रूप से identity करने की प्रक्रिया है। Authentication सुनिश्चित करता है कि व्यक्तिगत रूप से सिस्टम में एक्सेस की अनुमति दी गयी है, लेकिन उसमें किसी ऑपरेशन को करने के लिये rights authorization नहीं है। private तथा public, दोनों तरह के नेटवर्क में authentication, logon password के माध्यम से सम्पन्न होता है।

(iv) Message digest : Message digest फंक्शन एक algorithm है, जो variable मैसेज को fixed length value में कनवर्ट करता है। किसी particular algorithm से वही आउटपुट प्रोड्यूस होती जो इनपुट उसे दी गयी थी। Message digest function निम्नलिखित प्रॉपर्टीज को रखता है–

(i) Input message data की प्रत्येक binary digit, bit, message digest के content को प्रभावित करती है।

(ii) यदि इनपुट मैसेज की कोई बिट बदली जाती है तो message digest की प्रत्येक बिट सामान्यत बदली जाती है।

(iii) एक जैसे message digest के साथ दो messages को find करना infeasible होता है।

❑

*प्रश्न 14 – **फायरवाल की सीमाओं को समझाइये।***

Discuss the limitations of firewell. **(Dec., 2012/Jan., 2013)**

उत्तर–यद्यपि फायरवॉल किसी नेटवर्क की सुरक्षा के लिए प्रभावशाली साधन होते हैं, परन्तु फिर भी वे शत-प्रतिशत सुरक्षा की गारंटी नहीं देते। इसके कई कारण हैं, जो संक्षेप में निम्नलिखित हैं–

1. फायरवॉल यह मानते हैं कि सारे बुरे लोग उनके नेटवर्क से बाहर वाले हैं और नेटवर्क के अन्दर वाले सभी लोग अच्छे हैं, जिनके ऊपर पूरी तरह विश्वास किया जा सकता है। यह एक गलत कल्पना है, क्योंकि सभी भीतरी लोगों को सभी सूचनाएँ देखने की अनुमति नहीं दी जा सकती।

2. भले ही कोई कम्पनी अपने कर्मचारियों को चुनने में इतनी सावधान हो कि उनमें से कोई जानबूझकर कोई गलत कार्य नहीं करेगा, फिर भी नेटवर्क में कोई शरारतपूर्ण कोड डालकर फायरवॉलों को हराया जा सकता है। ऐसा नेटवर्क के किसी उपयोगकर्त्ता को इंटरनेट से कोई फाइल डाउनलोड करने के लिए राजी करके किया जा सकता है अथवा ई-मेल के साथ आये हुए किसी प्रोग्राम को चलाने के लिए कहकर किया जा सकता है।

3. फायरवॉल कई बार वैध उपयोगकर्त्ताओं के लिए अपना कार्य कराना कठिन बना देते हैं। कई बार फायरवॉल को ठीक से कॉनफिगर नहीं किया जाता (अर्थात् उसके नियम सही नहीं बनाये जाते)। इससे वे किसी नये अनुप्रयोग (Application) को नहीं पहचान पाते। यदि फायरवॉल किसी कार्य को नहीं करने देता है, तो उपयोगकर्त्ता यह सोचते हैं कि कोई कार्य कैसे किया जाये कि फायरवॉल बाधा न डाले अर्थात् उस को बिना रोकटोक के होने दे। उदाहरण के लिए, ई-मेल द्वारा फाइल ट्रांसफर करना एक प्रमुख कार्य होता है। फायरवॉल को प्रायः इस प्रकार कॉनफिगर किया जाता है कि वह बड़े ई-मेल संदेश को नहीं जाने देता। ऐसी स्थिति में उपयोगकर्त्ता को वह फाइल को कई टुकड़ों में तोड़कर कई बार में भेजनी पड़ती है। ऐसा करना बहुत झंझट वाला और उबाऊ होता है। इससे उपयोगकर्त्ता चिढ़ जाता है।

4. कई बार फायरवॉल किसी सेवा का अवैध उपयोग नहीं होने देते, परन्तु साथ ही वे वैध उपयोगकर्त्ताओं को भी वह सेवा प्राप्त करने से रोक देते हैं। इस स्थिति को सेवा-निषेध आक्रमण (Denial-of-service Attack) कहा जाता है। ऐसा घुसपैठियों की शरारत के कारण होता है, जो किसी कमजोरी का लाभ उठाकर आपके नेटवर्क में घुस जाते हैं। हालांकि इससे उन घुसपैठियों को कोई लाभ प्राप्त नहीं होता। इस स्थिति से पैकेटों के स्रोत आईपी पते की गहन जाँच करके बचा जा सकता है, जिसके लिए फायरवॉल को सही प्रकार से कॉनफिगर करना पड़ता है।

❑

*प्रश्न 15 – **डिजीटल सिग्नेचर किस प्रकार मैसेज की इंटीग्रिटी को सुनिश्चित करता है? व्याख्या कीजिये।***

Describe how digital signature can be used for ensuring message integrity?

Ans. Digital Signature : Digital signature, एक गणितीय प्रणाली है, जिसके द्वारा किसी digital message या document की प्रमाणिकता का प्रदर्शन किया जा सकता है। किसी valid digital signature से प्राप्तकर्ता (receiver) को यह विश्वास हो जाता है कि कोई मैसेज वास्तव में एक ज्ञात प्रेषण के द्वारा तैयार किया गया है तथा उसे बीच रास्ते में बदला नहीं गया है। digital signatures

Scanned by CamScanner

का प्रयोग मुख्यतः सॉफ्टवेयर वितरण, वित्तीय लेन देन और ऐसे ही अन्य मामलों में किया जाता है, जहाँ जालसाजी को पकड़ना महत्वपूर्ण होता है।

Digital signature में asymmetric cryptography का उपयोग किया जाता है। किसी असुरक्षित माध्यम से कोई मैसेज भेजने पर एक सही digital signature प्राप्तकर्ता को यह विश्वास दिला देता है कि वह मैसेज बताये जा रहे प्रेषक के द्वारा ही भेजा गया है। Digital signature होने पर कोई व्यक्ति यह दावा नहीं कर सकता है कि वे signature उसने नहीं किये हैं। Digital signature में निम्नलिखित तीन algorithm शामिल होते हैं।

(i) Key generating algorithm, जो सभी सम्भव प्राइवेट कुंजियों में से एच्छिक रूप में एक private key को चुनता है और उसकी corresponding पब्लिक कुंजी भी देता है।
(ii) Signing algorithm, जो किसी संदेश तथा एक प्राइवेट कुंजी से हस्ताक्षर तैयार कर देता है।
(iii) Signature algorithm, जो पब्लिक कुंजी तथा हस्ताक्षर देने पर उस संदेश की प्रमाणिकता को स्वीकार या अस्वीकार करता है।

निम्नलिखित Fig. में digital signature का उपयोग तथा उसकी जाँच करने की प्रक्रिया को स्पष्ट रूप से दर्शाया गया है–

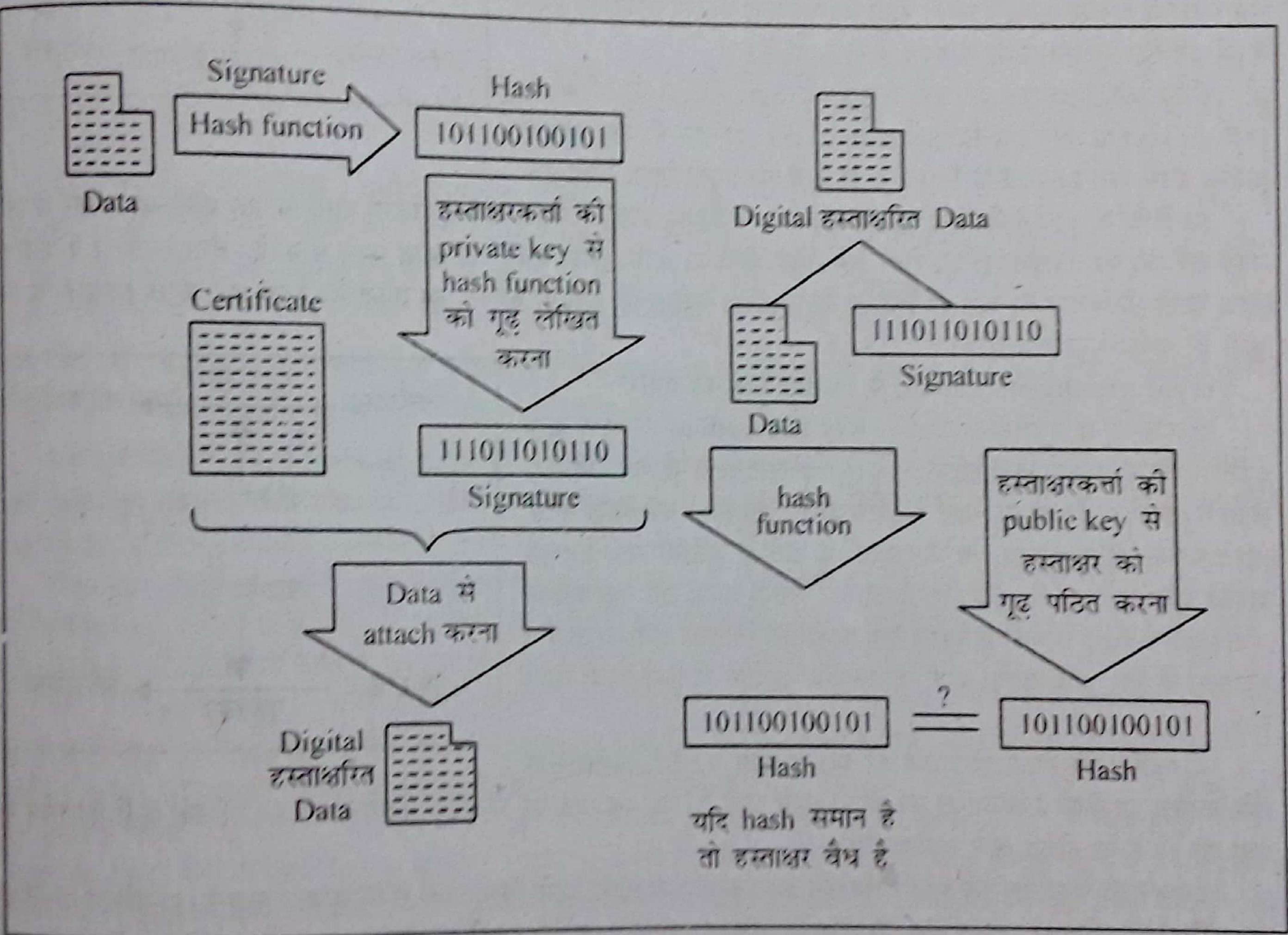


Fig. : Digital Signature Use and Checking Method

उपर्युक्त Fig. में किसी इलैक्ट्रॉनिक दस्तावेज के साथ डिजिटल हस्ताक्षर जोड़ने और उसकी जांच करने की विधि दिखायी गयी है। ❑

प्रश्न 16 – *क्रिप्टोग्राफी क्या है? क्रिप्टोग्राफी मैकेनिज्म में उपयोगी प्राइवेट एवं पब्लिक-की को समझाइये।*
What is cryptography? Explain public and private keys to be used for cryptography mechanism.

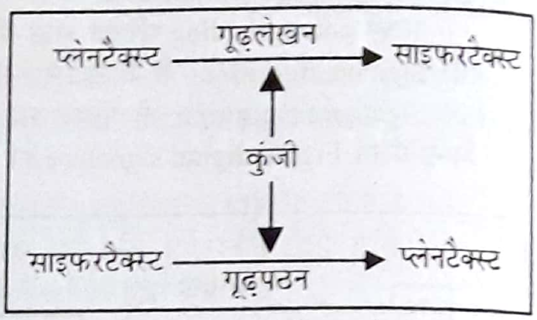
Ans. Cryptography : सूचनाओं को गुप्त रखने की प्रक्रिया तथा उसके अध्ययन को cryptography कहते हैं। इसे cryptology के नाम से भी जाना जाता है। कम्प्यूटर के क्षेत्र में cryptography का व्यापक प्रयोग किया जाता है, जैसे ATM cards, passwords

Scanned by CamScanner

तथा E-commerce इत्यादि। cryptography का मुख्य उपयोग किसी सूचना को दो सहभागियों के बीच इस प्रकार भेजना है कि अन्य लोग उसे न पढ़ सकें।

cryptography में मुख्यतः encryption तथा decryption प्रक्रिया का प्रयोग किया जाता है। किसी साधारण सूचना को अक्षरों या चिन्हों के किसी की समक्ष में न आने योग्य में बदलना encryption कहलाता है तथा इसके विपरीत किसी encrypted सूचना को उसके मूल रूप में बदलना decryption कहलाता है।

cryptography mechanism में private key या secret key का प्रयोग—

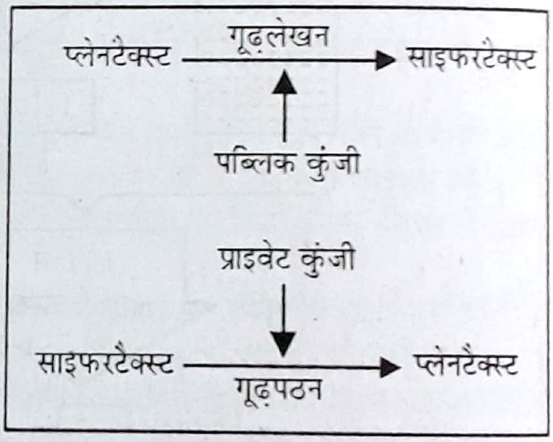


सीक्रेट कुंजी गूढ़लेखन (Secret Key Encryption)—सीक्रेट कुंजी क्रिप्टोग्राफी में गूढ़लेखन और गूढ़पठन दोनों क्रियाओं के लिए एक ही कुंजी का प्रयोग किया जाता है। इसलिए कोई संदेश अर्थात् प्लेनटैक्स्ट होने पर उसे गूढ़लेखन विधि द्वारा उस कुंजी का प्रयोग करके साइफरटैक्स्ट में बदला जाता है, जो कि मूल संदेश के बराबर आकार का ही होता है। गूढ़पठन में उसी कुंजी का प्रयोग करके उसे फिर से मूल संदेश में बदल लिया जाता है।

सीक्रेट कुंजी गूढ़लेखन को प्रायः सिंगल की (Single key) या प्राइवेट की (Private key) या सीमिट्रिक की (Symmetric key) गूढ़लेखन भी कहा जाता है, क्योंकि इसमें दोनों क्रियाओं के लिए एक ही कुंजी का प्रयोग किया जाता है।

इस विधि के उपयोग के लिए यह आवश्यक है कि किसी संदेश के प्रेषक और प्राप्तकर्त्ता दोनों ही उस कुंजी को जानते हों और उनमें इस बात का समझौता हो कि दोनों उसी साझा कुंजी का प्रयोग संदेश भेजने और प्राप्त करने में करेंगे। ऐसा करने पर वे कोई भी संदेश किसी भी माध्यम से, चाहे वह कितना भी असुरक्षित क्यों न हो, सुरक्षित रूप में भेज सकते हैं। इसमें शर्त केवल इतनी है कि उस कुंजी को पूर्णतः गुप्त रखा जाये।

cryptography mechanism में public key का प्रयोग—



पब्लिक कुंजी गूढ़लेखन (Public Key Encryption)—पब्लिक कुंजी गूढ़लेखन को कभी-कभी असीमिट्रिक की (Asymmetic key) गूढ़लेखन भी कहा जाता है। इसमें सीक्रेट की गूढ़लेखन की तरह कुंजियों का साझा नहीं किया जाता, बल्कि प्रत्येक व्यक्ति (प्रेषक और प्राप्तकर्त्ता) के पास दो कुंजियाँ होती हैं—एक प्राइवेट कुंजी (Private key), जो किसी को नहीं बतायी जाती, और एक पब्लिक कुंजी (Public key), जिसकी जानकारी सभी को होती है। पब्लिक कुंजी का उपयोग गूढ़लेखन के लिए और प्राइवेट कुंजी का उपयोग गूढ़पठन के लिए किया जाता है।

ध्यान दीजिए कि हम प्राइवेट कुंजी को 'प्राइवेट कुंजी' कहते हैं, सीक्रेट कुंजी नहीं, क्योंकि यह केवल एक व्यक्ति की अपनी कुंजी होती है। यह इस बात को भी स्पष्ट करता है कि हम पब्लिक कुंजी गूढ़लेखन की चर्चा कर रहे हैं या सीक्रेट कुंजी गूढ़लेखन की।

पब्लिक कुंजी क्रिप्टोग्राफी से हम वह सब कुछ कर सकते हैं, जो सीक्रेट कुंजी क्रिप्टोग्राफी से किया जा सकता है। हालांकि ये एल्गोरिथ्म थोड़े धीमे होते हैं। फिर भी पब्लिक कुंजी क्रिप्टोग्राफी अधिक उपयोगी है, क्योंकि इसको कॉनफिगर करना और उपयोग में लाना अपेक्षाकृत सरल होता है। इसलिए किसी संवाद (Communicaton) के प्रारम्भ में पब्लिक कुंजी का उपयोग करके दोनों पक्षों का अधिप्रमाणन (Authentication) किया जा सकता है और फिर शेष संवाद सीक्रेट कुंजी क्रिप्टोग्राफी द्वारा किया जा सकता है।

किसी संदेश के प्रेषण में पब्लिक कुंजी का उपयोग किस प्रकार किया जाता है, यह एक उदाहरण से अच्छी तरह समझा जा सकता है। मान लीजिए कि एक व्यक्ति 'क' दूसरे व्यक्ति 'ख' को एक संदेश किसी असुरक्षित माध्यम से भेजना चाहता है और 'क' की कुंजियों का जोड़ा (पब्लिक$_{क}$, प्राइवेट$_{क}$) है और 'ख' की कुंजियों का जोड़ा (पब्लिक$_{ख}$, प्राइवेट$_{ख}$) है। अब मान लीजिए कि 'क' और 'ख' एक दूसरे की पब्लिक कुंजियों को जानते हैं। इस स्थिति में 'क' द्वारा अपना संदेश 'ख' को 'ख' की पब्लिक कुंजी द्वारा गूढ़लेखित करके भेजा जाएगा। जिसे 'ख' द्वारा अपनी प्राइवेट कुंजी से गूढ़पठित किया जाएगा। इसी प्रकार 'ख' द्वारा अपना संदेश 'क' को 'क' की पब्लिक कुंजी द्वारा गूढ़लेखित करके भेजा जाएगा। जिसे 'क' द्वारा अपनी प्राइवेट कुंजी से गूढ़पठित किया जाएगा। इसे सूत्र रूप में नीचे समझाया गया है—

Scanned by CamScanner

व्यक्ति 'क'		व्यक्ति 'ख'
संदेश$_क$ का पब्लिक$_ख$ द्वारा गूढ़लेखन	———→	संदेश$_क$ का प्राइवेट$_ख$ द्वारा गूढ़पठन
संदेश$_ख$ का प्राइवेट$_क$ द्वारा गूढ़पठन	←———	संदेश$_ख$ का पब्लिक$_क$ द्वारा गूढ़लेखन

इस उदाहरण से स्पष्ट है कि इस विधि की सफलता के लिए सबको एक दूसरे की पब्लिक कुंजी का ज्ञान होना आवश्यक है। वास्तव में पब्लिक कुंजी को प्रचारित करना ही इस विधि की सबसे बड़ी चुनौती है।

पब्लिक कुंजी क्रिप्टोग्राफी का उपयोग मुख्यतः अधिप्रमाणन (Authentication) तथा डिजिटल सिग्नेचर (Digital signature) के उपयोग में किया जाता है। ❑

प्रश्न 17 – *फायरवाल की विशेषताओं को समझाइये।*
Discuss the feautres of firewall.

उत्तर–Firewall की प्रमुख विशेषतायें निम्नलिखित हैं–
(i) firewall, इंटरनेट तथा लोकल एरिया नेटवर्क के बीच में एक सुरक्षागार्ड की तरह कार्य करता है।
(ii) लोकल एरिया नेटवर्क से आने और जाने वाले समस्त नेटवर्क ट्रैफिक को, फायरवॉल अनाधिकृत एक्सेस या उपयोग को रोक देता है।
(iii) firewall, हमारे नेटवर्क में unauthorized एक्सेस को रोकता है।
(iv) यह unknown या suspicious स्थानों (locations) से आने वाली इनफॉरमेशन को ignore करता है।
(v) यह hardware या software या दोनों रूप में हो सकते हैं।
(vi) इंटरनेट से कनेक्ट होने पर हमारे सिस्टम में hacker को एक्सेस करने से रोकता है। ❑

प्रश्न 18 – *Firmware से आप क्या समझते हैं? क्या firewall firmware की category में आता है? समझाइये कैसे?*
What is Firmware? Is firewall a firmware? Explain, how?

उत्तर–कम्प्यूटर नेटवर्क में firmware, router के inside, embedded software होता है। wired routers तथा wireless routers दोनों firmware को रखते हैं। firmware, नेटवर्क प्रोटोकॉल्स security mechanism तथा हार्डवेयर डिवाइस की administrative capabilities के एक portion को इम्पलीमेन्ट करता है।

Firmware, router के inside, read-only memory chips के रूप में exist करते हैं। जब एक router की power, off हो जाती है, तब firmware, erase नहीं होता है और वह इनको बाहय रूप से hackers के द्वारा बदला जा सकता है। जब router को manufacture करने वाली कम्पनी इसके नये संस्करण को उपलब्ध कराती है। तब नेटवर्क owner इसे बदल सकता है।

अतः firmware, सॉफ्टवेयर है जो हार्डवेयर के एक piece में embed होता है। हम firmware को "software for hardware" के रूप में पुकार सकते हैं। firewall, firmware की category में आते हैं क्योंकि network firewall, firmware या software के रूप में एक प्रोग्राम है, जो कम्प्यूटर नेटवर्क को प्रोटेक्ट करने के लिये प्रयोग किया जाता है। तथा उस नेटवर्क से जुड़े कम्प्यूटर्स को malicious software से प्रोटेक्ट करने के लिये भी प्रयोग किया जाता है। सामान्यत दो प्रकार के network firewall होते हैं। जिनका प्रयोग कम्प्यूटर नेटवर्क को प्रोटेक्ट करने के लिये किया जा सकता है। पहला मुख्य रूप से hardware firewall होता है, जो एक device में स्वयं install होता है, यह firmware के रूप में होता है तथा सामान्यतः router या modem में install होता है। दूसरे टाईप का network firewall, software firewall होता है, जो एक कम्प्यूटर में अतिरिक्त सॉफ्टवेयर के रूप में install होता है, जिसे स्वयं कम्प्यूटर के माध्यम से आसानी से manage, control तथा remove किया जा सकता है। ❑

प्रश्न 19 – *Packet filter firewall किस layer पर कार्य करता है? विस्तार से समझाइये।*
In which layer packet filter firewall works? Explain in detail.

उत्तर–एक firewall, rules का एक सेट होता है, जो प्रत्येक packet पर apply किया जाता है। ये नियम निर्धारित करते हैं कि एक packet को pass किया जा सकता है या discard किया जा सकता है। जब एक नेटवर्क को प्रोटेक्ट करने की जरूरत होती है, तो firewall, run होते हैं। firewall, नेटवर्क के एक port पर unauthorised access को प्रोटेक्ट करते हैं। इंटरनेट/नेटवर्क पर डाटा, छोटे-छोटे pieces के रूप में travel करता है, इन्हें packets कहते हैं। प्रत्येक packet, metadata (कहां से पैकेट आ रहा है तथा कहां इसे भेजना है) को रखता है। ये packets, source से destination पर सही रूप में पहुंच जाये, इसके लिये packet filter firewall का प्रयोग किया

Scanned by CamScanner

जाता है। Packet filtering firewalls मुख्य रूप से OSI referene model की प्रथम तीन layer पर काम करते हैं, इसका अर्थ है कि मुख्य कार्य network तथा physcial layers के बीच में किया जाता है। तथा थोड़ा कार्य trasport layer पर source तथा destination port numbers को figure out करने के लिये किया जाता है। जब एक packet, sender (source) से originate होता है तथा एक firewall के माध्यम से filter होता है, तो device, packet filtering rules से match करने के लिये check करती है कि packet को pass किया जाये या reject किया जाये। जब packet, firewall के माध्यम से pass हो जाता है, तो यह protocol या port number के आधार पर packet को filter करता है तथा destination (receiver) के पास packet ट्रांसफर हो जाता है, निम्नलिखित Fig. में packet filtering firewall को चित्रित किया गया है–

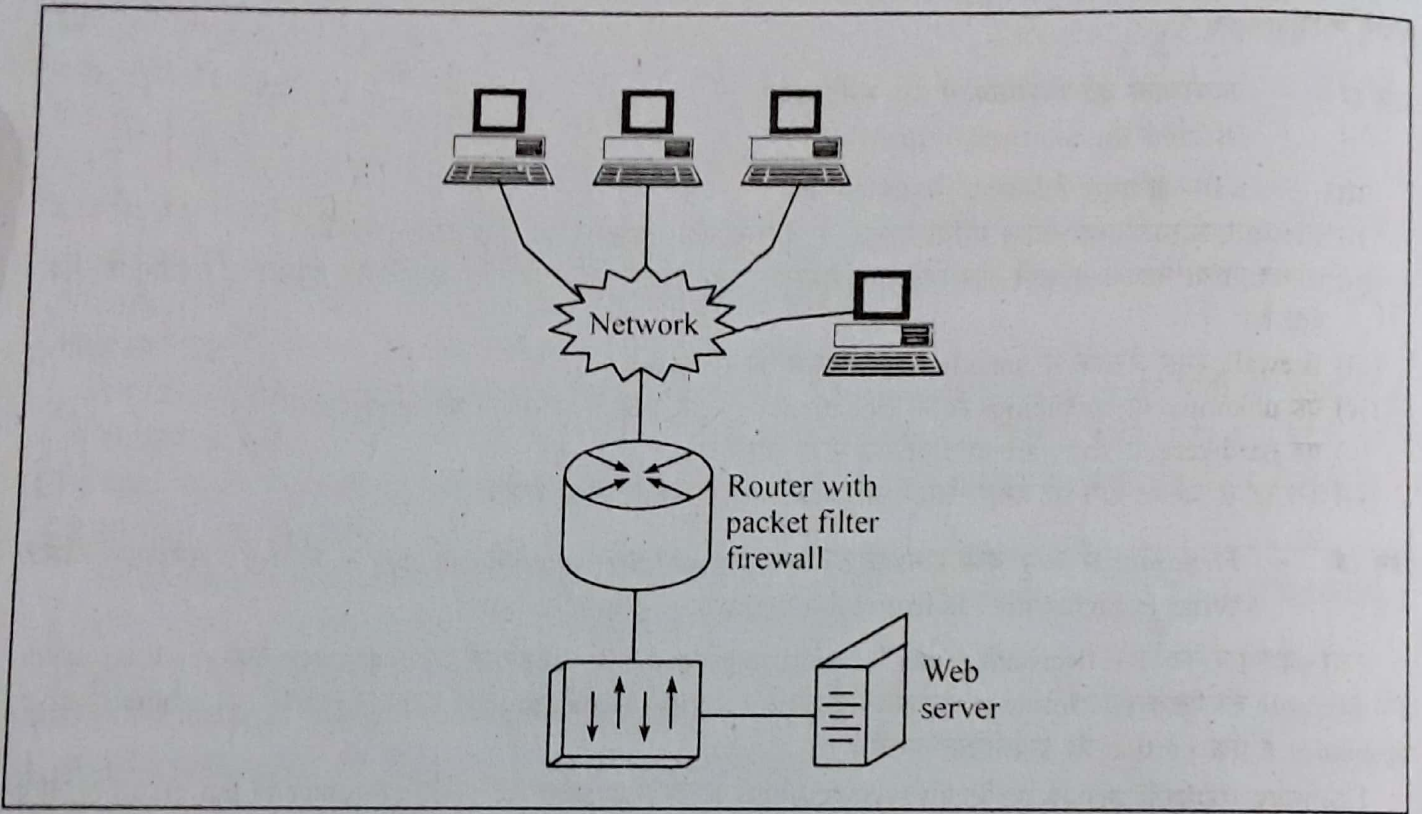


Fig. : Packet filtering firewall

❑

प्रश्न 20 – *E-mail को secure करने के लिये कौन-कौन सा protocol उपयोग किया जाता है? इस process को विस्तार से समझाइये।*

Which protocol is used to secure E-mail process? Explain this process in detail.

उत्तर–E-mail को source करने के लिये मुख्य रूप से तीन types के email protocols का प्रयोग कर सकते हैं–

(i) POP

(ii) IMAP

(iii) SMTP

(i) POP–POP को post-office-protocol के नाम से जाना जाता है। यह प्रोटोकॉल dial-up कनेक्शन पर आधारित है। यह प्रोटोकॉल, users को email retrieve करने की अनुमति तब देता है, जब online कनेक्ट हो जाते हैं तथा इन email को एक बार retrieve करने के पश्चात् बाद में इन पर कार्य किया जा सकता है, इस type के protocol का यह फायदा है कि e-mail को पढ़ने के लिये on-line कनेक्ट रहने की आवश्यकता नहीं है।

(ii) IMAP–IMAP, POP के पश्चात् डेवलप किया गया नया e-mail प्रोटोकॉल है। इसमें email में तभी एक्सेस कर सकते हैं, जब online कनेक्ट होते हैं। IMAP, विशेष रूप से broad band के द्वारा उपलब्ध किये गये fast connections के लिये उपयुक्त है। इसमें message सर्वर पर उपलब्ध होते हैं, अतः Online, multiple कम्प्यूटर्स के माध्यम से एक्सेस किया जा सकता है।

Scanned by CamScanner

(iii) SMTP—POP तथा IMAP प्रोटोकॉल के माध्यम से Incoming mail को handle किया जा सकता है। अतः POP तथा IMAP दोनों clients के लिये outgoing mail के लिये SMTP (Simple mail transfer protocol) का प्रयोग किया जाता है। जब हम POP या IMAP email account को email client software पर setup करते हैं, तो POP या IMAP के नाम incoming mail के लिये mail server computer पर अवश्य specify करने चाहिये। ❑

प्रश्न 21 – ISDN क्या है ? इसमें कौन-कौन से channels प्रयोग होते हैं? ISDN के द्वारा कौन-कौन सी सेवायें उपलब्ध होती हैं?

What is ISDN? Which channel are used in this? Which services are provided by ISDN?

या

ISDN Channels तथा ISDN Services को संक्षिप्त रूप में समझाइये।

Describe ISDN channels and ISDN services in short form.

उत्तर—ISDN—ISDN को Integrated services Digital Network के नाम से भी जाना जाता है। ISDN, कम्यूनिकेशन स्टैण्डर्ड का एक सेट है जो voice, video, data तथा दूसरी नेटवर्क सेवाओं के डिजिटल ट्रांसमिशन के लिये PSTN (Public Switched Telephone Network) पर प्रयोग किया जाता है। ISDN पहला टेलीकम्यूनिकेशनस सर्विस स्टैण्डर्ड था जिसे विशेष रूप से डिजीटल डाटा के लिये डिजाइन किया गया है। ISDN को पहले से स्थापित डिजिटिल टेलीफोन सिस्टम पर रन करने के लिये डिजाइन किया गया था।

ISDN Channels—ISDN bearer channels तथा data channel का प्रयोग करता है।

- **Bearer Channels**—प्रथम टाईप का channel 'bearer' channel या 'B' Channel है। ये channels वो होते हैं जो end-user के वास्तविक डाटा को carry करते हैं। Bearel channels 64 kbps की स्पीड से डाटा का ट्रांसफर करते हैं। B-channel किसी भी टाईप की digital information (Voice, data, video) को carry कर सकते हैं।
- **Data Channels**—द्वितीय टाईप का Channel 'Data' Channel या 'D' Channel होता है। इस Channel की स्पीड BRI के लिये 16 kpbs तथा PRI के लिये 64 kpbs होती है।

ISDN Service Types—ISDN दो types की services उपलब्ध कराता है।

(i) PRI (Primary Rate Interface)

(ii) BRI (Basic Rate Interface)

(i) PRI (Primary Rate Interface)—US में PRI, 23, 64kbps 'B' Channels तथा 64 kbps 'D' channel से मिलकर बना होता है। दूसरे देशों में PRI, 56 kbps 'B' Channels तथा 'D' Channel 64 kpbs से मिलकर बना होता है।

(ii) BRI (Basic Rate Interface)—BRI दो bearer channels तथा एक data channel से मिलकर बना होता है। US में BRI 64 kbps तथा 16 kbps data channel से मिलकर बना होता है। दूसरे देशों में BRI 60 kbps तथा 16 kbps data channel से मिलकर बना होता है। ❑

प्रश्न 22 – Baseband ISDN तथा Broadband ISDN में अन्तर बताइये।

State the difference between baseband ISDN and broadband ISDN.

उत्तर—Baseband ISDN तथा Broadband ISDN में अन्तर—Baseband ISDN तथा Broadband ISDN में मुख्य अन्तर निम्नलिखित हैं—

Baseband ISDN	Broadband ISDN
1. Baeband में डाटा digital signal के रूप में भेजा जाता है।	1. Broadband में डाटा analog signal के रूप में भेजा जाता है।
2. Baseband में Media की पूरी bandwidth का प्रयोग एक single channel के रूप में किया जाता है।	2. Broadband में प्रत्येक ट्रांसमिशन को band width के एक portion के रूप में assign किया जाता है। अतः same time पर multiple transmission संभव है।
3. Baseband कम्यूनिकेशन bidirectional होता है।	3. Broad band कम्यूनिकेशन unidirectional होता है।
4. baseband में FDM (Frequency Division Multiplexing) संभव नहीं है.।	4. Broadband में FDM (Frequency Division Multiplexing) संभव है।

❑❑❑

Scanned by CamScanner