Unit-3 Notes- Medium Access sub layer

The medium access control (MAC) is a sublayer of the data link layer of the open system interconnections (OSI) reference model for data transmission. It is responsible for flow control and multiplexing for transmission medium. It controls the transmission of data packets via remotely shared channels. It sends data over the network interface card.

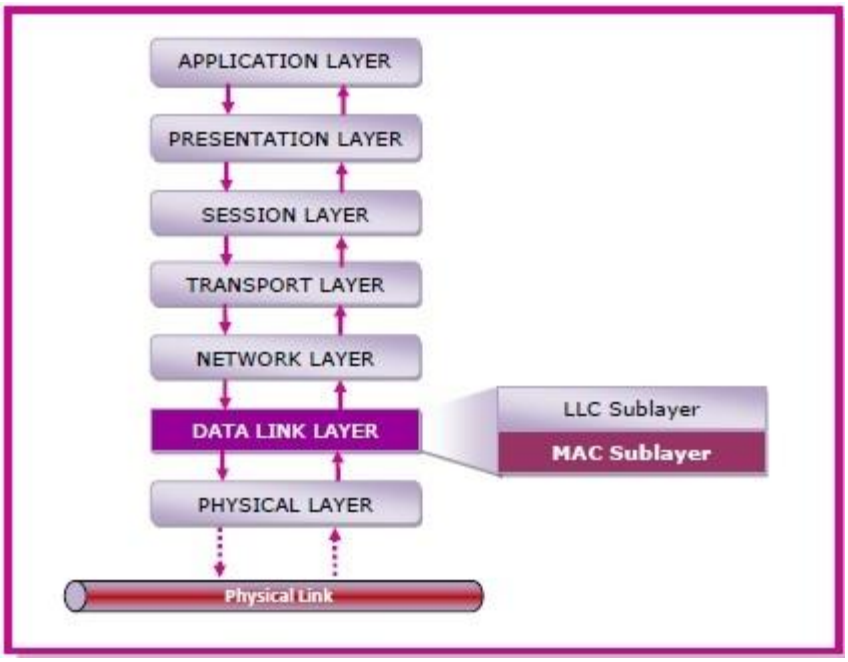
MAC Layer in the OSI Model

The Open System Interconnections (OSI) model is a layered networking framework that conceptualizes how communications should be done between heterogeneous systems. The data link layer is the second lowest layer. It is divided into two sublayers −

The logical link control (LLC) sublayer

The medium access control (MAC) sublayer

The following diagram depicts the position of the MAC layer −



Functions of MAC Layer

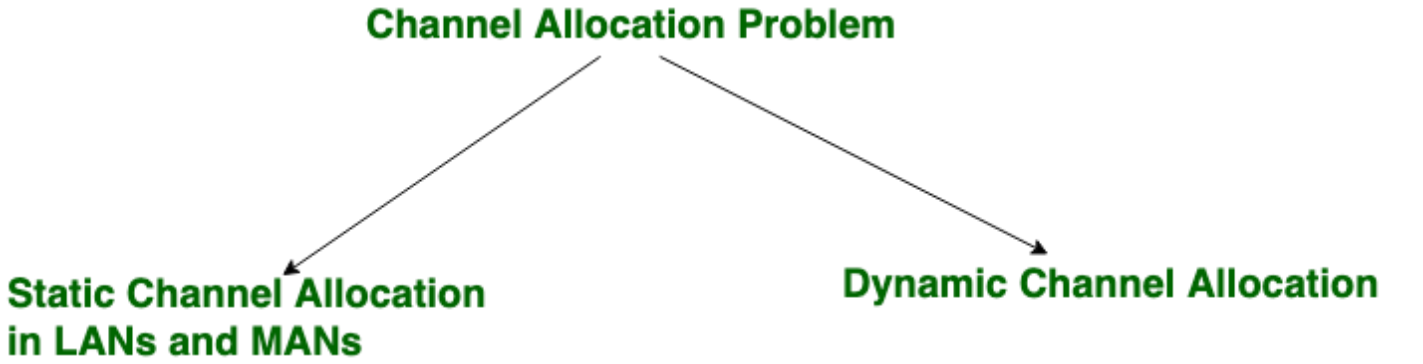
- It provides an abstraction of the physical layer to the LLC and upper layers of the OSI network.
- It is responsible for encapsulating frames so that they are suitable for transmission via the physical medium.
- It resolves the addressing of source station as well as the destination station, or groups of destination stations.
- It also performs collision resolution and initiating retransmission in case of collisions.

MAC Addresses

MAC address or media access control address is a unique identifier allotted to a network interface controller (NIC) of a device. It is used as a network address for data transmission within a network segment like Ethernet, Wi-Fi, and Bluetooth. MAC address is assigned to a network adapter at the time of manufacturing. It is hardwired or hard-coded in the network interface card (NIC). A MAC address comprises of six groups of two hexadecimal digits, separated by hyphens, colons, or no separators. An **EXAMPLE OF A MAC ADDRESS IS 00:0A:89:5B:F0:11.**

CHANNEL ALLOCATION PROBLEM IN COMPUTER NETWORK:-

Channel allocation is a process in which a single channel is divided and allotted to multiple users in order to carry user specific tasks. There are user's quantity may vary every time the process takes place. If there are N number of users and channel is divided into N equal-sized sub channels, Each user is assigned one portion. If the number of users are small and don't vary at times, than Frequency Division Multiplexing can be used as it is a simple and efficient channel bandwidth allocating technique. Channel allocation problem can be solved by two schemes: Static Channel Allocation in LANs and MANs, and Dynamic Channel Allocation.



Channel Allocation may be done using two schemes −

- Static Channel Allocation
- Dynamic Channel Allocation

Static Channel Allocation

In static channel allocation scheme, a fixed portion of the frequency channel is allotted to each user. For N competing users, the bandwidth is divided into N channels using frequency division multiplexing (FDM), and each portion is assigned to one user. This scheme is also referred as fixed channel allocation or fixed channel assignment. In this allocation scheme, there is no interference between the users since each user is assigned a fixed channel. However, it is not suitable in case of a large number of users with variable bandwidth requirements.

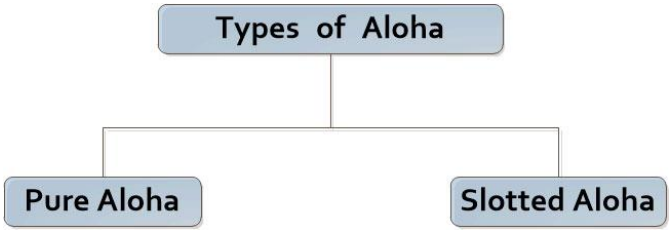
Dynamic Channel Allocation

In dynamic channel allocation scheme, frequency bands are not permanently assigned to the users. Instead channels are allotted to users dynamically as needed, from a central pool. The allocation is done considering a number of parameters so that transmission interference is minimized. This allocation scheme optimises bandwidth usage and results is faster transmissions. Dynamic channel allocation is further divided into centralised and distributed allocation.

LAN PROTOCOLS- ALOHA PROTOCOL:-

इसे वायरलेस LAN के लिए डिजाईन किया गया था लेकिन ये शेयर्ड माध्यम में भी प्रभावी है। ALOHA एक मल्टीप्ल एक्सेस प्रोटोकॉल है। जिनका उपयोग नेटवर्क में random access करने में किया जाता है। सन 1970 में Hawaii University के Norman Abram-son और उनके साथी ने चैनल एलोकेशन की समस्या को हल करने के लिए एक method को develop किया था। जिसे ALOHA System कहा जाता है। इस method में नेटवर्क को कोई भी user किसी भी टाइम में data को ट्रांसमिट कर सकता है। यदि एक से अधिक यूजर एक ही समय पर data का ट्रांसमिशन करता है। तो data का collision हो जाता है। जिससे डाटा ख़राब हो जाता है और तब सभी user को फिर से data को re-transmit करना पड़ता है। ALOHA का उपयोग Ground based radio broadcasting के लिए किया जाता है। ALOHA को नेटवर्क के किसी भी shared transmission medium में apply किया जा सकता है। Aloha को दो प्रकार में बाटां गया है जिसमे पहला pure aloha और दूसरा slotted aloha है। इसको रेडियो {वायरलेस लोकल एरिया नेटवर्क} के लिए निर्मित किया गया था परन्तु प्रयोग किसी भी shared सिस्टम में कर सकते है|

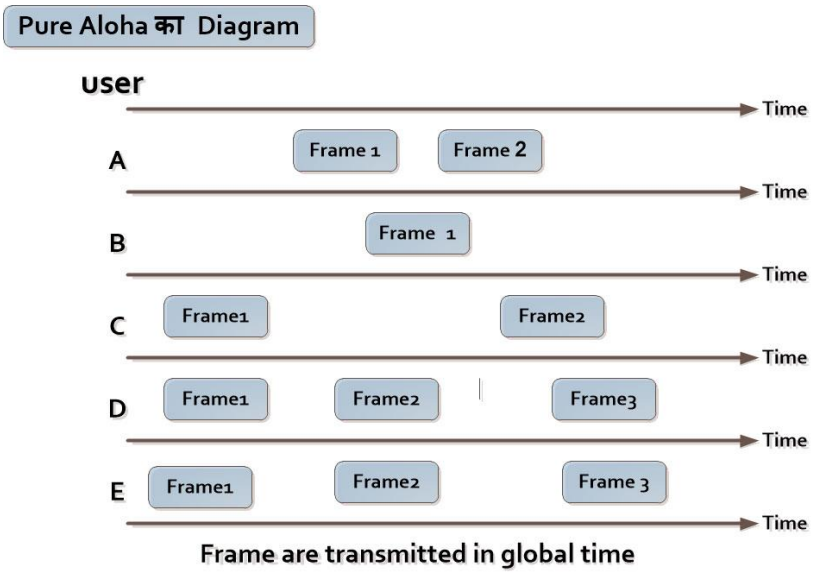
ALOHA यह दिखाता है कि किस प्रकार बहुत सारें सिस्टम्स एक मीडियम के साथ बिना किसी collision(टकराव) के access करते है. यह प्रोटोकॉल प्रत्येक सिस्टम को एक frame (फ्रेम) भेजता है परन्तु जब एक collision होता है तो फ्रेम को कुछ समय के लिए इन्तजार करना पड़ता है और फ्रेम दुबारा भेजा जाता है. यह प्रक्रिया तब तक चलती है जब तक सभी frame भेज नही दिए जाते. इस कारण इसमें collision की प्रायिकता बहुत अधिक है. तथा इस कारण ALOHA प्रोटोकॉल का throughput (प्रवाह क्षमता) बहुत ही कम केवल 18% है. ALOHA में collision इसलिए होता है क्योंकि यह एक मल्टीपल एक्सेस कम्युनिकेशन सिस्टम है तथा जब दो या दो से अधिक सिस्टम एक ही समय में एक चैनल में ट्रांसमिट करने का प्रयास करते है तो collision (टकराव) होता है.



Pure Aloha

Aloha के original version को ही pure aloha कहा जाता है। दुसरे शब्दों में pure aloha एक simple aloha version है। जिसमे प्रत्येक user, नेटवर्क में किसी भी समय data को ट्रांसमिट कर सकता है। इस aloha method में collision का रिस्क बहुत अधिक रहता है। इसलिए नेटवर्क में send किये गए data frame के status को जानने के लिए Acknowledgement method का उपयोग किया जाता है तथा collision के बाद destroy हुए data frame को फिर से ट्रांसमिट करना पड़ता है। यह बहुत ही सरल प्रोटोकॉल है अर्थात इसमें जब भी सिस्टम के पास डेटा भेजने के लिए होता है यह फ्रेम को ट्रांसमिट कर देता है इसमें समय continuous होता है. जब भी दो सिस्टम फ्रेम को ट्रांसमिट करते है तो collision होता है और frames नष्ट हो जाते है. Pure अलोहा में, यदि रिसीवर कोई acknowledgement नहीं देता है तो यह समझ लिया जाता है कि फ्रेम नष्ट हो गये है और फ्रेम्स को दुबारा ट्रांसमिट किया जाता है. Pure aloha की सबसे बड़ी कमी यह है कि इसमें collision के chances बहुत अधिक होते है.

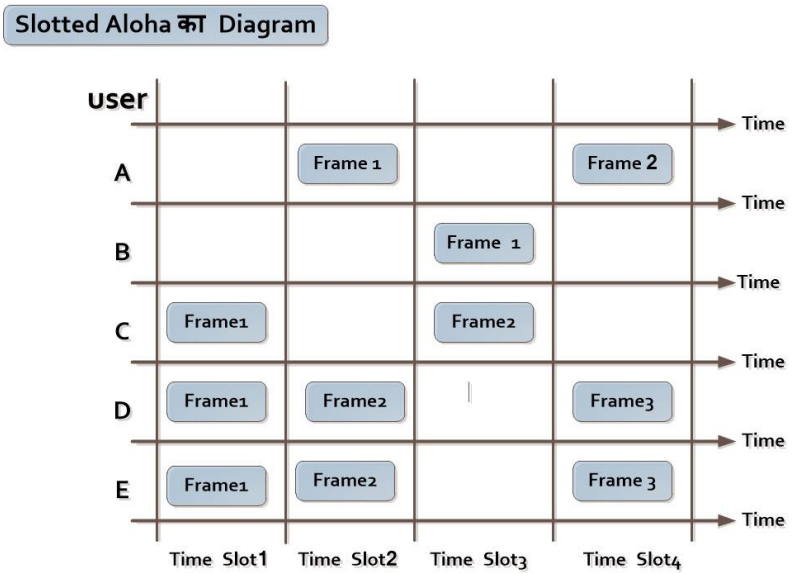
- Pure अलोहा का संवेदनशील समय (vulnerable time) 2x Tfr है.
- इसका सफल ट्रांसमिशन रेट S = G * exp(-2G) है.
- इसका अधिकतम throughput (प्रवाह क्षमता) 18% है. (जब G = ½)



Disadvantage of Pure Aloha

Pure aloha में communication चैनल का low utilization होता है। अथार्त communication channel के pure capacity का इस्तेमाल नहीं किया जा सकता है। इस method में चैनल का केवल 18.4% का utilization होता है। इसलिए इसका उपयोग केवल radio broadcasting में किया जाता है लेकिन इसका उपयोग satellite broadcasting में नहीं किया जाता है।

Slotted aloha



slotted aloha method में नेटवर्क के communication चैनल के ग्लोबल टाइम को विभिन्न टाइम स्लॉट में बाँट दिया जाता है। तथा user डाटा को ट्रांसमिट करने के लिए इन टाइम स्लॉट का उपयोग करता है। तथा कोई भी user किसी भी टाइम स्लॉट का उपयोग करके data को ट्रांसमिट कर सकता है। pure aloha के comparison में slotted aloha को काम्प्लेक्स अलोहा version कहा जाता है। जिसमे प्रत्येक user नेटवर्क में data को पहले से define किये गए टाइम स्लॉट में ट्रांसमिट करता है। slotted aloha का मुख्य advantage चैनल के utilization को बढ़ाना है। slotted aloha में communication चैनल के 36.4% का utilize होता है। इसलिए इसका उपयोग satellite broadcasting में किया जाता है। Slotted अलोहा को pure अलोहा की कार्यक्षमता को बेहतर बनाने के लिए विकसित किया गया था क्योंकि pure aloha में collision की सम्भावना बहुत ही अधिक होती है. इस aloha में systems के समय को slots (स्लॉट्स) में विभाजित कर दिया जाता है जिससे सिस्टम एक slot में केवल एक ही frame भेज सकता है और यह frame केवल slot के शुरूआत में ही भेजा जा सकता है. यदि कोई सिस्टम slot के शुरुआत में frame नहीं भेज पाता है तो उसे अगले slot के शुरू होने का इन्तजार करना पड़ता है. इस अलोहा में भी collision (टकराव) की सम्भावना होती है यदि दो सिस्टम एक time slot के शुरुआत में frame को ट्रांसमीट करने की कोशिश करते है तो. परन्तु यह pure aloha से बेहतर है क्योंकि इसमें collision की सम्भावना कम है.

- Slotted अलोहा का संवेदनशील समय (vulnerable time) Tfr है.
- इसका औसत सफल ट्रांसमिशन रेट S = G * exp(-G) है.
- इसका अधिकतम throughput (प्रवाह क्षमता) 37% है, जब (G=1).

Difference between Pure and Slotted Aloha

- Pure aloha एक सिंपल अलोहा version है जबकि slotted अलोहा कॉम्प्लेक्स अलोहा version है।
- Pure aloha में चैनल का 18.4% का यूटिलाइजेशन होता है जबकि slotted aloha में चैनल के 36.8% का यूटिलाइजेशन होता है।
- Pure aloha का उपयोग ग्राउंड बेस्ड रेडियो ब्राडकास्टिंग में किया जाता है जबकि slotted aloha का उपयोग satellite ब्राडकास्टिंग में किया जाता है।
- Pure aloha में data को ट्रांसमिट करने के लिए टाइम स्लॉट का उपयोग नहीं किया जाता है जबकि slotted aloha में data को ट्रांसमिट करने के लिए टाइम स्लॉट का उपयोग किया जाता है।

OVERVIEW OF IEEE STANDARDS:-

Stands for the "Institute of Electrical and Electronics Engineers" and is produced "I triple E." The IEEE is a professional association that develops, defines, and reviews electronics and computer science standards. Its mission is "to foster technological innovation and excellence for the benefit of humanity."

In 1963, the two organizations merged to become a single entity – the IEEE. Since then, the organization has established thousands of standards for consumer electronics, computers, and telecommunications.

While the Institute of Electrical and Electronics Engineers is based in the United States, IEEE standards often become international standards. The Institute of Electrical and Electronics Engineers is a standards setting body. Each of their standards is numbered and a subset of the number is the actual standard. The 802 family of standards is ones developed for computer networking. IEEE 802 is also an Institute of Electrical and Electronics Engineers (IEEE) standard set that covers the physical and data link layers of the Open Systems Interconnection (OSI) model. It defines standards and protocols for wired local area networks (WLAN), metropolitan area networks (MAN) and wireless networks; defines characteristics, operating procedures, protocols and services for networks that carry variable sized packets and specifies the development and handling of compatible devices and equipment. IEEE 802 is comprised of standards with separate working groups that regulate different communication networks, including IEEE 802.1, 802.3, 802.11 and 802.15. Below are a few examples of technologies standardized by the IEEE.

- **IEEE 1284 (Parallel Port) –** an I/O interface used by early desktop PCs
- **IEEE 1394 (Firewire) –** a high-speed interface designed for external hard drives, digital video cameras, and other A/V peripherals
- **IEEE 802.2 (Logical Link Control)–** specifies the general interface between the network layer (IP, IPX, etc) and the data link layer
- **IEEE 802.3 (Ethernet) –** it is the standard which Ethernet operates by. It is the standard for CSMA/CD (Carrier Sense Multiple Access with Collision Detection)
- **IEEE 802.5 (Token Ring) –** The token is a special frame which is designed to travel from node to node around the ring**.**
- **IEEE 802.11 (Wireless Network Standards/Wi-Fi) –** a series of Wi-Fi standards used for wireless networking
- **IEEE 802.16 (WiMAX) –** a wireless communications standard for transferring cellular data

IEEE 802.11 Wireless Network Standards:-

802.11 is the collection of standards setup for wireless networking. You are probably familiar with the three popular standards: 802.11a, 802.11b, 802.11g and latest one is 802.11n. Each standard uses a frequency to connect to the network and has a defined upper limit for data transfer speeds.

-802.11a was one of the first wireless standards. 802.11a operates in the 5Ghz radio band and can achieve a maximum of 54Mbps. Wasn't as popular as the 802.11b standard due to higher prices and lower range.

-802.11b operates in the 2.4Ghz band and supports up to 11 Mbps. Range of up to several hundred feet in theory. The first real consumer option for wireless and very popular.

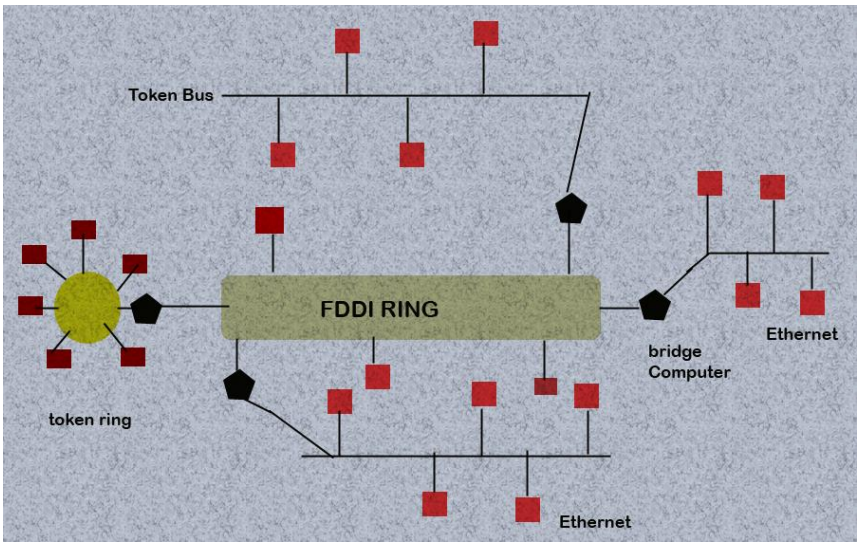
-802.11g is a standard in the 2.4Ghz band operating at 54Mbps. Since it operates in the same band as 802.11b, 802.11g is compatible with 802.11b equipment. 802.11a is not directly compatible with 802.11b or 802.11g since it operates in a different band.

FDDI:-

FDDI का तात्पर्य Fiber Distributed data interface है। यह एक specification है जो फाइबर ऑप्टिक्स मीडिया का उपयोग करने वाले 100 Mbps के टोकन रिंग को describe करता है। FDDI को IEEE 802.5 स्टैण्डर्ड के similar माना जाता है। FDDI को ANSI द्वारा सन 1986 में तैयार किया गया था।

FDDI को 100 Mbps की स्पीड में 200 किलोमीटर के अन्दर 100 स्टेशन पर रन किया जा सकता है। FDDI नेटवर्क के द्वारा ईथरनेट में 10 Mbps और टोकन रिंग में 4 Mbps को सपोर्ट करता है। FDDI नेटवर्क में दो नोड के बिच का दुरी एक किलोमीटर से कम होनी चाहिए। FDDI का उपयोग मुख्यत: नेटवर्क में high speed backbone बनाने के लिए किया जाता है। नेटवर्क बैकबोन का तात्पर्य नेटवर्क में होने वाले डाटा ट्रांसमिशन के लिए नेटवर्क आर्किटेक्चर होता है। जो एडवांस टेक्नोलॉजी से बनाया जाता है जिसकी क्षमता नेटवर्क में सबसे अधिक होती है नेटवर्क की परफॉरमेंस नेटवर्क के बैकबोन पर depend रहता है। FDDI एक हाई performance fiber optic LAN नेटवर्क होता है, जो कि 200 km का क्षेत्र cover करता है। FDDI नेटवर्क में डाटा स्पीड लगभग 100 Mbps होती है और इसमें लगभग 1000 स्टेशन कनेक्टेड रहते है। चूँकि इसमें high bandwidth होती हैं, इसलिए FDDI बहुत ही जल्द एक popular choice बन गयी थी high-speed backbones में इस्तमाल होने के लिए universities और businesses में. जहाँ एक समय में FDDI दुनिया का सबसे fastest LAN technology रहा काफी वर्षों के लिए, वहीँ बाद में इसे supersed कर लिया गया Fast Ethernet के द्वारा. जो की offer करता था 100 Mbps speeds वो भी काफी lower cost में. आज के समय में बहुत से networks इस्तमाल करते हैं Gigabit Ethernet, जो की support करता है speeds up to 1,000 Mbps तक.

- इस नेटवर्क(FDDI) की हाई band -width होने के करण इसे copper LANs connection के टाइम backbone की तरह यूज़ किया जाता है. FDDI नेटवर्क में multimode फाइबर का यूज़ करते है, क्योकि 100 Mbps स्पीड पर चलने वाले नेटवर्क के लिए singlemode फाइबर का यूज़ करना अतिरिक्त खर्चे को बढ़ा देता है जिसकी कोई जरुरत नहीं।
- FDDI, laser की जगह LEDs का यूज़ करता है
- FDDI केबलिंग में दो तरह कि fiber ring होती है, एक क्लॉक वाइज डायरेक्शन में ट्रांसमिशन करती है और दूसरी एंटी-क्लॉक वाइज डायरेक्शन में ट्रांसमिट करती है। अगर किसी कंडीशन में एक केबल ब्रेक होती है तब हम दूसरी केबल को बैकअप की तरह यूज़ कर सकते है।



Advantage of FDDI:-

- **High Bandwidth:** FDDI नेटवर्क की बैंडविड्थ 250 Gbps तक हो सकती है।
- **High Security:** FDDI नेटवर्क में फाइबर ऑप्टिक्स केबल के कारण इसकी सिक्यूरिटी काफी strong होती है।
- **Cable Distance:** FDDI नेटवर्क में सिग्नल को 200 किलोमीटर तक ट्रांसमिट किया जा सकता है।

Disadvantage of FDDI:-

- FDDI को नेटवर्क का काम्प्लेक्स Technology कहा जाता है क्युकी इस प्रकार के नेटवर्क के इंस्टालेशन और maintenance में बहुत अधिक technical skill की आवश्यकता होती है। FDDI बहुत ही महँगी technology है। क्युकी इसमें फाइबर ऑप्टिक्स केबल के साथ connector और adapter का उपयोग किया जाता है | जो काफी महँगी होती है।

DATA LINK LAYER:-

डाटा लिंक लेयर को ओपन सिस्टम इंटरकनेक्शन या OSI का दूसरा परत कहा गया है। इसकी जिम्मेदारी एक फिजिकल नेटवर्क लिंक के अंदर डाटा को ट्रांसमिट करने की होती है। इसे एक नोड से दूसरे नोड तक डाटा को पहुंचाने वाला सबसे भरोसेमंद सिस्टम माना जाता है। सारे लेयर में ये सबसे ज्यादा complicated और complex भी है। ये अपने अंदर के हार्डवेयर सिस्टम को छुपा कर उपरी परतों को केवल एक संचार के माध्यम कि तरह दिखता है। डाटा लिंक लेयर दो ऐसे होस्ट के बीच काम करता है जो आपस में किसी ना किसी तरह से सीधे जुड़े हुए होते हैं। ये डायरेक्ट कनेक्शन या तो पॉइंट टू पॉइंट हो सकता है या फिर ब्रॉडकास्ट। ये बिट बाई बाई बिट डाटा स्ट्रीम को सिग्नल में बदलता है और उसे अपने अंदर के हार्डवेयर में भेज देता है। फिर डाटा लिंक लेयर हार्डवेयर में उस डाटा को इलेक्ट्रिक सिग्नल के रूप में प्राप्त करने के बाद उसे फ्रेम वाले फॉर्मल में बदलता है और उपर वाले परतों को पहुंचाने का काम करता है।

डाटा लिंक लेयर की विशेषताएं

फिजिकल एड्रेसिंग

- फिजिकल एड्रेसिंग इस मामले में नेटवर्क एड्रेसिंग से काफी अलग है।
- नेटवर्क एड्रेसिंग किसी नेटवर्क में नोड और देवीचे के बीच का अंतर समझता है जिसके कारण ट्रैफिक को नेटवर्क में स्विच या rout करने में आसानी होती है।
- वहीं फिजिकल एड्रेसिंग लिंक-लेयर वाले लेवल पर devices कि पहचान करता है और समान फिजिकल माध्यम में सभी डिवाइस के बीच के अंतर को समझने में सक्षम होता है।
- इसका प्राइमरी फॉर्म है- मीडिया एक्सेस कण्ट्रोल जिसे हम MAC के नाम से जानते हैं।

नेटवर्क टोपोलॉजी

- नेटवर्क टोपोलॉजी के स्पेसिफिकेशन ये तय करते हैं कि एक नेटवर्क के अंदर सारे डिवाइस किस तरह से लिंक किये जाएँगे।
- कुछ मीडिया devices को बीएस टोपोलॉजी द्वारा जुड़ने कि इजाजत देते हैं जबकि कुछ रिंग टोपोलॉजी द्वारा। ईथरनेट तकनीक बस टोपोलॉजी का प्रयोग करता है जो juniper नेटवर्क के डिवाइस पर काम करते हैं।

एरर नोटीफीकेशन

- ये डाटा लिंक लेयर का एक उत्तम फीचर है जो उपरी परतों को पहले ही इस बात के लिए आगाह कर देता है अगर फिजिकल लिंक के अंदर कोई एरर आ जाए।
- जैसे उदाहरण के तौर पर सिग्नल का खो जाना, सीरियल कनेक्शन के बीच clocking सिग्नल का खो जाना और T1 या T3 लिंक के सबसे अंतिम छोर का खो जाना।

फ्रेम सिक्वेंसिंग

- डाटा लिंक लेयर फ्रेम सिक्वेंसिंग कि क्षमता रखता है जिसका मतलब ये हुआ कि अगर जो डाटा सीक्वेंस के बाहर ट्रांसमिट हो गयी हैं या सही क्रम में नही प्राप्त हुए हैं उन्हें ट्रांसमिशन के अंतिम छोर पर रिकॉर्ड किया जा सकता है।
- इसके बाद लेयर दो हेडर के अंदर डाटा payload के साथ ट्रांसमिट हुए पैकेज की इंटीग्रिटी की जांच कि जाती है (by means of Bit)।

फ्लो कण्ट्रोल

- फ्लो कण्ट्रोल डाटा लिंक लेयर में डाटा को प्राप्त करने वाले डिवाइस को डाटा के अंदर congestion (जमाव) को पकड़ने में मदद करता है।
- फिर वो सतरं में उपर या नीचे सभी पड़ोसियों को इस बात से पहले ही आगाह कर देता है।
- इसके बाद ये devices इस congestion कि सूचना को उपरी परत के प्रोटोकॉल को पहुंचा देते हैं ताकि डाटा का ट्रांसमिशन फिर से बहाल किया जा सके।

डाटा लिंक लेयर के सब-लेयर

अब हम डाटा लिंक के अंदर सब-लेयर्स के बारे में जानेंगे। डाटा लिंक लेयर कुल दो सब-लेयर में विभाजित होता हैं:

1. लॉजिक लिंक कण्ट्रोल (LLC), और
2. मीडिया एक्सेस कण्ट्रोल (MAC)

अब हम इन दोनों सब-लेयर्स को समझते हैं कि ये हैं क्या। एलएलसी सब-लेयर सिंगल लिंक नेटवर्क के अंदर के सारे डिवाइस के बीच के संचार को मैनेज करता है। ये लिंक लेयर फ्रेम्स के अंदर ऐसे फ़ील्ड्स को सपोर्ट करता है जो मल्टीप्ल हायर लेवल प्रोटोकॉल्स को एक सिंगल फिजिकल लिंक को साझा करने में सक्षम बनाते हैं। वहीं मैक सब-लेयर फिजिकल नेटवर्क माध्यम को दिए गये प्रोटोकॉल्स एक्सेस कि देख-रेख करता है। डिवाइस के सभी पोर्ट को मैक एड्रेस दिया जाता है जिसके कारण समान फिजिकल लिंक के सभी डिवाइस एक दूसरे को डाटा लिंक लेयर पर पहचान कर सकें।

डाटा लिंक लेयर का कार्य

फ्रेमिंग

डाटा लिंक लेयर नेटवर्क लेयर से पैकेज लेता है और उन्हें कुछ फ्रेम्स में बाँट देता है। फिर ये एक-एक बिट कर के ये सारे फ्रेम को हार्डवेयर में भेजता है। फिर वहां पर डाटा लिंक लेयर हार्डवेयर से सिग्नल लेता है और उन्हें फ्रेम में बदल देता है।

एड्रेसिंग

डाटा लिंक लेयर “लेयर-2 हार्डवेयर एड्रेसिंग मैकेनिज्म” पर काम करता है। इसमें लिंक के अंदर हार्डवेयर एड्रेस यूनिक होता है। ये एड्रेस इन हार्डवेयर को बनाते समय ही दे दिया जाता है।

सिंक्रोनाइजेशन

जब डाटा फ्रेम्स को लिंक के अंदर भेजा जाता है तब दोनों मशीन आपस में synchronize होने चाहिए नही तो डाटा का ट्रान्सफर सम्भव नही हो पाता।

एरर कण्ट्रोल

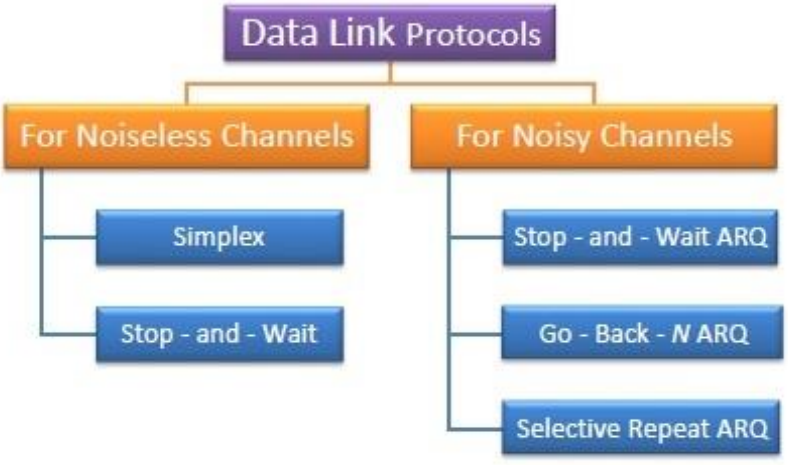
कभी-कभी सिग्नल के ट्रांजीशन में समस्या आ जाती है क्योंकि बिट में ख़राभी आ सकती है। इस स्थिति में इस गलती को पकड़ कर असली डाटा बिट्स को रिकवर करने कि कोशिश कि जाती है। इसके साथ ही डाटा भेजने वाले संदर को भी इस एरर कि सूचना दी जाती है।

मल्टी-एक्सेस

सब शेयर्ड लिंक के अंदर होस्ट डाटा को ट्रान्सफर करने कि कोशिश करता है तब इसके आपस में टकराने (Collision) कि काफी सम्भावना रहती है।डाटा लिंक लेयर CSMA/CD का मैकेनिज्म देता है जो मल्टीप्ल सिस्टम में शेयर किये गये डाटा को एक्सेस करने में सक्षम बनाता है और collision को भी रोकता है।

ELEMENTARY DATA LINK PROTOCOLS:-

Protocols in the data link layer are designed so that this layer can perform its basic functions: framing, error control and flow control. Framing is the process of dividing bit - streams from physical layer into data frames whose size ranges from a few hundred to a few thousand bytes. Error control mechanisms deals with transmission errors and retransmission of corrupted and lost frames. Flow control regulates speed of delivery and so that a fast sender does not drown a slow receiver.



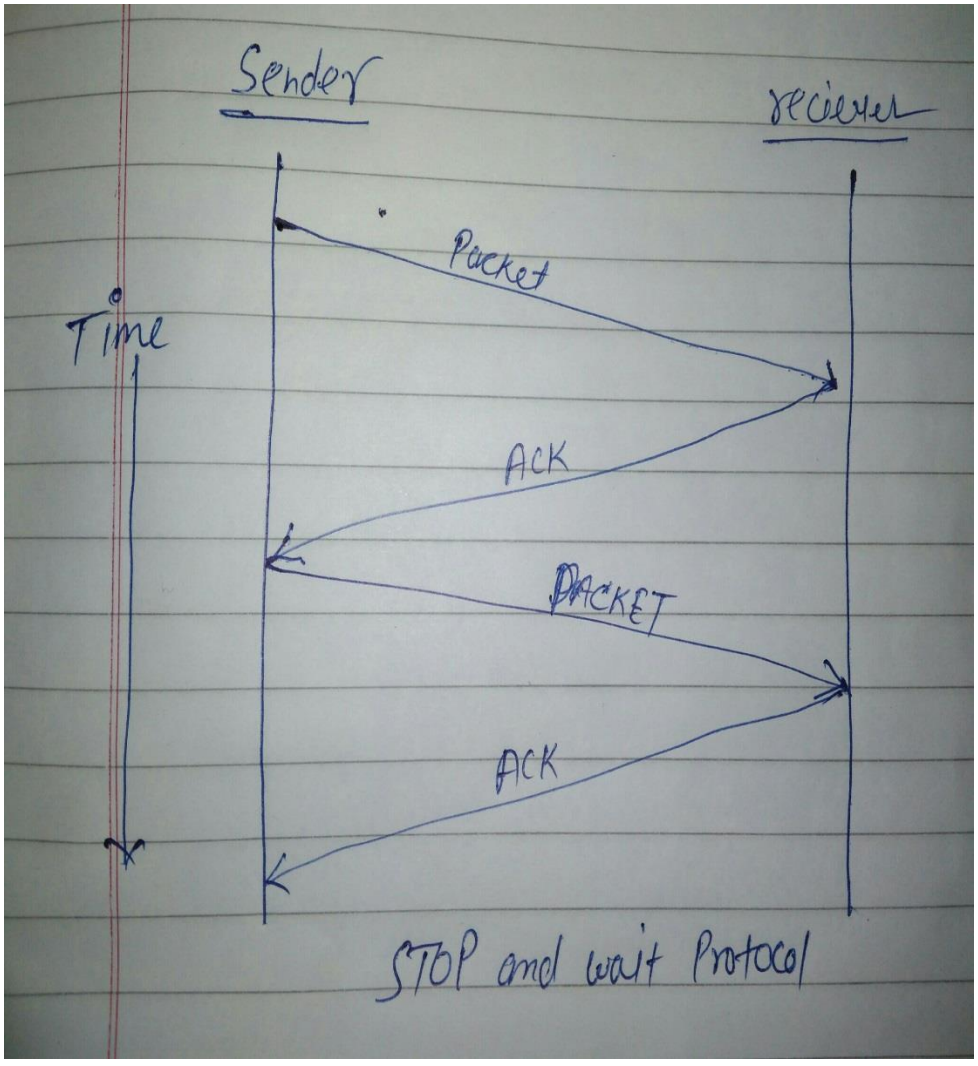
Types of Data Link Protocols:- Data link protocols can be broadly divided into two categories, depending on whether the transmission channel is noiseless or noisy.

Simplex Protocol

The Simplex protocol is hypothetical protocol designed for unidirectional data transmission over an ideal channel, i.e. a channel through which transmission can never go wrong. It has distinct procedures for sender and receiver. The sender simply sends all its data available onto the channel as soon as they are available its buffer. The receiver is assumed to process all incoming data instantly. It is hypothetical since it does not handle flow control or error control.

Stop – and – Wait Protocol

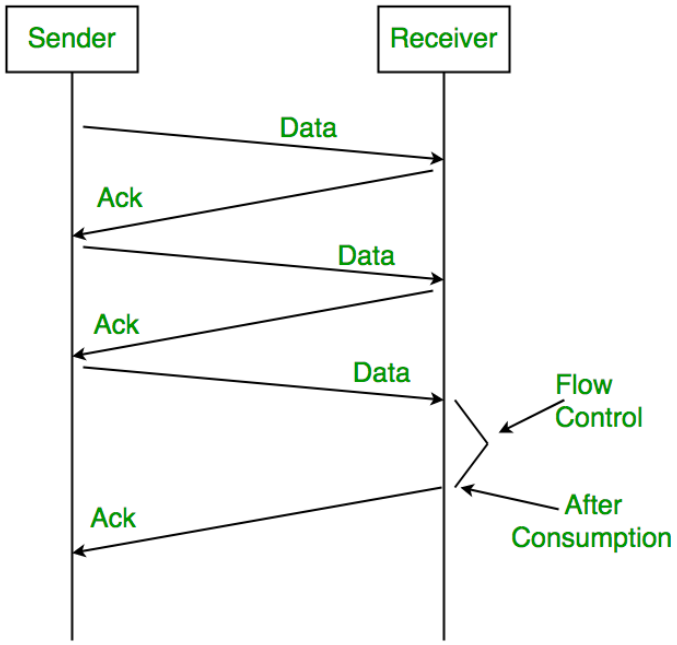
इसका प्रयोग connection oriented कम्युनिकेशन में किया जाता है तथा इसका प्रयोग डेटा लिंक लेयर तथा ट्रांसपोर्ट लेयर में होता है. stop & wait protocol में सेन्डर एक समय में केवल एक डेटा पैकेट को ही रिसीवर को send करता है और रिसीवर को जब डेटा पैकेट प्राप्त होता है तो वह sender को acknowledgement भेजता है. sender दूसरा पैकेट तभी send करता है जब पिछले वाले पैकेट की acknowledgement उसके पास आ गयी हो.



डेटा पैकेट भेजने की यह प्रक्रिया तब तक चलती रहती है जब तक कि sender के पास भेजने के लिए डेटा होता है. stop & wait protocol का मुख्य फायदा है इसकी accuracy. क्यूंकि यह अगला डेटा पैकेट तभी भेजता है जब पिछले वाले की acknowledgement मिल गयी हो. इससे डेटा पैकेट के lost हो जाने की संभावना खत्म हो जाती है. stop & wait protocol का सबसे बड़ा नुकसान यह है कि यह डेटा पैकेट्स के ट्रांसमिशन की गति को बहुत धीमा (slow) कर देता है. क्योंकि sender अगला पैकेट तब तक नहीं भेजता जब तक उसे पहले वाले कि acknowledgement प्राप्त नही हो जाती. इस कारण sender तथा reciever दोनों को infinite समय के लिए इन्तजार करना पड़ता है.

Stop – and – Wait ARQ

Stop – and – wait Automatic Repeat Request (Stop – and – Wait ARQ) is a variation of the above protocol with added error control mechanisms, appropriate for noisy channels. The sender keeps a copy of the sent frame. It then waits for a finite time to receive a positive acknowledgement from receiver. If the timer expires or a negative acknowledgement is received, the frame is retransmitted. If a positive acknowledgement is received then the next frame is sent.



The following transition may occur in stop-and-wait ARQ :-

- The Sender maintains a timeout Counter.
- When a frame is sent, the sender starts the timeout Counter.
- If acknowledgement of frame comes in time, the Sender transmits the next frame in queue.
- If acknowledgement does not come in time, the sender assumes that either the frame or its acknowledgement is lost in transmit. Sender ~~retransmit~~ retransmits the frame and starts the timeout Counter.
- If a negative acknowledgement is received, the sender retransmits the frame.

SLIDING WINDOW PROTOCOL

Sliding window protocols are data link layer protocols for reliable and sequential delivery of data frames. The sliding window is also used in Transmission Control Protocol. In this protocol, multiple frames can be sent by a sender at a time before receiving an acknowledgment from the receiver. The term sliding window refers to the imaginary boxes to hold frames. Sliding window method is also known as windowing.

Working Principle

In these protocols, the sender has a buffer called the sending window and the receiver has buffer called the receiving window.

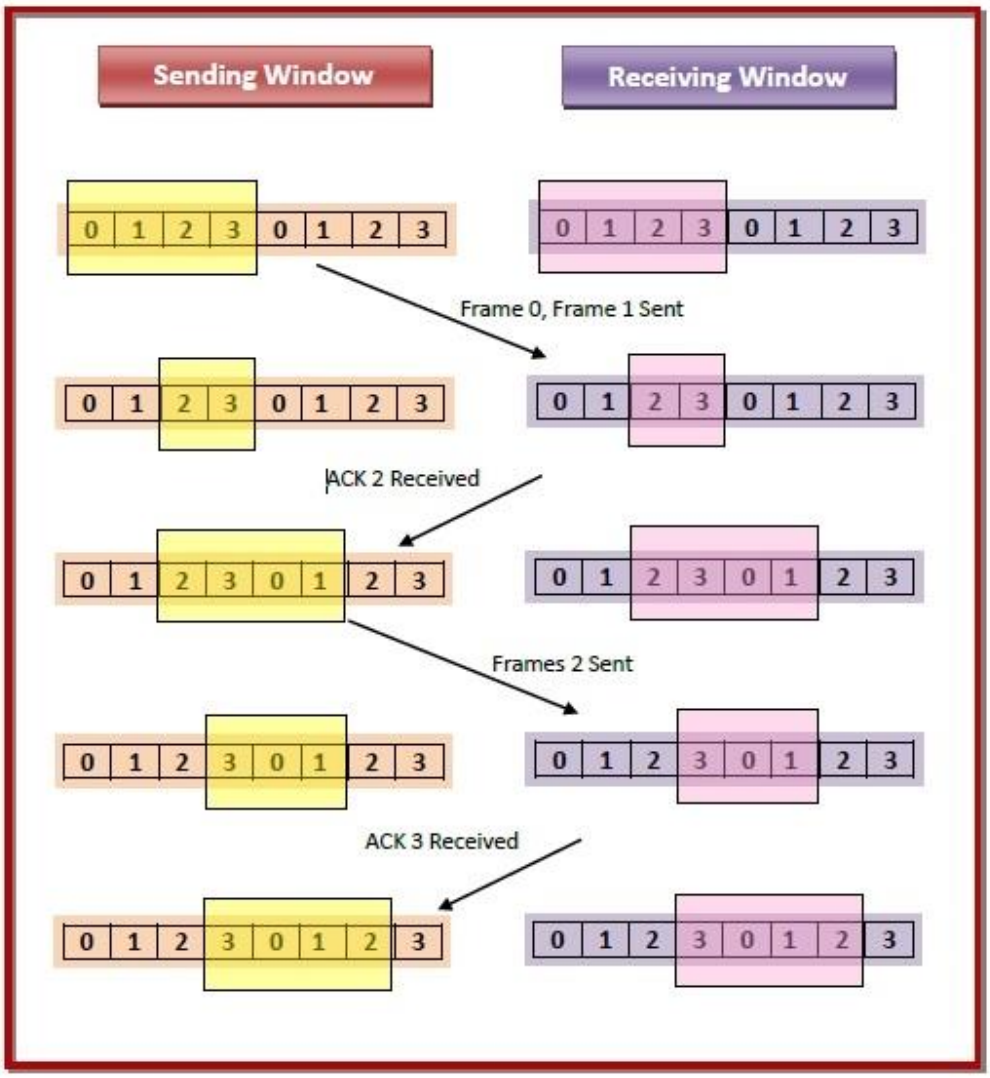
The size of the sending window determines the sequence number of the outbound frames. If the sequence number of the frames is an n-bit field, then the range of sequence numbers that can be assigned is 0 to 2^n-1. Consequently, the size of the sending window is 2^n-1. Thus in order to accommodate a sending window size of 2^n-1, a n-bit sequence number is chosen.

The sequence numbers are numbered as modulo-n. For example, if the sending window size is 4, then the sequence numbers will be 0, 1, 2, 3, 0, 1, 2, 3, 0, 1, and so on. The number of bits in the sequence number is 2 to generate the binary sequence 00, 01, 10, 11.

The size of the receiving window is the maximum number of frames that the receiver can accept at a time. It determines the maximum number of frames that the sender can send before receiving acknowledgment.

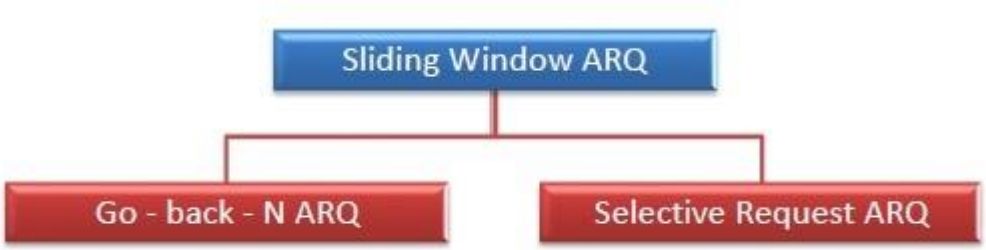
Example

Suppose that we have sender window and receiver window each of size 4. So the sequence numbering of both the windows will be 0,1,2,3,0,1,2 and so on. The following diagram shows the positions of the windows after sending the frames and receiving acknowledgments.



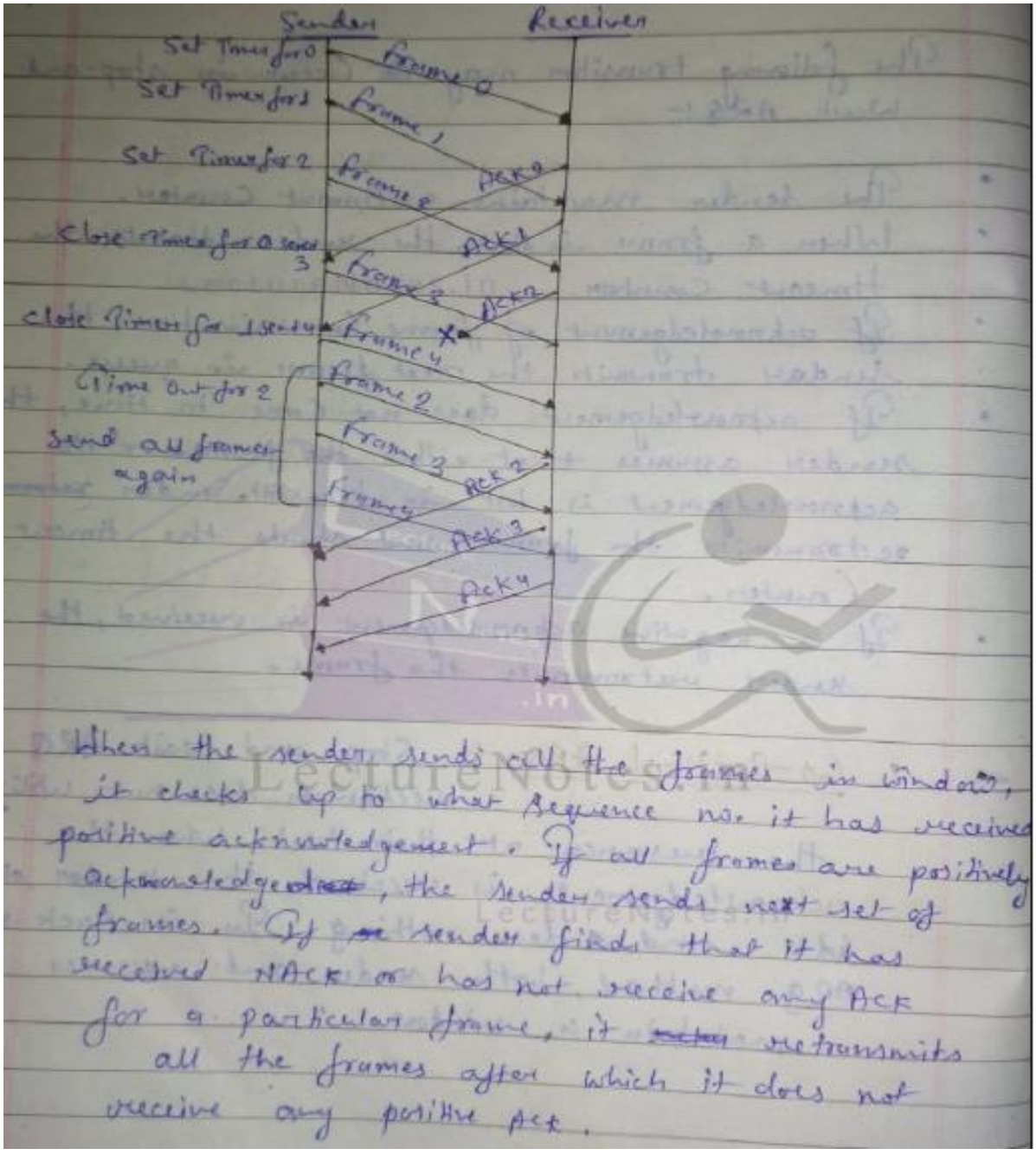
Types of Sliding Window Protocols

The Sliding Window ARQ (Automatic Repeat reQuest) protocols are of two categories –



Go – Back – N ARQ

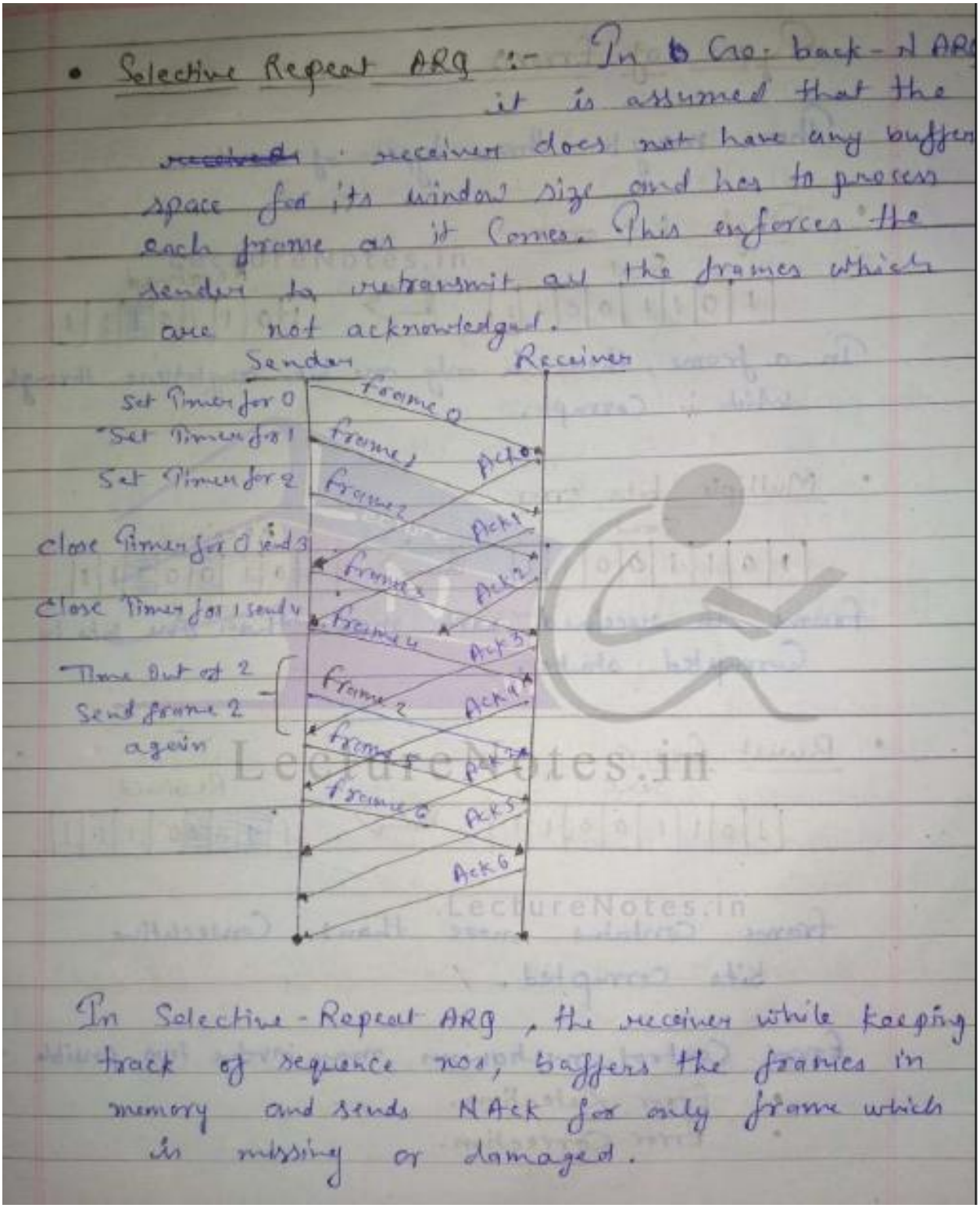
Go – Back – N ARQ provides for sending multiple frames before receiving the acknowledgement for the first frame. It uses the concept of sliding window, and so is also called sliding window protocol. The frames are sequentially numbered and a finite number of frames are sent. If the acknowledgement of a frame is not received within the time period, all frames starting from that frame are retransmitted.



Selective Repeat ARQ

This protocol also provides for sending multiple frames before receiving the acknowledgement for the first frame. However, here only the erroneous or lost frames are retransmitted, while the good frames are received and buffered.

Selective repeat protocol को Selective Repeat ARQ (Automatic Repeat reQuest) भी कहा जाता है. यह एक डेटा लिंक लेयर प्रोटोकॉल है जो कि sliding window विधी का प्रयोग करता है. Go back N प्रोटोकॉल अच्छी तरह कार्य करता है यदि उसमें errors कम होते है. परन्तु यदि line ख़राब होती है तो frames को दुबारा भेजने में बहुत सारीं bandwidth का नुकसान होता है. इसलिए हम Selective repeat का प्रयोग करते है.



Go-Back-N	Selective Repeat
इसमें यदि कोई फ्रेम corrupt या खो जाए तो उसके बाद आने वाली सभी frames को भी दुबारा भेजना पड़ता है.	इसमें केवल उसी फ्रेम को दुबारा भेजा जाता है जो corrupt या खो जाती है.
यदि इसमें error rate उच्च होता है तो यह बहुत सारीं bandwidth को बर्बाद कर देता है.	कम bandwidth का नुकसान होता है.
यह कम complex (कठिन) होता है.	यह ज्यादा complex होता है क्योंकि इसमें sorting तथा searching भी करनी पड़ती है. और इसको ज्यादा storage की भी आवश्यकता होती है.
इसमें sorting नही करनी पड़ती.	इसमें frames को सही क्रम में लाने के लिए sorting की जाती है.
इस में searching नहीं की जाती है.	खोये हुए frames को search करने के लिए इसमें searching ऑपरेशन को perform किया जाता है.
इसका प्रयोग ज्यादा किया जाता है.	इसका प्रयोग कम किया जाता है क्योंकि यह ज्यादा complex है.