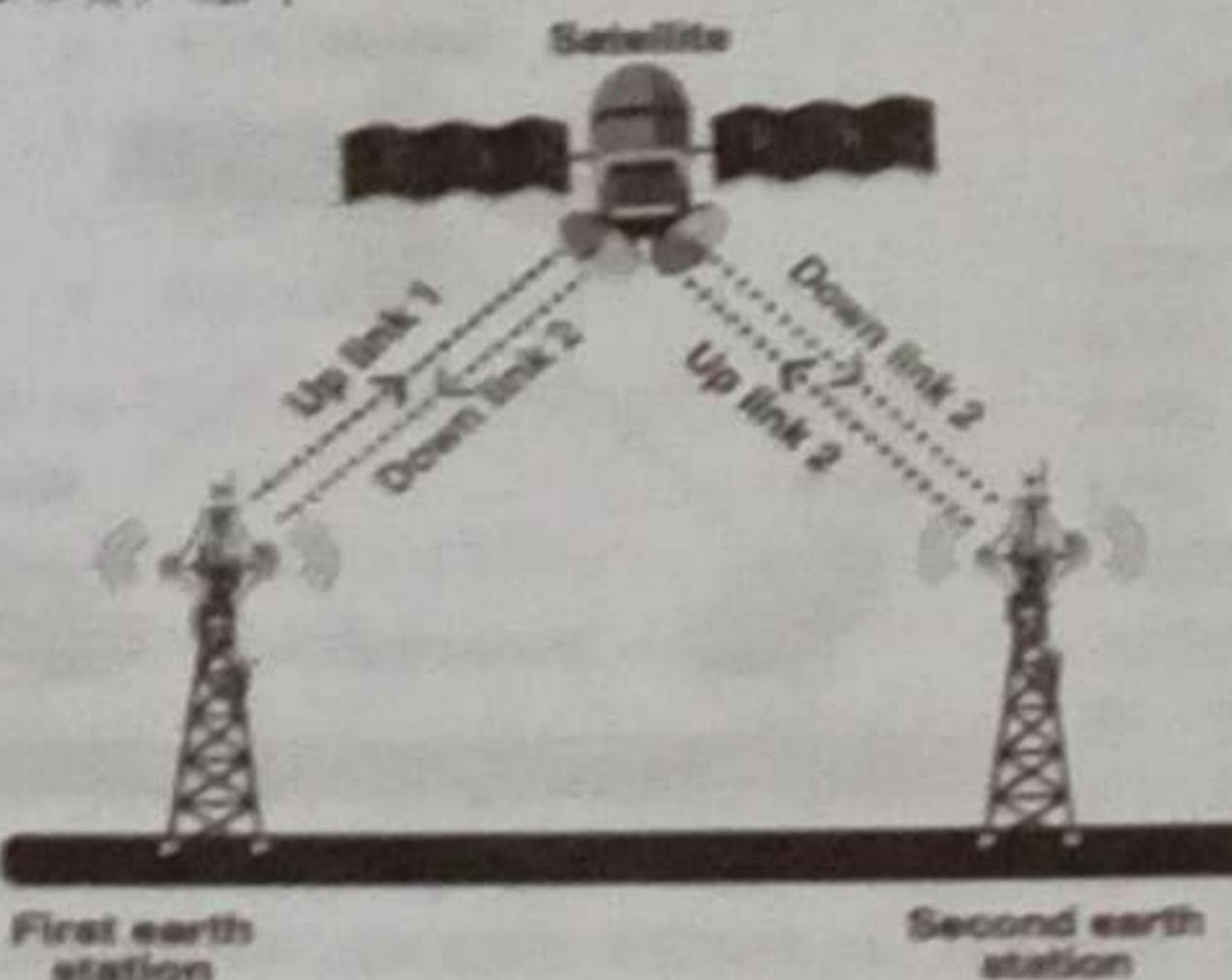


কমিউনিকেশন হল:

- রেডিও বা মিসিং ছান সার্টিস প্রসাম করা হয়।
- স্পেস অপারেশন সার্টিসের একটি অংশ প্রাক্তি।
- ইন্টারনেট সার্টিস বচকলিঙ্গ উপরের সাথে প্রদান করে।

বিনোদ স্যাটেলাইট কমিউনিকেশন বিনোদ স্যাটেলাইট কমিউনিকেশন সেকেনে দৃষ্টি আর্থ স্টেশনের মধ্যে তথ্য অদান-প্রদান করে থাকে। সিলভারলাই প্রথম আর্থ স্টেশন থেকে বিনোদ আর্থ স্টেশনে প্রেরণ করা হয় যাতে আর্থ স্টেশন এবং স্যাটেলাইটের মধ্যে দৃষ্টি আপলিঙ্গ এবং দৃষ্টি ডাউনলিঙ্গ থাকে।



প্রশ্ন ৫. স্যাটেলাইট কমিউনিকেশনের সুবিধা ও অসুবিধা লিখ।
উত্তর: স্যাটেলাইট কমিউনিকেশনের সুবিধা:

- সার্কিটের প্রাপ্তন করা সহজ।
- এই সার্কিটের ছান্তিজ্ঞানকা জালো।
- স্যাটেলাইট কমিউনিকেশনের সাথেযো প্রবিধীর প্রতিটি ছান কাচার করা যায়।
- বাবহাবকাৰী সম্পূর্ণলৈ নেটওয়াৰ্ক নিষ্কাশ করে।

স্যাটেলাইট কমিউনিকেশনের অসুবিধা:

- প্রাথমিক ব্যাপ অনেকে ব্যাবহাল।
- ফ্রিকোমেলি রুকেজ স্বাক্ষৰ আছে।

প্রশ্ন ৬. স্যাটেলাইট কমিউনিকেশনের আপ্রস্তুকেশন লিখ।
উত্তর: স্যাটেলাইট কমিউনিকেশনের আপ্রস্তুকেশন

- রেডিও সম্পর্কের এবং কোনো মোগাদোল
- ডিকি সম্পর্কের সেমন ডাইভেল টি হোৰ (DTH)
- ইন্টারনেট আপ্রস্তুকেশন সেমন ভেটা ছানাকৰের জন্য ইন্টারনেট সময়েল প্রদান, ভিলিঙ্গ আপ্রস্তুকেশন, ইন্টারনেট সার্টিস ইতাবি।
- সামৰিক আপ্রস্তুকেশন এবং নেভিগেশন
- বিমোট সেলিং আপ্রস্তুকেশন
- আবহাবকাৰী অবজ্য পৰিবেক্ষণ এবং পূর্ণাঙ্গ

প্রশ্ন ৭. স্পেস স্টেশন এবং প্রাক্তি স্টেশন ককে বলে?

উত্তর: স্পেস স্টেশন স্পেস স্টেশন মান একটি কৃতিম কঢ়াৰো যা মানুষের জন্য মহাকাশে বসবাস কৰা কৰাৰ জন্য বিজাইম কৰা হয়।

প্রাক্তি স্টেশন প্রাক্তি স্টেশন বিজিৰ ব্যবহাবকাৰী এবং আপ্রস্তুকেশনেৰ কাহে বিমোট সেলিং স্যাটেলাইট ভেটা স্পেস এবং টিম কৰাৰ জন্য কৈৰি কৰা হয়। যাতে আগীৰ আবহাবকাৰী কেজৰ সেমন আবহাবকাৰী ব্যৱৰো বা

CSIRO-এর মতো গবেষণা কেন্দ্ৰ অবস্থৰ থাকতে পাৰে। তাৰ স্টেশনগুলি স্বাক্ষৰণত নিৰ্দলিত প্ৰধান উপাদানগুলি নিম্বে পঢ়িত, এটা বিসিজ্ঞ আক্টোবা, একটি বিভ হৰ্ন, ওয়েভগাইত এবং বিসিভাৰ।

প্রশ্ন ৮. বেসবহ-১ স্যাটেলাইট বৰ্ণনা কৰোনা।

অবৰা বালাদেশে স্যাটেলাইট কমিউনিকেশন সৰ্বকে আলোচনা কৰে। উত্তৰ: বেসবহ-১ (BD-1), বালাদেশেৰ প্ৰথম কমিউনিকেশন স্যাটেলাইট, বালাদেশ টেলিকমিউনিকেশন বেসেটোৱি কৰিন (বিটআৰলি) বৰা কৈৰি কৰা হয়েছে। ২০১৮ সালৰ মে মাস স্যাটেলাইট বিজনেশনৰ আৰ্থ অৰবিটে (GEO) চালু কৰা হয়েছে। ১১৯.১°E অৰিয়ানৰে অৰবিটল অবস্থানে অৰীচৰ্ত, বেসবহ-১ বালাদেশেৰ প্ৰাচীয় এ্যাবাজ সম্প্ৰচাৰ ও টেলিযোগাবেগ পৰিবেৰ প্ৰস কৰে। এটি স্বাস্থি-টু-হোৰ (DTH) পৰিবেৰ সহ লাভজন পৰিবেৰলিকেও সহৰ্ষণ কৰে। এটি বজেপনসাৰ, ভাৰত, দেশ, ভূটান, শ্ৰীলঙ্কা, ভিলিপাইন, ইন্দোনেশিয়াৰ এবং বালাদেশ এৰ আৰম্ভি জলনীন কৃত কৃ-ব্যাক এবং সি-ব্যাক পৰিবেৰ সহৰ্ষণ কৰে।

বৃ-ব্যাক এবং সি-ব্যাক এৰ ফ্ৰিকুেন্চিৰ রেজ নিম্বেৰপৰা

ফ্ৰিকুেন্চিৰ ব্যাক	ফ্ৰিকুেন্চিৰ জো
সি-ব্যাক	৪-৮
বৃ-ব্যাক	১২-১৮

প্রশ্ন ৯. স্যাটেলাইট কমিউনিকেশনেৰ ফ্ৰিকুেন্চি ব্যাতসমূহেৰ অপ্রিত এবং ডাউনলাই ব্যাত লিখ।

উত্তৰ:

ফ্ৰিকুেন্চিৰ ব্যাক	ডাউনলাই ব্যাক (MHz)	অপ্রিত ব্যাক (MHz)
Uhf-Military	250-270	292-312
C Band Commercial	2700-4200	5925-6425
X Band Military	7250-7750	7900-8400
Ku Brand Commercial	11700-12200	14000-14500
K Brand Commercial	17700-21203	27500-30000
K Brand Military	20200-21200	43500-45500

প্রশ্ন ১০. আৰ্থ স্টেশনেৰ প্যারামিটাৰগুলো লিখ।

উত্তৰ: আৰ্থ স্টেশনেৰ প্যারামিটাৰসমূহ:

- এককোজাৱ, ডিকেজাৱ
- মুলোটি, ডিমুলোটি
- আপ-কনজাটোৱ, ভাটন-কনজাটোৱ
- এই প্যারামিটাৰ আপ্রিকোজাৱ, সেৱা প্যারামিটাৰ আপ্রিকোজাৱ

প্রশ্ন ১১. ফিলিটল স্যাটেলাইট কমিউনিকেশন ব্যাতসমূহৰ সুবিধা লিখ।

উত্তৰ: ফিলিটল স্যাটেলাইট কমিউনিকেশন ব্যাতসমূহৰ সুবিধা:

- সহজ ও সুবিধুল মালিন্টেজোৱ, পৰিবেৰ এজেন্স
- ফুলকুটি ফিলিটল ও স্বাক্ষৰণ ব্যৱহাৰ
- সোপানোসেৱ প্ৰেপৰেটোৱ
- মানব কৃলক্ষণি ও উচ্চ বিশুদ্ধতা
- ফিলিটল প্ৰক্ৰিতিৰ ব্যাপারে বৰ্ত, মুদ্ৰা, এবং ঘোট আৰ্থ স্টেশন উচ্চ দক্ষতাৰ সাথে কমিউনিকেশন সহৰ্ষণ কৰা হয়।
- ফিলিটল সিলভারলকে কোডিং কৰা সহজ কোল খুলু খুলু লিখু ও সেপনীয়তা বৰ্কা কৰা যায়।

Computer Network and Security

Syllabus: BPSC CS: Protocol, fundamentals of control protocol, Introduction and network types, LAN, MAN, WAN. Topologies: Star, switched, bus, ring. Ethernet LAN standards. Internetworking: Network interconnection, bridges, routers. Network layer protocols: IP, ARJP, ICMP, IP addresses. Unicast and multicast routing protocols. IPv6 congestion control, Transport layer protocol: TCP and UDP. Introduction to wireless LAN, VSAT, analog and digital cellular system. Network security: Types of attack, encryption techniques and digital signatures. ATM switches, ATM protocol; DNS, HTTP, Email.

NTRCA CS: Basic computer network concept; Network structure; Network software; Reference model; OSI Model, TCP/IP Model, X.25 Networks. Frame Relay, ATM Network, Medium Access sub-layer, Network Layer, Optical Fiber Network, Application Layer. Cryptography and cryptographic algorithms, Cryptography and network security.

NTRCA ICT (BM): ডাটা কমিউনিকেশন ও কমিউনিকেশন মিডিয়া কম্পিউটাৰ নেটওয়াৰ্ক ও নেটওয়াৰ্কৰ অৱোপ।

NTRCA ICT: Introduction: Overview of the Internet, Overview of Networking Protocols, Network Edge, Network Core, Protocol Layers / Service Model, General Networking Example; Application Layer: Principles of Networking Applications, Web and HTTP, FTP, E-mail, DNS; Transport Layer: Transport Layer Services, Multiplexing and De multiplexing, Connectionless Transport: UDP, Principles of Reliable Data Transport, Connection- Oriented Transport: TCP, Principles of Congestion Control, TCP Congestion Control; Network Layer: Datagram Networks, Inside a Router, Details of the Internet Protocol (IP), IP Sub netting, Routing Algorithms (Link State, Distance Vector), Routing in the Internet (Routing Information Protocol (RIP), Open Shortest Path First (OSPF), Border Gateway Protocol (BGP)).

বেসিক টিপ্প

১) **WWW(World Wide Web):** ১৯৮৯ সালে সুইজারল্যান্ডের বিজ্ঞানীগণ এটি উদ্বাবন করেন। WWW (World Wide Web) হচ্ছে একটা কম্পিউটার নেটওর্ক যা সারা বিশ্বে ছড়ানো। WWW কেই কলা হচ্ছে থাকে Web, এই ওয়েবে কম্পিউটারগুলো একটি অপরাদির সাথে কিছু নিয়ম ও ভাষা ব্যবহার করে যোগাযোগ করে থাকে। W3C (The World Wide Web Consortium) এই ভাষা এবং নিয়মগুলো তৈরী করে যাচ্ছে। ১৯৯৩ সালের মেক্সিকো থেকে W.W.W এর বহু ব্যবহারের প্রচলন শুরু হয়।

২) **ওয়েব আড্রেস/URL:** URL এর পূর্ণরূপ হচ্ছে Uniform Resource Locator. ওয়েব আড্রেস/URL হলো একটি ওয়েবপেজের এর ইউনিক আইডেন্স (Unique Address) যা ওয়েবের সর্বিস প্রদান করে। প্রতিটি ওয়েবের আড্রেস এর একটি আইপি আইডেন্স থাকে।

- a) Protocol
- b) Domain name
- c) Path to a specific web
- d) Page or location on a web page



Figure: Structure of a URL

৩) **টেলনেট(Telnet):** যে সার্ভিস এর মাধ্যমে কোন ব্যবহারকারী দূরবর্তী কোন অবস্থানের কোন কম্পিউটারে লগ ইন করতে পারেন এবং তা থেকে রিসোর্স ব্যবহার করতে পারেন সে সার্ভিসকে কে বলা হয় টেলনেট (Telnet)। টেলনেট লোকাল কম্পিউটারটিকে টার্মিনাল এবং দূরবর্তী অবস্থানের যে কম্পিউটারের সাথে সংযোগ স্থাপন করা হয় সেটিকে হোস্টের সাথে স্থূলনা করা যায়।

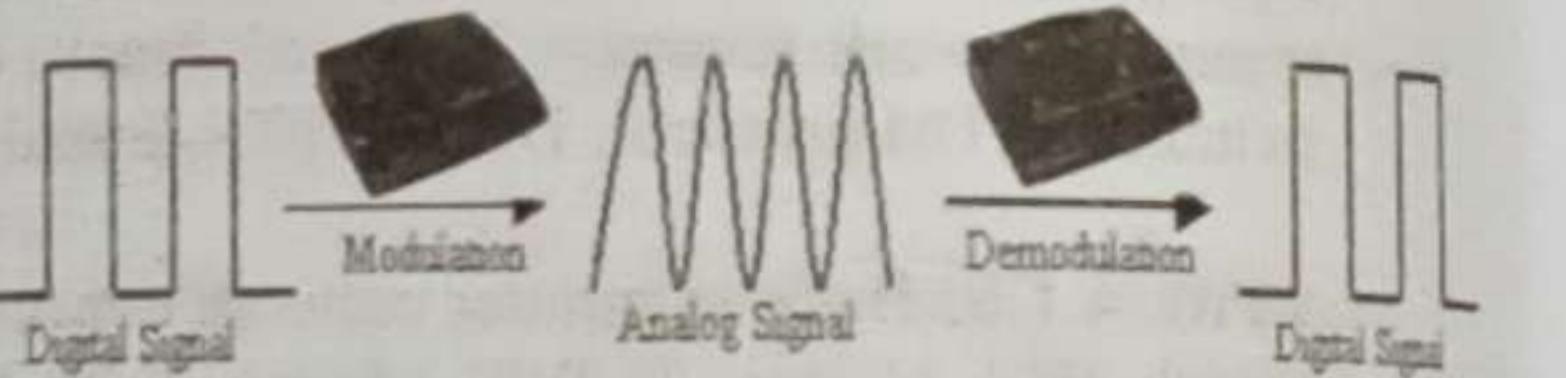
৪) **সার্ভার (Server):** সার্ভার মূলত একটি শক্তিশালী কম্পিউটার যা কেন্দ্রীয়ভাবে স্থাপিত হয়ে নেটওর্কের কেন্দ্র এবং কম্পিউটারসমূহের মধ্যে পারস্পরিক যোগাযোগ ও উপাত্ত বিনিয়োগের ব্যবহাৰ করে। একেতে খুবই শক্তিশালী প্রসেসর ব্যবহৃত হয় এছাড়াও থাকে অধিক ক্যাপ্শ মেমোরি ও সহায়ক মেমোরি।

৫) **ওয়েব ব্রাউজিং (Web Browsing):** ওয়েব ব্রাউজিং হলো পৃথিবীর বিভিন্ন দেশের সার্ভারে রাখা ওয়েব পেইজ পরিদর্শন প্রক্রিয়া। ওয়েব ব্রাউজিং এর মাধ্যমে ইন্টারনেটের তথ্য আহরণ করা সহজ।

৬) **ওয়েব সার্চ ইঞ্জিন(Web Search Engine):** কোন নির্দিষ্ট তথ্যের সংশ্লিষ্ট ওয়েবের সার্ভারের আইডেন্স জানা থাকলে খুব সহজে খুজে বের করা যায়। কিন্তু যদি আইডেন্স টি জানা না থাকে সেকেতে সার্চ ইঞ্জিন ব্যবহার করে সহজেই যে কোন তথ্য খুজে বের করা যায় না। কয়েকটি বহু ব্যবহৃত ওয়েব সার্চ ইঞ্জিন হচ্ছে: গুগল, বিং, ইয়াহ ইত্যাদি।

৭) **হাইপারটেক্স্ট (Hypertext):** ওয়ার্ড ওয়াইড ওয়েবের ভিত্তি হ্যাঙুমেন্ট এবং অন্যান্য মিভিয়া যা লিংক গুলির মাধ্যমে সংযুক্ত। এ লিংকগুলি হাইপারলিঙ্ক (Hyperlink) হিসাবে পরিচিত। হাইপারটেক্স্ট ইলেক্ট্রনিক ফরম্যাট যা ওয়ার্ড ওয়াইড ওয়েব (World Wide Web) এ সংরক্ষিত টেক্সট বা নথি। হাইপারটেক্স্ট এর মাধ্যমে ব্যক্তি (Text) সাথে অন্য একটির বার্তার লিংক দেওয়া যায়, যার কলে ইলেক্ট্রনিকভাবে অন্য জায়গায় থাকা টেক্সট এই লিংকে ক্লিক করে এক্সেস (Access) করতে পারে। এর বিশেষত্ব হলো এর সাহায্যে স্থেপন মধ্যে লিংক বা যোগসূত্র রাখা যায়। এর সাহায্যে ডকুমেন্টের বিভিন্ন শব্দ যাওয়া যায়।

৮) **মডেম(Modem):** মডেম হচ্ছে একটি Electronic ডিভাইস, নেটওর্কিং তথ্যবলি আদান-প্রদানের জন্য মডেম ব্যবহৃত হয়। Modem শব্দটি Modulation শব্দের Mod এবং Demodulation শব্দের Dem নিয়ে গঠিত। Modem আমল টেলিযোগাযোগ সর্কিটের মাধ্যমে সঞ্চালনের উপযোগী ডিজিটাল টো সিগন্যালগুলিকে মডুলেটেড এনালগ সিগন্যালে রূপান্তর করে এবং মোডুলেটেড সিগন্যালগুলিও রিসিভ করে এবং সেন্টালি ডিমডুলেটে ব্যবহার জন্য চিকিৎসা সিগন্যালে রূপান্তরিত করে।



৯) **ওয়েবপেইজ বা সাইট (Web Page or Site):** ইন্টারনেট আমাদের দিছে নানা প্রক্রিয়া বিভিন্ন তথ্য, আর এ তথ্যের বাহক হিসাবে কাজ করে ওয়েবপেইজ। ওয়েবপেইজ সাধারণত HTML, CSS, JavaScript ইত্যাদি বেসিক ল্যাংগুেজ ব্যবহার করে তৈরি করা হয়। আর এ সব ডকুমেন্ট বা সাইট গুলো সার্ভারে সংরক্ষণ করা থাকে। কতকগুলো ওয়েবপেজ নিয়ে একটি ওয়েবসাইট তৈরি করা হয় এবং প্রত্যেকটি ওয়েবসাইট এর জন্য নির্দিষ্ট কোন নাম বা ডোমেইন এর রূপ হয়।

১০) **সাইবার অপরাধ (Cyber Crime):** কম্পিউটার ক্রাইম বা সাইবার ক্রাইম কলতে কম্পিউটার এবং নেটওর্ক এর মাধ্যমে যে অপরাধ সংগঠিত হয় তাকে বুঝায়। সাইবার ক্রাইম হল: কম্পিউটার এক্ষেত্রে ব্যবহার করে যে কোন ব্যক্তি বা ব্যক্তিগোষ্ঠী সমষ্টি কে মানসিকভাবে হারানি এবং নানান ধরনের আপত্তিকর ব্যক্তিগত ভিত্তিও বা ইলেক্ট্রনিক ছবি প্রেরণ করা হয়।

১১) **ফ্যাক্স (Fax):** ফ্যাক্স, যা কি-না ইংরেজি ফ্যাক্সিমিলি (Facsimile) শব্দের সংক্ষেপ, একটি ইলেক্ট্রনিক যন্ত্র যা কোন ক্ষেত্র, স্থানীয়ভাবে ব্যক্তি বা দলগুলোর ছবি ইত্যাদি ডিজিটাল পর্যায়ে টেলিফোন তারের সহায়তায় একছান থেকে মুছতের মধ্যে অন্য ছানে পৌছানো যায়। টেলিফোনে যেমন শব্দ প্রেরণ করা হয়, ফ্যাক্স-এর মাধ্যমে তেমনি ইলেক্ট্রনিক ছবি প্রেরণ করা হয়।

১২) **টেলেক্স (Telex):** টেলেক্স এক প্রাকারের বিশেষ টেলিফোন ক্ষেত্রে যাতে বার্তা টাইপ হয়ে বের হয়। এ যন্ত্রে বার্তার কথাগুলো টেলিখিল্ডের সাহায্যে টাইপ হয়। অর্থাৎ এ যন্ত্রে প্রেরিত শব্দ বা কথাগুলো ব্যবহৃত ওয়েবের সার্চ ইঞ্জিন হচ্ছে: গুগল, বিং, ইয়াহ ইত্যাদি।

টেলিপ্রিন্টারের সাহায্যে টাইপ হয়ে প্রাপকের নিকট পৌছে যায়। যোগাযোগ ক্ষেত্রে এটা আধুনিক প্রযুক্তির এক ধরণ।

১৩) **ই-মেইল (E-mail):** ই-মেইল পূর্ণরূপ ইলেক্ট্রনিক মেইল (Electronic Mail)। এটি ইলেক্ট্রনিক ভাবে যোগাযোগ পদ্ধতি। কোন ই-মেইল অস্লে তা জমা থাকে ISP সার্ভারে অবস্থিত প্রাপকের মেইল বৰে। ই-মেইল username@domain.com নিয়ে গঠিত। ই-মেইল ঠিকানায় ডোমেইন নামের সর্বশেষ অংশটিকে বলা হয় আইএসপি। ১৯৭২ সালে ই-মেইল ঠিকানায় সর্বশেষ @ চিহ্ন ব্যবহার করা হয়। Netscape Communicator এর মাধ্যমে ই-মেইল পড়তে চাইলে যে ক্ষমতাটি নিতে হবে তা ইল-ফাইলের মাধ্যমে ই-মেইল address bitboxinfo@gmail.com ক্লায়েন্ট সার্ভার ম্যানেজমেন্ট।

১৪) **ওয়াইফাই (WiFi):** WiFi (ওয়াইফাই) এর পূর্ণরূপ হচ্ছে-Wireless Fidelity. WiFi (ওয়াইফাই) হচ্ছে ওয়ারলেস লোকাল এরিয়া নেটওর্ক ব্যবহার করার সাহায্যে বহনযোগ্য কম্পিউটারের সাথে সহজে ইন্টারনেট সংযুক্ত করা যায়। ওয়াইফাই যোগাযোগ ব্যবহার উচ্চ ফ্রিকোয়েন্সী রেডিও ওয়েব ব্যবহার করা হয়।

১৫) **সোশ্যাল নেটওয়ার্কিং (Social Networking):** সোশ্যাল নেটওয়ার্কিং হচ্ছে সামাজিক যোগাযোগ ও মাইক্রোব্লগিংয়ের একটি ওয়েবসাইট। খুব সহজেই ব্যবহারকারী বন্ধুদের সাথে তথ্য আদান প্রদান ও বিভিন্ন বিষয়ে মতামত, তথ্য ইত্যাদি বিনিয়োগ করা যায়। খুব সহজেই ও ব্যাপক সময়ে অডিও ভিত্তিত ছবি ইত্যাদি সংরক্ষণ, ছবি ছানান্তর, ছবি গ্রহণ ইত্যাদি করা যায়। কয়েকটি সোশ্যাল নেটওয়ার্কিং সাইট হচ্ছে ফেসবুক, টুইটার, ইনস্টাগ্রাম, টেলিগ্রাম, ভাইভার, হোয়াটস আপ ইত্যাদি।

১৬) **হটস্পট (Hot Spot):** হটস্পট (Hotspot) হলো এক ধরনের ওয়ারলেস নেটওয়ার্ক। যা মোবাইল ও কম্পিউটার ডিভাইস যেমন: ম্যাটেল, PDA, প্যান্ডা, নেটবুক, ল্যাপটপ ইত্যাদিতে ইন্টারনেট সংযোগ স্থাপন করে। ইহা নির্দিষ্ট এলাকা জুড়ে এমন একটি নির্ধারিত জায়গা স্থাপন করে। ইহা নির্দিষ্ট এলাকা জুড়ে এমন একটি নির্ধারিত জায়গা যেখানে ইন্টারনেটে প্রবেশ করা যায় ওয়ারলেস লোকাল এরিয়ার মাধ্যমে। মূলত একটি হটস্পট তৈরী করা হয়ে থাকে রাউটারের মাধ্যমে যা মূল সার্ভার কম্পিউটারের সাথে সংযুক্ত থেকে ক্লাউডিনভাবে ডাটা স্বরবরাহ করতে থাকে। বর্তমানে জনপ্রিয় তিনটি হটস্পট (Hotspot) প্রযুক্তি হলো: Bluetooth, Wi-Fi, Wi-MAX.



Figure: Hotspot

১৭) **ব্লুটোথ (Bluetooth):** Bluetooth হচ্ছে একটি ওয়ারলেস প্রযুক্তি যার মাধ্যমে একটি ওয়ারলেস প্যার্সোনাল এরিয়া নেটওয়ার্ক (WPAN) তৈরি করা যায়। ১৯৯৪ সালে টেলিকম তেকনোলজি এবং ব্লুটোথ উভয়েই ব্লুটোথ ডিভাইস প্রক্রিয়া করে। দশম শতাব্দির ডেনমার্কের রাজা হারাক্স ব্লুটোথ এর নামানুসারে এ প্রযুক্তিটির নাম রাখা হয়েছে Bluetooth. বর্তমানে আয় সকল ইলেক্ট্রনিক ডিভাইসে Bluetooth বিল্ট-ইন থাকে। তবে বিভিন্ন ডিভাইসে USB পোর্টের মাধ্যমেও Bluetooth সংযোগ দেওয়া যায়।

১৮) **Wi-Fi ব্যবহার করে একই সাথে একাধিক কম্পিউটারে ইন্টারনেট সংযোগ দেয়া যায়।**

Bluetooth এর কভারেজ এরিয়া সাধারণত ১০ মিটার হয়ে

থাকে। Bluetooth 2.0 এর সর্বোচ্চ ড

- c) এটি একটি গ্যারলেস লোকাল এরিয়া নেটওয়ার্ক ব্যবহাৰ।
- d) একটি নির্দিষ্ট এরিয়াৰ মধ্যে WiFi প্ৰযুক্তি ব্যবহাৰ কৰা সহজ।
- e) ওয়াইফাই লোকাল এরিয়া নেটওয়াৰ্কৰ তুলনাৰ সম্ভাৱ।
- f) ওয়াইফাই রাউটাৰ দিয়ে একাধিক ডিভাইসে একসাথে সংযোগ দেৱা সহজ।
- g) যে কোনও জ্বান দিয়ে ইন্টাৰনেট আ্যোৱেস কৰতে পাৰেন (আপনাৰ রাউটাৰেৰ সিগনাল অনুযায়ী)।
- h) কাঠামোগত ক্যাবলিং ইন্টাৰনেট সংযোগ ছাড়াই খুব সহজেই ওয়াইফাই ব্যবহাৰ কৰা যায়।
- i) ওয়াইফাই খুব চৰ্ত এবং সহজ। ওয়াইফাই সিস্টেম এবং এৰ প্ৰোটোকল ভলিন প্ৰযুক্তিগত জ্বানেৰ প্ৰয়োজন নেই।
- j) বিভিন্ন ধৰণেৰ ডিভাইসে WiFi ব্যবহাৰ কৰা যায়। যেমন: আৰ্টিফেন, ট্যাবলেট ডিভাইস এবং অন্যান্য পোতেৰ ডিভাইস।
- k) WiFi এক্সেন্টোৰ ব্যবহাৰ কৰে নেটওয়াৰ্ক প্ৰসাৰিত কৰতে পাৰেন।

WiFi এৰ অসুবিধা (Disadvantages of Wi-fi):

- a) কেবল হটস্পটগৰোতে এটি ব্যবহাৰ কৰা হয় এটি হচ্ছে ওয়াইফাই ব্যবহাৰেৰ সবচেয়ে বড় অসুবিধা।
- b) এৰ কাভাৰেজ খুব বেশি এৰিয়া জুৰে পাৰে যায় না।
- c) নিৰাপত্তা ব্যবহাৰ তুলনামূলকভাৱে দুৰ্বল।
- d) ওয়াইফাই প্ৰযুক্তিল ভাটা চলাচলেৰ গতি খুব একটা বেশি নহ।
- e) ডেটা ট্ৰান্সফাৰ রেট কৰে যায় যখন ব্যবহাৰকাৰী বা ওয়াইফাই নেটওয়াৰ্কেৰ সাথে সংযুক্ত কম্পিউটাৰেৰ সংখ্যা বৃদ্ধি পাৰে।
- f) ওয়াইফাই রাউটাৰে আমাদেৰ নেটওয়াৰ্কেৰ পাসওয়াৰ সুৰক্ষিত কৰতে বিভিন্ন এনক্ৰিপশন পদ্ধতি রয়েছে। আপনাৰ ওয়াইফাই পাসওয়াৰ হাক হওৱাৰ সংজ্ঞাৰ রয়েছে।
- g) ওয়াইফাই আ্যোৱেস প্ৰায় ৩০ থেকে ১০০ মিটাৰ পৰ্যন্ত (যেমন: ১০০ থেকে ৩০০ ফুট) সীমাবদ্ধ।
- h) ওয়াইফাই এৰ কাৰণে মানুষেৰ ঘাণ্ডা ক্ষতিও হতে পাৰে; যেমন: ক্যান্সাৰ, অন্দ্ৰোইড, অ্যাপোগোসিস এবং গৰ্ভবতী মহিলাদেৰ ওয়াইফাই ৰেডিওশনেৰ বাইৰে থাকাৰ পৰামৰ্শ দেওয়া হয়।
- i) সঠিকভাৱে সুৰক্ষিত না কৰা হলে লোকেৰা ব্যক্তিগত নেটওয়াৰ্ক আ্যোৱেস কৰতে পাৰে এবং তথ্য চুৰি কৰতে এবং এমনকি খাৰাপ উদ্দেশ্যে নেটওয়াৰ্ক ব্যবহাৰ কৰতে পাৰে।

WiFi এৰ ব্যবহাৰ(Aplications of WiFi):

- a) ওয়াইফাই অপশন থাকলে সব ধৰনেৰ ইলেক্ট্ৰনিক ডিভাইসে
- b) সীমিত এৰিয়াৰ মধ্যে WiFi প্ৰযুক্তি ব্যবহাৰ কৰা খুবই সহজ।
- c) ছাত্ৰ-ছাত্ৰীদেৰ ব্যবহাৰেৰ সুবিধাৰ্থে শিক্ষা প্ৰতিষ্ঠানে এৰ ব্যবহাৰ রয়েছে।
- d) বিমানবন্দৰ, হটেল, রেষ্টোৱাতে WiFi প্ৰযুক্তিৰ সেৱা প্ৰদান কৰা যায়।
- e) ওয়াইফাই ব্যবহাৰ কৰে বৰ্তমানে এক সাথে কয়েকজন মিলে একই ভিত্তিও গেম খেলা যায়।

১৮) ওয়াইম্যাক্স(WiMAX) কি? এৰ প্ৰকাৰভেদ এবং এটি কিভাবে কাজ কৰে? (What is Wi-Max? Classify it and explain how it works?) [NTRCA- 2010]

Wi-MAX এৰ পূৰ্বৰূপ হচ্ছে Worldwide Interoperability for Microwave Access ওয়াইম্যাক্স প্ৰযুক্তিৰ মাধ্যমে উচ্চ পৰ্যন্ত ব্রডব্যান্ড সেৱা, তাৰবিহীন ব্যবহাৰ বিহুত এলাকাজুড়ে ইন্টাৰনেট ওয়াৰলেস মেট্রোপলিটন এৰিয়া নেটওয়াৰ্ক (WMAN) এৰ জন্য মানুষী আৰ্দ্ধ হিসেবে গ্ৰহণ কৰা হয়। ১৯৯৮ সালে IEEE 802.16, ওয়াৰলেস মেট্রোপলিটন এৰিয়া নেটওয়াৰ্ক (WMAN) এৰ জন্য মানুষী আৰ্দ্ধ হিসেবে গ্ৰহণ কৰা হয়। এ প্ৰটোকলৰ ডেটা ট্ৰান্সিশন রেট ৫ মেগাবিট/সেকেণ্ড। WiMAX এৰ প্ৰধান দুটি অংশ রয়েছে। একটী হচ্ছে WiMAX এৰ বেস স্টেশন যা ইনডোৱ ও আউটডোৱ টাইপে নিয়ে গঠিত। অন্যটি হচ্ছে আ্যটেনাসহ WiMAX রিসিভাৰ, যা কোনো কম্পিউটাৰ বা ল্যাপটপে সংযুক্ত থাকে। একটি WiMAX বেস স্টেশন সাধাৰণত ১০ কিমি হতে তৱৰ কৰে ৬০ কিমি পৰ্যন্ত ব্রডব্যান্ড ইন্টাৰনেট আ্যোৱেস সুবিধা দিয়ে থাকে।

ওয়াইম্যাক্স এৰ প্ৰকাৰভেদ (Classification of Wi-Max):
ওয়াইম্যাক্স দুই প্ৰকাৰ। যথা:

ফিক্সড ওয়াইম্যাক্স (Fixed Wi-Max): ফিক্সড ওয়াইম্যাক্স IEEE 802.16D স্টাৰ্টাৰ্ড এৰ উপৰ ভিত্তি কৰে পৰিচালিত হয়। একেতে হচ্ছে প্ৰাপ্তি একটি রিসিভাৰ টাওয়াৰ (এটেনো) বসানো হয়। ব্যবহৃত হতে ১০ মিগা হার্টজ থেকে তৱৰ কৰে ৬৬ মিগা হার্টজ পৰ্যন্ত হাই ফিক্সেলি হৈ। ফিক্সড ওয়াইম্যাক্সেৰ বেজ এবং ব্যাডউইথ ক্যাপাসিটি বেশি হৈ। মোবিলিটি নেই। বলে এই পদ্ধতি সাধাৰণ ব্যবহাৰকাৰীদেৰ নিকট জনপ্ৰিয়তা পাৰিব।

মোবাইল ওয়াইম্যাক্স (Mobile Wi-Max): মোবাইল ওয়াইম্যাক্স IEEE 802.16E স্টাৰ্টাৰ্ড এৰ উপৰ ভিত্তি কৰে পৰিচালিত হয়। একেতে গ্ৰাহক প্রাপ্তি EDGE মডেমেৰ মতো একটি ওয়াইম্যাক্স মডেম ব্যবহাৰেৰ প্ৰয়োজন হয়। ২ মিগা হার্টজ থেকে তৱৰ কৰে ১১ মিগা হার্টজ পৰ্যন্ত লো ফিক্সেলি রেজেন্স ট্ৰান্সিশন হয়। বলে ঘিণ্ডি এলাকাৰ গৱেষণা অধৰাৰ সূৰ্যৰ আলোৱাই অকলাৰ কোন বাসায় ওয়াইম্যাক্স সিগনাল অন্যান্যে ওয়াইম্যাক্স মডেম দিয়ে রিসিভ কৰা সহজ। ফিক্সড ওয়াইম্যাক্সেৰ তুলনায় মোবাইল ওয়াইম্যাক্সেৰ ইনডোৱ ইউনিট আৰ্দ্ধ মডেমেৰ ক্ষেত্ৰে ইউজাৰকে ওয়াইম্যাক্স বেজ স্টেশনেৰ কাছাকাছি থাকে। হয়ে নাহালে ভিত্তিও সিগনাল লস হওয়াৰ আশঙ্কা থাকে।

ওয়াইম্যাক্স কিভাবে কাজ কৰে? (How Wi-Max Works?)
এই প্ৰযুক্তি মূলত দুইটি অংশেৰ উপৰ নিৰ্ভৰশীল: প্ৰথমত একটি টাওয়াৰ, যেটা কেবলকৈ সেলফোন টাওয়াৰেৰ সাথে তুলনা কৰতে পাৰেন এবং দ্বিতীয় যেটি রিসিভাৰ, যেটা আপনাৰ ফোন বা পিসিতে বিল্টইনভাৱে থাকে অথবা মডেমে থাকে কিংবা আলাদা রিসিভাৰ ডিভাইজ আইএসপি থেকে প্ৰদান কৰে। টাওয়াৰটি মূলত বিশাল এৰিয়া জুড়ে সিগনাল লুচে মাৰে এবং মোটামুটি ৩,০০০ বৰ্গ মাইল (৮০০০ বৰ্গ কিলোমিটাৰ) পৰ্যন্ত কৰতে প্ৰদান কৰতে পাৰে।

ওয়াইম্যাক্স টাওয়াৰ স্টেশনেৰ সাথে সমৰাপি হাই ব্যাডউইথ ইন্টাৰনেট কৰন্তোৰে কাজ কৰে, হতে পাৰে কেন তাৰেৰ মাধ্যমে টাওয়াৰে ইন্টাৰনেট আ্যোৱেস দেওয়া থাকে, আৰ এই ইন্টাৰনেটই টাওয়াৰ আংশিক WiMAX টেকনোলজি ব্যবহাৰ কৰে আপনাৰ ফোন বা রাউটাৰেৰ পৰ্যন্ত পৌছিব। আবাব একটি টাওয়াৰ আৱেকটি টাওয়াৰেৰ সাথে মাইক্ৰোজেল লিঙ্গে কৰা হচ্ছে।

ব্যবহাৰ কৰে কানেক্টেড থাকে, যেটাৰে ব্যাকহোল (Backhaul) বলা হয়। এই টেকনোলজিতে ব্যবহাৰ কৰা ট্ৰান্সিভাৰ অনেক বেশি দক্ষ হয়ে থাকে ফলে অনেক পৰিমাণে ভাটা অনেক কম এৰারে সেত কৰা সম্ভৱ হয়। এৰ ভেতও ফিক্সেলি অনেক বেশি হয়ে থাকে, মোটামুটি ৬৬ মিগাহার্জ পৰ্যন্ত ফিক্সেলি পাওয়া যেতে পাৰে, তাই অত্যন্ত হাই ব্যাডউইথ রেট প্ৰদান কৰতে সক্ষম হয়।

ওয়াইম্যাক্স এৰ সুবিধা (Advantages of Wi-Max):

- a) কভাৰেজ এৰিয়াৰ সাধাৰণত ১০ কিমি হতে তৱৰ কৰে ৬০ কিমি পৰ্যন্ত হয়ে থাকে।
- b) একক একটি স্টেশনেৰ মাধ্যমে হাজাৰ হাজাৰ ব্যবহাৰকাৰীকে ইন্টাৰনেট সেৱা দেৱা যায়।
- c) ফিক্সেলি ব্যাট লাইসেন্স বা লাইসেন্সবিহীন উভয়ই হতে পাৰে।
- d) প্ৰত্যক্ষ অঞ্চলেৰ সেৱা পাৰে যায়; এমনকি যেখানে কোনোৰ সংযোগ পৌছেনি সেখানেও।
- e) কোয়ালিটি অৰ্পণৰ নিচয়তা দেয়।
- f) তথ্য ও টেলিযোগামো সেবাগৰোপে প্ৰদান কৰা যায়।
- g) অন্যান্য ওয়াইম্যাক্স রিসিভাৰ, যা কোনো কম্পিউটাৰ বা ল্যাপটপে সংযুক্ত থাকে।

ওয়াইম্যাক্স এৰ অসুবিধা (Disadvantages of Wi-Max):

- a) দূৰত্ব বেশি হলে একাধিক বেজ স্টেশনেৰ প্ৰয়োজন হয়।
- b) নেটওয়াৰ্কেৰ অন্যান্য ওয়াৰলেস ডিভাইস সিগন্যালে প্ৰতিবন্ধকতা সৃষ্টি কৰতে পাৰে।
- c) সংহাল এবং রক্ষণাবেক্ষণ খৰচ বেশি।
- d) অনেক ব্যবহাৰকাৰী একই টাওয়াৰ আ্যোৱেস কৰায় সাৰ্ভিসেৰ সঠিক গুণগত মান বাজায় রাখা অনেকক্ষেত্ৰে কঠিন।
- e) অন্যান্য নেটওয়াৰ্ক যৈমন-ফাইবাৰ অপটিক, স্যাটেলাইট, ক্যাবল ইত্যাদিৰ সাথে তুলনা কৰলে ওয়াইম্যাক্স এৰ ডেটা রেট অত্যন্ত দীৰ্ঘাতিৰ।
- f) খাৰাপ আৰহাওয়া যেমন বৃক্ষিৰ কাৰণে এৰ সিগন্যালে বিষ ঘটতে পাৰে।
- g) বেশি বিদ্যুৎক্ষেত্ৰ ব্যবহাৰকাৰী প্ৰযুক্তি বিদূতেৰ সৱৰণাৰ নিচিত কৰতে হবে।

১৯) Bluetooth, ওয়াইফাই ও ওয়াইম্যাক্স এৰ মধ্যে পৰ্যাপ্ত পৰিবেশ (Difference between Bluetooth, Wi-Fi and Wi-Max):

Bluetooth	Wi-Fi	Wi-MAX
Bluetooth এৰ সার্ভাৰ		

২২) একটি URL, IP ঠিকানা এবং DNS কি? এবং, তাৰ কেন ভৱত্পূর্ণ? (What are URL, IP Address and DNS? And why they are important?) [INTRCA- 2010]

URL হল একটি ঘোষণা যা আপনাকে কোনো ওয়েবসাইটে পৌছাতে গ্রাউন্ডে টাইপ করতে হয়। প্রতিটি ওয়েবসাইটের একটি URL থাকে। উদাহরণ বলল: www.google.com, URL টি আপনাকে Google এর ওয়েবসাইটে নিয়ে যাবে।

প্রতিটি URL এবং একটি IP ঠিকানা থাকে। IP ঠিকানা হল একটি নথৰের কুম যা আপনার কম্পিউটারকে আপনি যে তথ্যের খোজ করছেন তা কোথায় পাওয়া যাবে সে সবকে জানায়। IP ঠিকানা একটি ফোন নথৰের মত- প্রক্রিয়াকে একটি লবা, জটিল ফোন নথৰ। IP ঠিকানা গুলি এত জটিল ও মনে রাখা কষ্টসাধ্য হওয়ায়, URL গুলি তৈরি করা হয়েছে। Google এর ওয়েবসাইটে যেতে IP ঠিকানা (45.232.34.253) টাইপ করার পরিবর্তে, আপনাকে তথ্যমাত্র URL টি টাইপ করতে হবে, www.google.com যেহেতু ইন্টারনেটে হচ্ছে পরিমানে ওয়েবসাইট এবং IP ঠিকানা যাবে, তাই আপনার গ্রাউন্ড ব্যক্তিগতভাবে জানাতে পারেন যে এর প্রত্যেকটি কোথায় অবস্থিত। যার কারনে প্রত্যেকটি খুজে দেখতে হয়। যার ফলে DNS (ডেমেন নেইম সিস্টেম) প্রযোজনীয়।

২৩) “অপটিক্যাল ফাইবার ক্যাবলকে নেটওয়ার্কের ব্যাকবোন বলা হয় কেন?” (Why fibre optic cable is called backbone of network?)

কারণ: অপটিক্যাল ফাইবার ক্যাবল হল এক ধরনের আলো পরিষ্কার তাৰ যা এক বা একাধিক অপটিক্যাল ফাইবার সমষ্টিয়ে তৈরি। অপটিক্যাল ফাইবার কাঁচ অথবা প্লাস্টিকের তৈরি এক ধরনের ডাই-ইলেকট্রিক (অন্তরক) পদাৰ্থ দ্বাৰা তৈৰি, যা আলো পরিবহনে সক্ষম। অপটিক্যাল ফাইবার ক্যাবলকে নেটওয়ার্কের ব্যাকবোন বলা হয় কারণ- এই ক্যাবল ইলেক্ট্রিক্যাল সিগনালের পরিবর্তে আলোক বা লাইট সিগনাল ট্রান্সিউট করে। এতে আলোকের পূর্ণ আভ্যন্তরীণ প্রতিফলন পদ্ধতিতে ডেটা উৎস থেকে গত্তব্যে গমন করে। পরিবেশের তাপ-চাপ ইত্যাদি

২৪) ফাইবার অপটিক্যাল ক্যাবল ইএমআই (EMI) মুক্ত কেন? (Why fibre optic cable is free from EMI?)

কারণ: অপটিক্যাল ফাইবার ক্যাবল হল এক ধরনের আলো পরিষ্কার তাৰ যা এক বা একাধিক অপটিক্যাল ফাইবার সমষ্টিয়ে তৈরি। অপটিক্যাল ফাইবার কাঁচ অথবা প্লাস্টিকের তৈরি এক ধরনের ডাই-ইলেকট্রিক (অন্তরক) পদাৰ্থ দ্বাৰা তৈৰি, যা আলো পরিবহনে সক্ষম। এটি ইলেকট্রিক সিগনালের পরিবর্তে আলোক বা লাইট সিগনাল ট্রান্সিউট কৰার ফলে অপটিক্যাল ফাইবার ক্যাবলে কোনো তড়িৎ এর উপস্থিতি নেই। অর্থাৎ অপটিক্যাল ফাইবার ক্যাবলে তড়িৎ এর উপস্থিতি না থাকার কারণে ক্যাবলটি ইএমআই (EMI) মুক্ত।

২৫) কেন ক্ষেত্ৰে Wi-Fi এর পরিবর্তে Wi-Max ব্যবহাৰ কৰা যুক্তিমূল্য-ব্যাধ্যা কৰা। (When Wi-Max is used instead of the Wi-Fi?)

ওয়াইমাই প্রযুক্তিৰ মাধ্যমে উচ্চ গতিৰ ব্রডব্যান্ড সেবা, তাৰিখীয় ব্যবহাৰ বিলৃত এলাকাজুড়ে ইন্টারনেট অ্যাক্সেস কৰাৰ সুযোগ পাবলো যাব। অৰ্থাৎ কভাৱেজ এৰিয়া সাধাৰণত 10 কিমি হৰতে শুধু কৰে 60 কিমি এৰ মধ্যে ইন্টারনেট সেবা প্ৰয়োজন হৈলো। এছাড়া প্ৰত্যুত্ত অৱকলেও উচ্চ গতিৰ ব্রডব্যান্ড সেবা পাওয়াৰ জন্য; এমনকি বেথানে ফোনৰ সহজে পৌছাতে গ্রাউন্ডে টাইপ কৰতে হয়। প্ৰতিটি ওয়েবসাইটেৰ একটি URL থাকে। উদাহৰণ বলল: www.google.com, URL টি আপনাকে Google এৰ ওয়েবসাইটে নিয়ে যাবে।

২৬) Wireless Ad-hoc Network (WANET) (ওজারলেস এডহক নেটওয়াৰ্ক):

একটি ওজারলেস এডহক নেটওয়াৰ্ক (WANET) হচ্ছে একধাৰেৰ লোকাল এৰিয়া নেটওয়াৰ্ক (LAN)। যাব কাৰনে কোনো রকমেৰ সাধাৰণ নেটওয়াৰ্কেৰ অৱকাঠামোৰ সৱজাম ব্যাতীত দুই বা ততোধিক ওজারলেস ডিভাইস তলো একে অপৱেৰ সাথে বিলৃতভাৱে যোগাযোগ হৈলো কৰতে পাৰে। যেমন: ওজারলেস রাউটাৰ বা অ্যারেলেস পয়েন্ট: যদি ওয়াই ফাই এডহক মোডে থাকে, নেটওয়াৰ্কেৰ প্ৰতিটি ডিভাইস এহে তাতা ফোৱাযোৰ্ড কৰে যা অন্য ডিভাইসেৰ জন্য, নিজেৰ জন্য নহ। কাৰণ এত হক নেটওয়াৰ্কেৰ মধ্যে থাকা ডিভাইস তলো সাধাৰণত তাৰিখীয় পিয়াৰ টু পিয়াৰ (P2P) নেটওয়াৰ্কেৰ আওতায় থাকে বলে একে অন্যেৰ রিসোৱ সৱাসৱি আ্যোৱেস কৰতে পাৰে। তাই এৱকম কাজ (যেমন: ফাইল শেয়াৰি, পিস্টিং ইত্যাদি) এৰ ক্ষেত্ৰে কেন্দ্ৰীয় সাৰ্ভাৰ অপ্রযোজনীয়। মৃত একটি এডহক নেটওয়াৰ্কেৰ ক্ষেত্ৰে কততলো ডিভাইসেৰ সংঘৰ বা নেটওয়াৰ্কেৰ কেন্দ্ৰীয় সাৰ্ভাৰ অপ্রযোজনীয়। এই জন্য দায়ী।

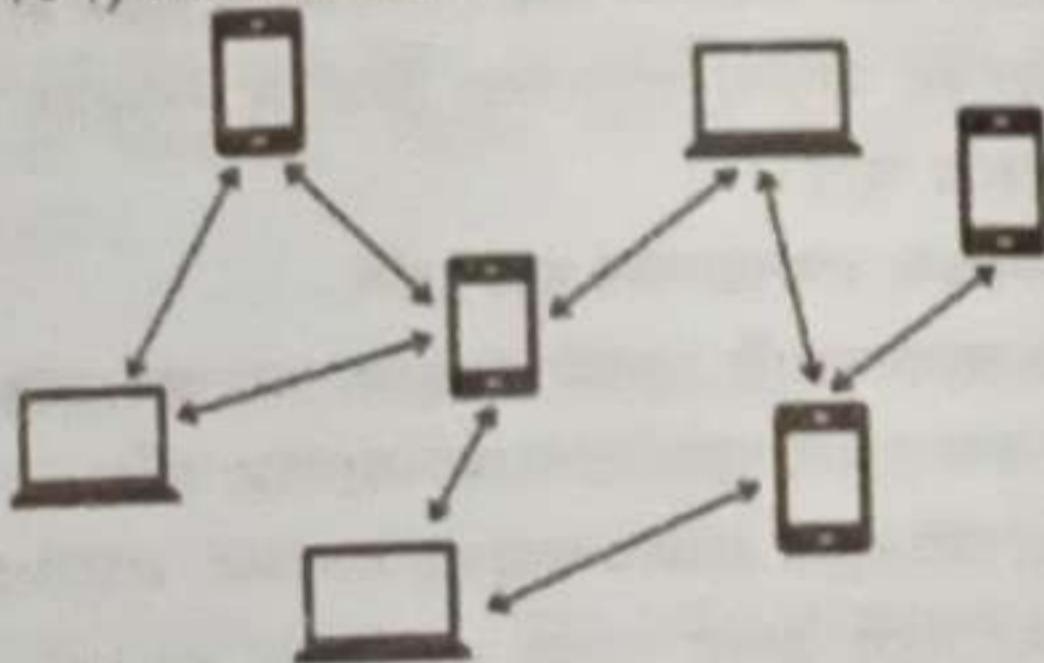


Figure: Wireless Ad-hoc Network (WANET)

২৭) Proxy Server (প্ৰিজি সাৰ্ভাৰ): Proxy হচ্ছে এক ধৰনেৰ কম্পিউটাৰ নেটওয়াৰ্ক যা User কে ইন্টারনেটেৰ সাথে পোৰাক্তভাৱে চূক কৰে দেয়। আৰ যাবা এই ধৰনেৰ সেবা দিয়ে থাকে, তাৰা হচ্ছে Proxy Server. অৰ্থাৎ User ও কম্পিউটাৰ Web এৰ মাবে অবহান কৰে Server. Proxy Server মাবে অবহানেৰ ফলে User ও কম্পিউটাৰ মাবে সৱাসৱি কোনো কানেকশন থাকে না। তাই এই সাইটেৰ মাবে সৱাসৱি কোনো কানেকশন থাকে না। আৰ User এৰ প্ৰস্তুত তথ্য গোপন থাকে। সহজ ভাবায় Proxy server এৰ মাধ্যমে ইন্টারনেট ব্যবহাৰকাৰীৰা নিজেদেৰ তথ্য গোপন রেখে ইন্টারনেট ব্রাউজ কৰতে পাৰে।

২৮) IEEE 802: IEEE 802 (আইইইই ৮০২) এৰ পূৰ্বৰূপ হচ্ছে Institute of Electrical and Electronics Engineers। ইয়ে প্ৰতিষ্ঠিত হয়: পহেলা জানুৱাৰি, ১৯৯২ সালে। প্ৰতিষ্ঠাতা হচ্ছে American Institute of Electrical Engineers, Institute of Radio Engineers নামেৰ একটা গুৰু। ইহাৰ প্ৰধান কাৰ্যালয় হেডকোৰ্টাৰ্স হচ্ছে: Piscataway, New Jersey, United States. ইহাৰ বৰ্তমান এক্সিকিউটিভস হচ্ছেন: Dr. Chanakya Kumar Jha, Dr. D. Devaraj. বৰ্তমানে এৰ সদস্য সংখ্যা ৮১৯,০০০ এৰ বেশি।

IEEE 802 (আইইইই ৮০২) লোকাল এৰিয়া নেটওয়াৰ্ক(ল্যান), পাৰসোনাল এৰিয়া নেটওয়াৰ্ক(প্যান), এবং মেটাপোলিটন এৰিয়া নেটওয়াৰ্ক(ম্যান) এৰ স্টাৰ্টাৰ্ড হিসেবে ব্যবহৃত হয়। আইইইই ৮০২ (IEEE 802) LAN/MAN Standards Committee (LMSC) এই স্টাৰ্টাৰ্ডকে মেইন্টেইন কৰে থাকে। IEEE 802 স্টাৰ্টাৰ্ডস ক্ষায়িলিতে মোট ১২ সদস্য রয়েছে, যাৰ সংখ্যা 802.1 থেকে 802.12, প্ৰত্যোকেৰ জন্য LMSC এৰ একটি নিবেদিত (Focus) Group রয়েছে।

২৯-১) Computer Network কাকে বলে? (What is Computer Network?) [ICT Ministry-11, BKKB-17, DIP-14, NTRCA-2014]

উত্তৰ: Hardware & Software এৰ বিসেৱাৰ সমূহ শোৱ কৰাৰ লকে একাধিক কম্পিউটাৰ কে নিয়ে গড়ে উঠা System কে Computer Network বলে।

২৯-২) Computer network এৰ প্ৰকাৰতেস লিখ? (Write down the classification of Computer Network.) [DIP-14 NTRCA-2014]

উত্তৰ: বিভিন্ন দিক বিবেচনা কৰে কম্পিউটাৰ নেটওয়াৰ্কেৰ শ্ৰেণীবিভাগ বা প্ৰকাৰতেস কৰা হয়। যেমন:

a) মালিকানাৰ উপৰ ভিত্তি কৰে ২ প্ৰকাৰ। যথা:

- i. Private ii. Public

b) উপোলজিৰ উপৰ ভিত্তি কৰে ৬ প্ৰকাৰ। যথা:

- i. Star ii. Ring iii. Bus

iv. Mesh v. Hybrid vi. Tree

c) কাৰ্যালয়ীৰ বৈশিষ্ট্যৰ উপৰ ভিত্তি কৰে ২ প্ৰকাৰ। যথা:

- i. Peer to Peer ii. Client Server

d) কাৰ্যালয়ীৰ পৰিধিৰ উপৰ ভিত্তি কৰে ৬ প্ৰকাৰ। যথা:

- i. LAN ii. MAN iii. WAN

iv. PAN v. WLAN vi. SAN

e) সুইচিং কৌশলৰ উপৰ ভিত্তি কৰে ৩ প্ৰকাৰ। যথা:

- i. Circuit Switched network

ii. Message Switched network

iii. Packet Switched network

f) নিৰ্মান কৌশলৰ উপৰ ভিত্তি কৰে ২ প্ৰকাৰ। যথা:

- i. Point to point ii. Broad cast/ Multipoint

২৯-৩) কম্পিউটাৰ নেটওয়াৰ্ক এৰ বৈশিষ্ট্য লিখ? (Write down the characteristics of Computer Networks.)

উত্তৰ: কম্পিউটাৰ নেটওয়াৰ্ক এৰ বৈশিষ্ট্য নিম্নে দেওয়া হলো:

i. Resource Sharing

ii. Performance (কৰ্মক্ষমতা)

iii. Reliability (নিৰ্ভৰণোপ্তা)

iv. Scalability (মাপযোগ্যতা)

v. Security (নিৰাপত্তা)

২৯-৪) কম্পিউটাৰ নেটওয়াৰ্ক আমোৰ কেন ব্যবহাৰ কৰাৰো / সুবিধা / প্ৰযোজনীয়তা লিখ? ? (Why we use Computer Network? or Write advantages/Neceessity of Computer Networks.) [Ministry of Health-14]

উত্তৰ: কম্পিউটাৰ নেটওয়াৰ্ক ব্যবহাৰ কৰাৰ কাৰণ/সুবিধা/প্ৰযোজনীয়তা তলো হলো:

(i) হার্ডওয়াৰ ও সফটওয়াৰ Share কৰাৰ জন্য।

(ii) Communication সহজে কৰাৰ জন্য।

(iii) Faster communication (ছুক্ত যোগাযোগ এৰ জন্য।)

(iv) Security (নিৰাপত্তাৰ জন্য।)

(

- (vi) Timeless (নিরবিন্দু কাজ করার জন্য।)
- (vii) Costless (বেশ কমানোর জন্য।)
- (viii) সূচ সূচকে সহজে অ্যাপ্লিকেশন এর জন্য।
- (ix) Network resource sharing
- (x) Data base sharing
- (xi) Centralized management (কেন্দ্রীয়ভাবে ব্যবহার করার জন্য।)
- (xii) Access to more than one operating system
- (xiii) Reliability (নির্ভয়েগতা জন্য।)
- (xiv) Increase system performance. (সিস্টেমের কার্যক্রম বৃদ্ধির জন্য।)

প্রশ্ন-৫) কম্পিউটার নেটওর্ক Element এর কোন কি কি? (What are the Elements of Computer Networks?)

উত্তর: কম্পিউটার নেটওর্ক element কোন হলো:

- Hardware
- Software
- Protocol

প্রশ্ন-৬) Computer Network এর ব্যবহার কেবল বা বিষ্ণু কিমুন।

উত্তর: Computer Network এর ব্যবহার কেবল বা বিষ্ণু কিমুন।

- Video Conference
- Email
- Educaiton
- Entertainment
- Business
- Resource
- Arts
- Information Technology
- Electronic Boolean Board
- Security
- Service

প্রশ্ন-৭) LAN, MAN & WAN কি? এর সূবিধা ও অসুবিধা লিখ ? Or LAN, MAN এবং WAN এর মধ্যে তুলনা কর। (What is LAN, MAN and WAN? Differentiate of each other.) [BPSC-14, Bangladesh Bank, ICT Ministry, NTRCA-2010, 2012]

উত্তর: LAN: LAN এর পূর্ণরূপ হল Local Area Network, যা নিকট সূচতের কম্পিউটার সমূহকে প্রস্তরে সাথে সংযুক্ত করার ব্যবহা করে। সাধারণত ১ থেকে 10 কি.মি. বা তার কম পরিসরের জায়গার মধ্যে প্রযোজনীয় স্থানে কম্পিউটার বা অল্যাকোনো পেরিফেরিয়ল ডিভাইস (হেডেন- প্রিন্টার) সংযুক্ত করে যে নেটওর্ক তৈরি করা হয় তাকে LAN বলে। বর্তমানে স্থানের মধ্যে 10Mbps থেকে 1000Mbps গতিবেগে তথ্য আদান-প্রদান করা যায়।

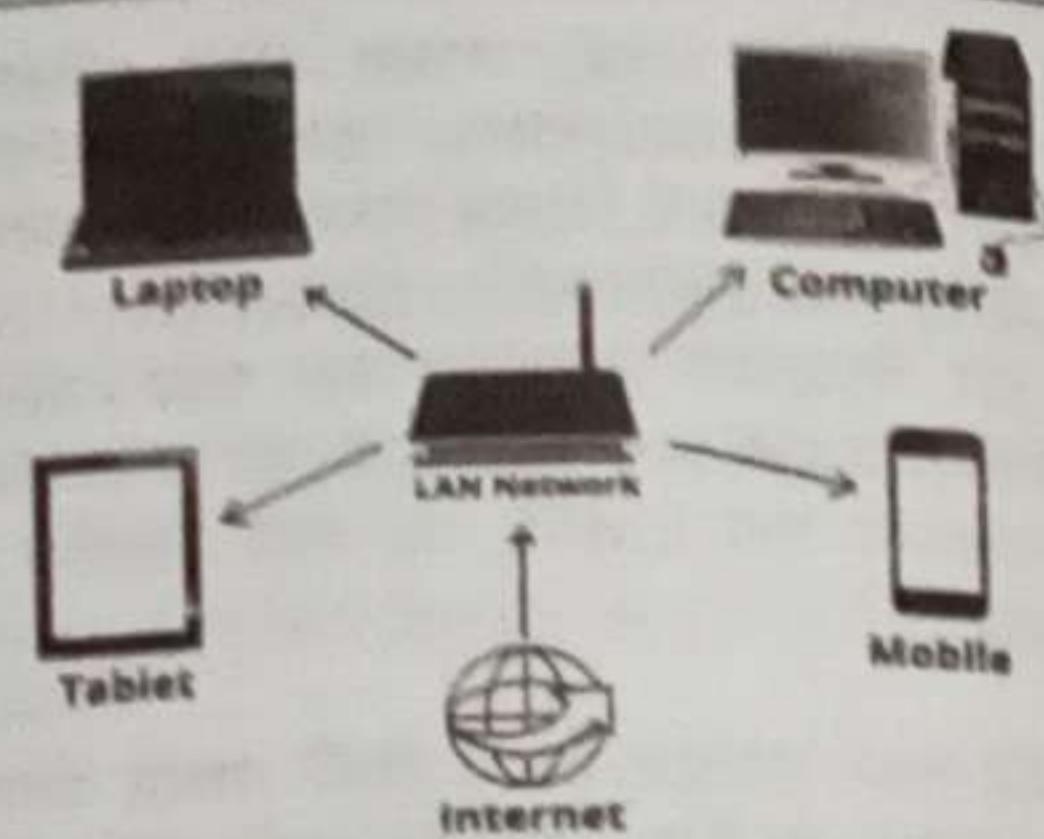


Figure: Local Area Network

LAN এর সূবিধা:

- Resource Sharing
- Software Applications Sharing
- Easy and Cheap Communication
- Centralized Data
- Data Security
- Internet Sharing
- Information sharing,
- Network Access

LAN এর অসুবিধা:

- High Setup Cost
- Privacy Violations
- Data Security Threat
- LAN Maintenance Job
- Covers Limited Area

MAN: MAN এর পূর্ণরূপ হল Metropolitan Area Network, যা দুই বা ততোধিক LAN এর সমরয়ে গঠিত। MAN এর Component হিসাবে Router, Switch, Hub, NIC Card, Cable, MODEM ইত্যাদি ব্যবহৃত হয়।

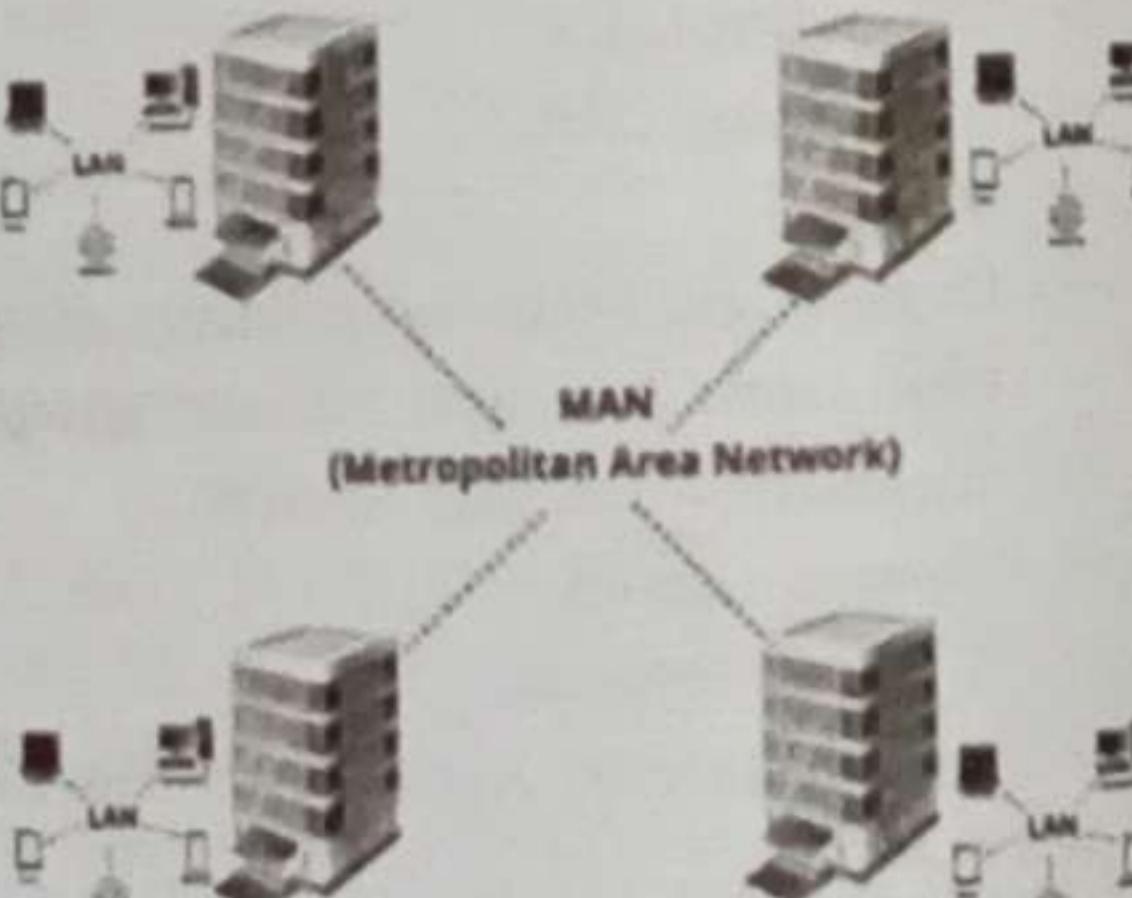


Figure: Metropolitan Area Network

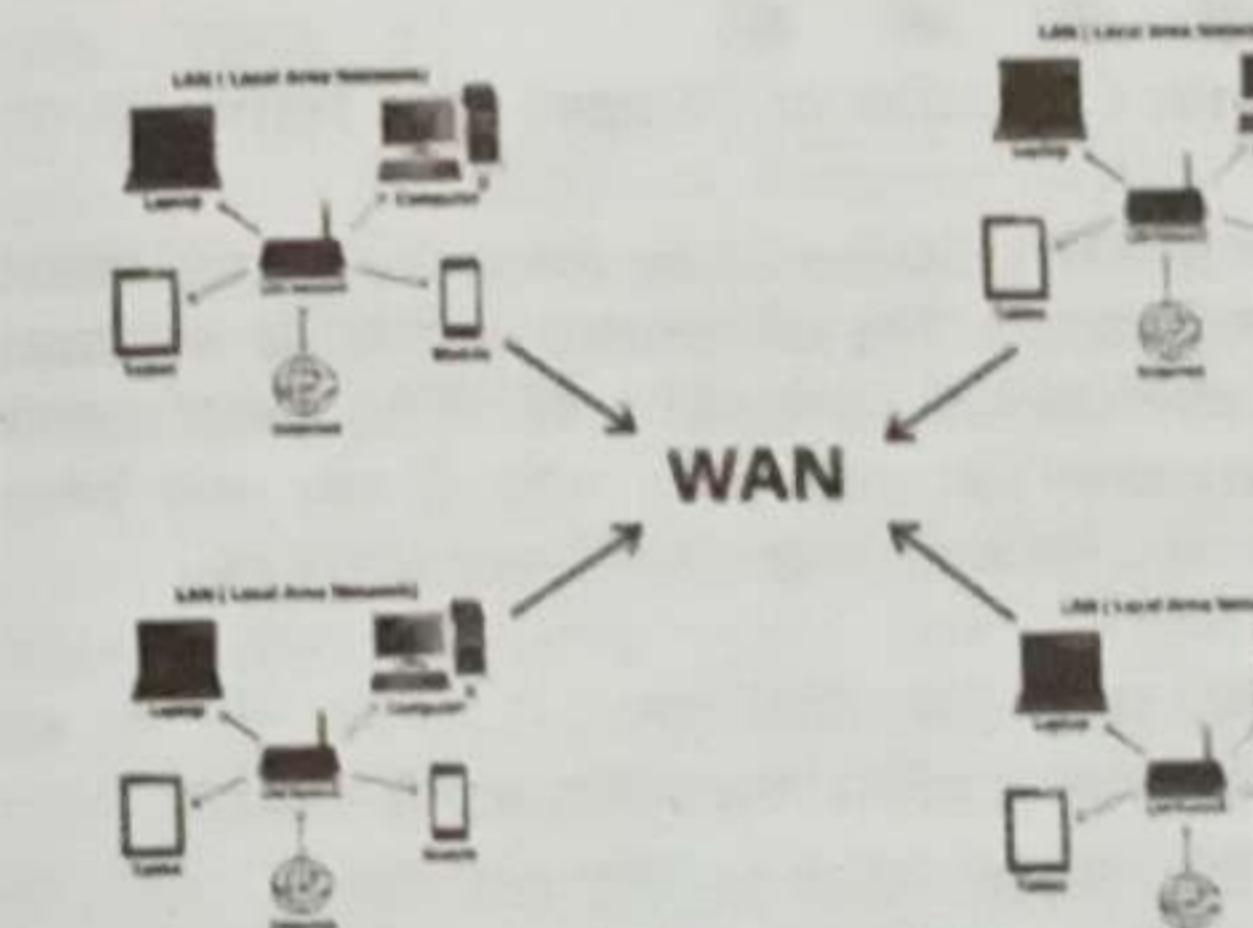
MAN এর সূবিধা:

- Less expensive
- Sending local emails
- High speed than WAN
- Sharing of the internet
- Conversion from LAN to MAN is easy
- High Security

MAN এর অসুবিধা:

- Difficult to manage
- Internet speed difference
- Hackers attack
- Technical people required to setup
- More wires required

WAN: WAN এর পূর্ণরূপ হল Wide Area Network যা একটি বৃহৎ জোগালিক সূচত / ছান অতিক্রম করে এবং ওয়াইফি এবিএল নেটওর্কগুলির মধ্যে টেলিযোগাযোগ ব্যবহা প্রতিষ্ঠিতা করে। Long distance Communication এর জন্য একাধিক MAN যুক্ত করে WAN গঠন করা হয়।



Collection of LANs = WAN

Figure: Wide Area Network

WAN এর সূবিধা:

- Covers large geographical area
- Centralized data
- A lot of application to exchange messages
- Sharing of software and resources
- Global business
- High bandwidth
- Distribute workload and decrease travel charges

WAN এর অসুবিধা:

- Security problems
- Needs firewall and antivirus software
- The setup cost is high
- Troubleshooting problems
- Server down and disconnection issue

প্রশ্ন-৮) LAN, MAN & WAN এর বৈশিষ্ট্য লিখ, উদাহরণ সহ। (Mention the Characteristics of LAN, MAN and WAN with example.)

উত্তর: LAN এর বৈশিষ্ট্য:

- টেটওয়ার্কে সহজে কম্পিউটার সমূহ সংযোগ করা যায়।
- বর্তমানে এর মাধ্যমে সেকেতে সর্বোচ্চ ১ জিবি পর্যন্ত গতিতে তথ্য আদান-প্রদান করা যায়। তবে সাধারণ গতি 10-100 Mbps পর্যন্ত হয়।
- বিপিন্টার, হাব, সেটওয়ার্ক ইন্টারফেস কার্ড ব্যবহার করে সেটওয়ার্কের কার্যক্রমতা বাঢ়ানো যায়।
- ছোট এলাকার মধ্যে এই সেটওয়ার্ক সহজেই তৈরি করা যায়।
- এ সেটওয়ার্কে কম্পিউটারসমূহ তার বা তারবিহীন সংযোগ প্রদান করা যায়।
- নেটওয়ার্ক হ্যাপন, রুটিগুলিকে ব্যবহার করা যায়।
- সীমিত দূরত্বের মধ্যে এর কার্যক্রম সীমাবদ্ধ।
- Data transfer rate high।
- অল্প খরচে ডাটা ট্রান্সিউট করা যায়।
- মিডিয়া হিসেবে Co-axial Cable, (জোড়া পাকানো তার) ও অপটিকক্যাল ফাইবার ব্যবহৃত হয়।

LAN এর উদাহরণ:

- Ethernet→Developed by Xerox Corporation.
- Omninet→Developed by Corvus system.
- Wi-Fi→Developed by Wifi alliance
- Apple talk→Developed by Apple GC

MAN এর বৈশিষ্ট্য:

- একাধিক LAN কে একত্রিত করে MAN গঠিত হয়।
- LAN এর তুলনায় গতি কম, তুলের হার অধিক, সময় বিলম্ব অধিক।
- এর বিস্তৃতি ১০-৩০ কিলোমিটার পর্যন্ত হতে পারে।
- Image, Compressed video transmission & PABX ও LAN সংযোগে MAN গঠিত হয়।
- ল্যানের চাইতে দ্রুত গতির ও খরচ কম।
- বেশি পরিমাণ তথ্য আদান-প্রদান করা যায়।
- এর মালিকানা সাধারণত কোন অর্গানাইজেশনের হয়ে থাকে।
- এটি সর্বাধিক ৫০ কিলোমিটার শহর জুড়ে বিস্তৃত।
- বেশিরভাগ ব্যবহৃত মাধ্যমটি অপটিকাল ফাইবার ক্যাবল হয়ে থাকে।

WAN এর বৈশিষ্ট্য:

- সংযোগ মাধ্যম হিসাবে Telephone line, Microwave বা Satellite Link ব্যবহৃত হয়।
- কয়েক কিমি হতে তরু করে কয়েক হাজার কি.মি পর্যন্ত বিস্তৃত হতে পারে।
- Data transfer speed LAN ও MAN এর তুলনায় কম।
- ক্লাউড কম্পিউটিং সুবিধা প্রাপ্ত যায়।

- c) বিভিন্ন তথ্য, প্রে-প্রিকা, বই, চলচ্চিত্র প্রভৃতি সংযোগ ও ব্যবহার করা যায়।
- f) ব্যক্তিগত বা সমাচারগত তাবে বুলেটিন বোর্ড গঠন করা যায়।
- g) অর্থ ধরচে পৃষ্ঠার যে কোনো হালে ভয়েজ ও ভিডিও যোগাযোগ করা যায়।

WAN এর উদাহরণ:

- a) ARPANET → Developed by Advanced Research Agency Network.
- b) INDOWET - Developed by computer Maintenance Corporation of India.
- c) Satenet-Satellite Network

প্রশ্ন-৯) প্যান (PAN) কাকে বলো? ইহার সুবিধা বা বৈশিষ্ট্য কোনো লিখুন। (What is PAN? Write down the characteristic and advantages of it's.)

উত্তর: প্যান (PAN) এর পূর্ণরূপ হচ্ছে Personal Area Network. কোনো ব্যক্তির নিকটবর্তী বিভিন্ন ডিভাইসের মধ্যে সংযোগ স্থাপন করে তথ্য আদান-প্রদানের নেটওয়ার্ক সিস্টেমকে PAN বলে। এর ব্যাপ্তি সাধারণত ১০ মিটার বা এর ক্ষেত্রে স্থানেই সীমাবদ্ধ থাকে। এই নেটওয়ার্ক তৈরির জন্য ট্রান্সিভিসন মিডিয়া হিসেবে ওয়্যারলেস মিডিয়াম (Wi-Fi, Bluetooth, USB, Fireware Bus... etc) ব্যবহার করা যায়।

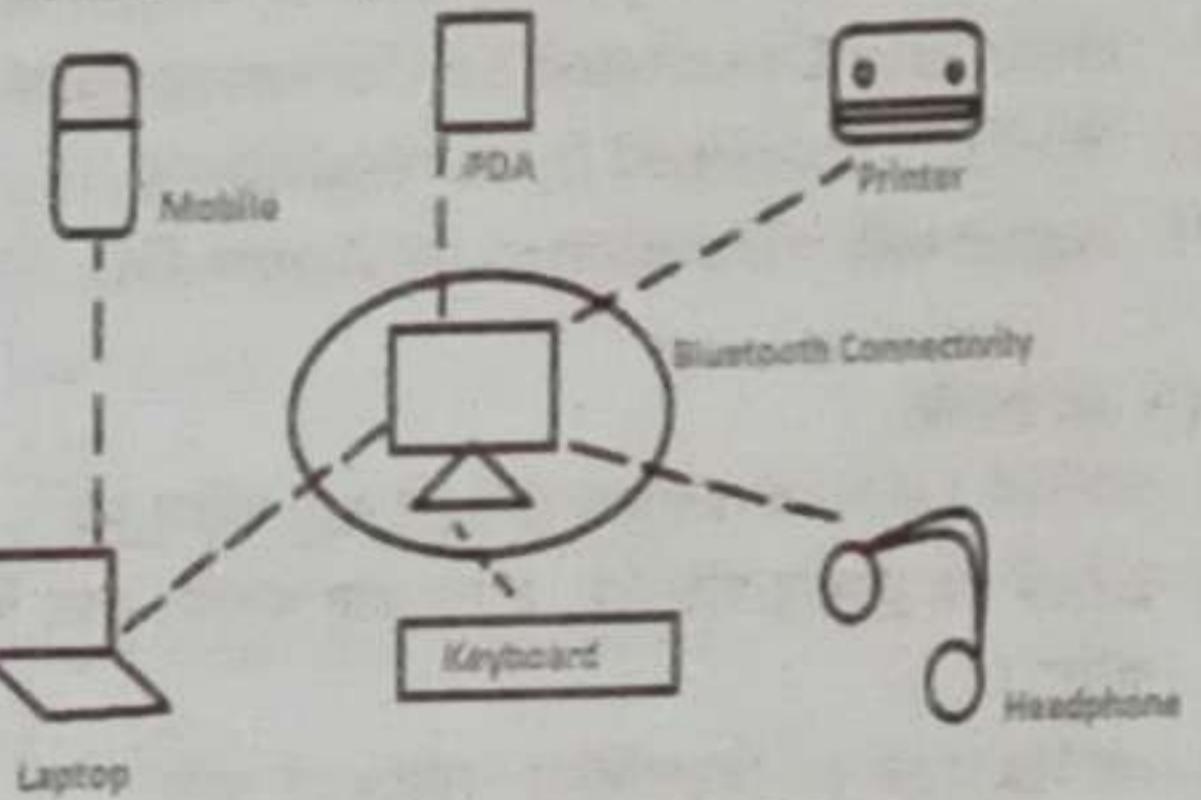


Figure: Personal Area Network

পার্সোনাল এরিয়া নেটওয়ার্কের (প্যান/PAN) বৈশিষ্ট্য ও সুবিধা:

- a) পার্সোনাল কম্পিউটার ডিভাইসসমূহের মধ্যে যোগাযোগের জন্য ব্যবহৃত হয়।
 - b) বাড়িতে বা অফিসে ব্যক্তিগত হোট প্রয়োজনে এ নেটওয়ার্কের জুড়ি নেই।
 - c) ঘরচ কম।
 - d) কম কামেলায় সহজেই যেকোন জায়গায় তৈরি করা যায়।
 - e) নেটওয়ার্ক কম ও সহজলভ নেটওয়ার্ক ব্যবহা।
 - f) এটিবিউশন হারিয়ে ফেলা মেসেজের জন্য ইহার অটোমেটিক রিট্রিভিউশন ব্যবহা আছে।
- প্রশ্ন-১১) LAN এর প্রকারভেদ লিখ? (Write the classification of LAN.)
- উত্তর: LAN দুই প্রকার। যথা:
- (a) Baseband: Transmission এর জন্য digital signal থেকে Analog signal এ পরিবর্তন করাকে Baseband বলে। এই সিস্টেমটি করার জন্য মডেম বা অন্য কিছুর প্রয়োজন হ্যান।
 - Technique:
 - (i) Token Passing Technique
 - (ii) Cambridge ring technique
 - (iii) Ethernet

প্রশ্ন-১০) ক্যান (CAN) কাকে বলো? ইহার সুবিধা বা বৈশিষ্ট্য কোনো লিখুন। (What is CAN? Write down the characteristic and advantages of it's.)

উত্তর: ক্যান (CAN): CAN এর পূর্ণরূপ হচ্ছে Controller or Campus Area Network. আমরা জানি যে ক্যাম্পাস মানে হল শিক্ষাপ্রতিষ্ঠান বা যেকোনো প্রতিষ্ঠানের নিমিট এবিয়া। অর্থাৎ এ নেটওয়ার্ক দুই বা ততোধিক LAN নিয়ে গঠিত হয় কিন্তু একটি মিশ্র কোম্পানিক এলাকায়, যেমন: কলেজ ক্যাম্পাস, ইভাস্ট্রিয়াল Complex অথবা মিলিটারি বাট্টরির মধ্যে সীমাবদ্ধ থাকে, তাকে Controller or Campus এবিয়া নেটওয়ার্ক বলে।

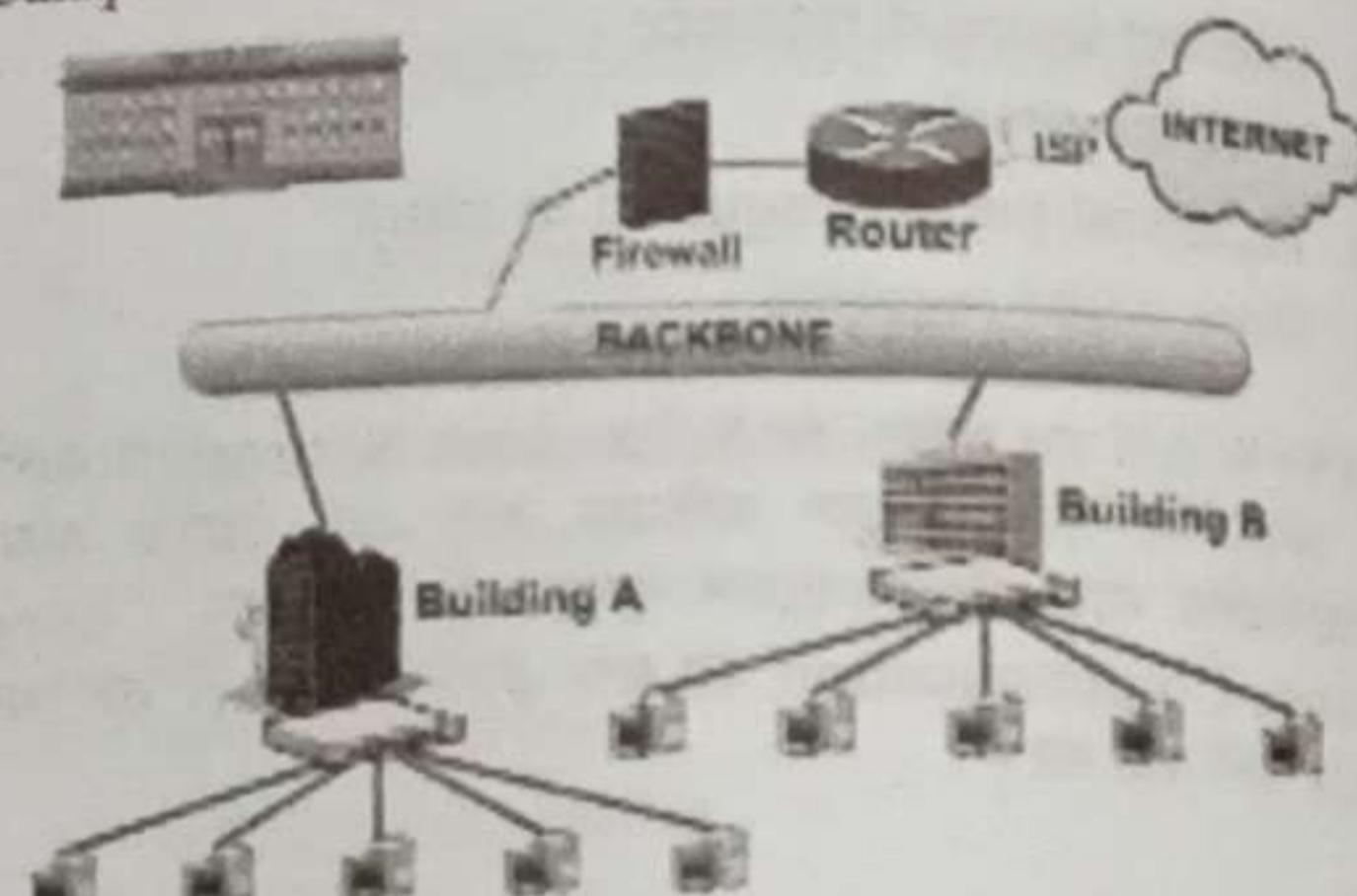


Figure: Controller or Campus Area Network

CAN কে MAN (Metropolitan Area Network) হিসেবে বিবেচনা করা যেতে পারে, কিন্তু এটি সাধারণত একটি সীমিত এলাকাকে গঠিত, যা আদর্শ MAN থেকে ছোট। এটা বিভিন্ন LAN, কেবল কেন্দ্রীয় ফায়ারওয়ার্ক, এবং একটি লিঙ্গ লাইন বা অন্য কোন উপরে ইন্টারনেটের সাথে সংযুক্ত করা থাকে, তাদের সমন্বয়ে তৈরি হয়।

ক্যান (CAN) এর সুবিধা বা বৈশিষ্ট্য কোনো লিখুন।

- a) ইহা মাল্টিকাস্ট ও মাল্টিমাস্টার বৈশিষ্ট্য সাপোর্ট করে।
- b) ক্যান বাস এর দৈর্ঘ্য সর্বোচ্চ ৮০ মিটার হতে পারে।
- c) ডিস্ট্রিবিউটেড নেটওয়ার্কের ক্ষেত্রে ইহার স্টার্টার্ট বাস আছে।
- d) Half Duplex যোগাযোগের জন্য ইহার সিস্টেম সিরিজে উভয়মুখী লাইন আছে।
- e) ইহার খরচ কম ও সহজলভ নেটওয়ার্ক ব্যবহা।
- f) এটিবিউশন হারিয়ে ফেলা মেসেজের জন্য ইহার অটোমেটিক রিট্রিভিউশন ব্যবহা আছে।

প্রশ্ন-১১) LAN এর প্রকারভেদ লিখ? (Write the classification of LAN.)

উত্তর: LAN দুই প্রকার। যথা:

(a) Baseband: Transmission এর জন্য digital signal থেকে Analog signal এ পরিবর্তন করাকে Baseband বলে। এই সিস্টেমটি করার জন্য মডেম বা অন্য কিছুর প্রয়োজন হ্যান।

Technique:

- (i) Token Passing Technique
- (ii) Cambridge ring technique
- (iii) Ethernet

(b) Broadband: Digital Signal কে Analog Signal এ পরিবর্তন না করে একটি Channel এর মধ্য দিয়ে প্রদান করাকে Broadband বলে। যা একাধিক সিগনাল কে Multiplexed করে ট্রান্সিভিট করা যায়।

প্রশ্ন-১২) LAN, MAN এবং WAN এর মধ্যে পার্থক্য কোনো লিখুন। (Write down the difference between LAN, MAN and WAN.)

উত্তর: LAN, MAN এবং WAN এর মধ্যে পার্থক্য কোনো লিখুন।

a) Data Flow এর উপর ভিত্তি করে ২ প্রকার। যথা:

- i) Communication Mode Operation
 - ii) Communication Loss Operation
- b) মালিকানার উপর ভিত্তি করে ২ প্রকার। যথা:
- i) Private Internet ii) Public Internet
 - Private Internet আবার ২ প্রকার। যথা:
 - i) Intranet ii) Extranet

Intranet: একটি প্রতিষ্ঠানের অভ্যন্তরীন যোগাযোগের জন্য ব্যবহৃত হয়। ইহা একটি ছোট Private Network যা সহজেই একে Control করা যায় এবং উপরের নিরাপত্তা ও গোপনীয়তা বজায় রাখা যায়।

Extranet: বিভিন্ন প্রতিষ্ঠানে ছাপিত Internet যুক্ত Computer সমূহ TCP/IP Protocol এর সহায়তায় পরিপন্থ সহ্যুক্ত হয়ে যে দলগত Private network গঠন করে তাকে Extranet বলে।

প্রশ্ন-১৪) Internet এর গঠন উপাদান কোনো লিখ? (Write the structured elements of Internet.)

উত্তর: Internet গঠন এর উপাদান কোনো লিখুন।

- a) Internet backbone (Fiber Optic/Submarine Cable)
- b) Interconnect Point
- c) ISP (Internet Service Provider)
- d) User
- e) Device (PC, Laptop, Mobile etc)

প্রশ্ন-১৫) Internet এর Service সমূহ লিখ? (Mention the services of Internet.)

উত্তর: Internet এর Service সমূহ হলো:

- a) Email Service
- b) Remote Login
- c) World Wide Web (WWW)
- d) Web search Engine
- e) FTP(File Transfer Protocol)
- f) Audio & Video Conferencing
- g) Telnet
- h) Internet Shopping
- i) Inter Ready Chat (IRC)

প্র-১৬) Network Performance কানেক্সনের Controller কি? (Write down the controller of increasing network performance.)

উত্তর: Network Performance কানেক্সনের Controller এর নাম:

- a) ইন্টেল
- b) এটেল
- c) মেডিয়া
- d) পিটেল

প্র-১৭) কিভাবে নেটওর্কের কার্যকরণ (Network Performance) কানেক্সনে বৃদ্ধি করা যায় (How to increase the performance newtork?)

উত্তর: নিচের উপর দিয়ে কোন কানেক্সনের কার্যকরণ কানেক্সনে বৃদ্ধি করা যায়। যেমন:

- a) Determine that your network is at fault
- b) Determine network topology
- c) Track and set baselines
- d) Quality of service and packet shaping
- e) Protocol acceleration
- f) Optimize network traffic flow
- g) Optimize WAN
- h) Shape your network traffic
- i) Use load balancing to distribute traffic
- j) Time improvements properly
- k) Offer guests a different network
- l) Limit personal bandwidth usage
- m) Use cloud services strategically
- n) Check for viruses or system defects
- o) Monitor for bottlenecks
- p) Update software and firmware

প্র-১৮) ইন্টারনেট এবং ইন্ট্রানেট এর মধ্যে পার্থক্য কি? (Write the difference between Internet and Intranet.)

উত্তর: নিচে ইন্টারনেট এবং ইন্ট্রানেট এর মধ্যে পার্থক্য লিখো হলো:

ইন্টারনেট	ইন্ট্রানেট
Internet হচ্ছে Interconnect Network, যা User, data, Tele communication কানেক্সন এবং PC এর সময়ে গতি এবং কন্ট্রোল করা যাবে এবং উপরের নিরাপত্তা ও সুরক্ষার কানেক্সনে সাথে বিশ্বে তার অদ্বান করা যাবে।	একটি প্রতিবাসীন অভিজ্ঞান যোগাযোগের জন্য ব্যবহৃত হয়। ইয়ে একটি ছোট Private network যা সহজেই একে Control করা যাবে এবং উপরের নিরাপত্তা ও সুরক্ষার কানেক্সনে সাথে বিশ্বে তার অদ্বান করা যাবে।
যে কোটি ব্যবহার করতে পারে।	নিমিট আজেন্সেগো ব্যবহারকারী ব্যবহার করতে পারে।
ত্বরিত অধিক	ত্বরিত কম
প্রারম্ভিক নেটওর্ক	আইডেন্ট নেটওর্ক
ইন্ট্রানেটের ক্লাউড কর নিরাপত্তা	নিরাপত্তা

প্র-১৯) ISDN কি? (What is ISDN?)

উত্তর: ISDN: ISDN হচ্ছে Integrated Service Digital Network এর সংক্ষিপ্ত রূপ। এটি একটি Digital Communication প্রক্রিয়া যা একই জানলের মধ্যে Digital Transmission, Voice & Digital Data Communication ইত্যাদি সুবিধা প্রদান করে।

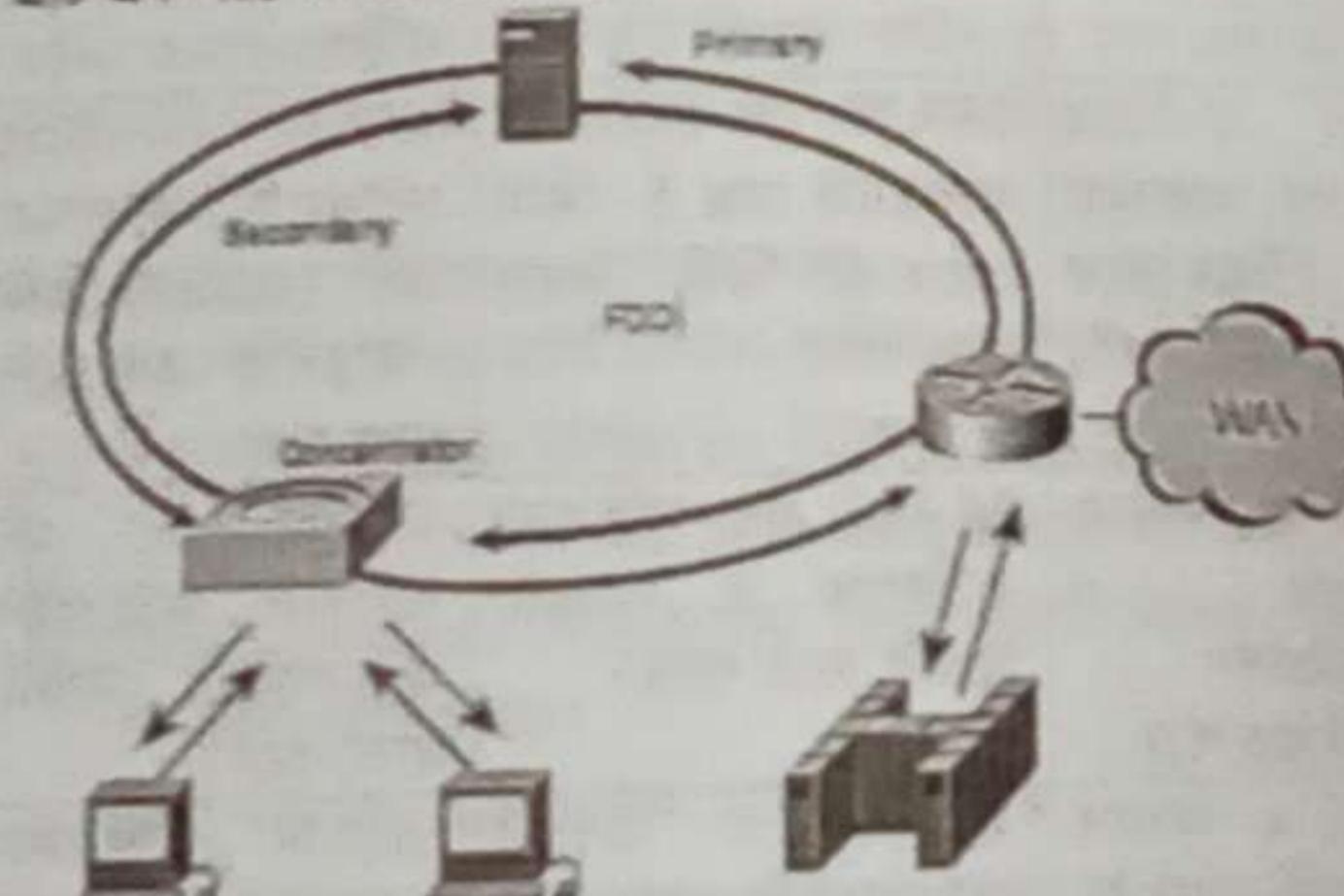
প্র-২০) দিয়ে দাইবিটি আকসেস LAN এর বৈশিষ্ট্য কি? (Write the charaectaristics of Demand priority access LAN.)

উত্তর: দিয়ে দাইবিটি আকসেস LAN (Demand Priority Access LAN) এর বৈশিষ্ট্য:

- a) এটি স্ট্রাইক
- b) এব এর মাধ্যমে ট্রান্সিশন করে।
- c) জন জোড়া তার ব্যবহৃত হয়।
- d) এটি ইন্টারনেট ও ট্রোকেন বিং উভয় প্যাকেট স্পোর্ট করে।
- e) এটি ব্যবহার করে দুইটি দাইবিটি সেক্সেলের জন্য অন্তর্ভুক্ত হয়।

প্র-২১) FDDI কি? এর সুবিধা ও অসুবিধা লিখো? (What is FDDI? Mention its Advantages and Disadvantadges.)

উত্তর: FDDI হচ্ছে Fiber Distributed Data Interface এর সংক্ষিপ্ত রূপ। FDDI হচ্ছে একবর্ণের নেটওর্ক স্টার্টার্ট, যা নিরাপত্তা এবং নেটওর্কের মধ্যে ফাইবার অপ্টিক সংযোগ ব্যবহার করে এবং ইয়ে 200 বিলিমিটার (128 মাইল) পর্যন্ত দূরত্ব বৃদ্ধি করতে পারে। এটি এক বর্ণের বিং ডিজিটিক নেটওর্ক।



FDDI এর সুবিধা সমূহ:

- a) এব এর পরিবর্তে কনসেন্ট্রেটর নামক ডিভাইস ব্যবহার হয়।
- b) অসামাজিক গতির এবং নির্ভরযোগ্য নেটওর্ক।
- c) সর্বোচ্চ নিরাপত্তা প্রদান করতে পারে।
- d) 250 মিলিসেকেন্ড পর্যন্ত ব্যাটেলেটাইভ অফার করতে পারে।
- e) 100 মেগাবিটস এর ডাটা রেইট ব্যাটেল করতে পারে।
- f) নেটওর্কের গতি বৃদ্ধির জন্য মাল্টিপল ট্রোকেন ব্যবহার করে।
- g) একই সাথে বেশ কয়েকটি FDDI ডিভাইস ডাটা ট্রান্সিশন করা পারে।

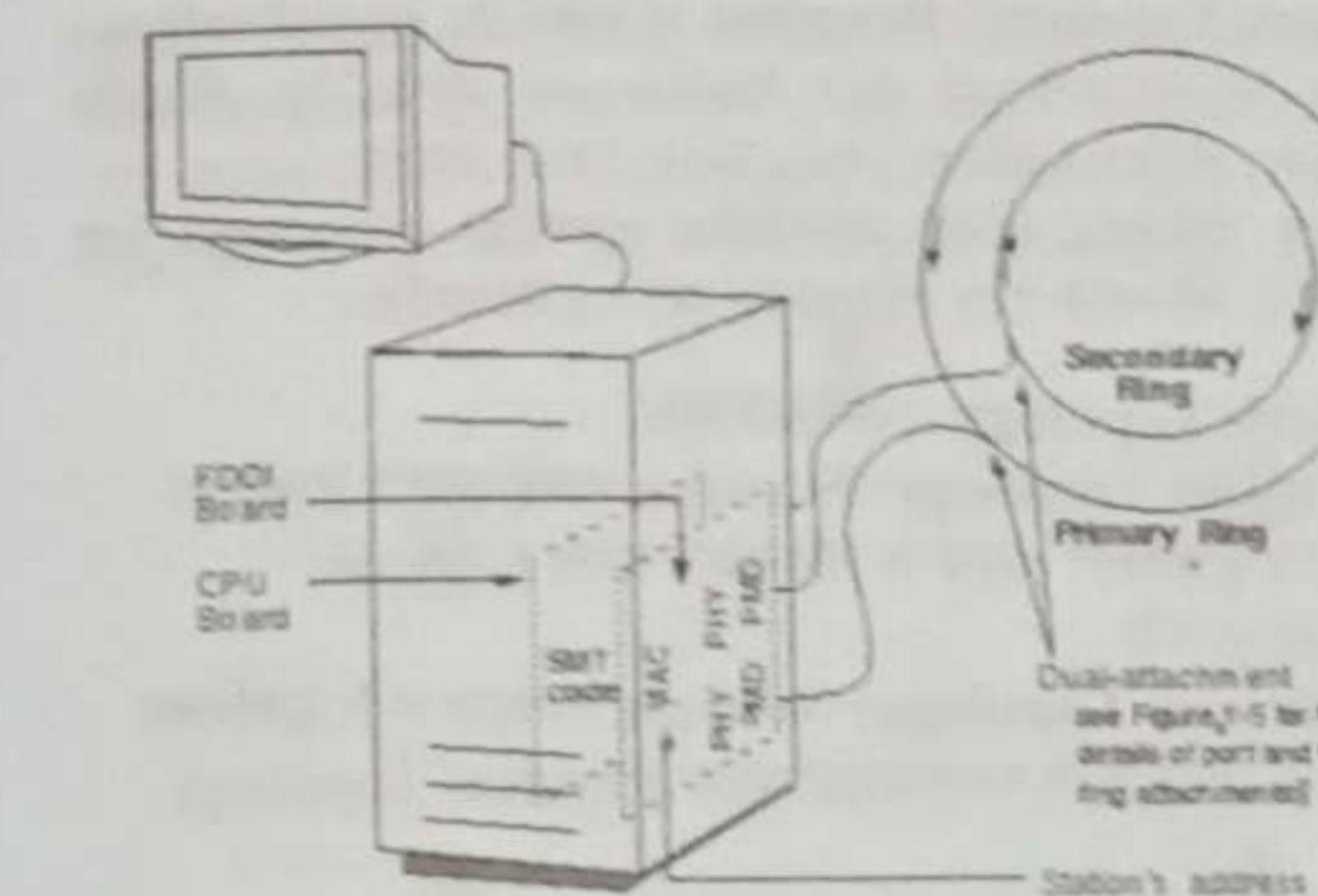
h) ফাইবার অপ্টিক ক্যাবল এর কারণে সহজে ভাসে না, যদিও অন্যান্য কেবল সহজে ভেঙে যায়।

FDDI এর অসুবিধা সমূহ:

- a) FDDI হচ্ছে কঠিন। যার কারণে ইন্সটলেশন ও মেইটেনেন্স এবং জন্য প্রচুর সময় ব্যবহারের প্রয়োজন হয়।
- b) FDDI এ Fiber Optical Cable ব্যবহৃত হয়। তাই এটি ব্যবহৃত হয়।
- c) সকলের মাল্টিপল বিং ফেইল ইওয়ার সঞ্চাবনা থাকে এবং বিং ব্যক্তি ইওয়ার সাথে সাথে সেই সঞ্চাবনা বৃদ্ধি পায়।

প্র-২২) FDDI উপাদান সমূহের নাম লিখো? (Write the elements of FDDI.)

উত্তর: FDDI এর Components/Elements এর নাম নিম্নে দেয়া হল:



প্র-২৩) Physical Layer Medium Dependent Sublayer (PMD)

প্র-২৪) Physical Layer Protocol Sublayer (PHY)

প্র-২৫) Media Access Control Sublayer (MAC)

প্র-২৬) Station Management Module (SMT)

প্র-২৭) Concentrator

প্র-২৮) Optical fiber (Primary এবং Secondary)

প্র-২৯) Converter

প্র-৩০) FDDI NIC card.

প্র-৩১) কনসেন্ট্রেটর কি? (What is concentrator?)

উত্তর: এটি একটি ডিভাইস। FDDI এ কোন হাব ব্যবহার হয় না। তার পরিবর্তে এই ডিভাইস ব্যবহার হয়।

প্র-৩২) বিভিন্ন ধরনের Communication Network এর নাম লিখো? (Write the different types of communication.)

উত্তর: বিভিন্ন ধরনের Communication network এর নাম:

- a) Radio Communication network
- b) Television Communication network
- c) Telephone Communication network
- d) Telegraph communication network

GPON ক্রত্যাক প্যাসিভ অপটিক্যাল আক্রেসের মতুন প্রজন্মের জন্য ITU-TG984 স্ট্যার্ড ভিত্তির GPON 2.5 ফিলারাইট/এস অঙ্গনীয় উচ্চ ব্যাডটাইথ ডাউনলিঙ্ক Rate সরবরাহ করে, Asymmetric বেশিটাইলি ক্রত্যাক ডেটা পরিষেবাদি বাজারে আরও EPON এর মাঝিমাম আউটপুট Optical পাওয়ার -28.00 dBm Optical পাওয়ার -32.00 dBm EPON এর Cost Lower EPON এর Cost Higher EPON এর জনপ্রিয় এরিয়া হচ্ছে: জনপ্রিয় এরিয়া হচ্ছে এশিয়া ও ইউরোপ।

এখনে, OLT: Optical Line Terminal
ONU: Optical Network Unit
ONT: Optical Network Terminal

Network Topology

প্রশ্ন-১) Network Topology কাকে বলে ? Network Topology এর প্রকারভেদ লিখ এবং বর্ণনা কর। (What is Network Topology? Describes it with its classification.) [SB & JB (IT/ICT)-18, ICT Ministry-11, BPSC-14, অঙ্গনীয় কার্যালয় -১০, NTRCA-2010, 2013, 2014, 2017, 2018]
উত্তর: যে পক্ষতিতে প্রতিটি কম্পিউটার প্রস্তুতের সাথে সংযুক্ত আছে তাতে প্রতিটি কম্পিউটার প্রস্তুতের সাথে সংযুক্ত করে। PONs এর চাইতে ইহা দ্রুত ইথারনেট ব্যবহার করা যাবার করে।

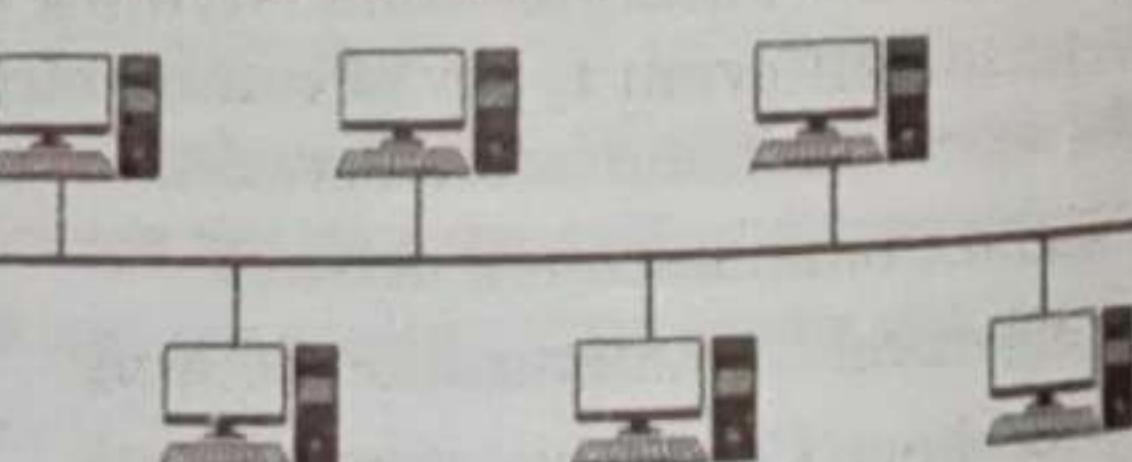
অপরদিকে EPON হল ডেটা, ভয়েস এবং ভিডিও পরিষেবা আক্রেস করার জন্য একটি একক ফাইবার-অপটিক আক্রেস সিস্টেমের মাধ্যমে একটি উন্নীয়মান ক্রত্যাক আক্রেস প্রযুক্তি। EPON GPON এর প্রতিশ্রুতি, যা এটিএম কোরের পরিষেবার ইথারনেট প্যাকেট ব্যবহার করে। EPON প্রতি সেকেতে ১ সিগালিট অপসিন্স্র এবং ডাউন স্ট্রিম রেট ব্যবহার করে। PONs এর চাইতে ইহা দ্রুত ইথারনেট ব্যবহার করা যাবার করে। FTTB বা FTTH অর্কিটেকচারের মধ্যে মাস্টিপোর্টেকে নির্দেশ করে। যেখানে একটি অপটিক্যাল ফাইবার একাধিক প্রাসে বা ব্যবহারকারীকে সার্ভিস দিতে ব্যবহৃত হয়।

প্রশ্ন-২) অপটিক্যাল ফাইবারের নেটওয়ার্কের ক্ষেত্রে EPON এবং GPON এর পার্থক্য ক্যাহ্য করুন? (What is the difference between EPON and GPON in optical fibre networks?) [NTRCA-2017]

উত্তর: অপটিক্যাল ফাইবারের নেটওয়ার্কের ক্ষেত্রে EPON এবং GPON এর পার্থক্য:

EPON	GPON
EPON হচ্ছে Ethernet Passive Optical Network এর সংক্ষিপ্ত রূপ।	GPON হচ্ছে Gigabit Passive Optical Network এর সংক্ষিপ্ত রূপ।
EPON IEEE 802.3h স্ট্যার্ডে তৈরি।	GPON ITUT G.984.1/2/3/4 স্ট্যার্ডে তৈরি।
EPON এর ডাউনলাইন হার হচ্ছে 1250 Mbit/s	GPON এর ডাউনলাইন হার হচ্ছে 1244/2488 Mbit/s
Products used- OLT- ONU	Products used- OLT-ONT
EPON এর লাইন কোডিং হচ্ছে 8B/10B	GPON এর লাইন কোডিং হচ্ছে NRZ(Non Return to Zero)
EPON এর গতি হার হচ্ছে 1.25G/1.25G	GPON এর গতি হার হচ্ছে 2.488G/1.244G
EPON এইথারনেট ব্যবহার হয় বিভাগীয় নেটওয়ার্ক হিসেবে।	GPON এ ATM,Ethernet, TDM ব্যবহার হয় বিভাগীয় নেটওয়ার্ক হিসেবে।
Customer attached: 55-64	Customer attached 100-115
EPON এর Bandwidth Efficiency হচ্ছে 72%	GPON এর Bandwidth Efficiency হচ্ছে 92%
EPON এর QoS (Quality of Service) ভালো তথ্য ইথারনেট এর জন্য।	GPON এর QoS(Quality of Service) ভালো ATM, TDM সহ।
EPON এর মাঝিমাম দূরত্ব হচ্ছে 10 or 20 Km	GPON এর মাঝিমাম দূরত্ব হচ্ছে 10 or 20 Km
EPON এর মাঝিমাম Split	GPON এর মাঝিমাম Split

Figure: Bus Topology



Form-36/B

Star Topology: Station সমূহ Connectivity device (Hub/Switch) এর সাথে সংযুক্ত হয়ে তথের আদান প্রদান করে। এ system এ কোন Station কাজ না করলেও System পুরোপুরি বন্ধ হয় না। Device হিসেবে Hub ব্যবহৃত হলে ডাটা সবচেয়ে ঘুরে বেড়ায় এবং যে Station এর Address এর সাথে মিলে যাব সেই Station ডাটা প্রাপ্ত করে।

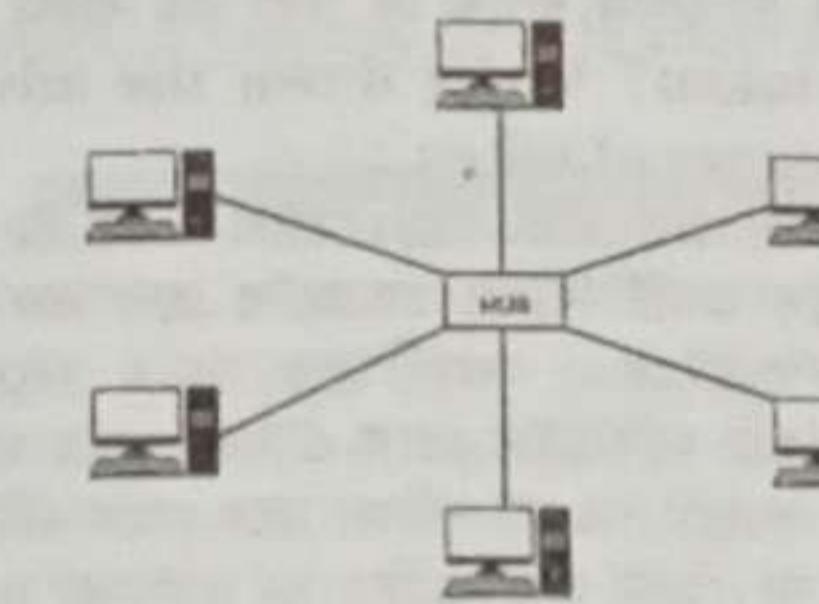


Figure: Star Topology

Ring Topology: দেখতে অনেকটা রিং এর মত। এখনে Station সমূহ শুধু ক্যাবল এর মাধ্যমে একটির সাথে অন্যটি সংযুক্ত থাকে। এতে দুটি ক্যাবল ব্যবহার হয়। এ নেটওয়ার্ক টপোলজি তে যদি মাঝের কোন Station নষ্ট হয়ে যায়, তবে সম্পূর্ণ নেটওয়ার্ক ব্যবহৃত হচ্ছে পড়বে।

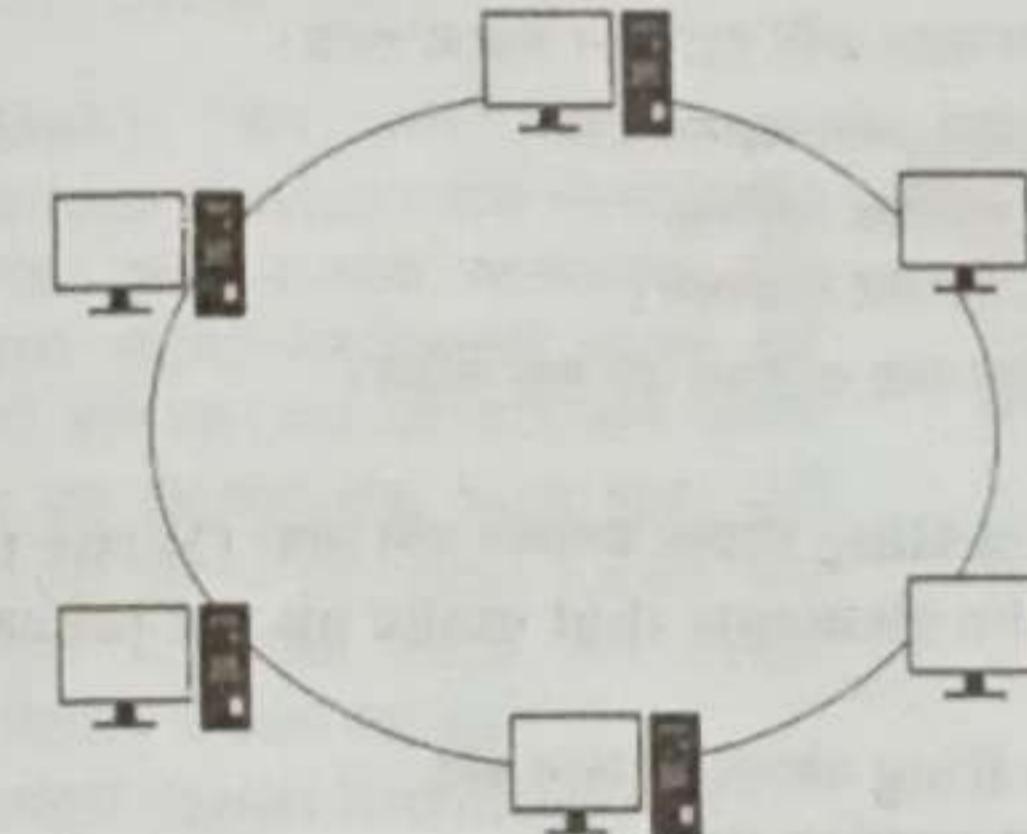


Figure: Ring Topology

Mesh topology: (মেশ টপোলজি): যদি কোনো নেটওয়ার্কে ডিভাইস বা কম্পিউটারগুলোর মধ্যে অতিরিক্ত সংযোগ থাকে তাহলে তাকে বলা হয় মেশ টপোলজি। অধিকাংশ মেশ টপোলজি নেটওয়ার্ক সত্ত্বকারের মেশ নেটওয়ার্ক নয়। এগুলো হলো আসলে হাইব্রিড মেশ নেটওয়ার্ক। এতে তথ্য অতিরিক্ত বা অপ্রয়োজনীয় লিঙ্ক থাকে। এতে ডেটা কমিউনিকেশনে অনেক বেশি নিষ্কাতা থাকে এবং নেটওয়ার্কের সমস্যা খুব সহজে সমাধান করা যায়। মেশ টপোলজিতে কম্পিউটারের সংখ্যা নির্ণয়ের সূত্র হলো: $C = \frac{n(n-1)}{2}$ [এখনে, n হলো কম্পিউটার বা নোডের সংখ্যা।]

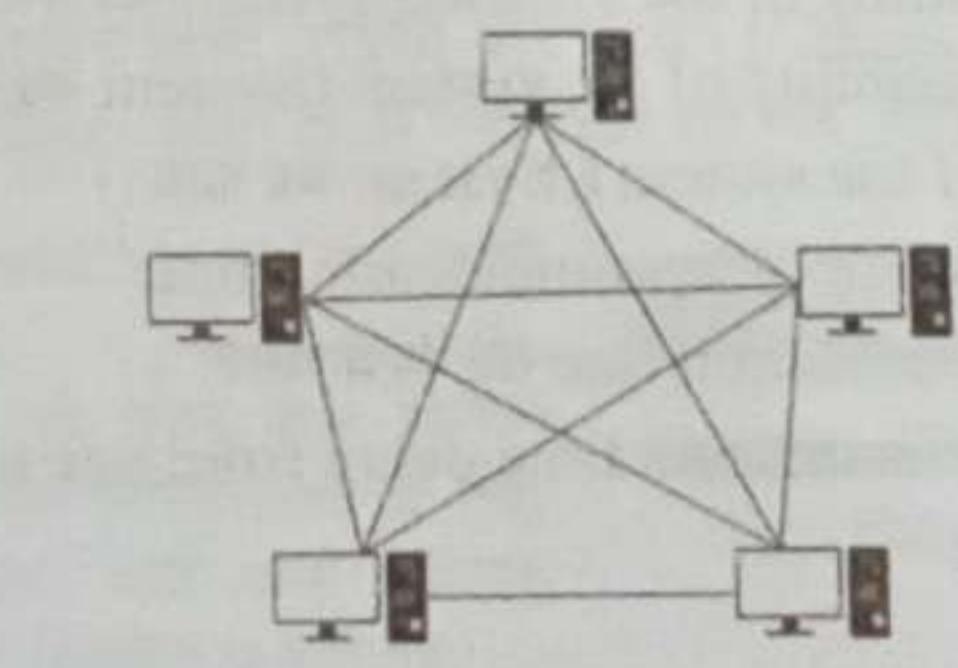


Figure: Mesh Topology

Hybrid topology (হাইব্রিড টপোলজি): বাস, স্টার, রিং ইত্যাদি টপোলজির সময়ে গঠিত নেটওয়ার্ক টপোলজিকে বলা হয় হাইব্রিড টপোলজি।

উদাহরণস্বরূপ: ইন্টারনেটকে এ ধরনের টপোলজি হিসেবে অভিহিত করা যায়। কেননা ইন্টারনেটে হালো বৃহৎ পরিসরে একটি নেটওয়ার্ক। যেখানে সব ধরনের টপোলজির মিশ্রণ দেখা যায়। টপোলজি তে প্রযোজনানুসারী নেটওয়ার্ক বৃক্ষ করার সুযোগ রয়েছে। কোন সমস্যা দেখা দিলে তা সহজেই নিয়ন্ত্রণ করা সম্ভব হয়। কোন এক অংশ নষ্ট হয়ে গেলে সম্পূর্ণ নেটওয়ার্ক নষ্ট না হয়ে অ্বস্থিতিতে নষ্ট হয়ে যায়।

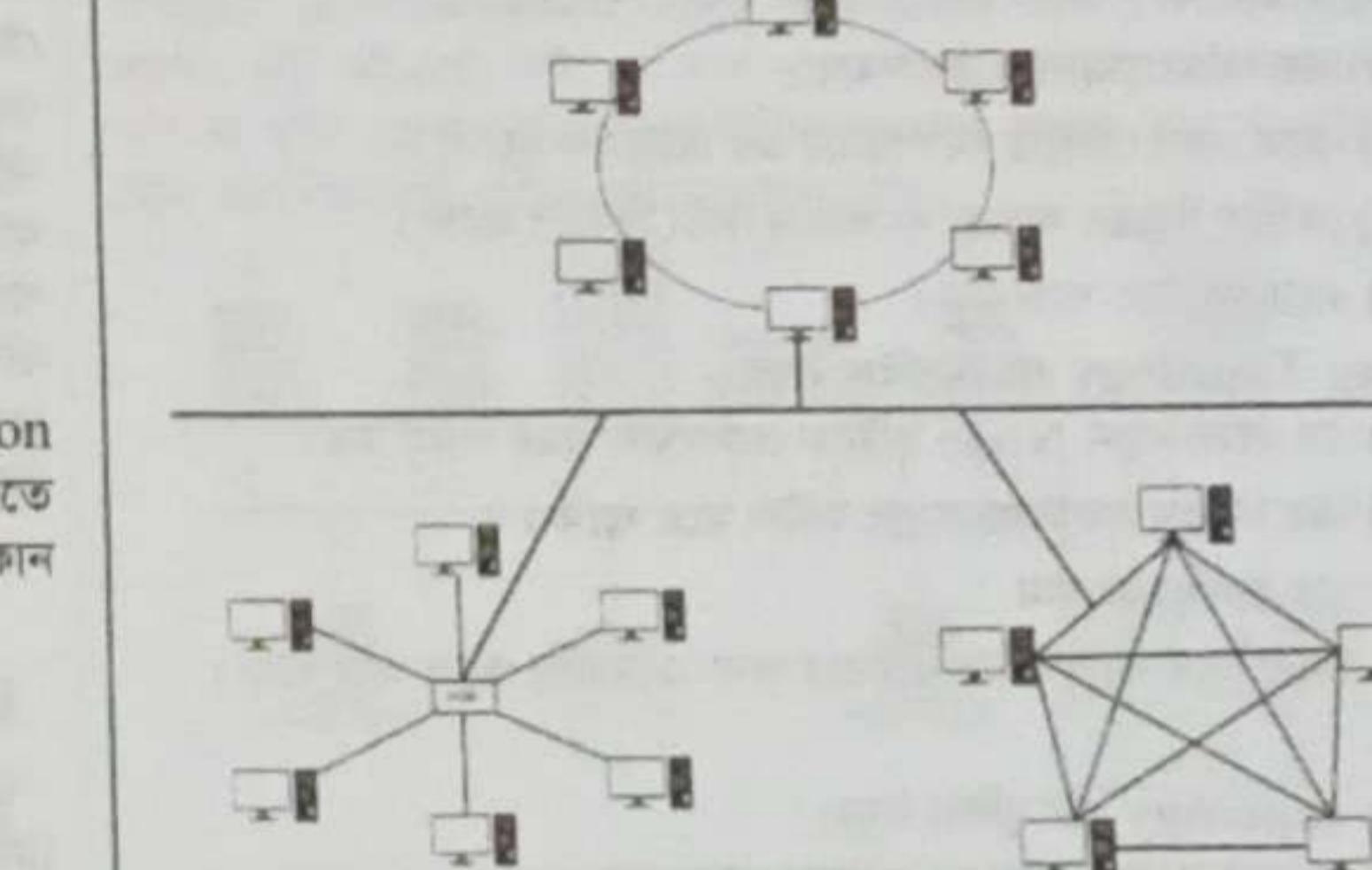


Figure: Hybrid Topology

Tree Topology: একটি Root node এর সাথে যাব যুক্ত করে Branch তৈরি করা হয় এবং Branch থেকে বিভিন্ন Node যুক্ত করা হয়। Branch এর সাথে নতুন হাব যুক্ত করে নেটওয়ার্ক সম্প্রসারণ করা যায়।

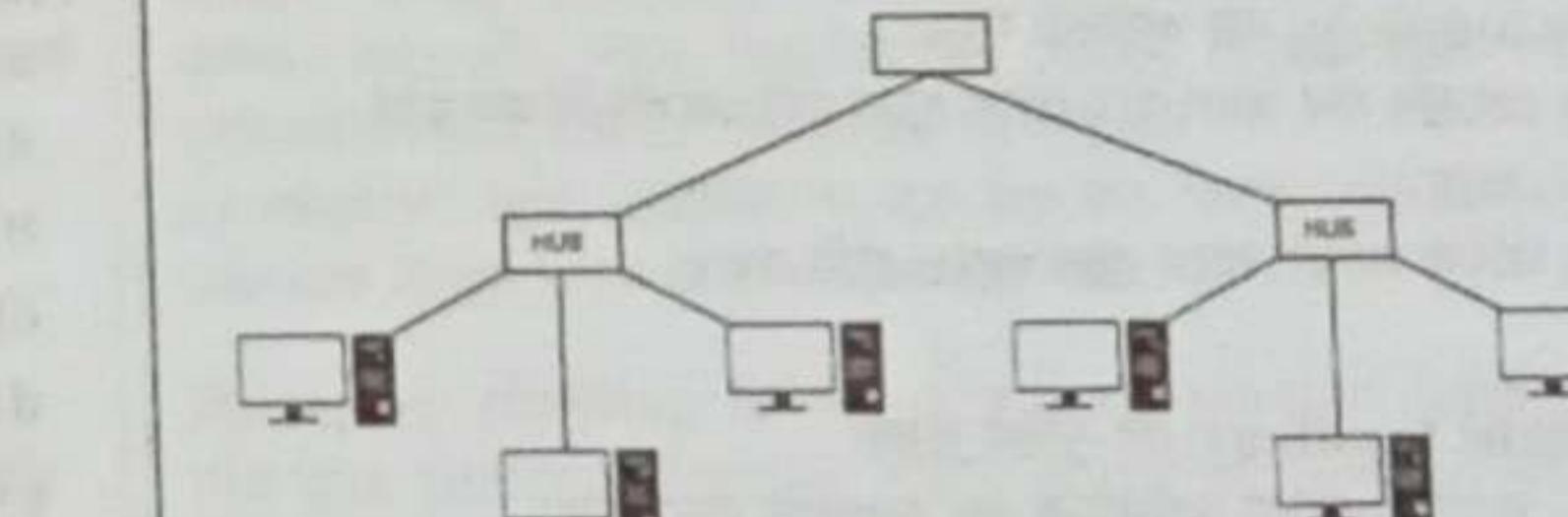


Figure: Tree Topology

প্রশ্ন-২) Bus, Star, Ring, Hybrid, Tree topology এর সুবিধা ও অসুবিধা লিখ? (Write Advantages and Disadvantages of Bus, Star, Ring, Hybrid, and Tree topology.) [BRTA-12]

উত্তর: **Bus topology** এর সুবিধা সমূহ:

- একটি মাত্র Physical line এর মাধ্যমে Data transmit হয়।
- কোন একটি কম্পিউটার অকেজো হয়ে গেলেও অন্য কম্পিউটার ব্যাকআপ করতে পারে।
- কম দৈর্ঘ্যের ক্যাবল লাগে বলে খরচও কম।
- ট্রান্সমিশন পক্ষতি অতি সাধারণ।

- Bus topology** এর অসুবিধা সমূহ:
- Physical media নষ্ট হয়ে গেলে পুরো সিস্টেম অকেজো হয়ে পড়ে।
 - এতে তুল নির্ধারণ ও সংশোধনে অসুবিধা হয়।
 - ডাটা ট্রান্সফার চাপ বেশি হলে দীর্ঘ সময় অপেক্ষা করতে হয়।
 - Collision ঘটে।

- Ring Topology** এর সুবিধা সমূহ:
- প্রতিটি কম্পিউটার নেটওয়ার্ক এ সমান Access হয়।
 - এর সংযোগ ব্যবহাৰ বেশ সহজ।
 - এতে কোন কেন্দ্ৰীয় কম্পিউটার এর প্ৰয়োজন হয় না।
 - কেন্দ্ৰীয় নিয়ন্ত্ৰণ ব্যবহাৰ না থাকায় ডাটা বিতরণ সহজ।
 - এতে সংযোগ খুচ কৰ।

- Ring Topology** এর অসুবিধা সমূহ:
- যে কোন নতুন Node সৃষ্টিতে যোগাযোগ সময় বৰ্ধিত হয়।
 - এর নিরাপত্তা সৃষ্টি যোগাযোগ সূৰ জটিল হয়ে থাকে।
 - এর জনপ্ৰিয়তা কৰ।
 - উভয় পথে কম্পিউটার ব্যৰ্থতাৰ জন্য এ পক্ষতি অচল হয়ে পড়ে।

- Star topology** এর সুবিধা সমূহ:
- সংযোগ ব্যবহাৰ সাধাৰণ, সংযোগ খুচ কৰ।
 - দ্রুত তথ্য আদান প্ৰদান কৰা যায়।
 - নতুন Node যুক্ত কৰা হলে তথ্য আদান প্ৰদানে কোন বৰ্ধিত সময় প্ৰয়োজন হয় না।
 - কোন ছানীয় কম্পিউটার ব্যৰ্থ হলে, নেটওয়ার্ক এর উপর কোন প্ৰভাৱ পড়ে না।

- Star topology** এর অসুবিধা সমূহ:
- কেন্দ্ৰীয় হাৰ অচল হয়ে গেলে পুরো নেটওয়ার্কই বিকল হয়ে পড়ে।
 - অধিক ক্যাবল লাগে বলে খুচ ও বেশি হয়।

- Hybrid topology** এর সুবিধা সমূহ:
- ব্যাপক এলাকা নেটওয়ার্ক এর আওতায় আনা যায়।
 - এতে যোগাযোগ রক্কাৰ জন্য একাধিক পথ পাওয়া যায়।
 - ডাটা ট্রান্সফাৰ অধিক বিশৃঙ্খল।
 - কোন অংশেৰ ব্যৰ্থতাৰ জন্য সময় System টি অকেজো হয় না।
 - নিদিষ্ট আকাৰ না থাকাৰ ইচ্ছা মত নেট সংযোগ কৰা যায়।

- Hybrid topology** এর অসুবিধা সমূহ:
- সংযোগ ব্যবহাৰ খুবই জটিল।
 - সংযোগ খুচ বেশি।
 - গতি কৰ।

- Tree topology** এর সুবিধা সমূহ:
- নতুন Branch তৈৰি কৰাৰ মাধ্যমে নেটওয়ার্ক এর সম্প্ৰসাৰণ কৰা যায়।
 - Office administration এৰ জন্য এই নেটওয়ার্ক উপযোগী।

- Tree topology** এৰ অসুবিধা সমূহ:
- Root নষ্ট হয়ে গেলে সমস্ত নেটওয়াৰ্কটি অকেজো হয়ে পড়ে।
 - Node ভলো শাৰী প্ৰশাৰাতে বিভক্ত হওয়াতে বিভিন্ন নোড অসমৰ্থ মধ্যে Communication কৰা জটিল।

প্ৰশ্ন-৩) টোকেন রিং টপোলজি বলতে কি বুঝ? এৰ সুবিধা ও অসুবিধা লিখ? (What is token? Write down the advantages and Disadvantages of token.)

উত্তৰ: এটি একটি রিং নেটওয়াৰ্ক গড়ে তোলে। এই রিং নেটওয়াৰ্ক টোকেন নামে পৰিচিত একটি বিশেষ ফৰমেটেৰ ফৰ্ম এক কম্পিউটাৰ থেকে আৱেকে কম্পিউটাৰে একমুখীভাৱে ঘূৰতে থাকে। এটিটি কম্পিউটাৰ তাৰ পাৰ্শ্ববৰ্তী কম্পিউটাৰ থেকে টোকেন পেয়ে থাকে। কোন কম্পিউটাৰ টোকেন পাওয়াৰ পৰ তা পৰীক্ষা কৰে দেখে এটি তাৰ জন্য পাঠানো হৈছে কি না। তাৰ জন্য প্ৰেৰিত না হলে তা অপৰ পাশেৰ কম্পিউটাৰে পাঠায়ে দেয়। এভাৱে টোকেন পুৱো নেটওয়াৰ্ক ঘূৰতে থাকে।

- টোকেন রিং টপোলজিৰ সুবিধা:
- নেটওয়াৰ্কৰ নোড সংখ্যা কমে গেলে ও নেটওয়াৰ্ক ভালভাৱে কাজ কৰে।
 - ব্যাক্তিগতভাৱে ক্ষেত্ৰ সংশোধন কৰতে পাৰে।
 - সংঘৰ্ষ ঘটাৰ কোন সমস্যা নেই।

- টোকেন রিং টপোলজিৰ অসুবিধা:
- ব্যৰহত যোগাযোগ ব্যৰহকল।
 - এটি ছাপন কৰা ও ট্ৰাবল তট কৰা কঠিন।

প্ৰশ্ন-৪) Token Ring গঠনেৰ উপাদান কোন লিখ? (Write the names of the elements that make up the token ring.)

- উত্তৰ: Token Ring গঠনেৰ উপাদান কোন:
- দুই বা ততোধিক PC
 - UTP বা STP Cable
 - Connecting device হিসেবে hub
 - Network interface card
 - RJ- 45 connector

প্ৰশ্ন-৫) Topology Selection এ বিবেচ্য বিষয়সমূহ লিখ? (Write down the considerations for topology selection.)

উত্তৰ: Topology Selection এ বিবেচ্য বিষয়সমূহ:

- Reliability of the system (System এৰ দক্ষতা।)
- Expandability of the system (System এৰ বৰ্ধিতায়ৰ কৰাৰ পথ।)
- Cost of the system (System এৰ ব্যায়।)
- Availability of communication line (Communication line এৰ সহজলভাৱ।)
- Data transmission time delay from one node to another

- Structure of the network system(Network System এৰ গঠন)
- Error detection solution(তুলছতি নিৰ্ণয় ও সংশোধন।)
- Software operation of the system
- Data transmission speed
- Installation process trouble shooting

- Function of switches
- Learning
- Forwarding
- Loop breaking {spanning tree protocol (STP)}
- Memory

Bridge (ব্ৰিজ): ব্ৰিজ একটি নেটওয়াৰ্ক ডিভাইস যা একটি বৃহৎ নেটওয়াৰ্ককে ছোট ছোট সেগমেন্টে বিভক্ত কৰে। এৰ সাহায্যে ডিভাৱ মাধ্যম অথবা ডিভাৱ কাঠামো বিশিষ্ট একাধিক নেটওয়াৰ্ককে সংযুক্ত কৰা যায়। এটি একাধিক ছোট নেটওয়াৰ্ককে সংযুক্ত কৰে একটি বৃহৎ নেটওয়াৰ্ক তৈৰি কৰে। এটি অনেকটা সুইচ বা হাৰ এৰ মত। একেতে পাৰ্শ্বক্ষ হলো, হাৰ বা সুইচ একই নেটওয়াৰ্কৰ বিভিন্ন নোডকে সংযুক্ত কৰে অন্যদিকে ব্ৰিজ একাধিক ছোট নেটওয়াৰ্ককে সংযুক্ত কৰে।

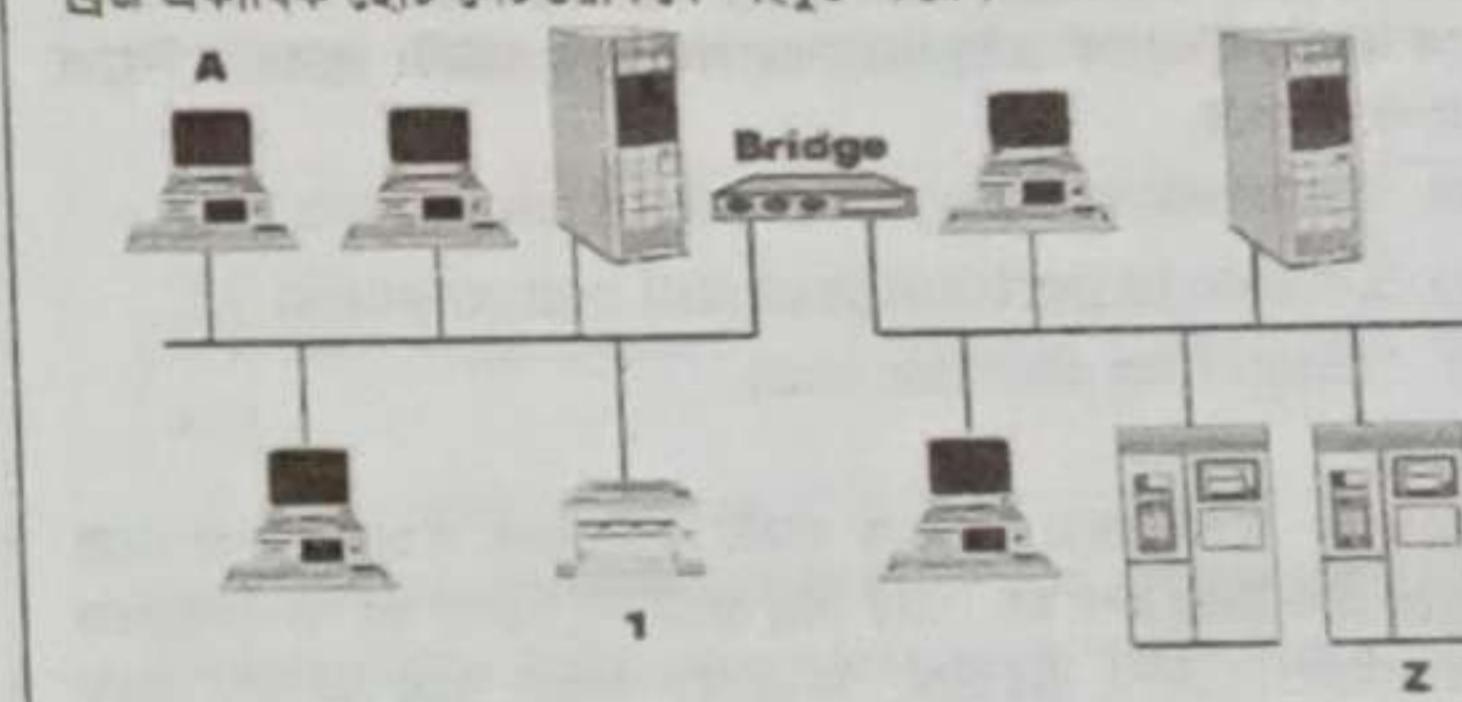


Figure: ব্ৰিজ ও ব্ৰিজ দ্বাৰা একাধিক নেটওয়াৰ্ক সংযুক্ত

ব্ৰিজ সাধাৰণত তিন প্ৰকাৰেৰ হয়ে থাকে। যেমন:

- লোকাল ব্ৰিজ: সৱাসিৱ LAN-এৰ মধ্যে যুক্ত।
- রিমোট ব্ৰিজ: দুটি LAN-এৰ মধ্যে গোইড এৰিয়া নেটওয়াৰ্ক তৈৰিতে ব্যৰহত হতে পাৰে। এটি বেখনে এড (end) নেটওয়াৰ্কৰ তুলনায় কানেকটিং লিংক ধীৰগতিসম্পন্ন সেখানে ব্যৰহত হতে পাৰে। বৃহদায়কৰ ক্ষেত্ৰে রাউটাৰ দ্বাৰা প্ৰতিশ্ৰুত কৰা হয়।
- ওয়্যারলেস ব্ৰিজ: একাধিক ল্যানকে যুক্ত কৰা অথবা ল্যানেৰ দ্বৰ্বলী স্টেশনকে সংযুক্ত কৰাৰ জন্য ব্যৰহত হতে পাৰে।

Repeater (রিপিটাৰ): রিপিটাৰ হচ্ছে একটি নেটওয়াৰ্ক ডিভাইস যা তাৰ কাছে তথ্য পেলে ইথাৰনেট পোর্টেৰ মাধ্যমে তা forward কৰে। এখনে সিগন্যালেৰ কোন পৰিবৰ্তন সাধিত হয় না। একটি নেটওয়াৰ্ক মিডিয়াৰ মধ্য দিয়ে ডেটা সিগন্যাল প্ৰাৰম্ভ কৰাৰ সময় নিন্দিষ্ট দৰছু অতিৰিক্ত কৰাৰ পৰ এটেনুৰোপনেৰ কাৰণে সিগন্যাল আস্তে আস্তে দৰ্বল হয়ে পড়ে। তখন এই সিগন্যালকে পুনৰোৰ্ক কৰে গত্বয়ে স্পৰ্শাতে হয়। মাৰামাদি অৰজনে থেকে এই কাজটি যে ডিভাইস কৰে থাকে মূলত তাকেই রিপিটাৰ বলে। এটি একটি 2-পোর্ট বিশিষ্ট ডিভাইস। রিপিটাৰ ফিজিক্যাল ল্যানেৰ কাৰ্জ কৰে।



Figure: Repeater (রিপিটাৰ)

Types:

- Amplification
- Signal processing repeater.

প্রশ্ন-১০) LAN Card বা NIC কি কাজ করে? (What is the function of LAN Card or NIC?)

উত্তর: LAN Card বা NIC এর কাজ:

- Collect IP address from network Layer. (নেটওয়ার্ক লেবেল থেকে আইপি এড্রেস সংগ্রহ করা।)
- Add destination MAC address. (ডেস্টিনেশন ম্যাচ এড্রেস যোগ করা।)
- Add Source MAC address. (সোর্স ম্যাচ এড্রেস যোগ করা।)
- Transform the frame into signal. (ফ্রেমকে সিগনালে রূপান্বয় করা।)
- বিসিভিং প্রাণে একই কাজ করবে উচ্চ নিক হতে।

প্রশ্ন-১১) MAC Address কি? ইহার বৈশিষ্ট্য কলো লিখুন। What is MAC Address? Write its Characteristics.) [BPSC-12, Multiple Ministry-16, NTRCA- 2016]

উত্তর: MAC এর পূর্ণরূপ হচ্ছে Media Access Control. এতে একটি Address থাকে। একটা ডিভাইসে Network Interface Card বা NIC থাকে, যার হার্ডওয়ার এড্রেস হলো এই MAC এড্রেস। IP এড্রেস মেধানে TCP বা নেটওয়ার্ক সম্পর্কযোগীর সাথে সংযুক্ত থাকে, আর MAC এড্রেস নেটওয়ার্ক এভান্টের হার্ডওয়ারের সাথে সম্পর্কযুক্ত। MAC এড্রেস হলো ইউনিক 48-বিটের হার্ডওয়ার নম্বর, যা NIC তৈরী করার সময় অন্যত্বকারক কোম্পানি কর্তৃক অন্যদল করা হয় এবং ইহা প্রতিশীর্ষ প্রতিটা ডিভাইসের ক্ষেত্রে ব্যৱহাৰ কৰা হয়। IEEE 802 এ, ডেটা লিঙ্ক স্তর প্রাথমিকভাবে দুই ভাবে বিভক্ত হয়-

- Logical Link Control (LLC) Sublayer.
- Media Access Control (MAC) Sublayer.

MAC এড্রেস মূলত ডেটা লিঙ্ক স্তরের Media Access Control (MAC) ব্যবহার করে।

Media Access Control					
01	22	5E	7F	84	CD
Organizationally Unique Identifier (OUI)		Network Interface Controller (NICs)			

MAC Address এর বৈশিষ্ট্য সমূহ:

- 48 bit address
- Hexadecimal number format
- For example: 1234. abcd .babc
- Generated by manufacturer
- Must be unique in the world

প্রশ্ন-১২) নিচের MAC Adress কলো কোন ধরনের বের করুন? (Find out what kind of MAC addresses are below.)

(a) 4C:23:10:4A:1A:2A

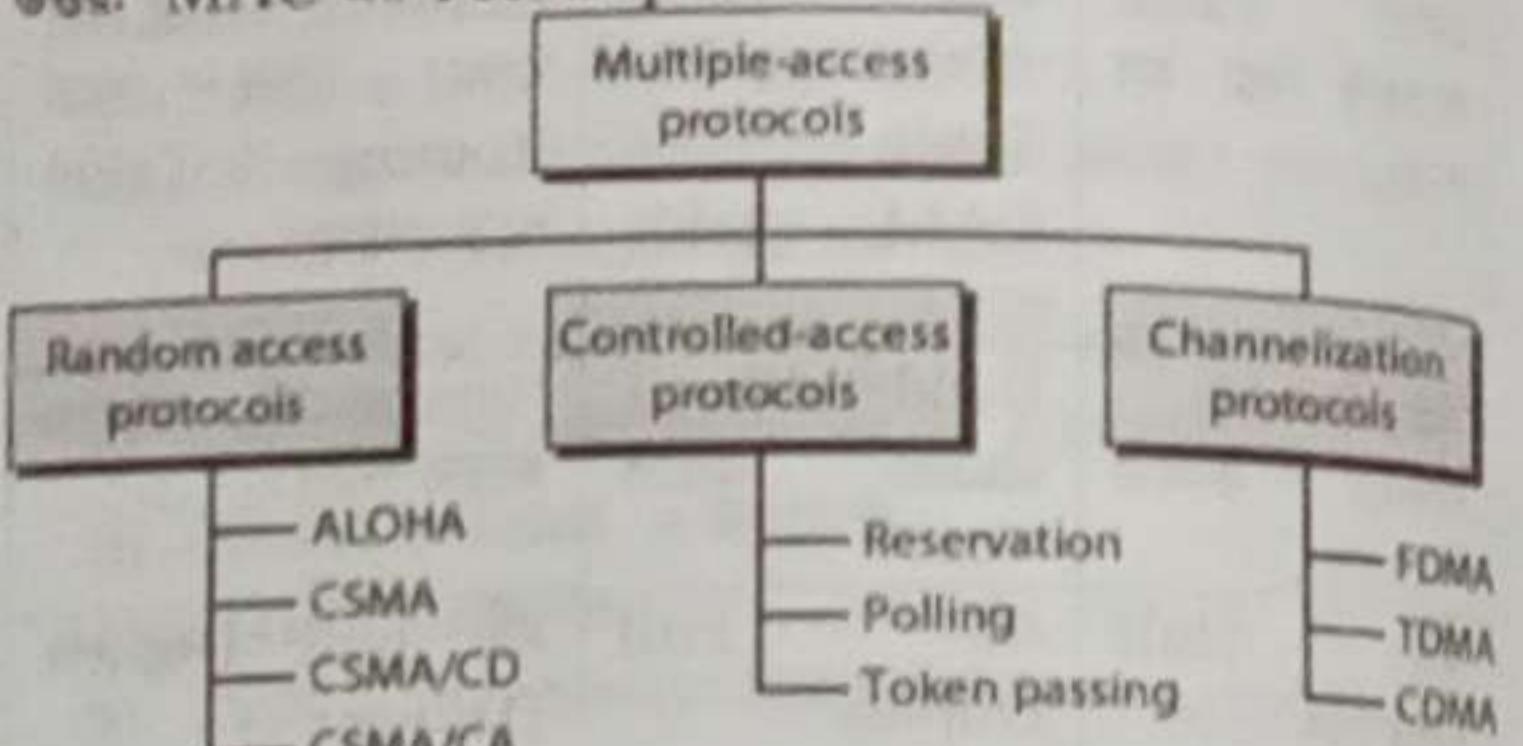
(b) 45:24:56:2B:24:12
(c) FF:FF:FF:FF:FF:FF

উত্তর:

MAC Address	Type
(a) 4C:23:10:4A:1A:2A	Unicast
(b) 45:24:56:2B:24:12	Unicast
(c) FF:FF:FF:FF:FF:FF	Broadcast (Ethernet frames with ones in all bits of the destination address (FF:FF:FF:FF:FF:FF) are referred as broadcast address.)

প্রশ্ন-১৩) MAC এর Technique কলো লিখ? (Write the technique of MAC.)

উত্তর: MAC এর Technique কলো:



প্রশ্ন-১৪) MAC Address এবং IP Address এর মধ্যে পার্থক্য কী? (What is the difference between MAC Address and IP Address?) [BPSC (AME)-2020]

উত্তর: MAC Address এবং IP Address এর মধ্যে পার্থক্য নিরূপণ:

MAC Address	IP Address
MAC Address এর পূর্ণরূপ- Media Access Control Address :	IP Address এর পূর্ণরূপ- Internet Protocol Address :
এটি Internet এ Computer এর Physical Address Identify করে।	এটি Internet এ Computer এর Connection Identify করে।
MAC এর Address bit সংখ্যা 48-bit :	এতে দুটি Address বিদ্যমান যথা: 1) IPv4 (Size- 32bit) 2) IPv6 (Size- 128bit)
এটি NIC card এর Manufacturer'রা Assign করে দেয়।	এটি Network administrator অথবা Internet Service Provider'রা Assign করে দেয়।
ARP Protocol ব্যবহার করে একটি Device এর MAC Address Retrieve করা যায়।	RARP Protocol ব্যবহার করে একটি Device এর IP Address Retrieve করা যায়।

প্রশ্ন-১৫) CSMA/CD বলতে কি বুঝ? CSMA/CD এর কার্যপদ্ধতি সংক্ষেপে লিখুন। (What is CSMA/CD? Briefly describes its functionality.)

উত্তর: CSMA/CD: এটি Media Access Control (MAC) এর একটি কর্তৃতপূর্ণ পদ্ধতি। এটি CSMA এর উন্নত সংস্করণ। পূর্ণনাম Carrier Sense Multiple Access with Collision Detection. এটির মূল বিষয় হল Collision Detect এর মাধ্যমে Media Access করবে। অর্থাৎ যদি Medium Idle থাকে তবে Data Transmit হবে। অন্যথায় অপেক্ষ করবে যদ্যপি না Idle হয়। Idle হলে Transmit করবে।

প্রশ্ন-১৬) একটি কোম্পানিতে ১০ টি কম্পিউটার আছে। ৫ টি কেবল কম্পিউটার সিলের মাধ্যমে সংযোগ করা হয়েছে। মুল নেটওয়ার্ক মুক্ত করার জন্য ডিভাইস ১ এবং মুল নেটওয়ার্ক মুক্ত করার জন্য ডিভাইস ২ হিসাবে কোন ডিভাইস টি ব্যবহার করবে? [TGCL-2017]

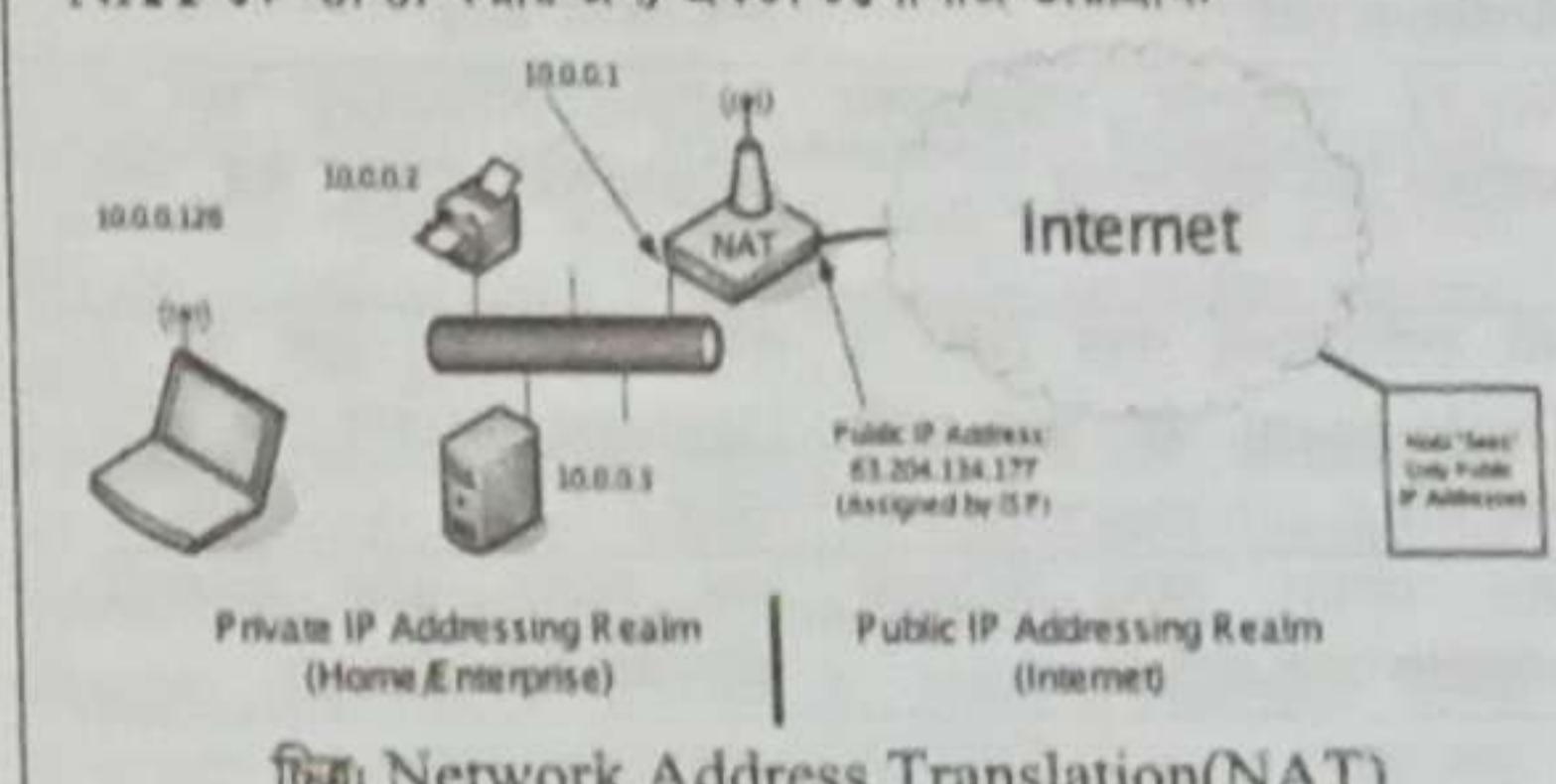
১. রাউটার
২. স্রীজ
৩. সুইচ

উত্তর: ডিভাইস ১ হিসাবে সুইচ ও ডিভাইস ২ হিসাবে রাউটার

প্রশ্ন-১৭) Network Address Translation (NAT) কি? ব্যাখ্যা করুন। (Briefly describes Network Address Translation with figure.) [BPSC-12, Food Ministry, SAE-2021]

উত্তর: Network Address Translation (NAT) IP address সংরক্ষণের জন্য ডিজাইন করা হয়েছে। এটি private IP network (যেতেলো নির্বাচিত IP address) তালিকে Internet এ মুক্ত হতে সহায় করে। NAT একটি রাউটারে চালিত হয়, সাধারণত মুল নেটওয়ার্ক একসাথে ডেটা প্রেসেন্ট করে এবং private IP address (যেতেলো নির্বাচিত IP address) তালিকে public address এ পরিবর্তন করে data packet অন্য নেটওয়ার্কে প্রেরণের আগে।

NAT কে ব্যাখ্যা করার জন্য একটা টপোলজি ডায়াগ্রাম:



টপো: Network Address Translation(NAT)

প্রশ্ন-১৮) Why do we need NAT? What are its advantages? (NAT আমাদের কেন প্রয়োজন? ইহাৰ সুবিধা সমূহ কি? [BPSC-12, Food Ministry, SAE-2021]

উত্তর: NAT এর প্রয়োজনীয়তা: Network Address Translation (NAT) আইপি আড্রেস সংরক্ষণের জন্য ডিজাইন করা হয়েছে। যা আইপি আড্রেস এর সংষ্কৃত প্রস্তুতি প্রদান করলে ব্যবহার করা হয়। সাধারণত পেটওয়ে রাউটারে NAT এন্অপ্ল করা থাকে। মূলত ইন্টারনেট আয়োজনে প্রাইভেট আইপি থেকে প্রাবল্যক আইপি কনভার্সনে NAT ব্যবহার করা হয়।

NAT ব্যবহারের সুবিধা সমূহ:

- বৈধতাবে আইপি এড্রেস সশ্রান্ন করার জন্য।
- নেটওয়ার্কের নিরাপত্তা প্রদান করার জন্য।
- প্রাবল্যক নেটওয়ার্ক সংযুক্তির ক্ষেত্রে ক্লেইভিলিটি বৃক্ষি পাও।
- নেটওয়ার্ক পরিবর্তন হলে নতুন করে এড্রেস সংযুক্ত করার প্রয়োজন হওয়া।
- এড্রেস ওভারলেপ হওয়ার প্রবন্ধন করে যাও।

Ques-6) Protocol Suite for TCP/IP vs Protocol Suite and its components? (What is Protocol suite? Why TCP/IP is called Protocol suite.)

Application	SMTP, POP3, Telnet, FTP, HTTP, NFS, NIS+, DNS, rlogin, RSH, RIP, S NMP
Transport	TCP/UDP/SPX/SCTP
Internet	IP/IPX/AppleTalk/ARP/RARP/ICMP/ICMP
Datalink	PPP, IEEE 802.2
Physical	Ethernet, Token ring, RS 232, others

ପିଆର୍ ମେମ୍ପାର୍ଟ୍ ର ଶ୍ରୀ ମେହାର ହିଲ୍ସ୍, ପରମିଳାରେ କ୍ଷେତ୍ରଜ୍ଞ
ଆକାଶ/ବାଯାନାକାଶ ମେହାର କେତେ ଉଚ୍ଚାଲିକ, ପିଆର୍ ମେହାର ନାମ
ଦେଖିବା କାହାର ।

ग्रन्ति) TCP/IP एवं उपर्याद कल्पना कार्यालयी लिखें। (Write the function of TCP?IP Layer.)

- a) Application Layer
 - b) Transport Layer
 - c) Internet Layer
 - d) Datalink Layer
 - e) Physical Layer

आवाहन लेवल (Application Layer): TCP/IP में Application Layer का फ़ॉर्म Protocol के साथ ही OSI में Application, Presentation, Session Layer के बहुत कम प्रभाव लाते हैं। इस लेवल पर Application Layer, Data Translation एवं Encoding, Dialog Control एवं File Transfer जैसे विकारालताएँ अपनायी जाती हैं। TCP/IP में Application Layer के अन्तर्गत मानक लोगों के द्वारा विकारालताएँ शामिल हैं, जैसे HTTP, SMTP, FTP, Telnet, SMTP, DNS आदि।

ট্রান্সপোর্ট লেয়ার (Transport Layer): Transport Layer OSI Model এবং Transport Layer এর অন্তর্ভুক্ত কাজ সম্পর্কের পথ
থাকে। এই কাজের কাজ হচ্ছে পিস্টুলেজারে কেটি প্র্যাকেটে সরবরাহ করা
এবং কেটি প্র্যাকেটের শিক্ষণ, উপরিকৃতি মিশ্রিত বা কেটি প্রিমে
হেস করা ইত্যাদি কাজ এটি করে থাকে। প্রেরিত কেটি এবং
প্রস্তুতকৃতি প্র্যাকেটের থেকে ধড় থাকে করে এটি কেটি থেকে প্রেরণ করে
কাজে কাজ করে খুই বা প্রত্যেকিক প্র্যাকেটে প্রেরণ করে। এই সেবার
জাঁচি পৌরুষের জন্য সু ব্যবস্থা প্রাপ্তিশূল ব্যবহার করে।

ইন্টেরনেট লেয়ের (Internet Layer): Internet Layer OSI Model এবং Network Layer এর ঘৰে একই কাজ সম্পর্কসম্বন্ধ কৰা হচ্ছে। এই লেয়ারের কাজ যোগী অ্যাড্রেসিং ও প্রাকেট রেপিচুলেশন কৰা মেট্রোলজি কৰে তো প্রাকেট রাইটিং। এই সিস্টামটি সেখ এবং সে যোগাযোগে কাজ রেপিচুলেশনে প্রাচীয়ে দেয়। এই লেয়ারে ফাঁটা প্রাকেট মেট্রোলজি অ্যাড্রেস যোগ কৰে এসক্যান্ডেন্সের মাধ্যমে। এই ক্ষেত্ৰে গুৰুত্বপূর্ণ ডিভাইস ক্যারিএট হচ্ছে রাইটিং, রাইটিং, পেরিটেলিং।

डेटा लिंक लेयर (Data link layer): डेटा-लिंक लेयर का काम है कि लोगों द्वारा डेटा को एटोमेटिकली बहुत सारांश करते, उदाहरण TCP/IP डेटा-लिंक लेयर का अनुकूल डेटा लिंक है जो "प्रोटोकॉल" का नाम करते। डेटा-लिंक लेयर को एटोमेटिकली बहुत सारा विद्युतीय IEEE 802.2 प्रोटोकॉल एवं प्रोटोकॉलों की समूहीयता (PPP प्रोटोकॉल)।

फिजिकल लेयर (Physical Layer): यह एक प्रौद्योगिकीय लेयर है जो डेटा को वायरलेस या लॉन्ग एंड रेंज एवं लॉन्ग एंड वायरलेस तरीके से असाइनमेंट करता है।

(e) Transport Control Protocol वा ट्रान्सपर्ट कंट्रोल प्रोटोकॉल (Explain the Transport Control Protocol protocol)
[NTUCA-2010]

कैप्टन TCP: कैप्टन ट्रायिलोव नाम से जारी रहा विशेष नाम का नाम
कैप्टन अमेरिका ब्रॉडबैंड कंपनी का है। एटी एंड पी
लॉन्ड का एक बड़ा हासिल नाम है जिसका उत्तराधिकारी का नाम
कैप्टन है। इसका नाम वे ब्रॉडबैंड कंपनी का नाम जैसा
गोल्डन बॉइट नाम की तरह भारत में एटी एंड पीलॉन्ड नाम
दिल्ली का दौसिंह नाम जैसा नाम है।

- a) डोटी परिवासना करा।
 - b) जारी रखा, लिंगाय एवं अन्य ग्रन्ति का बोला खिल रखना करा।
 - c) उत्तिष्ठ विकृति, लिंगायतेश्वारा एवं डोटी राम लिंगायते
वास्तुकुमारिय द्वारा लिंगायत बर्तना करा।
 - d) किनारे घोट राखना करे, जबकि किनारे स्थापना द्वितीय
सह तो ठिक करा।

IP: ইন্টারনেট প্লাটোকল (আইপি) এল ইন্টারনেটে কোটা কিমা এবং
রাষ্ট্রিক করা জন্য প্রয়োজনীয় requirement এর একটি সেট। আইপি
, ডিপিলি এবং ইন্টার্ন্সি সহ বিভিন্ন প্রাপ্তিশোভ প্লাটোকলের সাথে ব্যবহার
করা হয়। আইপি কোডের মধ্যে প্রাক্তের উৎস, গত্ত্ব এবং নির্দেশনের
জন্য কলা থাকে। কোর মধ্যে IP যে কো পাঠায়ে, সেটি থাকে।
Packet কিভাবে কোথায় থাকে তা আই Protocol Define করে।

ଅନ୍ତର୍ଭାବରେ ଅଧ୍ୟାତ୍ମିକ ଶଳ ଗୋଟୋକଲ୍ କଲ୍ପନାର ସାଥେ ଭାବପାଶର କେତେବେଳେଟି ଗୋଟୋକଲ୍ଟଟି ଉପଯୋଗୀ ତା ବେଳ କରନ୍ତି

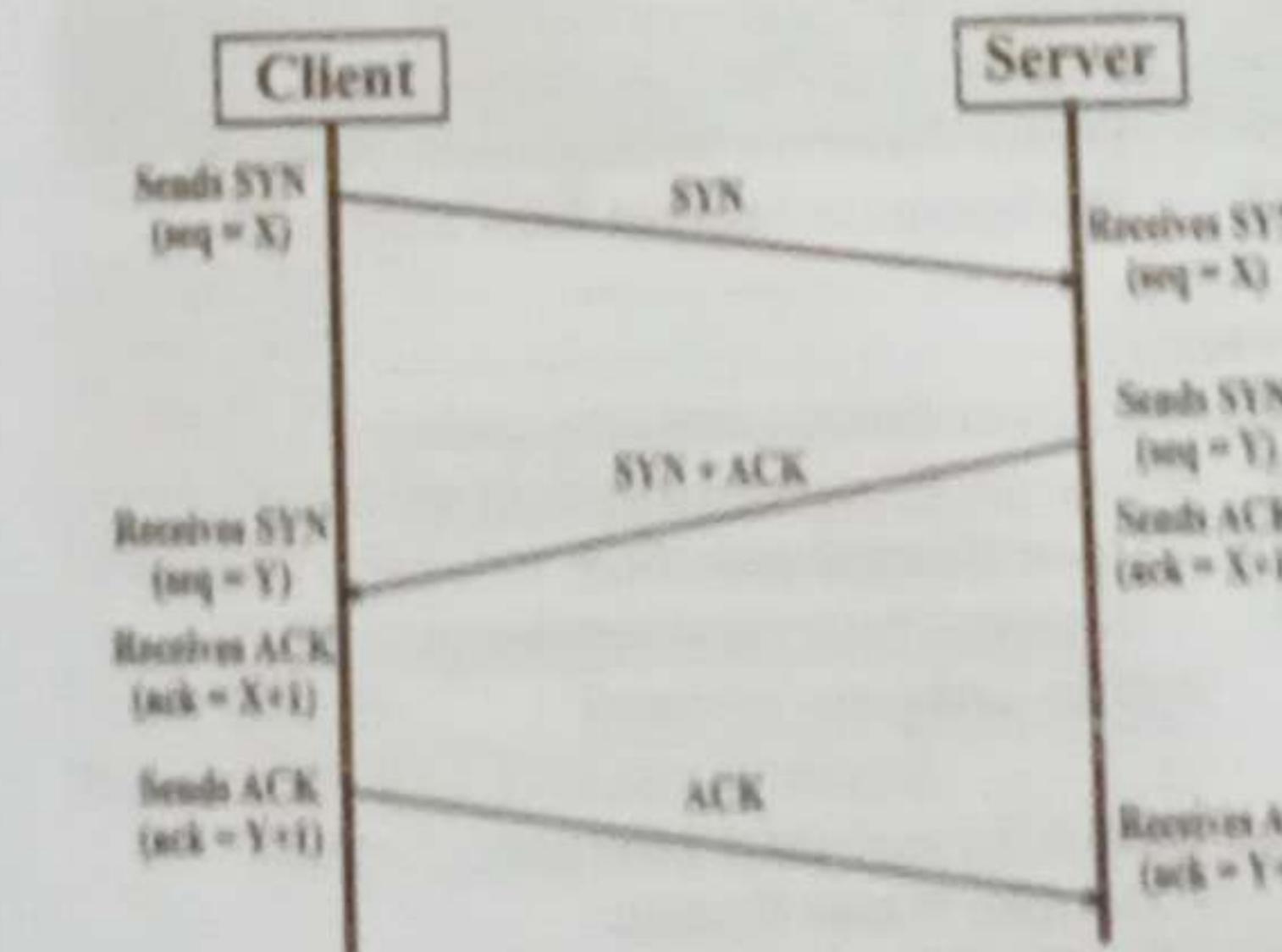
Application Protocols	Which One Is Suitable: TCP or UDP?
SMTP	TCP
SNMP	UDP
DHCP	TCP
TFTP	UDP
FTP	TCP
SSH	TCP

三

Application Protocols	Which One Is Suitable: TCP or UDP?
SMTP	TCP
SNMP	UDP
DHCP	UDP
TFTP	UDP
FTP	TCP
SSH	TCP

Ques-4) TCP protocol किसाबे काम करते? (How Transport Control Protocol works?)

উভয় TCP Protocol এবং কাজের প্রক্রিয়া: টিপিলি সহযোগিতার মুখ্য প্রযোজনেক সাধক সহযোগ অ্যালগরিদম নিয়ে কথা হচ্ছে। প্রযোজনেকের সময়, প্রাচীন এবং সার্ভার উভয়কেই করে প্রাপ্ত সিকেন্ডেল সময়ের সাথে একই ঘণ্টে থাকে যা কার্বিশানের প্রাপ্ত সিকেন্ডেলের প্রাপ্তি হিসাবে ব্যবহৃত হচ্ছে।



WILL IT WORK?	WITH WHICH APP?
Sends Transmission in Sequence	TCP or UDP?
Transmits Packets individually	
Uses higher transmission rate to support latency-sensitive apps	
Uses lower transmission rate to ensure reliability	
Transmissions include an 8-byte header	
Transmit Packet as stream	

三

Protocol Type	Protocol Function
Sends Transmission in Sequence	TCP
Transmits Packets individually	UDP
Uses higher transmission rate to support latency-sensitive apps	UDP
Uses lower transmission rate to ensure reliability	TCP
Transmissions include an 8-byte header	UDP
Transmit Packet as stream	TCP

শ্রেণী-১০) বাহ্যিকের কার্যকলি বা কার্যকলের সাথে জানপাশের কেন নেটওয়ার্ক কম্প্লেক্সের লিঙ আছে, তা লিখুন।

কার্যকলি বা কার্যকল	নেটওয়ার্ক কম্প্লেক্স: DHCP Server or DNS Server?
---------------------	---

Hold the TCP/IP setting to be distributed to the clients

VoIP	Connectionless
SSH	Connection Oriented
FTP	Connection Oriented

Resolves web URLs to IP Addresses

Stores a list of IP Addresses mapped to names

Assigns a default gateway to a Client

Assigns IP Addresses to enabled Clients

উত্তর:

কার্যকলি বা কার্যকল	নেটওয়ার্ক কম্প্লেক্স: DHCP Server or DNS Server?
Hold the TCP/IP setting to be distributed to the clients	DHCP Server
Resolves web URLs to IP Addresses	DNS Server
Stores a list of IP Addresses mapped to names	DNS Server
Assigns a default gateway to a Client	DHCP Server
Assigns IP Addresses to enabled Clients	DHCP Server

শ্রেণী-১১) বাহ্যিকের নেটওয়ার্কিং প্যারামিটারস বা প্রোটোকলস কেন সাথে জানপাশের কেনচির লিঙ আছে, তা লিখুন।

নেটওয়ার্কিং প্যারামিটারস বা প্রোটোকলস	Conection Oriented or Conectionless?
SMTP	
SNMP	
TFTP	
VoIP	
SSH	
FTP	

উত্তর:

নেটওয়ার্কিং প্যারামিটারস বা প্রোটোকলস	Conection Oriented or Conectionless?
SMTP	Connection Oriented
SNMP	Connectionless
TFTP	Connectionless

LDAPS = Lightweight Directory Access Protocol over TLS/SSL

DHCP = Dynamic Host Configuration Protocol

TFTP = Trivial File Transfer Protocol

NTP = Network Time Protocol

SNMP = Simple network management protocol

উত্তর: OSI & TCP/IP এর মধ্যে সম্পর্ক:
OSI Model

Application	Application
Presentation	
Session	
Transport	Transport
Network	Internet
Data link	Data link
Physical	Physical

Figure: OSI & TCP/IP এর মধ্যে সম্পর্ক

শ্রেণী-১২) DNS কেন TCP Protocol ব্যবহার না করে UDP Protocol ব্যবহার করে? যুক্তি দেখো। (Why does DNS use UDP and not TCP? Explain.)

উত্তর: DNS একটি Application Layer Protocol. আর সব Application Layer Protocol ট্রান্সপোর্ট প্রোটোকল অব UDP & TCP প্রোটোকলের মধ্যে যেকোন একটা ব্যবহার করে। TCP হচ্ছে Reliable (নির্ভরযোগ্য) এবং UDP Reliable (নির্ভরযোগ্য) নহ। DNS Reliable (নির্ভরযোগ্যতা) সাথে করেছে ইতিবিলি ব্যবহার করে। কিন্তু কেন? নিচে ইহার যুক্তি দেখো।

- UDP অনেক তেজ। TCP হচ্ছে বৈরাগ্যির কারণ ইহার জন্য 3-Way Handshake প্রয়োজন। আবার DNS সার্ভারের সেভ ও একটি গুরুত্বপূর্ণ ফার্মেল। DNS সার্ভার (যেহেতু তার UDP ব্যবহার করে) তারের সংযোগ থেকে রাখতে হবে।
- DNS এর রিকুরেন্ট সার্ভারসত ঘূর্বই ঘোট হয়ে থাকে এবং ইহা UDP সেলামেটের সাথে মানানসই।
- UDP Reliable (নির্ভরযোগ্য) নহ, কিন্তু Application প্রোটোকলে নির্ভরযোগ্যতা যোগ করতে পারে। একটি Application UDP ব্যবহার করতে পারে এবং নির্ভরযোগ্য হচ্ছে Application প্রোটোকলের মধ্যে একটি Timeout & Resend ব্যবহার করে।

উপরোক্ত চ টি কারনে DNS Reliable (নির্ভরযোগ্যতা) সাথে করেছে UDP ব্যবহার করে TCP নহ। যদিও TCP Reliable (নির্ভরযোগ্য)।

শ্রেণী-১৩) TCP/ IP এর Protocol কেন কি?

উত্তর: TCP Protocol:

BGP = Border Gateway Protocol

FTP = File Transfer Protocol

HTTP = Hyper Text Transfer Protocol

SMTP = Simple Mail Transfer Protocol

SNMP = Simple Network Management Protocol

MIME = Multipurpose Internet Mail Extension

IP Protocol:

ICMP = Internet control message protocol

IGMP = Internet group management protocol

OSPF = Open shortest path first

RSVP = Resource reservation protocol

UDP = User datagram protocol

UTP Protocol: [BUET-MS-17]

DNS = Domain Name System

LDAP = Lightweight Directory Access Protocol

শ্রেণী-১৪) ফাইল ট্রান্সফার প্রোটোকল এর বর্ণনা অনুযায়ী বাহ্যিকের সাথে জানপাশের স্টিক প্রোটোকল এর নাম লিখুন।

ফাইল ট্রান্সফার প্রোটোকল এর বর্ণনা	প্রোটোকল: FTP or TFTP
Does not require user authentication	
Uses UDP	
Uses TCP	
Uses ports 20 and 21	
Provides reliability when loading an IOS image upon boot up	
Uses port 69	

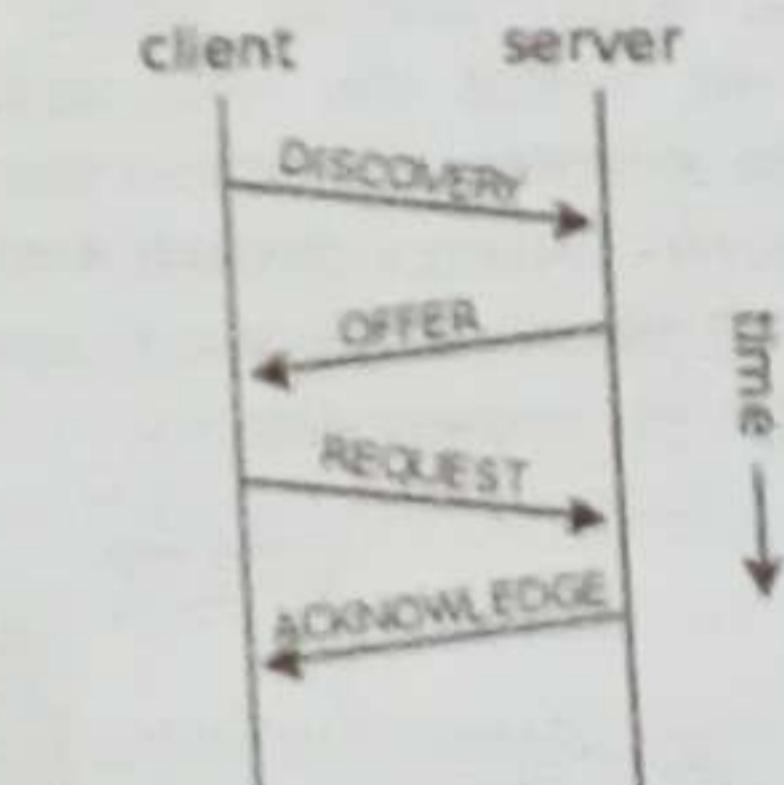
উত্তর:

ফাইল ট্রান্সফার প্রোটোকল এর বর্ণনা	প্রোটোকল: FTP or TFTP
Does not require user authentication	TFTP
Uses UDP	TFTP
Uses TCP	FTP
Uses ports 20 and 21	FTP
Provides reliability when loading an IOS image upon boot up	FTP
Uses port 69	TFTP

Note: FTP: File Transfer Protocol
TFTP: Trivial File Transfer Protocol)

শ্রেণী-১৫) OSI & TCP/IP এর মধ্যে সম্পর্ক কেন লিখুন[ICT Ministry-2017]

Figure: DHCP Timing Diagram



Q3-25) How can VPN provide secure communication platform? Explain site-to-site VPN and remote-access VPN using necessary figures. [UPSC-12 Food Ministry, SAE-2021]

द्वारा एक संस्कृत विद्युतीय अनुसन्धान केंद्र बनाया गया है। इसके अलावा एक विश्वविद्यालय भी इसके लिए तैयार किया जा रहा है। इसके अलावा एक विश्वविद्यालय भी इसके लिए तैयार किया जा रहा है। इसके अलावा एक विश्वविद्यालय भी इसके लिए तैयार किया जा रहा है। इसके अलावा एक विश्वविद्यालय भी इसके लिए तैयार किया जा रहा है।

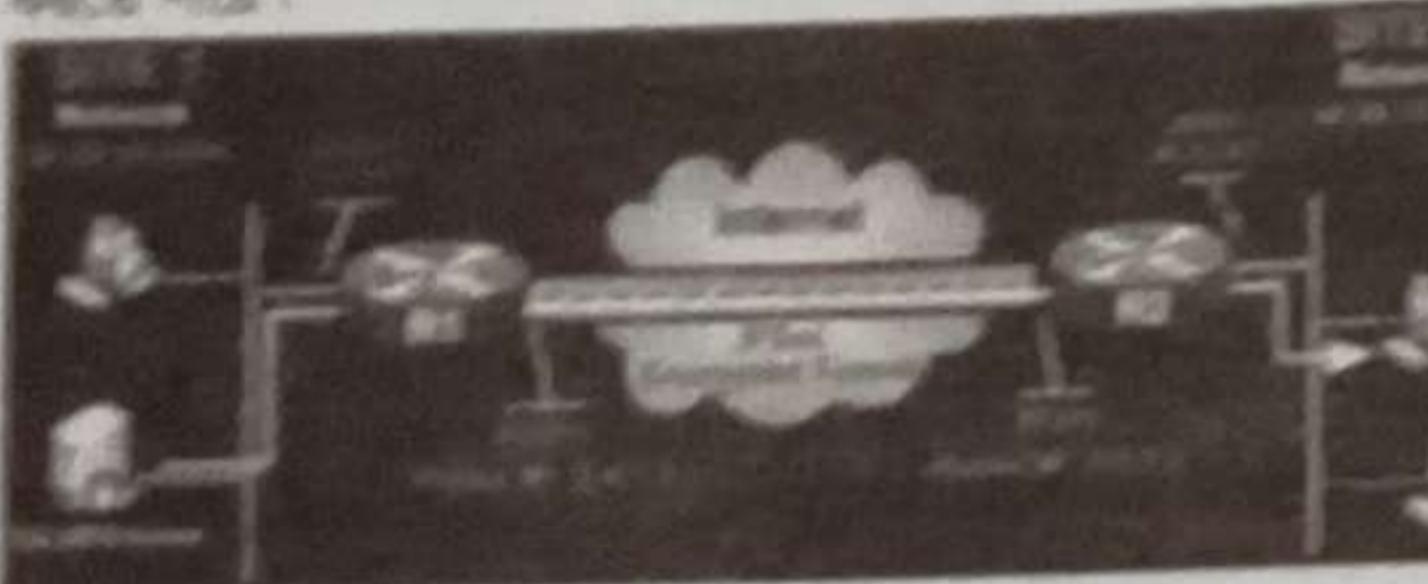


Figure: HTTPS Block Virus

Remote access VPN: Remote Access VPN ଯେବେଳେ ଏହି ସମ୍ବନ୍ଧ କରାଯାଇଲୁ ଯାଏ ଏହି ଏକି ଯାତି ଯାତି ଯେବେଳେ
କରାଯାଇଲୁ ଏହି ପ୍ରତିକିର୍ଣ୍ଣ ଅର୍ଥାତ୍ ଏହି ଯୋଗଦାନ କରି ଯାଏଇବେ ଏହି ଯୋଗଦାନ
ଏହି ସମ୍ବନ୍ଧଟି IPsec (IP Security) କେ ଯୁଦ୍ଧକ କରିବାରେ ଆବଶ୍ୟକ ଏହି
ଯୋଗଦାନ ଏହି ଏକି ଡିଫେନ୍ସିଵ ଲୋକଙ୍କ ଯାଏ Connection Setup କରିବାରେ
ଏହି ଯୋଗଦାନ ଏହି SSL VPN କେ ଯୁଦ୍ଧକ କରିବାରେ

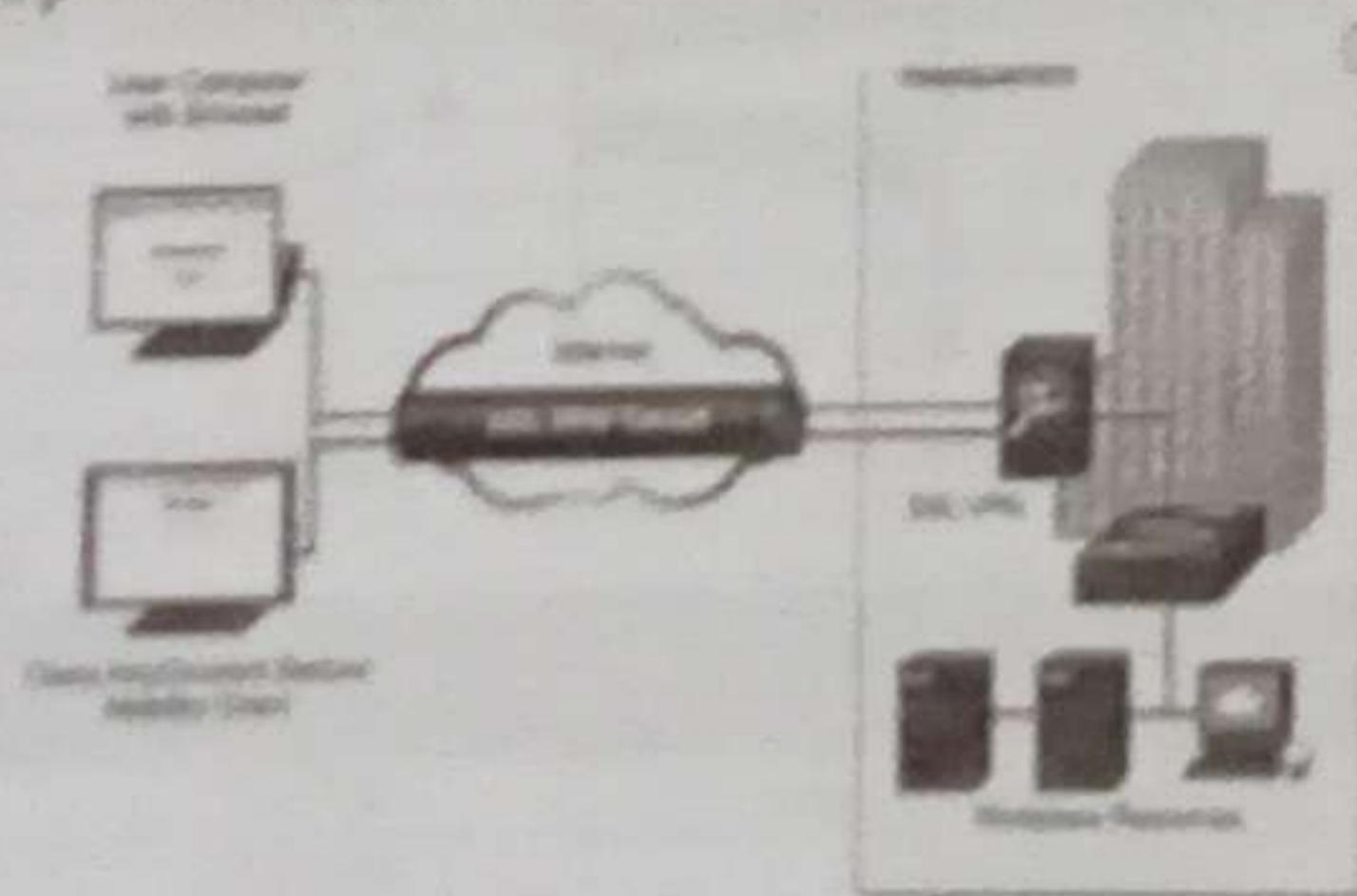


Figure TCP Three-Way Handshake

Q-36) HTTPS के द्वारा कौन सी Website का संचरण किया जाता है ?

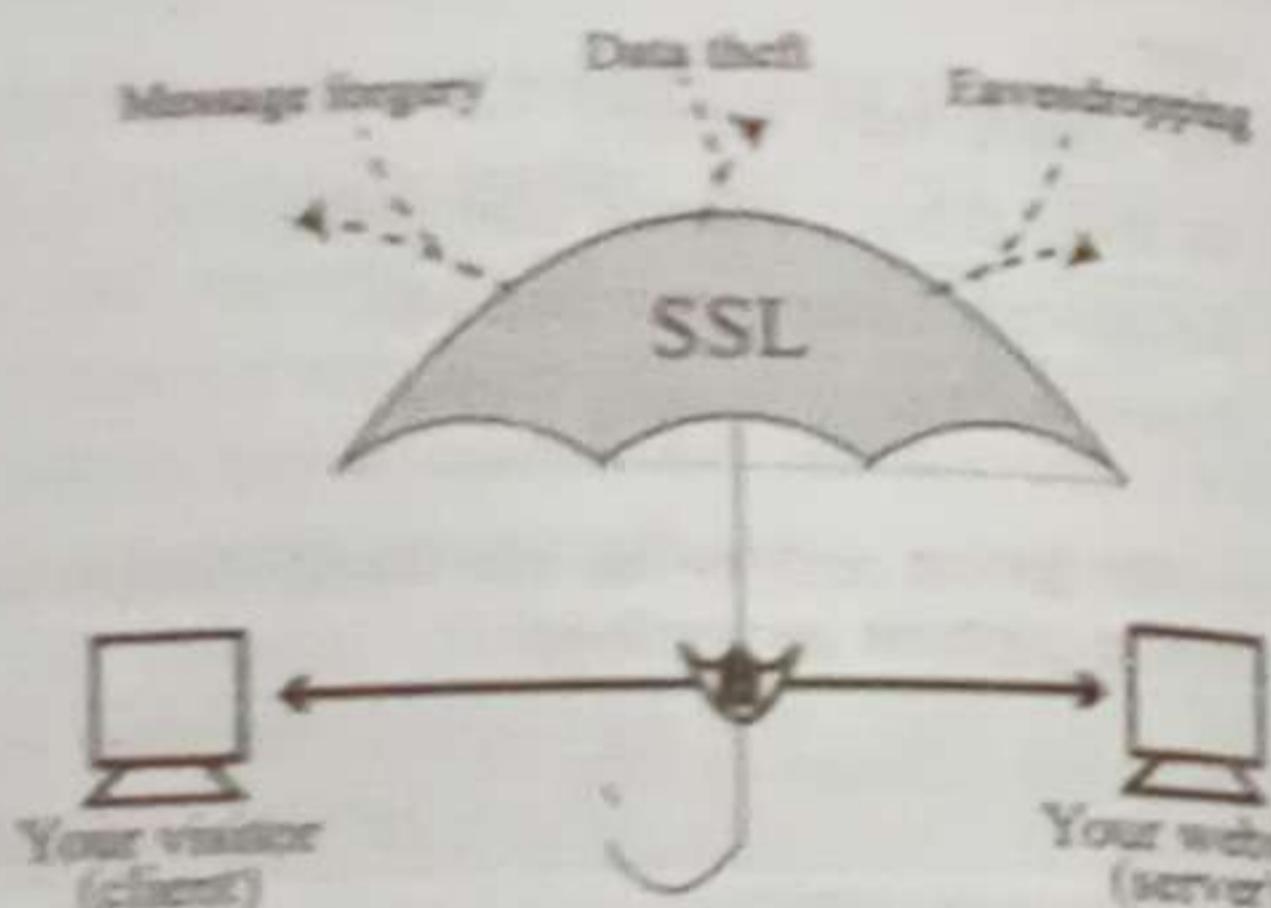
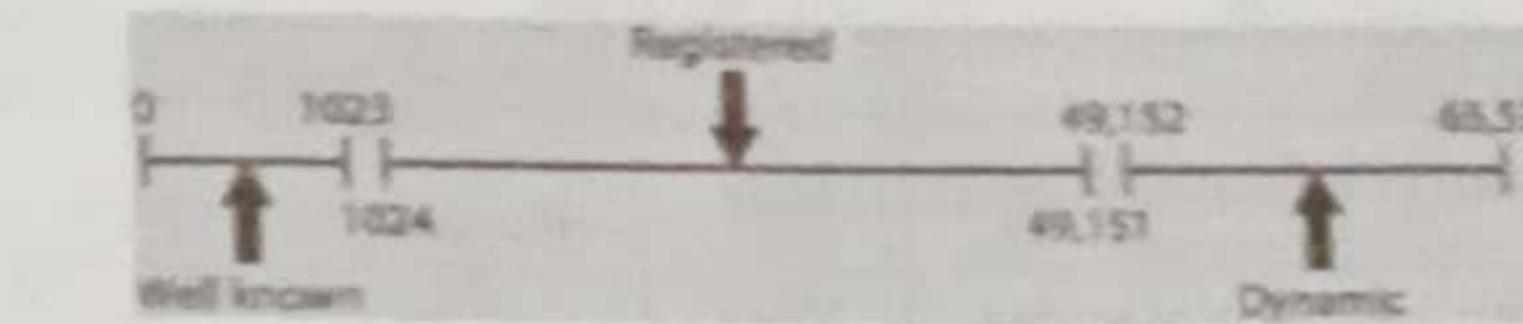
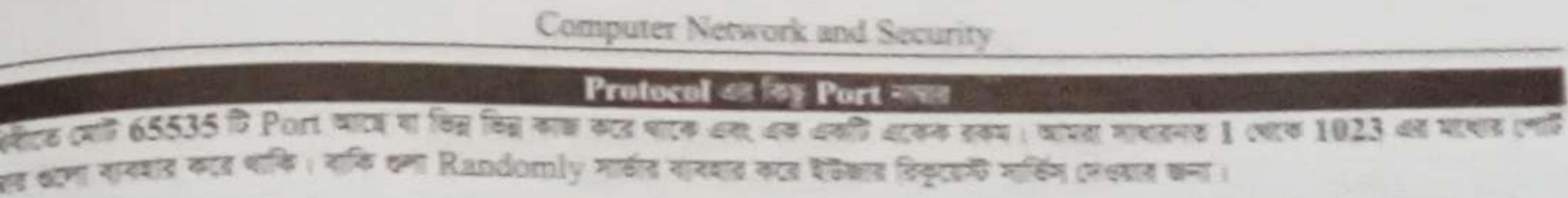


Figure: HTTPS Block Virus

Ques-20) TCP 3-Way Handshake क्या है? (What is TCP 3-Way Handshake?)



TCP/UDP Protocol ଏଇ ନିତ୍ୟ ଲିଙ୍କ୍ସ୍ ପୋର୍ଟ କାମ କେଣା ?

Port Number	TCP/UDP Protocol	Description or Comments
7	Echo	Echo (one-to-all, one-to-one) is a group communications protocol
20	FTP	File Server for File Control
21		File Server for File Transfer
22	SSH or SCP	Secure Shell or Secure Copy Protocol
23	Telnet	Telertype Network Protocol
25	SMTP	Simple Mail Transfer Protocol
53	DNS	Domain Name System
67	DHCP	Dynamic Host Configuration Protocol
68		
69	TFTP	Trivial File Transfer Protocol
70	Gopher	Gopher is an Internet protocol used for distributed storage of document
80	HTTP	Hyper Text Transfer Protocol
110	POP3	Post Office Protocol Version 3.0
123	NTP	Network Time Protocol
143	IMAP4	Internet Message Access Protocol 4
161	SNMP	Simple Network Management Protocol
162		
179	BGP	Border Gateway Protocol
318	TSP	Tunnel Setup Protocol
443	HTTP over SSL	Hyper Text Transfer Protocol over Secure Socket Layer
465	SMTP over SSL	Simple Mail Transfer Protocol over Secure Socket Layer
520	RIP	Routing Information Protocol
521	RIPng (IPv6)	Routing Information Protocol next generation
554	RTSP	Real Time Streaming Protocol
546	DHCPv6	Dynamic Host Configuration Protocol version 6
547		
587	SMTP	Simple Mail Transfer Protocol
902	VMware Server	Virtual Machine Software Server
989	FTP over SSL	File Transfer Protocol over Secure Socket Layer
990		
993	IMAP4 over SSL	Internet Message Access Protocol 4 over Secure Socket Layer
995	POP3 over SSL	Post Office Protocol Version 3.0 over Secure Socket Layer

প্রশ্ন-১১) RAS কি? RAS এর Protocol গলো লিখ? RAS এর সীমাবদ্ধতা কী কী? (What is RAS? Write the protocols of RAS. Also write the limitation of RAS.)

উত্তর: RAS: Remote Access Service এবং Windows NT-তে Remote Access Software এর মাধ্যমে Telephone line এর সহায়গ্রাম দ্রবণী Computer দ্বারা মধ্যে সংযোগ স্থাপন করে তখন তাকে RAS বলে।

RAS এর Protocol গলো:

- Access Protocol
- Authentication Protocol
- Tunneling Protocol

RAS এর সীমাবদ্ধতা গলো:

- নিরাপত্তার অভাব।
- Public telephone line এর দুরকার হয়।
- Modem এর প্রয়োজন হয়।
- NT Operating System এর প্রয়োজন হয়।

প্রশ্ন-১২) TCP এবং UDP এর মধ্যে পার্থক্য গলো লিখুন। (What is the difference between TCP and UDP?) [DIP-12, BUET-MS-17]

উত্তর: TCP এবং UDP এর মধ্যে পার্থক্য গলো নিচেরূপ:

TCP	UDP
TCP এর পূর্ণরূপ হচ্ছে: Transmission Control Protocol.	UDP এর পূর্ণরূপ হচ্ছে: User Datagram Protocol.
TCP তথ্য প্রেসেন্সের আগে কম্পিউটার ভর্তোর মধ্যে একটি সংযোগ স্থাপন করে।	UDP একটি সিস্টেম ভেটা এবং কর্মসূচীর জন্য প্রস্তুত কিনা তা পরীক্ষা না করে সরাসরি ডেস্টিনেশন কম্পিউটারে ভেটা প্রেসেন্স করে।
ইহার কানেকশন টাইপ হচ্ছে: Connection Oriented.	ইহা কানেকশন টাইপ হচ্ছে: Connectionless.
ইহার নির্ভরযোগ্যতা অনেক বেশি।	ইহার নির্ভরযোগ্যতা অবিশ্বাস্য বা অধিক।
ইহার গতি ধীর।	ইহার গতি অতি দ্রুত।
ইহার হেডার সাইজ ২০ বাইটের।	ইহার হেডার সাইজ ৮ বাইটের।
TCP ভেটা স্বীকৃতি (Acknowledgement) নেব এবং যদি ব্যবহারকারী অনুরোধ করে তবে তা পুনরায় পাঠানোর ক্ষমতা রাখে।	এটি স্বীকৃতি (Acknowledgement) এবং করে না, বা এটি হারিয়ে যাওয়া ভেটা পুনরাবৃত্তি (Retransmit) করে না।
Application ভেটা ইন্টারফেস হচ্ছে Stream based.	Application ভেটা ইন্টারফেস হচ্ছে Message based.
ইহার Error Checking এর	ইহার Error Checking এর

পারফর্ম করে না।	পারফর্ম করে থাকে।
Handshake Protocol যেমন: SYN, SYN-ACK, ACK ব্যবহার করে।	Handshake Protocol ব্যবহার করেনা (তাই Connectionless Protocol.)
মানেজকৃত সকল ভেটা Retransmitted করতে পারে।	মানেজকৃত সকল ভেটা Retransmitted করতে পারে না।
TCP প্রক্রিয়া সাপোর্ট করে না।	UDP প্রক্রিয়া সাপোর্ট করে।
ইহার Overheads কম, তবে UDP এর চেয়ে বেশি।	ইহার Overheads বৃহৎ কম।
ইহা ছেট থেকে মাঝারি পরিমাণে ভেটার ক্ষেত্রে উপযুক্ত।	ভেটার পরিমাণ ছোট থেকে অচির হলে ইহা উপযুক্ত।
ইহা সেখানে ব্যবহার করা উচিত যেখানে ভেটা ট্রান্সিভারের ক্ষেত্রে নির্ভরযোগ্যতা বেশি দরকার।	ইহার সেখানে ব্যবহার করা উচিত যেখানে ভেটা সরবরাহের পত্তির বিষয়টি গুরুত্বপূর্ণ।
ইহার Application ও প্রোটোকল গলো হচ্ছে: FTP, Telnet, SMTP, IMAP ইত্যাদি।	ইহার Application ও প্রোটোকল গলো হচ্ছে: DNS, BOOT Strap, DHCP, TFTP ইত্যাদি।

প্রশ্ন-১৩) HDLC প্রটোকল কী এর বিভিন্ন বৈশিষ্ট্যসমূহ ব্যাখ্যা কর। (What is HDLC Protocol? Mention its characteristics.) [BPSC-2014]

উত্তর: HDLC (High-level Data Link Control) হলো General Purpose Protocol যা OSI রেফারেন্স মডেলের ভেটা লিঙ্ক লেভেলের কাজ করে এবং Physical Layer এর Services এ ব্যবহৃত হয়। তাছাড়া ট্রান্সিভার এবং রিসিভার মধ্যে একটি নির্ভরযোগ্য পথের ব্যবহা করে।

HDLC প্রটোকলের বৈশিষ্ট্যসমূহ:

- Station types
 - Primary station
 - Secondary station
 - Combined station
- Configurations
 - Unbalanced
 - Balanced
 - Symmetrical
- Response modes
 - Normal Response Mode (NRM)
 - Asynchronous Balanced Mode (ABM)
 - Asynchronous Response Mode (ARM)

প্রশ্ন-১৪) PPP এর ফ্রেম ফরম্যাট দেখো এবং এটিটি ফিল্ড বর্ণনা কর। (Show the Frame formate of PPP and Explain each fields.) [BPSC-12, Multiple Ministry-16]

উত্তর: নিচের চিত্রে PPP (Point-to-Point-Protocol) এর Frame Format দেখানো হলো:

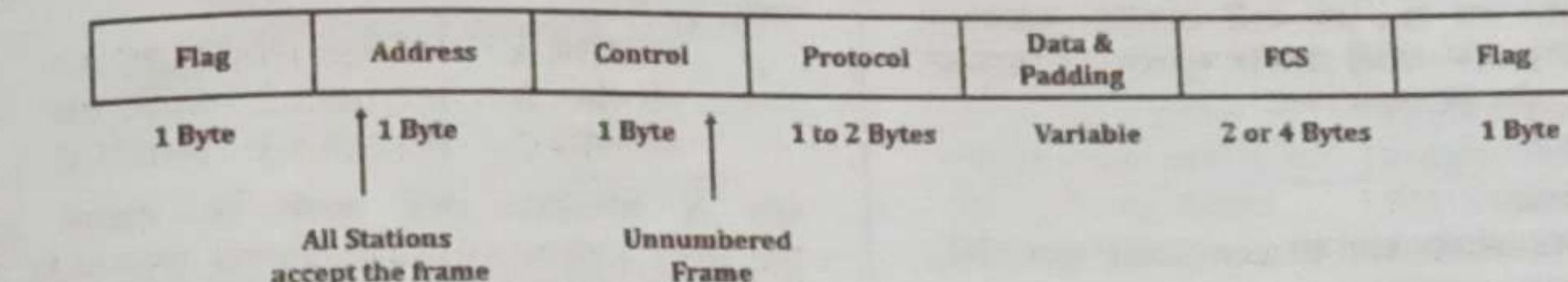


Figure: PPP (Point-to-Point-Protocol) Frame format

PPP (Point-to-Point-Protocol) এর Frame Format HDLC Frame Format এর মতোই। নিচে ইহার বিভিন্ন ফিল্ডের বর্ণনা করা হলো:

Flag field:

- ✓ PPP Frame সবসময় স্টার্টড HDLC Flag সহকারে শুরু এবং শেষ হয়।
- ✓ ফ্লাগ বাইট ১ বাইটের হয় এবং ইহা 01111110

a) Address field:

- ইহা ১ বাইটের ফিল্ড এবং সবসময় 11111111 হয়।
- এই আর্ড্রেস হচ্ছে প্রক্রিয়া আর্ড্রেস।
- আর্ড্রেস ফিল্ডের সবও গলো 1's দ্বারা বৃক্ষায় যে সব স্টেশন ফ্রেম একচেন্ট করতে পারবে।

b) Control field:

- ✓ কন্ট্রোল ফিল্ড ও ১ বাইটের হয়।
- ✓ HDLC এর মধ্যে এই ফিল্ড U-frame (unnumbered ফরম্যাট ব্যবহার করে।
- ✓ ইহার ভ্যালু সবসময় 00000011 দ্বারা বৃক্ষায় যে, এই ফ্রেম কোনো সিকুরিটি নাম্বার ব্যবহার করেনা।
- ✓ এই ফিল্ডে কোন flow control বা error control নেই।

c) Protocol field:

- ✓ ভাটা ফিল্ডে কোন প্রকারের ভেটা থাকবে তা প্রোটোকল ফিল্ড টিক করে দেয়।
- ✓ ইহা ব্যাহারকারীর ভেটা বা অন্যান্য তথ্য ব্যবহার করে।

d) Data field:

- ✓ ইহার দৈর্ঘ্য ভেরিয়েবল টাইপের।
- ✓ যদি লাইন সেট আপের সময় LCP ব্যবহার করে দৈর্ঘ্য টিক না করা হয়, তাহলে ডিফল্ট লেখ ১৫০০ বাইট ব্যবহার করা হয়।
- ✓ ইহা ব্যাহারকারীর ভেটা বা অন্যান্য তথ্য ব্যবহার করে।

e) FCS field:

- ✓ FCS এর অর্থ হচ্ছে Frame Check Sequence
- ✓ ইহা 2 বা 8 বাইটের হয়ে থাকে।
- ✓ ইহা চেকসাম (checksum) ব্যবহার করে।

প্রশ্ন-১৫) DHCP কি? কিভাবে কাজ করে? (What is DHCP?

How it works?) [BTCL-17, BB-17]

উত্তর: DHCP হলো Dynamic Host Configuration

Protocol এটি ইন্টারনেট প্রটোকলের মধ্যে কাজ করে। network এর ক্লাইট কম্পিউটারে সংযোগ আইপি এড্রেস বিতরণ করে। কোন নেটওয়ার্কের টার্মিনাল গলো একে অপরের সাথে আইপি এড্রেসের মাধ্যমে যোগাযোগ করে। আর সেই আইপি এড্রেস সাধারণত আমরা টিক করে দেই। কিন্তু DHCP প্রোটোকল একটি থাকলে এর মাধ্যমে আইপি না বসিয়ে দিলেও একটি আইপি পেয়ে যাবে। এই ধরন আপনার যোবাইল যন্ত্রে কোন একটি ওয়াইফাই নেওয়ার্কে যুক্ত হয় তখন

একটি সংযোগ আইপি পেয়ে যায়। DHCP সার্ভার মূলত, নেটওয়ার্কে আইপি টিক করে দেয়। সাধারণত, গেটওয়ের রাউটার DHCP সার্ভিস প্রদান করে থাকে।

প্রশ্ন-১৬) DNS কি? (What is DNS?)

উত্তর: DNS হল IP address কে ইংরেজী অক্ষরের কিছু স্ট্রিং এবং সাথে মাল্টিপল করা। DNS একটি URL (www.google.com) কে IP টিকানাতে ক্লিক করে। IP Address কে খুব সহজেই ব্যবহারযোগ্য করে তোলার জন্য ইংরেজী অক্ষরের কোন নাম ব্যবহার করা হয়। কারেক্টর ফর্মে (Form) দেওয়া কম্পিউটারের একটি

নামকেই বলে ডোমেইন নেম (Domain Name) যেমন-IP Address ৫ 203.91.139.2 এর পরিবর্ত্তন bijoy.net. কোমেন নেম ব্যবহার করা যায়। ইন্টারনেট সুব্যবস্থার শত শত এলাকায় বিভিন্ন। এগুলোকে ডোমেইন বলে হয়। এক একটি ডোমেইনে অনেকগুলো হোস্ট বা কম্পিউটার থাকে। এতিথে ডোমেইন কতগুলো সাব ডোমেইনে বিভক্ত থাকে। ডোমেইন দুই ধরনের। যথা:

1. Generic
2. Countries

Generic: প্রচলিত ডোমেইন গুলো হল .com, .edu, .gov, .int, .mil, .net, .org.

Countries: ডোমেইন হিসেবে ব্যবহার করার জন্য প্রতিটি দেশের সংক্ষিপ্ত নাম ব্যবহার করা হয়। যেমন: .bd (বাংলাদেশ), .pk(পুরুষাজ), .in(ভারত)।

প্রশ্ন-১৭) DNS & DHCP Server এর মধ্যে পার্থক্য লিখ? (What is the difference between DNS and DHCP?)

উত্তর: DNS & DHCP server এর মধ্যে পার্থক্য নিম্ন দেখো হল:

DNS	DHCP
এর পূর্ণান্বয় হল Domain Name System.	এর পূর্ণান্বয় হল Dynamic Host Configuration Protocol.
Active directory তৈরি করতে হয়।	Active directory তৈরির মুৰ প্রয়োজন নেই।
Automatic IP address তৈরির ব্যবহাৰ আছে।	তৈরির ব্যবহাৰ আছে।

প্রশ্ন-১৮) HTTP প্রটোকল কি? (What is HTTP protocol?)

উত্তর: HTTP এর পূরো নাম Hyper Text Transfer Protocol.

হাইপারটেক্সট প্রটোকল ডেটা যোগাযোগের জন্য ব্যবহৃত একটি আপ্লিকেশন প্রটোকল। এটি ওয়ার্ক ওয়াইট ওয়েবে ডেটা যোগাযোগের ভিত্তি। এটি ওয়েবে প্রাইভেট ভিত্তির জন্য একটি স্ট্যান্ডার্ড সরবরাহ করে যা ব্যবহারকারীদের ইন্টারনেটের মাধ্যমে তথ্য বিনিয়ন করতে সহায়তা করে।

প্রশ্ন-১৯) ICMP প্রটোকল কি? (What is ICMP protocol?)

উত্তর: ICMP এর পূর্ণান্বয় হল Internet Control Message Protocol. এটি ইন্টারনেট প্রটোকল সুইটের একটি ভর্তুপূর্ণ Protocol. এটি এমন এক ধরণের প্রটোকল যার মাধ্যমে নেটওয়ার্ক তথ্য ইন্টারনেট কানেক্টিভিটির নিয়ন্ত্রণ এবং কোর ট্রাকলশুটিং করা যায়। নেটওয়ার্ক সেক্টরে এটি সবচেয়ে বড় ব্যবহৃত প্রটোকল। ICMP একটি Layer-3 প্রটোকল। ICMP প্রটোকলের মাধ্যমে নেটওয়ার্কের বিভিন্ন সমস্যা ডায়াগনসিস করা হয় এবং আইপি অপারেশনে কোন সমস্যা তৈরী হলে একটি ICMP Message এর মাধ্যমে তা সোর্স হোষ্টকে অবহিত করা হয়। একটি ICMP Message এর বিভিন্ন ধরণের Type & Code রয়েছে।

প্রশ্ন-২০) ARP কি? ARP কিভাবে কাজ করে? (What is ARP protocol? and How it works?)

উত্তর: ARP হলো Address Resolution Protocol. নেটওয়ার্কের ইন্টারনেটের ম্যাক এড্রেস এবং হোস্ট আইপি সংযোগ করে। মন করি, একটি নেটওয়ার্কে তিনটি কম্পিউটার স্বতন্ত্র মাধ্যমে বৃক্ত আছে।

কম্পিউটার A	192.168.1.1	MAC AA
কম্পিউটার B	192.168.1.2	MAC BB
কম্পিউটার C	192.168.1.3	MAC CC

এখন A কম্পিউটার থেকে আপনি পিঁ করলেন: ping 192.168.1.3 সুইচের ARP টেবিল ঢেক করে দেখেন MAC CC তে 192.168.1.3 আইপি আছে। তাই সে যোগাযোগ করবে।

যদি এই টেবিলে 192.168.1.3 আইপি না থাকে তবলে সে এই কাঁকা বা খালি প্যাকেট ব্রডকাস্ট করবে “কার আইপি 192.168.1.3 সবাই এই প্যাকেটটি পাবে এবং যার আইপি ফিল্বে সে Reply পাঠাবে ম্যাক এড্রেসসহ। তখন ARP টেবিল আপডেট হবে। যুক্তি নির্দিষ্ট সময় পর পর ARP লিট আপডেট করবে। কোন মাধ্যম নেটওয়ার্ক থেকে বাইরে চলে গেলেও একই ভাবে ARP Reply হবে।

প্রশ্ন-২১) সেলুলার নেটওয়ার্ক হ্যান্ডঅফ কিভাবে কাজ করে?

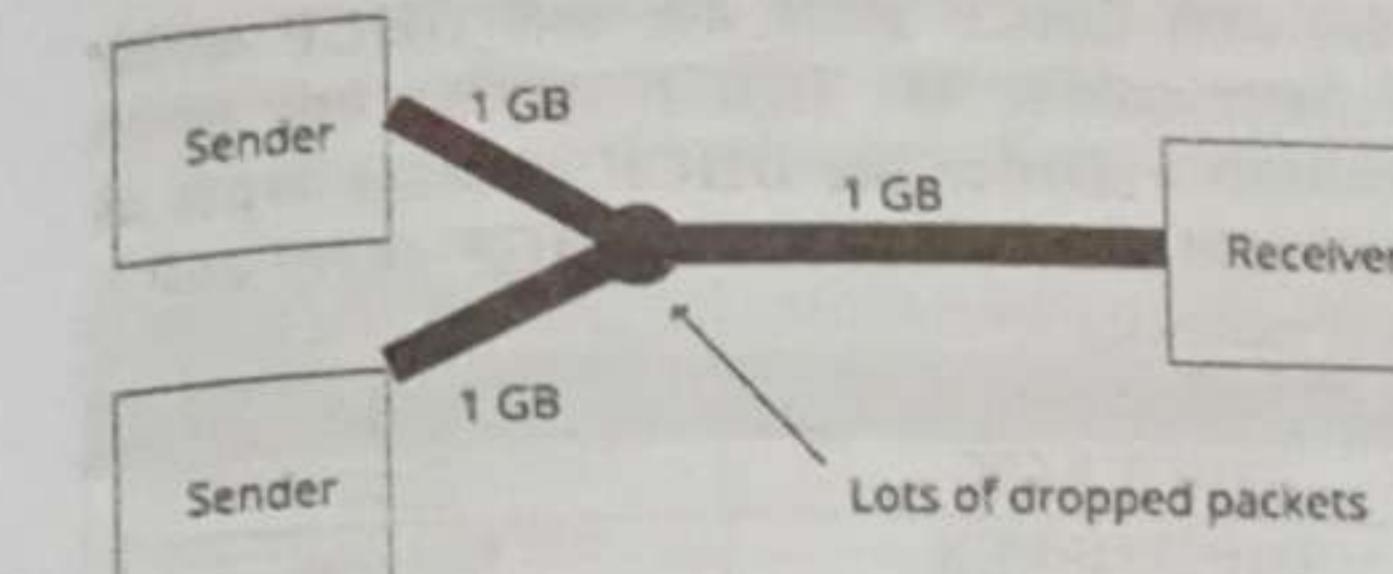
উত্তর: হ্যান্ডঅফ হল একটি চ্যানেল থেকে অন্য চ্যানেল সক্রিয় কল বা ডেটা সেশন ছানাক্ত করার প্রক্রিয়া। স্যাটেলাইট যোগাযোগে, এটি এক পৃথিবী স্টেশন থেকে অন্য ছানে ছানাক্ত করা প্রক্রিয়া। একজন কলার বা ডেটা সেশন ব্যবহারকারী বাইন পরিবেরার জন্য হ্যান্ডঅফ প্রয়োজন। হ্যান্ডঅফকে হ্যান্ডওভার কলা হয়।

হ্যান্ডঅফ কিভাবে কাজ করে: মোবাইল আসিস্টেট হ্যান্ডঅফ (MAHO) এমন একটি কৌশল যা মোবাইল ডিভাইস সাহায্যে সে স্টেশন কন্ট্রোলারকে (BSC) অন্য একটি বিএসসিস্টেট(BSC) ক্ষেত্রে ছানাক্ত করতে সহায়তা করে। এটি GSM সেলুলার নেটওয়ার্কের ব্যবহৃত হয়। হ্যান্ডঅফটি কেবলমাত্র মোবাইল ডিভাইসের জন্য অশ্বারূহ ছাড়াই BSC এবং মোবাইল সুইচিং সেন্টারের (MSC) কাজ করে। তবে, GSM এ যখন কোন মোবাইল স্টেশন যোগাযোগের জন্য সময় সুটি ব্যবহার না করে, তখন এটি নিকটস্থ বিএসসি সিগনাল্যারের তদনান পরিয়াপ্ত করে এবং বিএসসিস্টেট(BSC) এই প্রেরণ করে। বিএসসি এই তথ্য অনুসারে হ্যান্ডঅফ করে।

প্রশ্ন-২২) Congestion Control কি? Congestion Control কিভাবে দূর করা যায়? (What is Congestion control? How can be Congestion Control remove?)

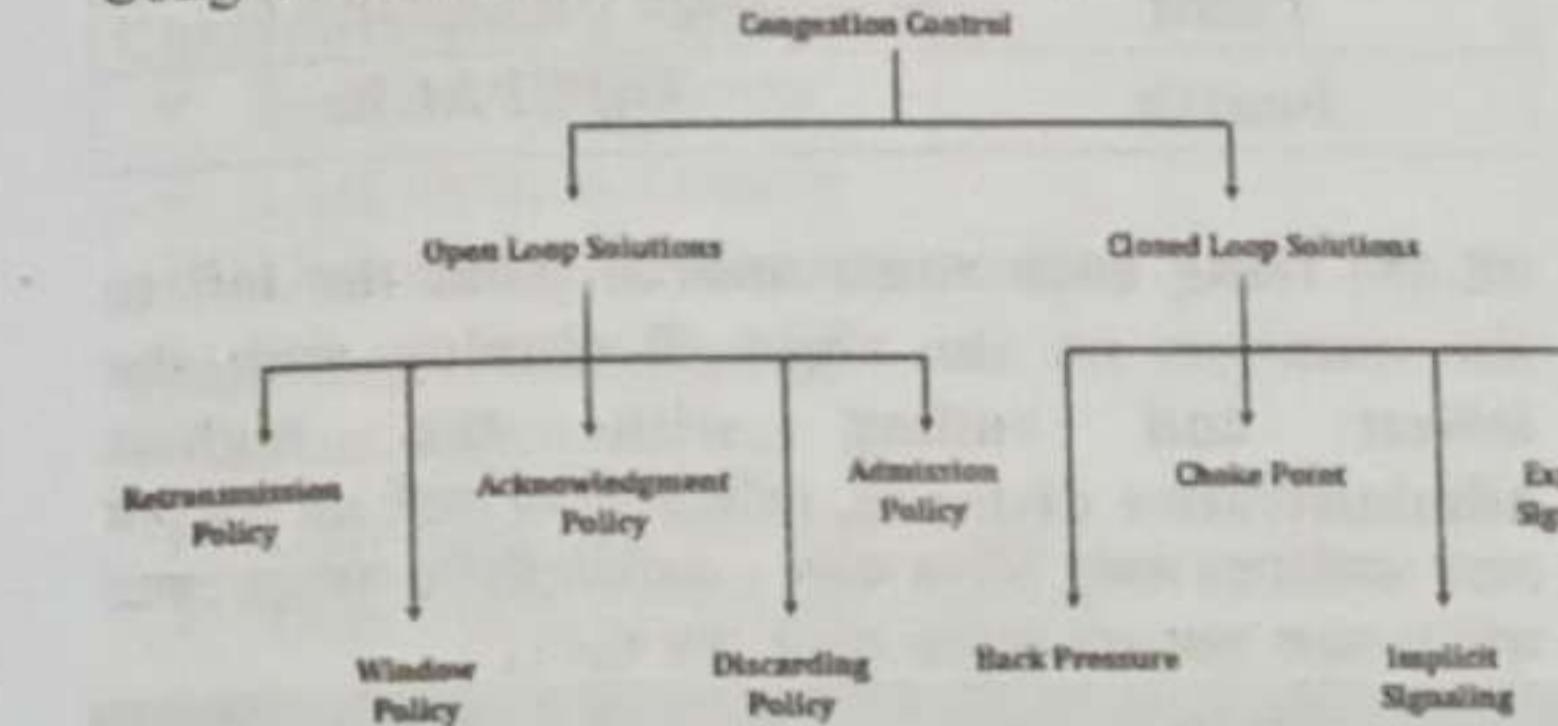
উত্তর: Congestion Control: যখন নেটওয়ার্কের লোড, ইয়ে ধূরণ ক্ষমতার (Capacity) চেয়ে বেশি হয়ে যাব তখন তারে Congestion বলে। [In English: Congestion in network may occur if the load on the network is greater than Capacity of network]

প্যাকেট সুইচ নেটওয়ার্কে সেভারের ডাটা প্যাকেট সাইজ বা পার্কে সংখ্যা নেটওয়ার্কে ব্যবহৃত নেটওয়ার্ক ডিভাইসের ইনপুট বাসগুলো তে বেশি বা বড় হলে Congestion হয়, লোড বেড়ে যাব যাব নেটওয়ার্কের গতি কমে যায়।



এখনে দুইটি সেভার ডাটা পাঠাবে, একটি সেভার ডাটা পাঠানোর পর নেটওয়ার্ক লেয়ার ডিভাইস এর ইনপুট বাকার ফুল হলে বিভীষণ সেভার এর ডাটা রিসিভ করতে পারবেনা ইহাকেই Congestion বলা হয়।

কিন্তু মেকানিজম এবং টেকনিক এর মাধ্যমে Congestion দূর করাকে Congestion Control বলে। Congestion Control দূর করার টেকনিক সমূহ:



প্রশ্ন-২৪) Compare and contrast between IP TV and VoIP. (আইপিটিভি এবং ভিপিআইপি এর মধ্যে পার্থক্য লিখুন।)

উত্তর: IP TV: IP TV কর্তৃত কর্তৃত এবং “স্ট্র্যাট টিভি” হিসাবে পরিচিত, আইপিটিভি (ইন্টারনেট প্রটোকল টিভি) একটি transmission প্রটোকল যা কোনও আয়নে, স্যাটেলাইট বা তারের পরিবর্তে উচ্চ গতির ইন্টারনেট সংযোগের মাধ্যমে ডেটা প্যাকেট প্রেরণ করে একটি Managed নেটওয়ার্কের মাধ্যমে টেলিভিশন প্রোগ্রাম দিয়ে।

VOIP: ভয়েস ওভার ইন্টারনেট প্রটোকল (ভিপিআইপি), এমন একটি প্রযুক্তি যা আপনাকে নির্যামিত (বা আয়নালগ) ফোন লাইনের পরিবর্তে ব্রডব্যাংক ইন্টারনেট সংযোগে ব্যবহার করে ভয়েস কল করতে দেয়।

প্রশ্ন-২৫) What is DNS? TCP/IP is used in DNS?

উত্তর: Domain Name System (DNS) হোস্টনের এবং ডোমেইন নাম তালি ইন্টারনেটে আইপি আয়নেস ক্রান্তির করার জন্য একটি ব্যবহাৰ। যা TCP/IP প্রটোকল ব্যবহার করে। প্রতিটি IP Address এর বিপরীতে একটি করে Domain Name আছে। আপনি Domain Name লিখেও ওভার সাইট আয়েস করতে পারবেন বা IP Address লিখে। যেহেতু IP Address মনে রাখা কঠিন তাই DNS System বিহয়িকে সহজ করেছে। মনে করুণ আপনি bitboxbd.com ওয়েবসাইটে ব্রাউজ করতে ক্লিকনাটি লিখলেন browser তার Cache এ DNS Record ঘোজ করে Corresponding IP Address পাওয়া যায় কিনা যদি পাওয়া যায় তাহলে Domain Name কে IP Address এ কনভার্ট করবে, আর যদি পাওয়া না যায় তাহলে DNS Server এ ঘোজ করা হয় এবং domain name কে IP Address এ কনভার্ট করে প্রাঙ্গন আপনার ব্রাউজারে প্রদর্শন করা হবে।

Yes, TCP/IP is used in DNS.

প্রশ্ন-২৬) Distinguish Between HTTP and HTTPS. (HTTP এবং HTTPS এর মধ্যে পার্থক্য লিখুন।)

উত্তর: নিম্ন HTTP এবং HTTPS এর মধ্যে পার্থক্য দেখো হলো:

HDLC	PPP
HDLC এর পূর্ণরূপ হচ্ছে for High-level Data Link Control.	PPP এর পূর্ণরূপ হচ্ছে Point-to-Point Protocol.
HDLC একটি বিট অরিয়েটেড	PPP একটি বাইট অরিয়েটেড

HTTP	HTTPS
ইন্টারনেটের প্রার্টোকল HTTP হচ্ছে Hyper Text Transfer Protocol এর সংক্ষিত রূপ।	ইন্টারনেটের প্রার্টোকল HTTPS হচ্ছে Hyper Text Transfer Protocol Secure এর সংক্ষিত রূপ।
Unsecured.	HTTP-এর একটি এক্সেনশন (Extension) হচ্ছে HTTPS। তাই বলা যায় যে, HTTP অপেক্ষা HTTPS অধিক নিরাপদ।
Application layer এ ব্যবহার হচ্ছে।	Transport layer এ ব্যবহার হচ্ছে।
Encryption করা হচ্ছে না।	Encryption ব্যবহার হচ্ছে।
Certificate সরকার হচ্ছে না।	Certificate সরকার হচ্ছে।
পোর্ট নাম্বার হলো: 80	পোর্ট নাম্বার হলো: 443.
man-in-the-middle eavesdropping attacks হচ্ছে পারে।	man-in-the-middle and eavesdropping attacks অভিহত করতে পারে।
উদাহরণ: internet forums, educational sites.	উদাহরণ: Banking Websites, Payment gateway, Shopping Websites, etc.

প্রশ্ন-২৭) মনে করুন, আপনি একজন প্রকৌশলী। আপনাকে একটি ক্লাউডে ওয়ার্কস্টেশনে নেটওর্ক কনফিগুরেশন প্যারামিটার যাচাই করার দায়িত্ব দেওয়া হয়েছে এবং তিনি শিক্ষার কাছে রিপোর্ট করার জন্য বলা হয়েছে। সেই অনুযায়ী বামপাশের নেটওর্ক প্যারামিটার এর সাথে ডানপাশের নেটওর্ক প্রক্রিয়ার তালু সন্মত করুণ।

Network Configuration Parameters	Node Identifiers
192.168.1.120	Broadcast Address
192.168.1.255	Default Gateway
192.168.1.1	Host IP Address
192.168.1.254	MAC Address
B8-76-3F-7C-57-DF	Last Assignable IP Address in the Subnet

Network Configuration Parameters	Node Identifiers
192.168.1.120	Host IP Address
192.168.1.255	Broadcast Address
192.168.1.1	Default Gateway
192.168.1.254	Last Assignable IP Address in the Subnet
B8-76-3F-7C-57-DF	MAC Address

প্রশ্ন-২৮) একটি DHCP ক্লায়েন্ট এবং একটি DHCP সার্ভার যেখানে যেভাবে মেসেজ হচ্ছে। DHCP মেসেজের ধরণ অনুসরে সার্ভারে সার্জান। (Order the DHCP message types as they would occur between a DHCP client and a DHCP server.)

DHCP Message	Order
DHCPACK	First
DHCPOFFER	Second
DHCPDISCOVER	Third
DHCPREQUEST	Fourth

উত্তর:

Order	DHCP Message
First	DHCPDISCOVER
Second	DHCPOFFER
Third	DHCPREQUEST
Fourth	DHCPACK

প্রশ্ন-২৯) Drag each route source from the left to the numbers on the right. Beginning with the lowest and ending with the highest administrative distance. (প্রতিটি রুটের সের্ভিস এর বাবে নির্বাচিত করে তাকে ক্লিয়েড করতে পারে।) এভিনিউস্ট্রিট দূরবৃত্তে ক্লিয়েড করে সর্বোচ্চ দূরত্বে শেষ হবে।)

Route Source	Random Order
Connected	1
EBGP	2
EIGRP	3
OSPF	4
RIP	5
Static	6

উত্তর:

Right Order	Route Source
1	Connected
2	Static
3	EBGP
4	EIGRP
5	OSPF
6	RIP

[Note: EBGP: External Border Gateway Protocol
EIGRP: Enhanced Interior Gateway Routing Protocol; OSPF: Open Shortest Path First
RIP: Routing Information Protocol]

প্রশ্ন-৩০) ডানপাশের ২ প্রকারের নেটওর্কিং টাইপের সাথে বামপাশের নেটওর্কিং এর বৈশিষ্ট্য তালু চিহ্নিত করুন? (Drag and drop to the characteristics of networking from the left onto the correct networking types on the right.)

Characteristics of Networking	Control Based Networking	Traditional Networking
Focused on Network		
Focused on Devices		
User input is a Configuration		
User input is a policy		
Uses white list security model		
Uses black list security model		

উত্তর:

Controller-Based Networking:

- ✓ Focused on network
- ✓ User input is a policy
- ✓ Uses white list security model

Traditional Networking:

- ✓ Focused on devices
- ✓ User input is a configuration
- ✓ Uses black list security model

প্রশ্ন-৩২) ডানপাশের সংশ্লিষ্ট সেবার ক্লো বামপাশের ফার্শন ক্লোর সাথে মিলিয়ে দেখান। (সব ফার্শন ব্যবহৃত নাও হতে পারে।) [Match the functions to the corresponding layers. (Not all options are used)]

Functions	Corresponding Layers: Access Layers, Distribution Layer, Core Layer?
Provides high-speed Backbone connectivity	
Implements personal firewalls on the client computers	
Provides Networks access to the user	
Implements Networks access policy	
Represents the Networks edge	
Establishes layer-3 routing boundaries	
Function as an aggregator for all the campus blocks	

উত্তর:

Functions	Corresponding Layers: Access Layers, Distribution Layer, Core Layer?
Provides high-speed Backbone connectivity	Core layer
Implements personal firewalls on the client computers	
Provides Networks access to the user	Access layer
Implements Networks access policy	Distribution layer
Represents the Networks edge	Access layer
Establishes layer-3 routing boundaries	Distribution layer
Function as an aggregator for all the campus blocks	Core layer

প্রশ্ন-৩৩) বামপাশের WLAN কল্পনানেটস তলোর সাথে ডানপাশের সঠিক বর্ণনার মিলয়ে লিখুন।

Dynamic Interfaces	Device that provides Wi-Fi devices with a connection to wired network
Access Point	Device that manages access points
Service Port	Used to support mobility management of the WLC
Virtual Interface	Applied to the WLAN for wireless client communication
Wireless LAN Controller	Used for out of band management of a WLC

উত্তর:

Device that provides Wi-Fi devices with a connection to wired network	Access Point
Device that manages access points	Wireless LAN Controller
Used to support mobility management of the WLC	Service Port
Applied to the WLAN for wireless client communication	Dynamic Interfaces
Used for out of band management of a WLC	Virtual Interface

প্রশ্ন-৩৪) বামপাশের AAA functions তলোর সাথে ডানপাশের AAA services তলোর মিল আছে? সঠিক উত্তর লিখুন।

AAA Functions	Which One? Authentication, Authorization, Accounting
Records user activities	
Restricts the services that are available to a user	
Identifies the user	
Control the action that a user can perform	
Provides analytical information for the network administrator	
Verified the password associated with a user	

উত্তর:

AAA Functions	Which One? Authentication, Authorization, Accounting
Records user activities	Accounting

Restricts the services that are available to a user	Authorization
Identifies the user	Authentication
Control the action that a user can perform	Authorization
Provides analytical information for the network administrator	Accounting
Verified the password associated with a user	Authentication

প্রশ্ন-৩৫) Drag the OSPF parameters to the correct places on the right. (OSPF প্যারামিটারের সাথে কোণটি সামঞ্জস্য তা লিখুন।)

OSPF Parameters	Must be Unique/ Must Match
Netmask	
OSPF Process ID	
Router ID	
IP Address	
Area ID	
Timers	

OSPF Parameters	Must be Unique/ Must Match
Netmask	Must Match
OSPF Process ID	Do not Need
Router ID	Must be Unique
IP Address	Must be Unique
Area ID	Must Match
Timers	Must Match

[Note: Process ID numbers between neighbors do not need to match for the routers to establish an OSPF adjacency. The OSPF process number ID is an internally used identification parameter for an OSPF routing process and only has local significance.]

প্রশ্ন-৩৬) VoIP কাকে বলে? ইহার ব্যবহার ও অ্যাপ্লিকেশন লিখুন। (What is VoIP? Mention its application.)

উত্তর: VoIP এর পূর্ণরূপ হলো- Voice over Internet Protocol. VoIP হচ্ছে ডেটা নেটওর্কের মেম ইন্টারনেটের মাধ্যমে টেলিফোন কল আদান-প্রদান করার বিশেষ পদ্ধতি। ইন্টারনেটের কলেজিয়া এক মাল্টিমিডিয়া অ্যাপ্লিকেশন ব্যবহার করে তাই, ডেটা ও ভিডিও আদান-প্রদান করার পদ্ধতিকে VoIP টেকনোলজি বলে। VoIP ইন্টারনেটের একটি চমকান্দ ব্যবহার।

এ VoIP টেকনোলজি বর্তমানে টেলিযোগাযোগের অন্যতম শর্করা হিসেবে ব্যবহৃত হচ্ছে। VoIP তে ডেটা নেটওর্ক, ইন্টারনেট বা IP নেটওর্কের মাধ্যমে Real time ভয়েস ডেটা সিগন্যাল আবাসন করা যায়।

প্রদান করা যায়। ১৯৯৬ সালে আন্তর্জাতিক টেলিমিডিয়ানিকেশন ইউনিয়ন (ITU) ইন্টারনেট প্রটোকল ব্যবহার করে ভয়েস ডেটা পাঠানোর স্ট্যান্ডার্ড নির্ধারণ করে দেয়। বর্তমান ইন্টারনেটের হাই স্পীড ব্যাট্টেইথ ব্যবহার করে ডেটা এবং ভয়েস উভই একই কানেকশনের মাধ্যমে আদান প্রদান করা যায়। VoIP এর মাধ্যমে অনেক কম খরচে কম্পিউটার এবং ইন্টারনেট কানেকশন ব্যবহার করে পৃথিবীর যে কোন প্রান্তের মাধ্যমে সাথে যতক্ষণ ইচ্ছা কর্ত্তা বলা যাবে।

VoIP এর ব্যবহার:

- a) টেলিফোন (Telephone)
- b) ফ্যাক্স (Fax)
- c) পিএবিএজ সিস্টেম (PABX System)
- d) ডোর ইন্টারকম (Door Intercom)

VoIP অ্যাপ্লিকেশন:

- a) নেট টু ফোন (Net 2 Phone)
- b) এমএসএল ম্যাসেজার (MSN Messenger)
- c) নেটমিটিং (NetMeeting)
- d) কুল টক (Cool Talk)
- e) স্কাইপ (Skype)

প্রশ্ন-৩৭) VoIP কি পদ্ধতিতে কাজ করে? ব্যাখ্যা করুণ।

(How does VoIP work? Explain.

উত্তর: প্রচলিত পদ্ধতির টেলিফোন Public Switched Telephone Network (PSTN) ব্যবহার Circuit Switching পদ্ধতি ব্যবহার করে ডেটা আদান-প্রদান করা হয়, ফলে এতে ফোন লাইন ব্যাস্ত থাকলে অন্য ব্যবহারকারীকে লাইন ছিঁ না হওয়া পর্যন্ত অপেক্ষা করতে হয়। কিন্তু VoIP টেলিফোনে এ অনুধাব দূর করার জন্য Circuit Switching-এর পরিবর্তে Packet switching পদ্ধতি ব্যবহার করা হয়। VoIP গেটওয়ে PSTN থেকে প্রাপ্ত ভয়েস ডেটাকে সংকুচিত করে প্যাকেট ডিজিটাল সিগন্যালে রূপান্তর করে। অতঃপর তা IP নেটওর্কের মাধ্যমে আদান-প্রদান করে। কৃত কৃত প্যাকেট আকারে ডেটা প্রেরণ করা হয় বলে একই সময় একই চ্যানেলে ব্যবহার করে একাধিক কল আদান-প্রদান করা যায়। তাই এ পদ্ধতিতে একই সময়ে বেশি কল করা যায়।

প্রশ্ন-৩৮) ACL কাকে বলে? কত প্রকার ও কি কি? ACL এর কাজ সংক্ষেপে লিখুন। (What is ACL? Classify it and Define its function is shortly.)

উত্তর: ACL: ACL এর পূর্ণরূপ হল Access Control List. Access Control List সাধারণত ব্যবহার করা হয় প্যাকেট ফিল্টারিং এর জন্য। Access Control List সাধারণত দুই ধরনের হয়ে থাকে। যেমন:

- a) Standard ACL এবং
- b) Extended ACL.

যদি এমন হয় যে, কোন বিশেষ কম্পিউটার নিদিষ্ট কোন হোস্ট বা সার্ভারের সাথে কমিউনিকেশন করতে পারবে না সেখানে ACL এর মাধ্যমে এই কাজটি করা যায়। ACL এর মাধ্যমে যে কোন হোস্টকে অন্য যে কোন হোস্ট এর সাথে যোগাযোগ করা থেকে বিরুদ্ধ রাখা যায়। ACL এর মাধ্যমে কোন হোস্টকে অন্য কোন হোস্ট এর জন্য শুধু

Block করার জন্যই নয় প্রয়োজনে কোন হোস্ট এর জন্য কোন প্রটোকলকেও Block করা যায়।

প্রশ্ন-৩৯) ACL ব্যবহার করার উদ্দেশ্য কোন কি? (Write the purposes of using ACL?)

উত্তর: নিচের উদ্দেশ্য তলো ব্যবহারের জন্য আমরা ব্যবহার করে থাকি। যেমন:

- ✓ ট্রাফিক নিয়ন্ত্রণ করার জন্য অর্ধাং ACL এর মাধ্যমে বলে দেয়া যায় কোন ট্রাফিক তলো আগে Access পাবে আর কোন তলো পাবে না।
- ✓ রাউটিং অপেক্ষে কাজের জন্য অর্ধাং রাউটার তলো তাদের নিজেদের মধ্যে রাউটিং অপেক্ষে বিনিয়ন করে। বাইরে থেকে কোন রাউটার এর অপেক্ষে যেন রাউটিং টেবিল মুক্ত হয়ে কোন ট্রাফিক তৈরি না করে সেজন্য একসেস কন্ট্রোল লিস্ট ব্যবহার করা যায়।
- ✓ আইপি প্যাকেট ফিল্টারিং অর্ধাং একসেস কন্ট্রোল লিস্ট এর মাধ্যমে অন্তর্মুখী ও বাইর্গামী প্যাকেটগুলো ফিল্টার করে নেটওর্কে Highly Secure করা যায়।

প্রশ্ন-৪০) Standard ACL ও Extended ACL এর Range

ও তাদের সম্পর্কে সংক্ষেপে লিখুন। (Explain Standard ACL and Extended ACL range. Also explain them in shortly.)

উত্তর: Range Of ACL: প্রতিটি ACL এর একটি রেজ রয়েছে। এই রেজ এর নামার দেশেই রাউটার বুর্বতে পারে যে এটি কোন ধরনের ACL। নিচে ACL এর রেজ নামার তুলু ধরা হল।

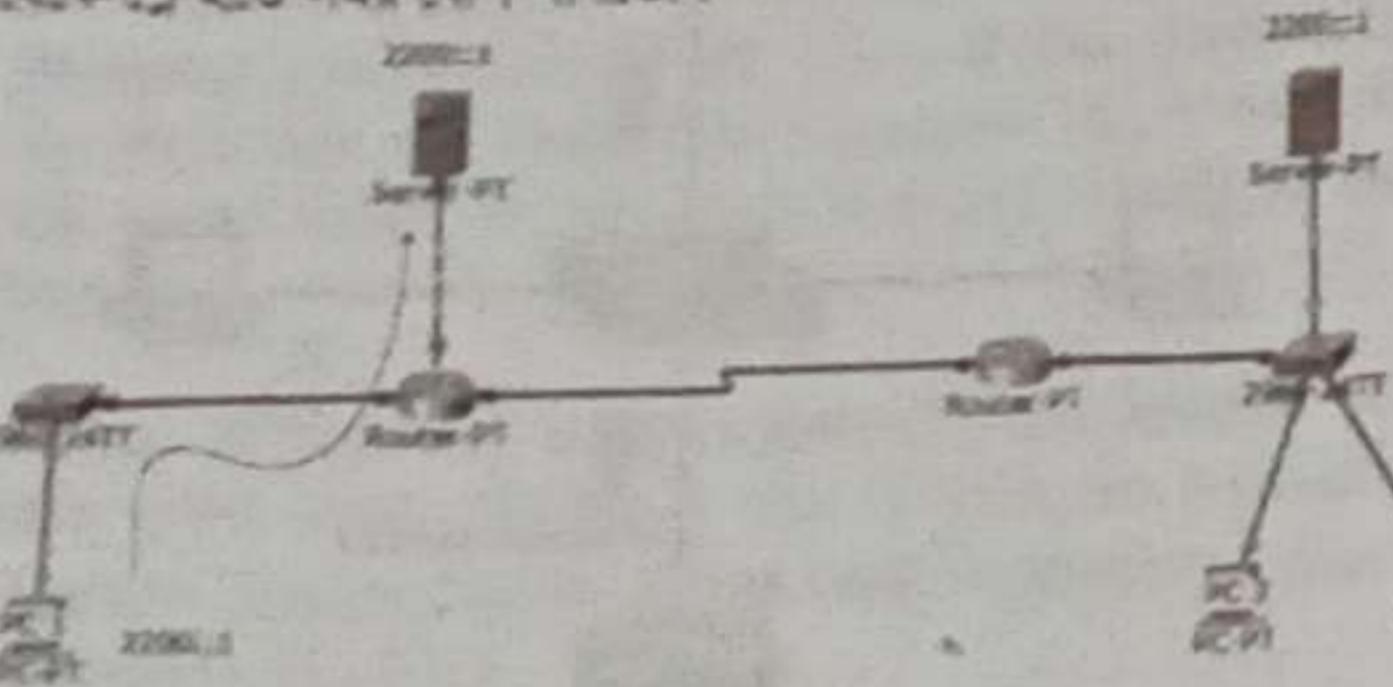
Range For Standard ACL: 1-99 and 1300-1999

Range For Extended ACL: 100-199 and 2000-2699

যখন ACL কে Implement করা হয়, তখন এই নামার সম্মত ব্যবহার করতে হয়। Standard ACL এর ক্ষেত্রে এই রেজ হল 1 থেকে 99 পর্যন্ত এবং 1300 থেকে 1999 পর্যন্ত নামার ব্যবহার করা হয়। যদি রাউটারে এই রেজ এর কোন ACL কে Implement করা থাকে তাহলে রাউটার সহজেই বুর্বতে পারে যে এটি Standard ACL। আর এই রেজ যদি 100 থেকে 199 এবং 2000 থেকে 2699 পর্যন্ত এর মধ্যে কোন নামার থাকে তাহলে রাউটার তখন বুর্বতে নেই যে এটি Extended ACL.

Standard ACL: Standard ACL অধুনাত্ম সোর্স অ্যাড্রেস নিয়ে কাজ করে। Standard ACL এ সোর্স অ্যাড্রেস কে কোন প্যাট্রোলুর হোস্ট এর জন্য Block করা যায়। Standard ACL Implement করার সময় ঘৰ্তা সংজ্ঞান এর কাছ

প্রাবে: আমরা যখন ইটিটির প্রাটেজ করি তখন আমরা নিকটবর্তী TCP/IP আইপি আড়েসকে ৫টি ভাগে ভাগ করা হয়েছে। দেখুন সার্ভার থেকে ভিত্তি প্রে হয়, না হল অনুরিকার মেইন ডাটা সেক্টোর থেকে প্রে হতে সবচেয়ে শাখাজোঠ।



শ্রেণি-৫) ভার্সন (Version) অনুসারে আইপি আড়েস কত ধরার কি কি? (How many types and what are the IP addresses according to the version?)

উত্তর: ভার্সন অনুসারে আইপি আড়েস দুই ধরার। যথা:

- a) IPv4 (আইপি প্রোটোকল ভার্সন 4)-32 bit
- b) IPv6 (আইপি প্রোটোকল ভার্সন 6)-128 bit

[Note: আইপি আড়েসিং এর জন্য কিছু কিছু মৌলিক বিষয় সম্পর্কে অবগত থাকা প্রয়োজন। দেখুন: Bit, Byte, Octet, Least Significant Bit (LSB), Most Significant bit (MSB), Host, Network Segment.]

IPv4 (ইন্টারনেট প্রোটোকল ভার্সন 4)

আমরা যে আইপি কলো ব্যবহার করি তা হলো IPv4. নিম্নে IPv4 সম্পর্কে আলোচনা করা হলো:

- ✓ IPv4: Total No of Octet: 4
- ✓ Total No of bits in each octet: 8
- ✓ Total No of bits = 32 (মানে IPv4 হলো 32 bits এর)

8 bit	8 bit	8 bit	8 bit
Octet	Octet	Octet	Octet

- ✓ Total No of IP addressing $2^{32} \geq 4.3\text{billion}$ (গ্রাহ)
- ✓ একটি Octet $2^8 = 256$ (0-255) পর্যন্ত Addressing করে।
- ✓ Starting (Binary Value) = 00000000=0 (Decimal Value)
- ✓ Ending (Binary Value) = 11111111=255 (Decimal Value)

[Note: আমরা তথাকথি Octet দেখেই বুঝতে পারবো যে IP কি কেন কৈলে IP Address.]

শ্রেণি-৬) IPv4 এর প্রকারভেদ লিখ এবং আলোচনা কর। (Write and discuss the types of IPv4.) [BRTA-12, BPSC-12, ICT Ministry (AP)-11]

উত্তর: IPv4 এর প্রকারভেদ নিম্নে আলোচনা করা হলো: ক্লাস অনুসারে TCP/IP আইপি আড়েসকে ৫টি ভাগে ভাগ করা হয়েছে। দেখুন সার্ভার থেকে ভিত্তি প্রে হয়, না হল অনুরিকার মেইন ডাটা সেক্টোর থেকে প্রে হতে সবচেয়ে শাখাজোঠ।

- a) Class A (ক্লাস এ)
- b) Class B (ক্লাস বি)
- c) Class C (ক্লাস সি)
- d) Class D (ক্লাস ডি)
- e) Class E (ক্লাস ই)

Class-A (ক্লাস-এ): Class-A আইপি আড়েস এর অন্তর্ভুক্ত হলো নেটওর্ক আড়েসের জন্য এবং শেষে ৩ টি অক্টেট হলো হোস্ট আড়েসের জন্য। অর্থাৎ প্রথম 8 টি বিট হলো নেটওর্ক আড়েসের জন্য এবং শেষের ২৪টি বিট হলো হোস্ট এর জন্য। Class A আইপি আড়েস শুরু হয় 0.0.0.0 থেকে 127.255.255.255 পর্যন্ত। যখন নেটওর্কের পরিমাণ বেশি এবং হোস্ট আড়েসের পরিমাণ বেশি হলে তখন আমরা দেখানে Class C এর আইপি আড়েস ব্যবহার করতে পারি। উদাহরণ: 192.0.1.1 থেকে 223.255.254.254

Network	Host	Host	Host
8 Bit	8 Bit	8 Bit	8 Bit

IP Address range (0-127):

0	থেকে	0-127
0 0000000		0 1111111

- ✓ 0.0.0.0 নেটওর্ক Address এর জন্য ব্যবহৃত হয়।
- ✓ 127.0.0.0 Loop Back Address/Broadcast Address এর জন্য ব্যবহৃত হয়।
- ✓ Default Subnet Mask (SM) = 255.0.0.0
- ✓ Total No of Networks = $2^7 = 128$
- ✓ Total No of Hosts = $2^{24} = 16,777,216$
- ✓ Total No of Valid Hosts = $2^{24}-2 = 16777214$

[Note: এই Class-A এর প্রথম অক্টেটের প্রথম Value (MSB) এর মান 0 Fixed (নির্দিষ্ট) কিন্তু পরের মে 7 টি Value আরে এর Change হতে পারে। Host ID সব সব চেইঞ্চেবল (পরিবর্তনশীল)]

Class-B(ক্লাস-বি): Class-B আইপি আড়েসটি শুরু হয় 128.0.0.0 থেকে এবং শেষে হয় 191.255.255.255 পর্যন্ত। এর প্রথম 16 টি বিট ব্যবহার করা হয় নেটওর্ক আড়েসের জন্য এবং শেষের 16 টি বিট ব্যবহার করা হয় হোস্ট আড়েসের জন্য। যদি একটি নেটওর্কের নেটওর্ক আড়েস ও হোস্ট আড়েসের সম্মত সমস্য সমরকর তখন আমরা Class B এর আইপি আড়েস ব্যবহার করতে পারি। উদাহরণ: 128.1.0.1 থেকে 191.255.255.254

IP Address Range (128-191):

128	থেকে		191
10 000000			10 111111
Network	Network	Host	Host
8 Bit	8 Bit	8 Bit	8 Bit

- ✓ Default Subnet Mask (SM) = 255.255.0.0

✓ Total No of Network = $2^{14} = 16,384$

✓ Total No of Hosts = $2^{16} = 65,536$

✓ Total No of Valid Hosts = $2^{16}-2 = 65,534$

[Note: এই Class-B এর প্রথম অক্টেটের প্রথম দুইটি Value (MSB) 10 Fixed, বাকী সব চেইঞ্চেবল (পরিবর্তনশীল)]

Class-C (ক্লাস-সি): Class-C আইপি আড়েসটি শুরু হয় 192.0.0.0 থেকে এবং শেষে হয় 223.255.255.255 পর্যন্ত। এই ক্লাসের প্রথম 24 টি বিট ব্যবহার করা হয় নেটওর্ক আড়েসের জন্য এবং শেষের 8 টি বিট ব্যবহার করা হয় হোস্ট আড়েসের জন্য। যখন নেটওর্কের নেটওর্ক আড়েসের পরিমাণ বেশি এবং হোস্ট আড়েসের পরিমাণ কম সমরকর তখন আমরা দেখানে Class C এর আইপি আড়েস ব্যবহার করতে পারি। উদাহরণ: 192.0.1.1 থেকে 223.255.254.254

Network	Network	Network	Host
8 Bit	8 Bit	8 Bit	8 Bit

IP Address Range (192-223):

192	থেকে	223
110 00000		110 11111

Unchangeable Bit
Network Bit Host Bit
110 00000.00000000.00000000.00000000

- ✓ Default Subnet Mask (SM) = 255.255.255.0
- ✓ Total No of Networks = $2^{21} = 2,097,152$
- ✓ Total No of Hosts = 256
- ✓ Total No of Valid Hosts = $2^8-2 = 254$

[Note: এই Class-C এর প্রথম অক্টেটের প্রথম Value (MSB) 110 Fixed, বাকী সব চেইঞ্চেবল (পরিবর্তনশীল)]

Class-D (ক্লাস-ডি): Class D হচ্ছে একটি বিশেষ প্রেসিডেন্ট আইপি আড়েস। এর মেঝে হলো 224.0.0.0 থেকে 239.255.255.255 পর্যন্ত। Class D এর আইপি আড়েস সবার জন্য উন্মুক্ত না এবং এই নেটওর্কের আইপি আড়েস সমূহ Multicast Group এর জন্য ব্যবহার করা হয়। উদাহরণ: 224.0.0.0 থেকে 239.255.255.254

Network	Network	Network	Host
8 Bit	8 Bit	8 Bit	8 Bit

IP Address Range (192-223):

224	থেকে	239
1110 0000		1110 1111

- ✓ Default Subnet Mask (SM) = 255.255.255.0
- ✓ Total No of Network = $2^{20} = 1,048,576$
- ✓ Total No of Hosts = $2^8 = 256$
- ✓ Total No of Valid Hosts = $2^8-2 = 254$

[Note: এই Class-D এর প্রথম অক্টেটের প্রথম চারটি Value (MSB) 1110 Fixed, বাকী সব চেইঞ্চেবল (পরিবর্তনশীল)]

Class-E (ক্লাস-ই): IP Address এর 240.0.0.0 থেকে 255.255.255.255 পর্যন্ত কোন ক্লাস নেই। এই ক্লাসের প্রথম 24 টি বিট ব্যবহার করা হয় নেটওর্ক আড়েসের জন্য। এই ক্লাসের প্রথম 8 টি বিট ব্যবহার করা হয় হোস্ট আড়েসের জন্য। যখন নেটওর্কের নেটওর্ক আড়েসের পরিমাণ বেশি এবং হোস্ট আড়েসের পরিমাণ কম সমরকর তখন আমরা দেখানে Class E এর আইপি আড়েস ব্যবহার করতে পারি। উদাহরণ: 240.0.0.0 থেকে 254.255.255.254

Network	Network	Network	Host
8 Bit	8 Bit	8 Bit	8 Bit

- a) মানুষার কনফিগারেশন করতে হবে।
- b) ম্যানুয়াল আইপি বা স্টিটিক আইপি অধিক হাতে হবে থাকে।
- c) এর সবচেয়ে বড় অসুবিধা হচ্ছে খরচ।
- d) লিঙ্গেল গোটে ইহার নিরাপত্তা নিয়ে উৎসে তৈরি হয়।

IPv6 (ইন্টারনেট প্রোটোকল জন্মন ৬)

প্রশ্ন-১০) IPv6-এর ইতিহাস সম্পর্কে লিখুন? (Write about the history of IPv6.)

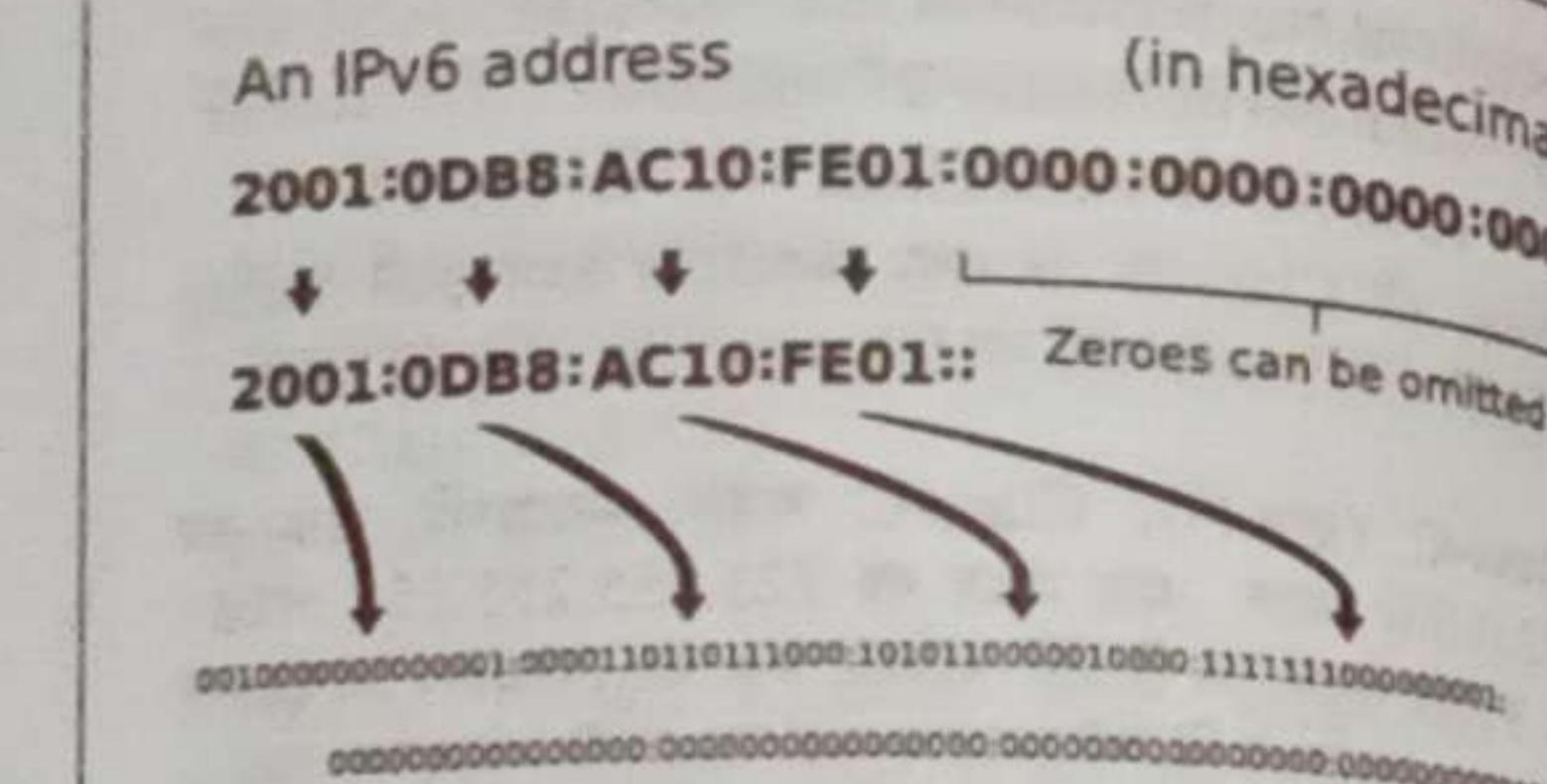
উত্তর: IPv6 সংক্রান্তের আগে প্রথম এসেছে IPv4 সংক্রান্ত। ১৯৮৩ সালে এই IPv4 -এর আসে। এরপর ১৯৯০-এর দিকে বিশ্বে তৃতীয় ইন্টারনেট সম্পর্কসারণের পর ভাবনার আসে। IPv4-এর মে নির্দিষ্ট ঠিকানা তা নিয়ে বিশ্বের সব সংযুক্ত ডিভাইসের মৌলিক ঠিকানা দেওয়া সম্ভব হবে না। সেই সময় থেকে ১৯৯২ সালে আসতেই সেখা যায়। IPv4 -এর মোট ঠিকানার ৬০ শতাংশ ব্যবহার হবে গেছে। এর সম্ভবতা ছিল ৪০০ কোটি ঠিকানা। তখন দুটি পরিকল্পনা নেয়ে ইন্টারনেট কর্পোরেশন ঘর অ্যাসাইন নেইমিং আভ. নামের ন বা (ICAN), একটি হলো, আইপি ঠিকানা যেন আর অপচয় ন হয়। IPv4 -এ মেঘে আছে তা পরিকল্পনা অনুযায়ী বিতরণ করা। আরেকটি হলো নতুন আইপি সংক্রান্ত তৈরির পরিকল্পনা।

এসবের জন্য আইক্যান গঠন করল ইন্টারনেট অ্যাসাইন নম্বর অধিবিত (IANA)। কাজ করে করে ইন্টারনেট ইন্ডিনিয়েশন টাক্ষণ্যের। 1997-1998 সালে নতুন সংক্রান্তের বস্তু আদর্শ ঠিক হলো এবং আইপিএম প্রথম তাদের এজাইএল 4.3 অপারেটিং সিস্টেমে IPv6 ব্যবহার করে। এরপর 2012 সালে ছাড়া হলো IPv6। যদিও এর চূড়ান্ত সংক্রান্ত আসে 2017 সালে। এতে ঠিকানা শেষ হওয়ার তার নেই। কারণ এখানে 340 ট্রিলিয়নের বেশি ঠিকানা রয়েছে।

প্রশ্ন-১১) IPv6 সম্পর্কে মৌলিক তথ্য তলো লিখুন। (Write Basic information about IPv6.)

উত্তর: IPv6 এর মৌলিক তথ্য:

- ✓ IPv6 হলো Internet Protocol Version-6.
- ✓ IPv6 এ প্রতিটি আইপি আইড্রেসকে অক্ষের জন্য মোট ৮ টি অশ্ব থাকে এবং প্রতি অশ্বে 16 বিট অর্থাৎ মোট 128 বিট অযোজন।
- ✓ প্রতিটি ডাট ভট (:) দ্বারা পৃথক করা হয়।
- ✓ IPv6 এর আইড্রেস সাধারণত Hexadecimal ফরম্যাটে দেখা হয়।
- ✓ যেমন: 2001: 0DB8: AC10: FE01: 0000: 0000: 0000: 0000 এক্ষেত্রে শুধুগুলো বাদ দেওয়া যেতে পারে। অর্থাৎ 2001: 0DB8: AC10: FE0:: দেখা যেতে পারে।
- ✓ IPv6 দ্বারা মোট 2^{128} বা 3.4×10^{38} or 340 undecillion সংখ্যক অধিতীর্য আইড্রেস তৈরি করা সম্ভব।



প্রশ্ন-১২) IPv4 ও IPv6 এর মধ্যে পার্থক্য লিখুন? (Write the difference between IPv4 and IPv6.)

উত্তর: IPv4 ও IPv6 এর মধ্যে পার্থক্য নিচেরূপ:

IPv4	IPv6
IPv4 হলো Internet Protocol Version-4	IPv6 হলো Internet Protocol Version-6
IPv4 এর Address Length 32-বিট।	IPv6 এর Address Length 128-বিট।
IPv4 এর Address নথিকরে মধ্যে বাইনারি সংখ্যা উপজাপন করে।	অনন্দিকে, IPv6 এর Address তালি হেক্সাডিজিমালে বাইনারি সংখ্যা প্রকাশ করে।
IPv4 এর ক্ষেত্রে ফ্রাগমেন্টেশন সেভিং ও ফেরয়ার্ডিং Routes সম্পর্ক হয়।	IPv6 এর ক্ষেত্রে ফ্রাগমেন্টেশন সেভার (Sender) দ্বারা সম্পর্ক হয়।
IPv4 এর Header File Length: 20-60 বাইট।	IPv6 এর Header File: 40 বাইট নিষিট।
IPv4 Error যাচাইয়ের জন্য হেডার বিন্যাসে চেকসাম (Checksum) ক্ষেত্র ব্যবহার করে।	IPv6 Error যাচাইয়ের জন্য হেডার বিন্যাসে চেকসাম (Checksum) ক্ষেত্র ব্যবহার করে।
IPv4 ম্যানুয়াল কনফিগারেশন অববা কনফিগারেশন সাপোর্ট করে।	IPv6 অটোমেটিক্যালি অববা রিনাস্টারিং আইড্রেস কনফিগারেশন সাপোর্ট করে।
Number of header fields: 12	Number of header fields: 8
IPv4 5 টি ক্লাসে (Class A to E) বিভক্ত।	IPv6 অনলিমিটেড সংখ্যক আইপি আইড্রেস স্টেট করার ক্ষমতা রয়ে।
IPv4 VLSM (Variable Length Subnet mask) support করে।	IPv6 VLSM (Variable Length Subnet mask) support করেন।
IPv4 এর ব্যবহারের উপর ইন্টারনেট নিরাপত্তা নির্ভর করে কারণ নিরাপত্তার কথা ভেবে ইহা ডিজাইন করা হচ্ছে।	IPv6 এর ক্ষেত্রে ইন্টারনেট সিকিউরিটি প্রটোকল বিট-ইন থাকে এবং ইহার সঠিক কী ইনফ্রাস্ট্রাকচার দ্বারা ব্যবহার করা হয়।
সিস্টেম ম্যানেজমেন্টের জন্য SNMP প্রোটোকল ব্যবহার করা হয়।	SNMP প্রোটোকল সাপোর্ট করেন।
IPv4 RIP (Routing)	IPv6 RIP (Routing)

Information Protocol প্রোটোকল সাপোর্ট করে না। ইহা স্টিটিক রাউটিং ব্যবহার করে।	Information Protocol প্রোটোকল সাপোর্ট করে না। ইহা স্টিটিক রাউটিং ব্যবহার করে।
ম্যাক আইড্রেস ম্যাপ করার জন্য ARP (Address Resolution Protocol) প্রোটোকল ব্যবহার করা হয়।	ম্যাক আইড্রেস ম্যাপ করার জন্য NDP (Neighbour Discovery Protocol) প্রোটোকল ব্যবহার করা হয়।
IPv4 Unicast, Broadcast, and Multicast টাইপের হয়ে থাকে।	IPv6 Unicast, Multicast, and Anycast টাইপের হয়ে থাকে।
উদাহরণ: 192.168.10.2	উদাহরণ: 2001:0db8:0000:0000:0000:0000:0000:0000
	00:ff00:0042:7879

Write the advantages of creating Subnet?) [ICT Ministry-11]

উত্তর: বড় নেটওয়ার্ক কে ছোট নেটওয়ার্কে বিভক্ত করার পদ্ধতিকে বলা হয় সাবনেট। সাবনেট মাঝ এর কাজ হলো আইপি এড্রেসের কোন বিটগুলো নেটওয়ার্ক আইডি আর কোন বিট গুলো হোস্ট আইডি তা শনাক্ত করা। সাবনেট মাঝ না থাকলে কম্পিউটার বুকতে পারে না আইপি এড্রেসের কোন অংশ নেটওয়ার্ক আইডি আর কোন অংশ হোস্ট আইডি। সাবনেট করার সময় যে বিষয়টি মনে রাখতে হবে, তা হলো 128 192 224 240 248 252 254 255 এই সংখ্যা গুলো সাবনেট মাঝ এর হয়ে থাণে।

Subnet তৈরির সুবিধাসমূহ হল:

- কম নেটওয়ার্ক প্রোটোকল।
- উন্নত নেটওয়ার্ক প্রকরণযোগ্য।
- সহজ ব্যবহারপ্রণালী।
- নেটওয়ার্ক বিভক্ত করার সুবিধা।
- সহজে বিভক্ত করার সুবিধা।

প্রশ্ন-১৩) Classless Inter-Domain Routing (CIDR) কি? (What is Classless Inter-Domain Routing (CIDR)?)

উত্তর: CIDR হল একটা পদ্ধতি যার সাথায়ে ISP (Internet Service Provider) কোম্পানিগুলো বাসা বা অফিসে আইপি Assign (বরাদ্দ) করে। তবু সাইজের উপরে ভিত্তি করে এই আইপিগুলো দেওয়া হয়। যেমন: আপনার ISP থেকে পাওয়া আইপি এরকম হতে পারে: 192.168.10.32/28। আইপি (IP) দেখে আপনি সহজেই বলে দিতে পারবেন আপনার সাবনেট মাস্টিপি কি। এখানে Slash Notation (/) এর অর্থ হল কতগুলি বিট অন আছে (অর্থাৎ কতগুলি 1 আছে)। আপনার এই আইপিতে 28 টি বিট (অর্থাৎ 1 আছে)। আপনার এই আইপিতে 28 টি বিট (অর্থাৎ 1 আছে)। 11111111. 11111111. 11111111. 11110000। সুতরাং, আপনার সাবনেট মাঝ হল: 255.255.255.240

প্রশ্ন-১৪) Classful IP কি? Classless IP কি? (What is Classful and Classless IP?) [BPSC-17]

উত্তর: Classful IP: আইপি আইড্রেস মেজ 5 টি ভিত্তি ক্লাসে বিভক্ত ক্লাস A,B,C,D,E। যে IP Class এর নেটওয়ার্ক প্রিফিক্স (Prefix) আর হোস্ট নামার ফিল্ড, এদের কে ক্লাস ফুল আইপি বলে।

Class A: 10.1.0.0/8

Class B: 128.2.0.0/16

Class C: 192.16.8.0/24

Classless IP: যে IP Class এর নেটওয়ার্ক প্রিফিক্স (Prefix) আর হোস্ট নামার ফিল্ড নয়, এদের কে Classless আইপি বলে।

Class A: 10.1.0.0/12

Class B: 128.2.0.0/20

Class C: 192.16.8.0/25

প্রশ্ন-১৫) সাবনেট মাঝ কি? (What is Subnet Mask?)

উত্তর: সাবনেট মাঝ এর কাজ হলো IP Address এর কোন বিটগুলো Network Id এবং কোন বিট গুলো Host Id তা শনাক্ত করা।

প্রশ্ন-১৬) সাবনেট এবং সাবনেট Mask কি? Subnet তৈরির সুবিধা লিখ? (What is Subnetting and Subnet mask?)

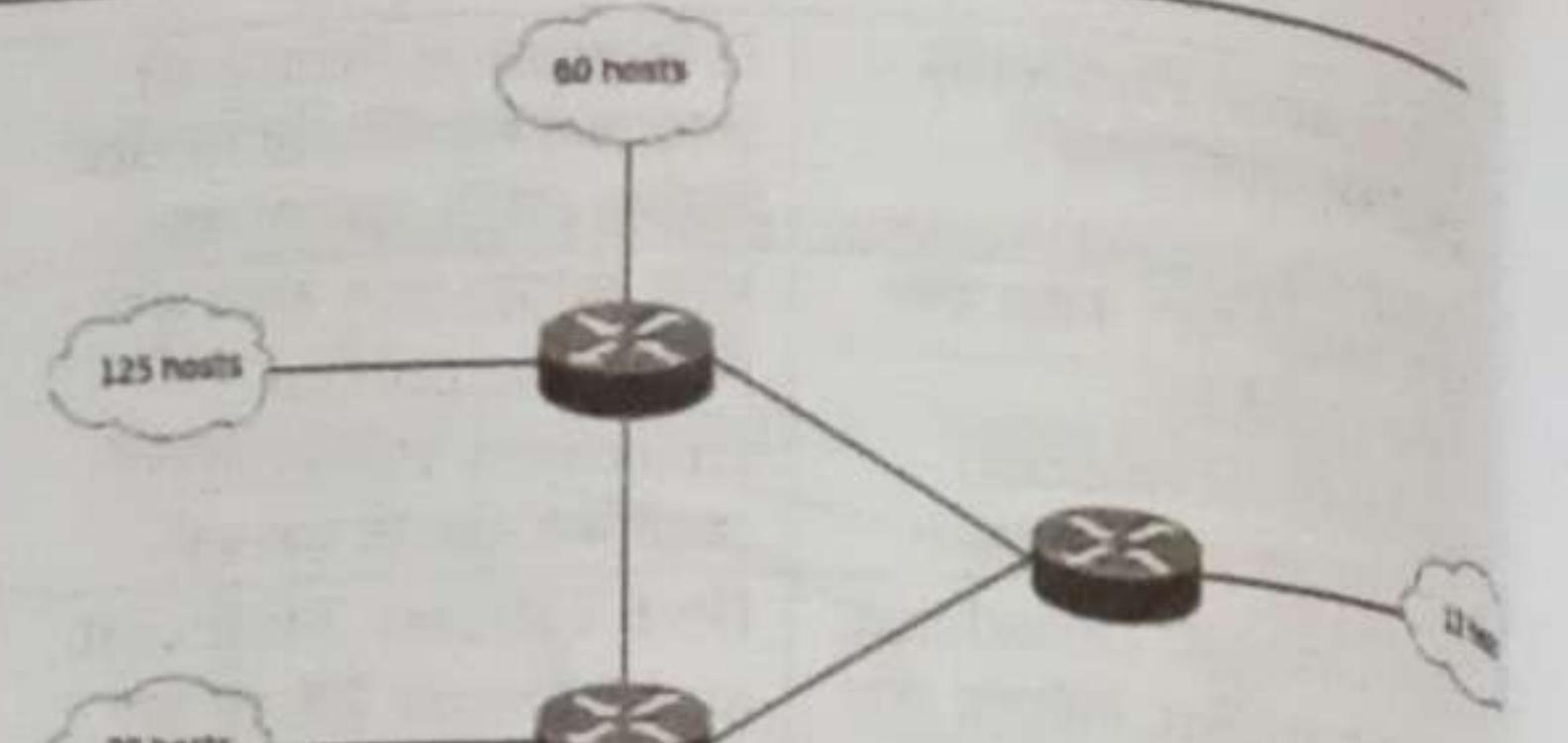
প্রশ্ন-১৯) VLSM কাকে বলে? VLSM কেন ব্যবহার করা হয়?
(What is VLSM? And Why we use VLSM?)

উত্তর: VLSM: VLSM এর পূর্ণরূপ হচ্ছে Variable Length Subnet Mask. VLSM নেটওয়ার্ক এর একটি অতি গুরুত্বপূর্ণ বিষয়। এর মাধ্যমে একটি নেটওয়ার্কের বিভিন্ন অংশে ভিন্ন সাবনেট মাঝে ব্যবহার করা হয়।

VLSM ব্যবহার করার কারণ: আইপি আড্রেস গুলোকে সংক্ষিপ্তভাবে ব্যবহার করার জন্য বা কাজে লাগানোর জন্য কিংবা আইপি আড্রেসের অপ্রযুক্তির কমানোর জন্য VLSM এর প্রয়োজন হয়। আমরা যখন সাবনেটিং করি তখন আমাদের প্রতিটি নেটওয়ার্কে সমান সংখ্যক আইপি আড্রেস থাকে। কিন্তু আমরা যখন কোন অফিসে কাজ করবো তখন দেখবো সেখানে অনেক গুলো ডিপার্টমেন্ট (যেমন: আইটি, ইচেট আর, একাউটস ইত্যাদি) থাকে এবং প্রত্যেক ডিপার্টমেন্টে আলাদা আলাদা সংখ্যক আইপি আড্রেসের প্রয়োজন হবে। আমরা যখন সাবনেটিং করে আলাদা আলাদা ডিপার্টমেন্টের জন্য আলাদা আলাদা নেটওয়ার্ক আসাইন করবো তারপরও দেখতে পারবো অনেক আইপি আড্রেসে Unused বা অব্যবহৃত থেকে যাবে। কোন ডিপার্টমেন্টে আমাদের আইপি লাগবে ১০০ টি আবার কোন ডিপার্টমেন্টে লাগতে পারে ১০ টি। যেখানে ১০ টি আইপি লাগবে সেখানে অব্যাহী অনেক আইপি আড্রেস অব্যবহৃত থেকে যাবে। আমরা এই সমস্যা সমাধান করতে পারি VLSM এর মাধ্যমে। তাই বলাই যায় যে, এই অব্যবহৃত আইপি আড্রেস এর সংখ্যা কমানোর জন্যই আমরা VLSM করে থাকি।

প্রশ্ন-২০) উদাহরণসহ VLSM এর Design ও Implementation আলোচনা করুন? (Briefly describes the Design and Implementation of VLSM with an example.)

উত্তর: VLSM এর Design: একটি নেটওয়ার্কে যত বেশি আইপি লস কমানো যায়, সেই নেটওয়ার্কের পারফর্মেন্স তত বেশি ভাল হবে। নেটওয়ার্ক যত ছোট হবে ত্রুটকাটি তত কম হবে। VLSM ডিজাইন এর ক্ষেত্রে যে বিষয়টা লক্ষ্য করা উচিত তা হলো, প্রথমে কোন ডিপার্টমেন্ট এর সবচেয়ে বেশি যত আইপি লাগবে তার উপর ভিত্তি করে প্রথমে সাবনেটিং করা। এরপর তার চেয়ে কম আইপি লাগবে কোন ডিপার্টমেন্টে তার উপর ভিত্তি করে আবার এইপর এই সাব নেটওয়ার্কটিকে আবার সাবনেটওয়ার্ক এ বিভক্ত করা। এভাবে প্রত্যেকটি ডিপার্টমেন্টে যে পরিমাণ আইপি আড্রেস প্রয়োজন তার উপর ভিত্তি করে কোন নেটওয়ার্ককে মাস্টিশুল সাবনেটওয়ার্ককে বিভক্ত করা যায়। VLSM ডিজাইনে সবসময় বড় নেটওয়ার্ক থেকে ছোট নেটওয়ার্কের দিকে যাওয়া হবে।



VLSM নেটওয়ার্ক এর Implementation: ধরি, বিটক্স মুদ্রের অফিসে ৪টি ডিপার্টমেন্ট আছে এবং এই ৪ টি ডিপার্টমেন্টেকে আলাদা আলাদা নেটওয়ার্কে রাখবো। এই ৪টি ডিপার্টমেন্ট হল:

- a) বুক প্রিন্টিং ডিপার্টমেন্ট
- b) পরীক্ষা নিয়ন্ত্রক ডিপার্টমেন্ট
- c) বুক সেলস এবং একাউটস ডিপার্টমেন্ট
- d) এডভারটাইজমেন্ট ডিপার্টমেন্ট

এই প্রত্যেকটি ডিপার্টমেন্টে বিভিন্ন পরিমাণের আইপি আড্রেস প্রয়োজন। ধরি, বুক প্রিন্টিং ডিপার্টমেন্ট এর জন্য 60 টি, পরীক্ষা নিয়ন্ত্রক ডিপার্টমেন্ট এর জন্য 25 টি, বুক সেলস এবং একাউটস ডিপার্টমেন্টের জন্য 12 টি এবং এডভারটাইজমেন্ট ডিপার্টমেন্টের জন্য 5 টি আইপি আড্রেস প্রয়োজন। ধরি, আমরা 192.168.16.0/24 এই নেটওয়ার্কটি ব্যবহার করবো।

বুক প্রিন্টিং ডিপার্টমেন্ট: সবচেয়ে বেশি আইপি আড্রেস প্রয়োজন বুক প্রিন্টিং ডিপার্টমেন্টের জন্য 60 টি। যদি 192.168.16.0/24 এই নেটওয়ার্কটিকে 192.168.16.0/26 সাবনেটে বিভক্ত করি। হোস্ট বিট থেকে আরো 2 টি বিট নেটওয়ার্ক এর জন্য নেওয়া হয় তাহলে এখানে 4 টি সাবনেটওয়ার্ক পাওয়া যাবে। এখানে Block Size হবে 64 এবং প্রতিটি নেটওয়ার্ক এ 62 টি করে হোস্ট থাকবে। বুক প্রিন্টিং ডিপার্টমেন্টের জন্য প্রয়োজন 60 টি। তাহলে প্রথম নেটওয়ার্কটি বুক প্রিন্টিং ডিপার্টমেন্টের জন্য ব্যবহার করতে পারি যেখানে হোস্ট রয়েছে 62 টি। যার ফলে এইক্ষেত্রে কোন আইপি অব্যবহৃত থাকছেন।

পরীক্ষা নিয়ন্ত্রক ডিপার্টমেন্ট: এখন দ্বিতীয় নেটওয়ার্কটি যদি পরীক্ষা নিয়ন্ত্রক ডিপার্টমেন্টের জন্য ব্যবহার করা হয়, তাহলে অনেক গুলো আইপি অব্যবহৃত থেকে যাচ্ছে। এখানে দ্বিতীয় নেটওয়ার্কটি হলো 192.168.16.64/26। কিন্তু পরীক্ষা নিয়ন্ত্রক ডিপার্টমেন্টের জন্য আইপি প্রয়োজন 30 টি। এই নেটওয়ার্কটিকে এমন ভাবে বিভক্ত করে হবে যাতে আইপি অব্যবহৃত না থাকে এবং প্রয়োজনীয় আইপি 6 পাওয়া যায়। যদি 192.168.16.64/26 এই নেটওয়ার্কটিকে 192.168.16.64/27 এই সাবনেটে বিভক্ত করা হয় তাহলে Block Size হবে 32 এবং প্রতিটি নেটওয়ার্ক এ ব্যবহৃত আইপির সংখ্যা হবে 30 টি। তাহলে পরীক্ষা নিয়ন্ত্রক ডিপার্টমেন্টের জন্য 192.168.16.64/27 এই নেটওয়ার্কটিকে ব্যবহার করা যাবে, যার ফলে এইক্ষেত্রে কোন আইপি অব্যবহৃত থাকছেন।

বুক সেলস এবং একাউটস ডিপার্টমেন্ট: এখন 192.168.16.96/27 নেটওয়ার্কটি যদি বুক সেলস এবং একাউটস ডিপার্টমেন্টের জন্য ব্যবহার করা হয়, তাহলে অনেকগুলি আইপি লস হবে। তাই এই নেটওয়ার্কটিকে আবার সাবনেটে বিভক্ত করতে পারি। যদি এই নেটওয়ার্কটিকে 192.168.16.96/28 এই সাবনেটে বিভক্ত করি তাহলে হোস্ট পাব 14 টি। আর বুক সেলস এবং একাউটস ডিপার্টমেন্টের আইপি প্রয়োজন 12 টি, যার ফলে তাহলে আইপি লস করে যাচ্ছে।

এডভারটাইজমেন্ট ডিপার্টমেন্ট: এই ডিপার্টমেন্টের জন্য আইপি প্রয়োজন 5 টি। যদি 192.168.16.96/28 নেটওয়ার্ক এর পরের নেটওয়ার্ক 192.168.16.112/28 (এখানে Block Size হবে 16) নেটওয়ার্কটিকে এডভারটাইজমেন্ট ডিপার্টমেন্টের জন্য ব্যবহার করা হয়, তাহলে অনেক আইপি লস হবে; তাই পুনরায় এই নেটওয়ার্কটিকে সাবনেটওয়ার্কে বিভক্ত করা যায়। যদি 192.168.16.112/28 এই নেটওয়ার্কটিকে 192.168.16.112/29 এই সাবনেটওয়ার্কে বিভক্ত করা হয়, তাহলে নেটওয়ার্ক এর এখানে Block Size হবে 8 এবং এডভারটাইজমেন্ট ডিপার্টমেন্ট আইপির প্রয়োজন 5 টি।

উপরের আলোচনায় প্রতিটি ডিপার্টমেন্টের জন্য আলাদা আলাদা নেটওয়ার্ক ব্যবহার করা হয়েছে এবং এই প্রতিটি নেটওয়ার্ক আলাদা আলাদা সাবনেটে বিদ্যমান। সংক্ষেপে পুরো বিষয়টা টেবিল আকারে দেখানো হলো:

ডিপার্টমেন্টের নাম	হোস্ট অর্ধেক স	Block Size	হোস্ট পাবে	নেটওয়ার্ক আইপি	শুরুকাটি আইপি
বুক প্রিন্টিং ডিপার্টমেন্ট	60 টি	64	62 টি	192.168.16.0/26	255.255.2
পরীক্ষা নিয়ন্ত্রক ডিপার্টমেন্ট	25 টি	32	30 টি	192.168.16.64/27	255.255.2
বুক সেলস এবং একাউটস ডিপার্টমেন্ট	12 টি	16	14 টি	192.168.16.96/28	255.255.2
এডভারটাইজমেন্ট ডিপার্টমেন্ট	5 টি	8	6 টি	192.168.16.112/29	255.255.2

মূলত এভাবেই VLSM এর মাধ্যমে একটি নেটওয়ার্ককে মাস্টিশুল নেটওয়ার্কে বিভক্ত করে আবার বা আইএসপি কোম্পানি নেটওয়ার্কের আইপি লস করাতে পারি বা কমিয়ে থাকে।

সাবনেটিং এর কারণ

বড় আকারের নেটওয়ার্ক তৈরীর সবচাইতে বড় চালেজ হচ্ছে প্রতিটি কম্পিউটারের জন্য একটি করে IP Address বরাদ্দ করা। কারন

আমরা পুরোই আলোচনা করেছি যে, ক্লাস এ নেটওয়ার্কে প্রথম 8 বিট ব্যবহার করা হয় নেটওয়ার্ক আইডি + হোস্ট আইডি + নেটওয়ার্ক আইডি + সাবনেট আইডি + হোস্ট আইডি প্রথমে কিছু প্রশ্নের উত্তর দ্বৰূপ।

- * আপনি কতগুলো কম্পিউটারের জন্য IP Address দ্বৰূপ হচ্ছেন?
- * আপনার কতগুলো নেটওয়ার্কটিকে কতগুলো ছোট নেটওয়ার্কে (সাবনেট) ভাগ করতে চান?

সহজে Network Address, Broadcast Address, Subnet Mask বের করার জন্য নিচের technique টা মনে রাখবেন:

Network Address: All network bit as it is, (যা আছে তাই থাকবে) all host bit 0.

Broadcast Address: All network bit as it is, host bit all 1.

Subnet Mask: All network bits 1, all host bit 0.

ক্লাস এ (Class A) সাবনেটিং

আমরা পুরোই আলোচনা করেছি যে, ক্লাস এ নেটওয়ার্কে প্রথম 8 বিট ব্যবহার করা হয় নেটওয়ার্ক আইডি + পরবর্তী 24 বিট ব্যবহার করা হয় হোস্ট বিট হিসেবে। সুতরাং বলতে পারি যে ক্লাস-এ সিলেক্ট কম্পিউটারের জন্য একটি করে IP Address বরাদ্দ করা। কারন

ব্যবহার করা হবে। আর ক্লাস-এর ডিফল্ট সাবনেট মাঝ হলো:
255.0.0.0

ক্লাস-বি এর ক্ষেত্রে একটি (1) বিট অন করে সাবনেট করে।
10.0.0.0/9 [এর মান হচ্ছে এখানে 9 টি বিট 1 হবে।]
সাবনেট মাঝ: 255.128.0.0 [বাইনারি- 11111111.1
0000000.00000000.00000000]
মোট নেটওয়ার্ক সংখ্যা= $2^7=2$ টি
মোট হোস্টের সংখ্যা= $2^{23}=83,38,608$ টি
মোট ভালিত হোস্টের সংখ্যা= $2^{23}-2=83,38,606$ টি [প্রতিটি
নেটওয়ার্কের জন্য।]
সাবনেট আইডি=256-128=128

নেটওয়ার্ক-১ এর ক্ষেত্রে:
নেটওয়ার্ক আইডি = 10.0.0.0
প্রথম ভালিত হোস্ট = 10.0.0.1
বিত্তীয় ভালিত হোস্ট = 10.0.0.2
তৃতীয় ভালিত হোস্ট = 10.0.0.3

শেষ ভালিত হোস্ট = 10.127.255.254
এবং ব্রডকাস্ট আড্রেস = 10.127.255.255
নেটওয়ার্ক-২ এর ক্ষেত্রে:
নেটওয়ার্ক আইডি = 10.128.0.0
প্রথম ভালিত হোস্ট = 10.128.0.1
বিত্তীয় ভালিত হোস্ট = 10.128.0.2
তৃতীয় ভালিত হোস্ট = 10.128.0.3

শেষ ভালিত হোস্ট = 10.255.255.254
এবং ব্রডকাস্ট আড্রেস = 10.255.255.255
**একইভাবে আবার ক্লাস- এ এর ক্ষেত্রে দুইটি (2) বিট অন করে
সাবনেট করি।**
10.0.0.0/10 [এর মান হচ্ছে এখানে 10 টি বিট 1 হবে।]
255.192.0.0 [বাইনারি- 11111111.11
000000.00000000.00000000]

মোট নেটওয়ার্ক সংখ্যা= $2^2=4$ টি
মোট হোস্টের সংখ্যা সংখ্যা= $2^{22}=41,94,304$ টি
মোট ভালিত হোস্টের সংখ্যা= $2^{22}-2=41,94,302$ টি [প্রতিটি
নেটওয়ার্কের জন্য।]
সাবনেট আইডি = 256-192=64

নেটওয়ার্ক-১ এর ক্ষেত্রে:
নেটওয়ার্ক আইডি = 10.0.0.0
প্রথম ভালিত হোস্ট = 10.0.0.1
বিত্তীয় ভালিত হোস্ট = 10.0.0.2
তৃতীয় ভালিত হোস্ট = 10.0.0.3

শেষ ভালিত হোস্ট = 10.63.255.254
এবং ব্রডকাস্ট আড্রেস = 10.63.255.255
নেটওয়ার্ক-২ এর ক্ষেত্রে:
নেটওয়ার্ক আইডি = 10.64.0.0
প্রথম ভালিত হোস্ট = 10.64.0.1
বিত্তীয় ভালিত হোস্ট = 10.64.0.2
তৃতীয় ভালিত হোস্ট = 10.64.0.3

শেষ ভালিত হোস্ট = 10.127.255.254
এবং ব্রডকাস্ট আড্রেস = 10.127.255.255
নেটওয়ার্ক-৩ এর ক্ষেত্রে:
নেটওয়ার্ক আইডি = 10.128.0.0
প্রথম ভালিত হোস্ট = 10.128.0.1
বিত্তীয় ভালিত হোস্ট = 10.128.0.2
তৃতীয় ভালিত হোস্ট = 10.128.0.3

শেষ ভালিত হোস্ট = 10.191.255.254
এবং ব্রডকাস্ট আড্রেস = 10.191.255.255
নেটওয়ার্ক-৪ এর ক্ষেত্রে:
নেটওয়ার্ক আইডি = 10.192.0.0
প্রথম ভালিত হোস্ট = 10.192.0.1
বিত্তীয় ভালিত হোস্ট = 10.192.0.2
তৃতীয় ভালিত হোস্ট = 10.192.0.3

শেষ ভালিত হোস্ট = 10.255.255.254
এবং ব্রডকাস্ট আড্রেস = 10.255.255.255

কোনো পরিকার যদি এভাবে প্রশ্ন করা হয়: 10.0.0.0/8 অতোক
সাবনেট এ কমপক্ষে 5000 হোস্ট থাকবে। তাহলে নিচের প্রশ্ন তাদের
উত্তর লিখুন।

প্রশ্ন-২১) কতগুলো বিট অন করতে হবে 5000 হোস্ট তৈরি করা
জন্য? (How many bit should be On to create 5000
Host?)
উত্তর: $2^{12}-2=4096-2=4094$ [এখানে 12 বিট অন করলে আরো
হোস্ট পাওয়া যাবে 4094 টি। কিন্তু আমাদের হোস্ট লাগবে কমপক্ষে 5000
টি, তাই আবার 12 বিট অন করতে পারবোনা।]
আবার, $2^{13}-2=8192-2=8190$; অর্থাৎ 13 বিট অন করলে
আমাদের প্রয়োজন সম্পূর্ণ হবে।

প্রশ্ন-২২) তাহলে নতুন সাবনেট কর হবে?
উত্তর: আমরা জানি, ক্লাস-এ এর ডিফল্ট সাবনেট যেহেতু 255.0.0.0
কিন্তু এখানে আরো 13 বিট অন করা হচ্ছে, তাহলে (অর্থাৎ- 11111111.
11111111.111 00000.000000000) আসে প্রথম 8 বিটের
জন্য 255. পরবর্তী 8 বিটের জন্য 255 তাহলে বাকী তাকে 3 বিট।
3 বিটের মান হলো 224. সুতরাং সাবনেট মাঝ হলো:
255.255.224.0

প্রশ্ন-২৩) Block সাইজ কত?
উত্তর: $2^{13}=8192$

প্রশ্ন-২৪) ৫ম নেটওয়ার্কটি কি?
উত্তর: প্রথম নেটওয়ার্ক: 10.0.0.0
বিত্তীয় নেটওয়ার্ক: 10.0.32.0
তৃতীয় নেটওয়ার্ক: 10.0.64.0
চতুর্থ নেটওয়ার্ক: 10.0.96.0
পঞ্চম নেটওয়ার্ক: 10.0.128.0

ক্লাস-বি (Class B) সাবনেটিং
পূর্বেও আলোচনায় বলা হয়েছে যে, নেটওয়ার্কিং এর ক্ষেত্রে যদি উভয়
এর অর্ধাং হোস্ট আইপির সংখ্যা এবং নেটওয়ার্ক আইপির সংখ্যা
সম্পরিমান প্রয়োজন হয় তখন আমরা ক্লাস-বি ব্যবহার করবো।
এখানে ক্লাস বি আইপিসের সাবনেটিং করার সময় মনে রাখতে হবে যে
মাঝে প্রথম দুইটি অকটেড 16 বিট অবশ্যই 1 হবে। অর্থাৎ প্রথম 16
বিট হলো নেটওয়ার্ক আর পরবর্তী 16 বিট হলো হোস্ট আইডি। ক্লাস
বি এর ডিফল্ট সাবনেট মাঝ হলো 255.255.0.0।

**অন্য, ক্লাস বি এর ক্ষেত্রে একটি (1) বিট অন করে সাবনেটিং করে
দেখি।**
172.16.0.0/17 [এর মান হচ্ছে এখানে 17 টি বিট 1 হবে।]
সাবনেট মাঝ: 255.255.128.0 [বাইনারি- 11111111.11111111.
11111111.00000000.00000000]
মোট নেটওয়ার্ক সংখ্যা= $2^1=2$ টি
মোট হোস্টের সংখ্যা= $2^{15}=32,768$ টি
মোট ভালিত হোস্টের সংখ্যা= $2^{15}-2=32,766$ টি [প্রতিটি
নেটওয়ার্কের জন্য।]
সাবনেট আইডি = 256-128=128

নেটওয়ার্ক-১ এর ক্ষেত্রে:
নেটওয়ার্ক আইডি = 172.16.0.0
প্রথম ভালিত হোস্ট = 172.16.0.1
বিত্তীয় ভালিত হোস্ট = 172.16.0.2
তৃতীয় ভালিত হোস্ট = 172.16.0.3

শেষ ভালিত হোস্ট = 172.16.127.254
এবং ব্রডকাস্ট আড্রেস = 172.16.127.255

নেটওয়ার্ক আইডি = 172.16.128.0
প্রথম ভালিত হোস্ট = 172.16.128.1
বিত্তীয় ভালিত হোস্ট = 172.16.128.2
তৃতীয় ভালিত হোস্ট = 172.16.128.3

শেষ ভালিত হোস্ট = 172.16.255.254
এবং ব্রডকাস্ট আড্রেস = 172.16.255.255

**একইভাবে আবার ক্লাস বি এর ক্ষেত্রে দুইটি (2) বিট অন করে
সাবনেটিং করি।**

172.16.0.0/18 [এর মান হচ্ছে এখানে 18 টি বিট 1 হবে।]
সাবনেট মাঝ: 255.255.192.0 [বাইনারি- 11111111.11111111.
11111111.11111111.11111111.00000000]
মোট নেটওয়ার্ক সংখ্যা= $2^2=4$ টি
মোট হোস্টের সংখ্যা= $2^{14}=16,384$ টি
মোট ভালিত হোস্টের সংখ্যা= $2^{14}-2=16,382$ টি [প্রতিটি
নেটওয়ার্কের জন্য।]
সাবনেট আইডি = 256-192=64

নেটওয়ার্ক-১ এর ক্ষেত্রে:
নেটওয়ার্ক আইডি = 172.16.0.0
প্রথম ভালিত হোস্ট = 172.16.0.1
বিত্তীয় ভালিত হোস্ট = 172.16.0.2
তৃতীয় ভালিত হোস্ট = 172.16.0.3

শেষ ভালিত হোস্ট = 172.16.63.254
এবং ব্রডকাস্ট আড্রেস = 172.16.63.255
নেটওয়ার্ক-২ এর ক্ষেত্রে:
নেটওয়ার্ক আইডি = 172.16.64.0
প্রথম ভালিত হোস্ট = 172.16.64.1
বিত্তীয় ভালিত হোস্ট = 172.16.64.2
তৃতীয় ভালিত হোস্ট = 172.16.64.3

শেষ ভালিত হোস্ট = 172.16.127.254
এবং ব্রডকাস্ট আড্রেস = 172.16.127.255

নেটওয়ার্ক-৩ এর ক্ষেত্রে:
নেটওয়ার্ক আইডি = 172.16.128.0
প্রথম ভালিত হোস্ট = 172.16.128.1
বিত্তীয় ভালিত হোস্ট = 172.16.128.2
তৃতীয় ভালিত হোস্ট = 172.16.128.3

শেষ আলিপ্ত হোস্ট= 172.16.191.254
এবং প্রতিকর্ত আড্রেস= 172.16.191.255

নেটওর্ক এবং স্বতন্ত্র
নেটওর্ক আইডি = 172.16.192.0
প্রথম আলিপ্ত হোস্ট = 172.16.192.1
বিশীর আলিপ্ত হোস্ট = 172.16.192.2
তৃতীয় আলিপ্ত হোস্ট = 172.16.192.3

শেষ আলিপ্ত হোস্ট= 172.16.255.254
এবং প্রতিকর্ত আড্রেস= 172.16.255.255

[Note: একটু মেজে কলানোই মনে পড়ব যে, চকচিত পরীক্ষার কালোজ এ বিশুলিনালভে পরীক্ষার কি মানের প্রশ্ন আসে। এই কলানো, তাইনা]

প্রশ্ন-২৫) 172.16.16.137/22 অইপি দিয়ে নিচের উভ তঙ্গ বের করুন? (Using this IP 172.16.16.137/22 find the answer of the following question.)

১. ইহার স্বতন্ত্র মাঝ কত?
২. Block সাইজ কত?
৩. ইহার নেটওর্ক আড্রেস কত?
৪. ইহার প্রতিকর্ত আড্রেস কত?
৫. প্রথম আলিপ্ত আড্রেস কোনটি?
৬. শেষ আলিপ্ত আড্রেস কোনটি?
৭. প্রথমটী নেটওর্ক আড্রেস কোনটি?
৮. কত জলে আলিপ্ত আড্রেস আছে?
৯. ইহা কি হোস্ট, নেটওর্ক এবং প্রতিকর্ত আড্রেস?

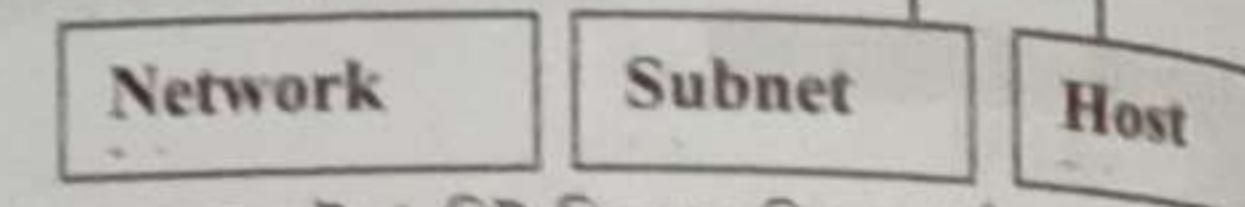
জিভ: 172.16.16.137/22 [এর মানে হচ্ছে এখানে 18 টি বিট (One ক ওN)] হবে।

১. ইহার স্বতন্ত্র মাঝ 255.255.252.0 [|||||,|||||,|||||,00.00000]
২. Block সাইজ: $2^{10} - 4 * 256 = 1024$
৩. নেটওর্ক আড্রেস : 172.16.16.0/22
৪. প্রতিকর্ত আড্রেস : 172.16.19.255/22 যেহেতু প্রথমটী নেটওর্ক: 172.16.20.0/22
৫. প্রথম আলিপ্ত আড্রেস: 172.16.16.1/22
৬. শেষ আলিপ্ত আড্রেস: 172.16.19.254/22
৭. প্রথমটী নেটওর্ক: 172.16.20.0/22
৮. মোট আলিপ্ত আড্রেস আছে: $2^{10} - 2 = 1024 - 2 = 1022$
৯. 172.16.16.137/22 ইহা একটি হোস্ট

ক্লাস-সি (Class C) স্বতন্ত্র

ক্লাস সি এড্রেসের সাথে স্বতন্ত্র মাঝ ব্যবহারের সময় মনে রাখতে হবে যে একে প্রথম তিনটি অকটেত 24 টি অবশ্যই । হবে। একটি সি ক্লাস এর নেটওর্ক দিয়ে নিচে বলনা করা হলো:

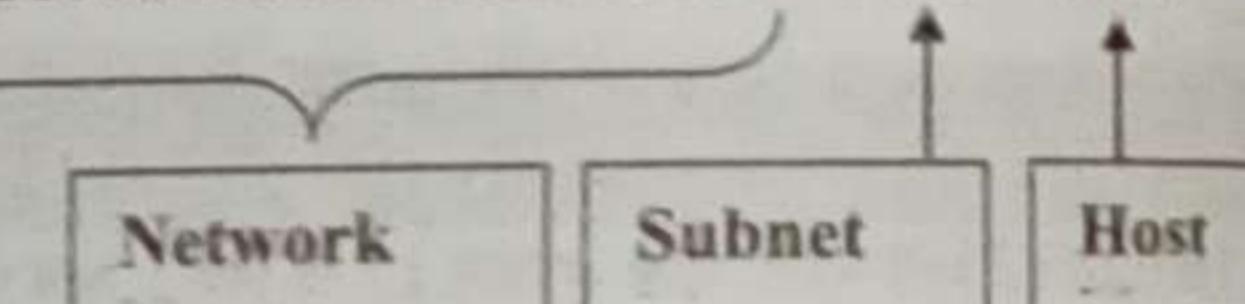
ধরি, অইপি আড্রেস=192.168.10.0/24
হোস্ট লাগবে = 14 টি করে। তাহলে, $2^4 - 2 = 14$ অর্থাৎ 4 টি জন
এর জন্য বাকি 4 বিট স্বতন্ত্র বিট।
ধরি, অইপি আড্রেস= 192.168.10.0/28
এখানে শেষে 28 বলতে নেটওর্ক আইডি+স্বতন্ত্র আইডি। এবং
জানি ক্লাস সি তে 24 টি বিট নেটওর্ক আইডি থাকে বাকি 4 টি
স্বতন্ত্র আইডি। একটু ভাল ভাবে দেখলে বাইনারিতে দেখি:
11000000.10101000.00001010. 0000 0000



তাহলে এখানে স্বতন্ত্রে 4 টি দিয়ে যাচ্ছিমাম $2^4 = 16$ টা স্বতন্ত্র
তৈরি করা যাবে। এখানে হোস্ট 4 টি দিয়ে যাচ্ছিমাম $2^4 = 16$ টি
হোস্ট তৈরি করা যাবে। তাহলে হোস্ট হবে: 192.168.10.0 হবে
192.168.10.15, এখানে প্রথম আড্রেসকে নেটওর্ক আইডি আ
শেষ আড্রেস কে প্রতিকর্ত আইডি বলে। তাহলে:
Network Address= 192.168.10.0
Broadcast Address= 192.168.10.15
First Valid Host= 192.168.10.1
Last Valid Host= 192.168.10.14
Subnet Mask= 255.255.255.240

এখানে স্বতন্ত্র মাঝ কিভাবে হল?

মনে রাখতে হবে তখ হোস্ট বিট গুলো 0 আর সকল বিট । করে নিয়ে
হবে পরে অকটেত ধরে ডিসিম্যাল মান কসাতে হবে। যাই । টা স্বতন্ত্র
করা হল আর ১৫ টা স্বতন্ত্র করা যাবে। পরের টা স্বতন্ত্রে টা যাই
তাহলে,



Network Address=192.168.10. 16
Broadcast Address=192.168.10. 31
First Host=192.168.10. 17
Last Host=192.168.10. 30
Subnet Mask=255.255.255.240

এখানে প্রশ্ন আসতে পারে Network Address=192.168.10.
16 কিভাবে হল?

মনে রাখতে হবে প্রথম স্বতন্ত্র এর 4 টা স্বতন্ত্র বিট-ই 0 লি,
মনে 0000 ছিল এখন পরের টাৰ জন্য 0001 হবে এই ভাবে ||||
পৰ্যট যাবে মানে 0 থেকে 15 পৰ্যট মোট 16 টা স্বতন্ত্র তৈরি কৰা
হবে।

যদি 5 টা স্বতন্ত্র টা তৈরি করতে বলা হয় তাহলে উভৰ টা হকে
Network Address=192.168.10. 64
Broadcast Address=192.168.10. 79
First Host=192.168.10. 65

Last Host=192.168.10. 78
Subnet Mask=255.255.255.240

প্রশ্ন-২৬) তোমাকে একটা নেটওর্ক ডিজাইন করতে বলা হল
Appropriate Classful IP Address Use করে যেখানে:

Engineering Department = 40 Host

Human Resource Department = 20 Host

Sales Department = 20 Host

Technical Support Department = 20 Host

Executive Management Department= 20 Host

লাগবে অথবা, বের কৰ: Network Address, Broadcast

Address and Subnet Mask

উভৰ: Engineering Department:

192.168.100.0/26

NA=192.168.100.0/26

BA=192.168.100.63

SM=255.255.255.192

Human Resource Department:

NA=192.168.100.64/27

BA=192.168.100.95

SM=255.255.255.224

Sales Department:

NA=192.168.100.96/27

BA=192.168.100.127

SM=255.255.255.224

Technical Support Department:

NA=192.168.100.128/27

BA=192.168.100.159

SM=255.255.255.224

Executive Management Department:

NA=192.168.100.160/27

BA=192.168.100.191

SM=255.255.255.224

BA: 172.16.4.255/24
SM: 255.255.254.0

প্রশ্ন-২৮) From a given IP like 10.2.3.20/22 find out host Number and Subnet mask? [BTCL-17]

উভৰ: Total Host No = $(2^{10}-2)=1022$ Hosts

Subnet Mask=255.255.252.0

প্রশ্ন-২৯) Let the IP of a host is 10.1.2.146/28. Find the broadcast & network address of this network.

[BPSC-Instructor]

উভৰ: Network Address: 10.1.2.144/28

Broadcast Address: 10.1.2.159/28

প্রশ্ন-৩০) Consider the following IP address

203.208.166.66/27 [প্রধানমন্ত্রীর কার্যালয় - ২০০৮]

a) What is the Subnetmask?

b) What is Subnet Address?

c) What is Broadcast Address?

উভৰ:

a) Subnet Mask = 255.255.255.224

b) Subnet Address=203.208.166.64/27

11001011.11010000.10100110.010 00000	Network Address
	S.A

c) Broadcast address = 203.208.166.95/27

প্রশ্ন-৩১) IP address- 192.168.5.44/26 হতে Subnet mask and Network address বের কৰ? (Find out the Subnet Mask and Network Address in following IP Address; 192.168.5.44/26) [SB & JB (IT/ICT)-18]

উভৰ: Subnet Mask: 255.255.255.192

Network Address: 192.168.5.0/26

প্রশ্ন-৩২) IP address- 172.18.10.0/23 হতে Subnet mask, Subnet address, Start address, Network address and Broadcast address বের কৰ ? [BCSCL-17]

উভৰ: Subnet Mask: 255.255.254.0

Subnet Address:172.18.10.0/23

Start Address: 172.18.10.1/23

Broadcast Address: 172.18.11.255/23

LAN-2:

NA: 172.16.4.0/24

প্রশ্ন-৩৩) Drag and drop the IPv4 network subnets from the left onto the correct usable host ranges

on the right. (বামপাশের আইপি ভার্সন 8 এর নেটওয়ার্ক সাবনেট
অনুসরে তান পাশের সঠিক আইপি এড্রেস রেজ চিহ্নিত করুণ।)

172.28.228.144/18	172.28.228.1 - 172.28.229.254
172.28.228.144/21	172.28.224.1 - 172.28.231.254
172.28.228.144/23	172.28.228.129 - 172.28.228.254
172.28.228.144/25	172.28.228.145 - 172.28.228.150
172.28.228.144/29	172.28.192.1 - 172.28.255.254

উত্তর:

172.28.228.144/18	172.28.192.1 - 172.28.255.254
172.28.228.144/21	172.28.224.1 - 172.28.231.254
172.28.228.144/23	172.28.228.1 - 172.28.229.254
172.28.228.144/25	172.28.228.129 - 172.28.228.254
172.28.228.144/29	172.28.228.145 - 172.28.228.150

প্রশ্ন-৩৮) বামপাশের নেটওয়ার্ক প্যারামিটারের সাথে ডানপাশের সঠিক
মানটি লিখুন। (Drag and drop the networking
parameters from the left onto the correct values
on the right.)

Networking Parameter	Values
Default Gateway	00:0C:22
Host IP Address	00:0C:22:83:79:A3
NIC MAC Address	192.168.1.193
NIC Vendor OUI	192.168.1.200
Subnet Mask	255.255.255.192

উত্তর:

Networking Parameter	Values
Default Gateway	192.168.1.193
Host IP Address	192.168.1.200
NIC MAC Address	00:0C:22:83:79:A3
NIC Vendor OUI	00:0C:22
Subnet Mask	255.255.255.192

প্রশ্ন-৩৬) একটি প্রতিষ্ঠান একটি আইপি আড্রেস দ্রুত সাপোর্ট করে, এ দ্রুতের একটি আড্রেস 205.16.37.39/28 হলে এ দ্রুতের First IP Address & Last IP Address আড্রেস কত?

উত্তর:

205	.	16	.	37	.	0	0	1	0	0	1	1	1
Network Bit				Subnet Bit				Host Bit					
205	.	16	.	37	.	0	0	1	0	0	0	1	First Address
													Last Address
First Address		205.16.37.33											
Last Address		205.16.37.46											

প্রশ্ন-৩৭) 192.20.0.0/27 এই আড্রেস এর জন্য কতটি সাবনেট আছে এবং প্রতিটি সাবনেটে কতটি করে হোস্ট আছে?

উত্তর:

192	.	20	.	0	.	0	0	0	0	0	0	0	0
Network Bit				Subnet Bit				Host Bit					

সাবনেট সংখ্যা = $2^3 = 8$; হোস্ট সংখ্যা = $2^5-2 = 30$

[Note: OUI: An Organizationally Unique Identifier (OUI) is a 24-bit number that uniquely identifies a vendor, manufacturer, or other organization.]

প্রশ্ন-৩৫) দেওয়া আছে, নেটওয়ার্ক আড্রেস 172.18.10.0/23. নেটওয়ার্ক আড্রেস কে চারটি সমান সাবনেটে ভাগ করলে অতলে সাবনেট আড্রেস, স্টার্ট আড্রেস, সাবনেট মাঝ এবং ব্রডকাস্ট আড্রেস কত? (A Given IP Address is: 172.18.10.0/23, If this address is divid by equal 4 subnet. Find out the each 4 subnet address, Start address, Subnet mask, broadcast address.)

উত্তর:

1 st সাবনেট	2 nd সাবনেট
সাবনেট আড্রেস: 172.18.10.0/25	সাবনেট আড্রেস: 172.18.10.128/25
স্টার্ট আড্রেস: 172.18.10.1	স্টার্ট আড্রেস: 172.18.10.129
সাবনেট মাঝ: 255.255.255.128	সাবনেট মাঝ: 255.255.255.128
3 rd সাবনেট	4 th সাবনেট
সাবনেট আড্রেস: 172.18.11.0/25	সাবনেট আড্রেস: 172.18.11.128/25
স্টার্ট আড্রেস: 172.18.11.1	স্টার্ট আড্রেস: 172.18.11.129
সাবনেট মাঝ: 255.255.255.128	সাবনেট মাঝ: 255.255.255.128
ব্রডকাস্ট আড্রেস: 172.18.11.127	ব্রডকাস্ট আড্রেস: 172.18.11.255

প্রশ্ন-৩৮) 182.44.82.16/26 এই আড্রেস এর জন্য প্রথম এবং শেষ আড্রেস কত? [SEO (IT) JB-2015]

উত্তর:

182	.	44	.	82	.	0	0	0	1	0	0	0	0
Network Bit				Subnet Bit				Host Bit					
182	.	44	.	82	.	0	0	0	0	0	0	0	1
First Address													Last Address

প্রথম আড্রেস: 182.44.82.1; শেষ আড্রেস: 182.44.82.62

প্রশ্ন-৩৯) 211.17.180.0 /24 আইপি আড্রেস দেওয়া আছে আভিমিনিস্ট্রাটর ৩২ টা সাবনেট করতে চাইলে সাবনেট মাঝ কি হবে? এবং এতি
সাবনেটে কতটি করে হোস্ট হবে, প্রথম ও শেষ সাবনেটের জন্য প্রথম ও শেষ আড্রেস কত হবে?

উত্তর:

211	.	17	.	180	.	0	0	0	0	0	0	0	0
Network Bit				Subnet Bit				Host Bit					
211	.	17	.	180	.	1	1	1	1	0	0	0	0

প্রথম সাবনেট	শেষ সাবনেট

<tbl_r cells="2" ix="3" maxc

Solution:

Subnet	Network Address	Host Address	Broadcast Address
Subnet Mask: 255.255.255.224			
First Subnet	192.168.162.0	192.168.162.1 to 192.168.162.30	192.168.162.31
Second Subnet	192.168.162.32	192.168.162.33 to 192.168.162.62	192.168.162.63
Third Subnet	192.168.162.64	192.168.162.65 to 192.168.162.94	192.168.162.95
Fourth Subnet	192.168.162.96	192.168.162.97 to 192.168.162.126	192.168.162.127
Fifth Subnet	192.168.162.128	192.168.162.129 to 192.168.162.158	192.168.162.159
Sixth Subnet	192.168.162.160	192.168.162.161 to 192.168.162.190	192.168.162.191
Seventh Subnet	192.168.162.192	192.168.162.193 to 192.168.162.222	192.168.162.223
Eight Subnet	192.168.162.224	192.168.162.225 to 192.168.162.254	192.168.162.255

Question-2) The bitBox Group would like to subnet its network (195.5.5.0) so that there are 50 Separate subnets. They will need only 2 hosts in each subnet. Complete each of the following:
 [Note: Because there are so many subnets, you don't need to write them all out. If you can fill in the information required below (the subnet mask, the addresses for the first few subnets, and the total number of subnets created), you obviously get the idea.]

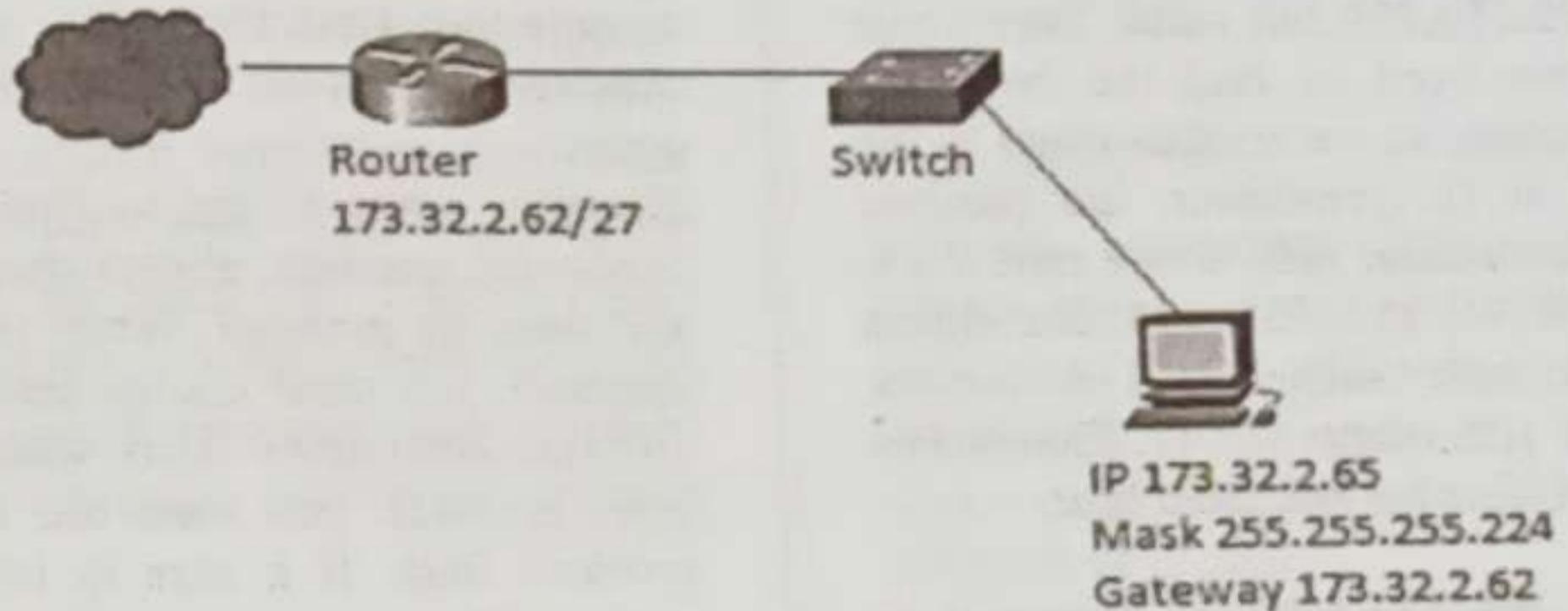
Subnet	Network Address	Host Address	Broadcast Address
Subnet Mask: 255.255.255.----			
First Subnet	195.5.5.----	195.5.5.---- to 195.5.5.----	195.5.5.----
Second Subnet	195.5.5.----	195.5.5.---- to 195.5.5.----	195.5.5.----
Third Subnet	195.5.5.----	195.5.5.---- to 195.5.5.----	195.5.5.----
Fourth Subnet	195.5.5.----	195.5.5.---- to 195.5.5.----	195.5.5.----
Fifth Subnet	195.5.5.----	195.5.5.---- to 195.5.5.----	195.5.5.----
Sixth Subnet	195.5.5.----	195.5.5.---- to 195.5.5.----	195.5.5.----
Seventh Subnet	195.5.5.----	195.5.5.---- to 195.5.5.----	195.5.5.----

How many subnets are actually created with this subnet mask you used?

Solution:

Subnet	Network Address	Host Address	Broadcast Address
Subnet Mask: 255.255.255.22			
First Subnet	195.5.5.0	195.5.5.1 to 195.5.5.2	195.5.5.3
Second Subnet	195.5.5.4	195.5.5.5 to 195.5.5.6	195.5.5.7
Third Subnet	195.5.5.8	195.5.5.9 to 195.5.5.10	195.5.5.11
Fourth Subnet	195.5.5.12	195.5.5.13 to 195.5.5.14	195.5.5.15
Fifth Subnet	195.5.5.16	195.5.5.17 to 195.5.5.18	195.5.5.19
Sixth Subnet	195.5.5.20	195.5.5.21 to 195.5.5.22	195.5.5.23
Seventh Subnet	195.5.5.24	195.5.5.25 to 195.5.5.26	195.5.5.27

There are 64 subnets are actually created with this subnet mask i used!!!

Question-3) What is the problem in this Network?**Solution:** 11111111.11111111.11111111.11100000

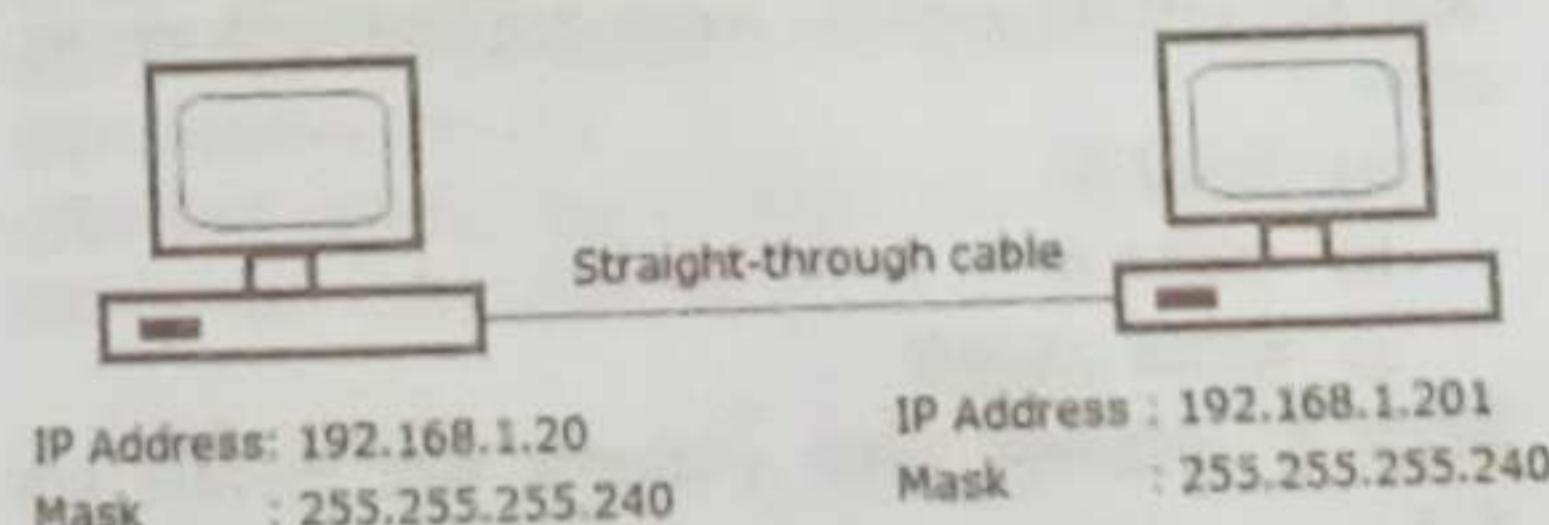
Magic Number is: 32
 N1 → 0 – 31
 N2 → 32 – 63
 N3 → 64 – 95
 N4 → 96 – 127

Router is in network N2
 Host is in network N3
 So the router and the host are in separate networks.
 So if 173.32.2.62/26
 Subnet Mask is: 255.255.255.192
 Magic Number is: 64

N1 → 0 – 63
 N2 → 64 – 127
 N3 → 128 – 191
 N4 → 192 – 255

Also is a separate network, so change Ip address of the host to be any address in the following range:
 173.32.2.33 to 173.32.2.61

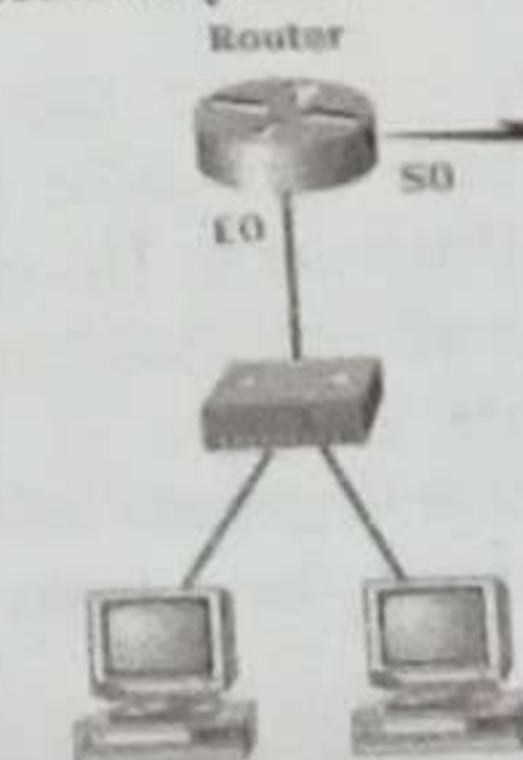
Question-4) A network administrator is connecting hosts A and B directly through their Ethernet interfaces, as shown in the illustration. Ping attempts between the hosts are unsuccessful. What can be done to provide connectivity between the hosts?
 [ANE, BCC-Lab -2021]

**Answer:**

1. A crossover cable should be used in place of the straight-through cable.
 2. The subnet masks should be set to 255.255.255.0.
- Because, first, if you have two hosts directly connected, as shown in the graphic, then you need a crossover cable. A straight-through cable won't work.

Second, the hosts have a different mask, which puts them in different subnets. The easy solution is just to set both masks to 255.255.255.0 (/24).

Question-5) Using the following illustration, what would be the IP address of E0 if you were using the eighth subnet? The network ID is 192.168.10.0/28 and you need to use the last available IP address in the range. The zero subnet should not be considered valid for this question. [ANE, BCC-Lab-2021]



Answer: 192.168.10.142

Because, A /28 is a 255.255.255.240 mask. Let's count to the ninth subnet (we need to find the broadcast address of the eighth subnet, so we need to count to the ninth subnet). Starting at 16 (remember, the question stated that we will not use subnet zero, so we start at 16, not 0), 16, 32, 48, 64, 80, 96, 112, 128, 144. The eighth subnet is 128 and the next subnet is 144, so our broadcast address of the 128 subnet is 143. This makes the host range 129-142. 142 is the last valid host.

Question-6) Network 206.143.5.0 was assigned to the Acme Company to connect to its ISP. The administrator of Acme would like to configure one router with the commands to access the Internet. Which commands could be configured on the Gateway router to allow Internet access to the entire network?

Answer:

```
Gateway (config) # ip route 0.0.0.0 0.0.0.0  
206.143.5.2  
Gateway (config-router) # network 206.143.5.0  
default
```

Because, there are actually three different ways to configure the same default route, but only two are shown in the answer. First, you can set a default route with the 0.0.0.0 0.0.0.0 mask and then specify the next hop, as in option A. Or you can use 0.0.0.0 0.0.0.0 and use the exit interface instead of the next hop. Finally, you can use option D with the ip default-network command.

Question-7) You are working on a router that has established privilege levels that restrict access to certain functions. You discover that you are not able to execute the command show running-configuration. How can you view and confirm the access lists that have been applied to the Ethernet 0 interface on your router?

Answer: show ip interface Ethernet 0

Because, the only command that shows which access lists have been applied to an interface is show ip interface Ethernet 0. The command show access-lists displays all configured access lists, and show ip access-lists displays all configured IP access lists, but neither command indicates whether the displayed access lists have been applied to an interface.

Question-8) What command will permit SMTP mail to only host 1.1.1.1?

Answer: access-list 110 permit tcp any host 1.1.1.1 eq smtp

Because, when trying to find the best answer to an access-list question, always check the access-list number and then the protocol. When filtering to an upper-layer protocol, you must use an extended list, numbers 100, 199 and 2000-2699. Also, when you filter to an upper-layer protocol, you must use either tcp or udp in the protocol field. If it says ip in the protocol field, you cannot filter to an upper-layer protocol. SMTP uses TCP.

Question-9) You get a call from a network administrator who tells you that he typed the following into his router:

```
Router (config) #router ospf 1  
Router (config-router) #network 10.0.0.0 255.0.0.0  
area 0
```

He tells you he still can't see any routes in the routing table. What configuration error did the administrator make?

Answer: The wildcard mask is incorrect. Because, the administrator typed in the wrong wildcard mask configuration. The wildcard should have been 0.0.0.255

Network Security

প্র-১) ক্রিপ্টোগ্রাফি কি? এটা কিভাবে করা হয়? (What is Cryptography? How is it done?) [ICT-Lecture, NTRCA-2011, 2014, 2015, 2016, 2017, 2018]

উত্তর: ক্রিপ্টো (Crypto) শব্দ থেকে ক্রিপ্টোগ্রাফি (Cryptography) শব্দালোচন উৎপন্ন। আর, ক্রিপ্টো শব্দের অর্থ হচ্ছে স্কুনো (Hidden)। তাহলে ক্রিপ্টোগ্রাফি অর্থ হচ্ছে ‘তাপ্তকবিদ্যা’। অর্থাৎ ক্রিপ্টোগ্রাফি এমন এক ধরণের বিন্যা যা কিন্তু তাকে গোপন করা বা স্কুনোর জন্য ব্যবহৃত হয়। অন্যভাবে কথে গেলে ক্রিপ্টোগ্রাফি হল এক ধরণের কৌশল বা টেকনিক যাতে Plain Text ভাষাকে এনক্রিপ্ট করা হয় যেনে ভাষা বোঝা ও ব্যাখ্যা কর্তৃপক্ষে হয়। বেশ কিছু অ্যালগরিদম ব্যবহার করে ক্রিপ্টোগ্রাফি করা হয়। যেমন:

- সিক্রেট কোড
- প্রাবলিক কোড
- ম্যাসেজ ডাইজেন্স

সিক্রেট কোড এনক্রিপ্শন: প্রেরক ও প্রাপকের কাছে Private key থাকে।

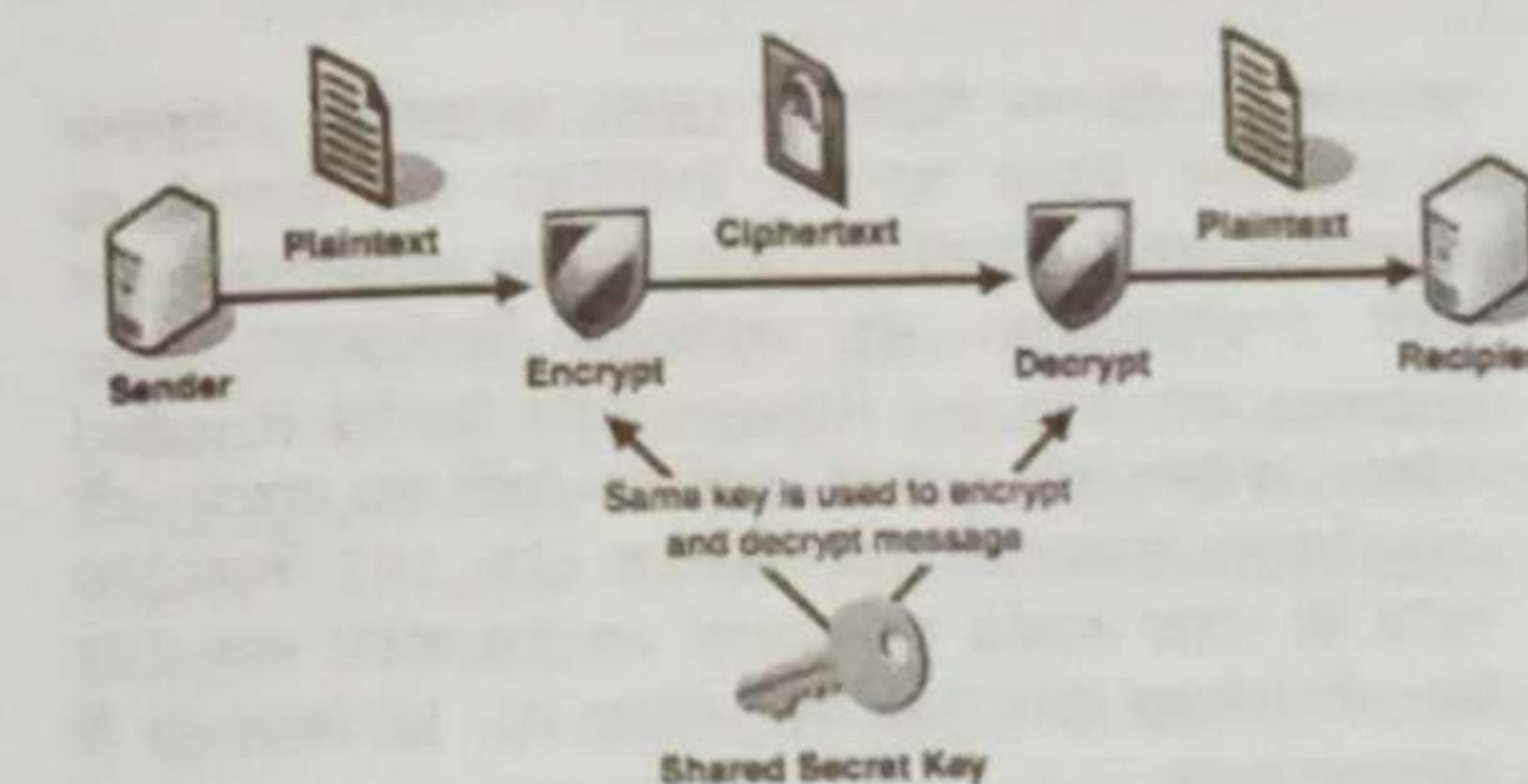
প্রাবলিক কোড এনক্রিপ্শন: এই এনক্রিপ্শন ব্যবহার সব ইউজারের কাছে Private key থাকে। শেষের জোরেইনে এটি সহজ নয়।
ম্যাসেজ ডাইজেন্স: অকৃত তথ্য প্রেরণ করা হয় না, সক্রিয় যা প্রেরণ করা হয়। এইভাবে প্রাপক থেকে সেই সামৰ্থ্যকাল অনুসরে নির্ণয় করে ভাষা নির্ধারণ করা হয়। MD-5 Hashing এর মধ্যে ডাইজেন্সের উদাহরণ।

প্র-২) What is meant by Encryption and Decryption? (এনক্রিপশন ও ডিক্রিপশন কাকে বলে?) [SAE-Agriculture Ministry-2021]

উত্তর: Encryption: যে প্রক্রিয়ায় অ্যালগরিদম ব্যবহার করে নেটওর্কের তথ্য কে প্রসেস করে সবার কাছে পড়ার অযোগ্য (Unreadable) করে তোলা হয়, তাকে ভেটা এনক্রিপশন বলে। এনক্রিপশনকৃত ভাষাকে এনক্রিপ্ট বা সাইফার টেক্সট বলে। মূলত ভাষারের নিরাপত্তা ব্যবস্থা শক্তিশালী করার জন্য ভেটা এনক্রিপশন করা হয়। ভেটা এনক্রিপশনের অনেকগুলো পক্ষতি রয়েছে, তার মধ্যে বহুল ব্যবহৃত ওটি পক্ষতি হলো:

সিজার কোড (Caeser Code)

- ভেটা এনক্রিপশন স্ট্যার্ড (Data Encryption Standard)
- আন্তর্জাতিক ডেস এনক্রিপশন এলগরিদম (IDEA)

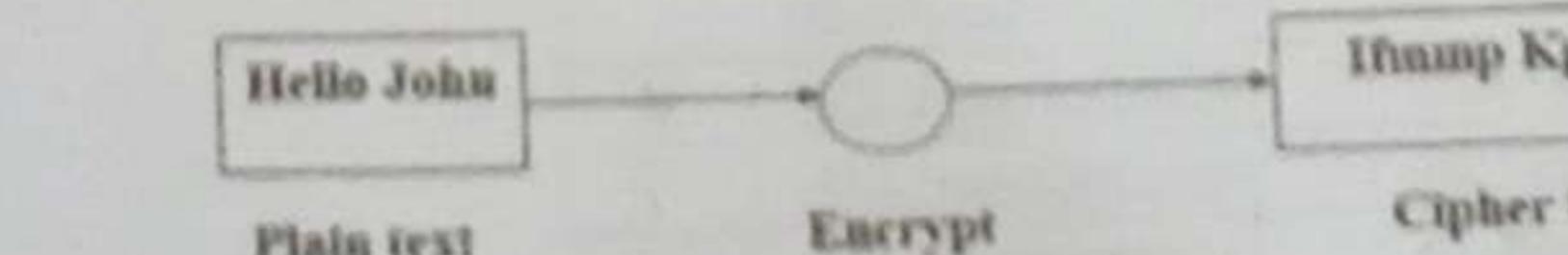


Decryption: আমরা আগেই জেনেছি যে এনক্রিপশনের মাধ্যমে ভাষাকে এনক্রিপ্ট করা ভাষাকে এনক্রিপ্ট ভাষা বা সাইফার টেক্সট বলে। পরে এই এনক্রিপ্ট ভাষা বা সাইফার টেক্সট রিভ করার জন্য বা Plain টেক্সট (Normal text / Human Readable text) রিপার্স করার পক্ষতিকে ডিক্রিপশন বলে।

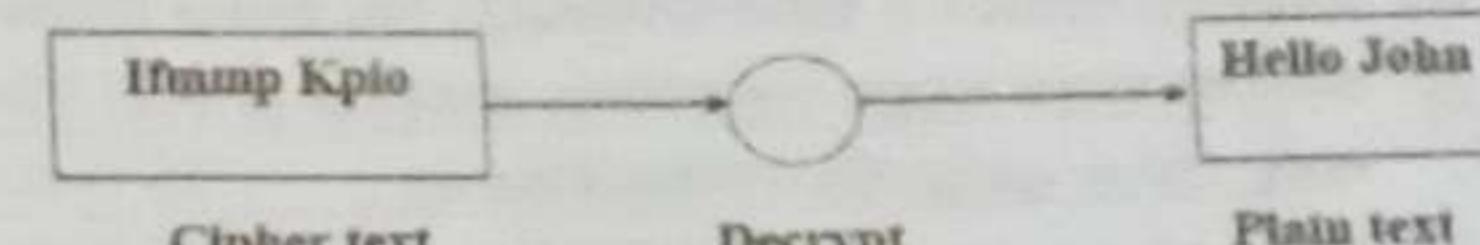
প্র-৩) প্রেইন টেক্সট ও সাইফার টেক্সট, এনক্রিপশন অ্যালগরিদম ও সিকিউরিটি কোড কি? (What are Plain text and Cipher text, Encryption algorithm and Security code?)

উত্তর: যে পক্ষতিতে মূল ভেটাকে বিশেষ কোডের মাধ্যমে পরিবর্তন করা হয় তাকে ভেটা এনক্রিপশন বলে। অনিদিষ্ট বা অপরিচিত বাকির হাত থেকে ভেটাকে পোশনীয়তা রক্ষা করার জন্য বা ভেটা সিকিউরিটির জন্য ভেটা এনক্রিপশন করা হয়।

প্রেইন টেক্সট (Plain Text): এনক্রিপ্ট করার পূর্বের ভেটা যা পাঠ করা যায় তাকে প্রেইন টেক্সট বলে।



সাইফারটেক্সট (Cipher-text): এনক্রিপ্ট করার পরের ভেটা যা পাঠ করা যায় না তাকে সাইফারটেক্সট বলে।



এনক্রিপশন অ্যালগরিদম (Encryption Algorithm): যে গাণিতিক ফর্মুলার মাধ্যমে প্রেইন টেক্সট থেকে সাইফারটেক্সট এ রূপান্বয় করা হয় তাকে এনক্রিপশন অ্যালগরিদম বলে।

সিকিউরিটি কোড (Security key or Code): যে গোপন সংরক্ষণ বা কোডের মাধ্যমে ভেটা এনক্রিপ্ট ও ডিক্রিপ্ট করা হয় তাকে সিকিউরিটি কোড বলে।

প্র-৪) ভেটা এনক্রিপ্ট করার বিভিন্ন পক্ষতি আলোচনা কর। (Explain different types of Data Encryption Algorithm.)

- উত্তর: ভেটা এনক্রিপ্ট করার বিভিন্ন পক্ষতি প্রধানত তিনটি। যেহেন:
- সিজার কোড (Caesar Code)
 - ভেটা এনক্রিপশন স্ট্যার্ড (Data Encryption Standard-DES)
 - আন্তর্জাতিক ডেস এনক্রিপশন অ্যালগরিদম-IDEA
 - ট্রিপল ডিইএস (Triple DES)
 - অভ্যন্তর এনক্রিপশন স্ট্যার্ড (Advanced Encryption Standard-AES)

সিজার কোড (Caesar Code): এ পক্ষতিতে ইংরেজি প্রত্যেক বর্বরের জন্য নিম্নিষ্ঠ ক্রম অনুসৰি নিম্নিষ্ঠ বর্ণ ব্যবহার করা হয়।
যেহেন: ইংরেজি প্রত্যেক বর্বরকে তার পরবর্তী বর্ণ ঘাসা প্রতিস্থাপন করলে-bitBox শক্তির এনক্রিপশনকৃত শক্তি হলো cjuCpy। এখানে মূল শক্তের প্রত্যেক বর্বরের পরবর্তী বর্ণ ব্যবহার করে এনক্রিপ্ট করা হয়েছে।

ভেটা এনক্রিপশন স্ট্যার্ড (Data Encryption Standard-DES):

- এ পক্ষতিতে মূল ভেটাকে প্রত্যেক বর্ণকে ইংরেজি বর্ণমালার ক্রম অনুসৰে অবস্থান নির্ধারণ করা হয়। যেহেন: A এর অবস্থানগত মান 1 এবং C এর অবস্থানগত মান 3।

0	S	I	18	R
1	A	10	19	S
2	B	11	20	T
3	C	12	21	U
4	D	13	22	V
5	E	14	23	W
6	F	15	24	X
7	G	16	25	Y
8	H	17	26	Z

0→null
1→A
2→B
...
26→Z

- b) অবস্থানগত সংখ্যাকে 8 দ্বারা গুণ করা হয়।
 c) উপর্যুক্ত মানকে অবস্থান ধরে বর্ণমালার ক্রমানুসারে যে বর্ণটি পাওয়া যায় তা এনক্রিপ্টেড বর্ণ হিসাবে ধরা হয়।
 d) উপর্যুক্ত 26 অল্পকা বড় হলে উপর্যুক্ত 26 দ্বারা মডুলাস (%) করে সেই ভালু নিতে হবে বা ভাগ(/) করে ভাগশেষ নির্ণয় করা হয়। একেতে ভাগশেষের মানকে অবস্থান ধরে বর্ণমালার ক্রমানুসারে যে বর্ণটি পাওয়া যায় তা এনক্রিপ্টেড বর্ণ হিসাবে ধরা হয়।

এ পদ্ধতিটি CAESAR শব্দটি এনক্রিপ্ট করি:

$$\begin{array}{rcl} C & = & 3X8 = 24 \rightarrow X \\ A & = & 1X8 = 8 \rightarrow H \\ E & = & 5X8 = 40 \rightarrow 40 \mod 26 \rightarrow \text{ভাগশেষ } 14 \rightarrow N \\ S & = & 19X8 = 152 \rightarrow 152 \mod 26 \rightarrow \text{ভাগশেষ } 22 \rightarrow V \\ A & = & 1X8 = 8 \rightarrow H \\ R & = & 18X8 = 144 \rightarrow 144 \mod 26 \rightarrow \text{ভাগশেষ } 14 \rightarrow N \end{array}$$

সুতরাং CAESAR শব্দটি এনক্রিপ্ট হয়ে XHNVHN হয়ে পেল, যা Cipher-text হিসেবে পরিচিত।

ইন্টারনেট্যাশনাল ডেটা এনক্রিপশন অ্যালগরিদম (IDEA): ইন্টারনেট্যাশনাল ডেটা এনক্রিপশন অ্যালগরিদম হলো সুইজারল্যান্ড এর জুরিখের ETH (ETH Zurich, Eidgenössische Technische Hochschule (ETH) Zürich, Other name, Swiss Federal Institute of Technology in Zurich) তে উভাবিত একটি অ্যালগরিদম। যা 128 বিট কী-সম্পর্ক একটি ব্লক সাইফার ব্যবহার করে যার ব্লক সাইজ 64 বিটের এবং এটিকে প্রচলিত বিভিন্ন এনক্রিপশন পদ্ধতির চাইতে তুলনামূলকভাবে অনেক বেশী নিরাপদ একটি এনক্রিপশন পদ্ধতি বলে মনে করা হয়। মূলত এই অবিকাশ ইউরোপিয়ান সেশনগোতে এই পদ্ধতির প্রয়োজন করা হয়েছে। অবাসিয়াক কাজে বিনামূল্যেই IDEA কে ব্যবহার করা যায়। তবে বাসিয়াক কাজে ব্যবহার করার জন্য লাইসেন্স কিনতে হয়।

ট্রিপল ডিইএস (Triple DES): ট্রিপল ডিইএস হলো বাস্তুত কিছু নিরাপত্তা প্রদান করতে DES কে ব্যবহার করার একটি পদ্ধতি। ইয়া প্রতিটি ডেটাকে Block করতে তিনবার DES সাইফার অ্যালগরিদম

প্রশ্ন-৫) চিঠের Plaintext এবং Ciphertext ক্যারেক্টার দেখানো হলো মডুলো 26 এর মধ্যে। "hello" বার্তাটি key=15 ধরে আভিটি সিফারটি ব্যবহার করে এনক্রিপ্ট করুন। [NTRCA-2015]

Plaintext →	a b c d e f g h i j k l m n o p q r s t u v w x y z
Ciphertext →	A B C D E F G H I J K L M N O P Q R S T U V W X Y Z
Value →	00 01 02 03 04 05 06 07 08 09 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25

উত্তর: আমরা প্রতিটি ক্যারেক্টার এনক্রিপশন অ্যালগরিদম ব্যবহার করে তৈরি করবো।

Plaintext: h → 07	Encryption: (07 + 15) mod 26	Ciphertext: 22	W
Plaintext: e → 04	Encryption: (04 + 15) mod 26	Ciphertext: 19	T
Plaintext: l → 11	Encryption: (11 + 15) mod 26	Ciphertext: 00	A
Plaintext: l → 11	Encryption: (11 + 15) mod 26	Ciphertext: 00	A
Plaintext: o → 14	Encryption: (14 + 15) mod 26	Ciphertext: 03	D

এনক্রিপ্টকৃত ফলাফল হচ্ছে: "WTAAD"

প্রশ্ন-৬) উপরের চিঠে হতে "WTAAD" বার্তাটি key=15 ধরে আভিটি সিফারটি ব্যবহার করে ডিক্রিপ্ট করুন।

উত্তর: আমরা প্রতিটি ক্যারেক্টার ডিক্রিপ্শন অ্যালগরিদম ব্যবহার করে তৈরি করবো।

Ciphertext: W → 22	Decryption: (22 - 15) mod 26	Plaintext: 07	h
Ciphertext: T → 19	Decryption: (19 - 15) mod 26	Plaintext: 04	e
Ciphertext: A → 00	Decryption: (00 - 15) mod 26	Plaintext: 11	l
Ciphertext: A → 00	Decryption: (00 - 15) mod 26	Plaintext: 11	l
Ciphertext: D → 03	Decryption: (03 - 15) mod 26	Plaintext: 14	o

ডিক্রিপ্টকৃত ফলাফল হচ্ছে: "hello"

প্রশ্ন-৭) নিচের চিঠে হতে "Computer Networks" এই মেসেজটি এনক্রিপ্ট করুন? (Encrypt the "Computer Network" message from the image in below.)

Plaintext →	a b c d e f g h i j k l m n o p q r s t u v w x y z
Ciphertext →	N O A T R B E C F U X D Q G Y L K H V I J M P Z S W

উত্তর: AYQLJIRHGRIPYHXV

প্রশ্ন-৮) Polyalphabetic Clifiers কি? Monoalphabetic Ciphers কেন ভাল? (What is Polyalphabetic Cipher?)

Why Monoalphabetic Cipher is good?

উত্তর: একটি Polyalphabetic cipher হল Substitution এর উপর ভিত্তি করে যেকোন সাইফার, যা Multiple Substitution Alphabets ব্যবহার করে। সভ্যত �Vigenere সাইফার একটি পলিঅলফাবেটিক সাইফারের স্বচেতে পরিচিত উন্নাহরণ, যদি ও ইয়া একটি বিশেষ ক্ষেত্রে Simplified হয়ে থাকে। Polyalphabetic cipher এ, এনক্রিপশন কী এর উপাদান অনুসারে প্রতিশ্বাসনের নিয়ম অন্তর থেকে অন্তর ক্রমাগত পরিবর্তিত হয়।

উন্নাহরণ: যদি "a" প্রথমে enciphered হয় তবে "N" হবে। Polyalphabetic ciphers এর সুবিধা হল letter frequency hide (শুকাতে) করতে পারে। তাই এই প্রকার এনক্রিপশন এ Brute-Force Attack Key শুরু করে আটক প্রতিরোধ করা যায়।

প্রশ্ন-৯) Polyalphabetic autokey cipher ব্যবহার করে যথিম সানিয়াকে মেসেজ সেট করতে চাচ্ছে, যদি পারিস্কী কী $k_1 = 12$ এবং মেসেজটি "Attack is today" হয় তাহলে এনক্রিপ্টেড হলে কি হবে?

উত্তর: অক্ষর বাই অক্ষর Enciphering হয়, প্রত্যেক Plaintext ক্যারেক্টার পরিবর্তন হয় তার ইন্টিজার ভালু দ্বারা, সিফারটেক্ট হওয়ার জন্য প্রথম ক্যারেক্টারের সাথে Plaintext ইন্টিজার ভালুর সাথে কী হিসেবে আগের Plaintext ইন্টিজার ভালু ব্যবহার হবে, নিম্নে উন্নাহরণ দেওয়া হল: ভালু $k_1 = 12$ "Attack is today"

$$\begin{array}{ll} P = P_1 P_2 P_3 \dots & C = C_1 C_2 C_3 \dots \\ \text{Encryption: } C_i = (P_i + k_i) \bmod 26 & \text{Decryption: } P_i = (C_i - k_i) \bmod 26 \\ \text{initial key value } k_1 = 12. & \end{array}$$

Enciphering:	a t t a c k i s t o d a y
P's Values:	0 19 19 0 2 10 8 18 19 14 3 0 24
Key stream:	12 0 19 19 0 2 10 8 18 19 14 3 0
C's Values:	12 19 12 19 2 12 18 0 11 7 17 3 24
Ciphertext:	M T M T C M S A L H R D Y

Deciphering:	M T M T C M S A L H R D Y
C's Values:	12 19 12 19 2 12 18 0 11 7 17 3 24
Key stream:	12 0 19 19 0 2 10 8 18 19 14 3 0
P's Values:	0 19 19 0 2 10 8 18 19 14 3 0 24
Plaintext:	a t t a c k i s t o d a y

প্রশ্ন-১০) উপরুক্ত উদাহরণ ও ভাষ্যকাম সহ Asymmetric-Key Ciphers বর্ণনা কর। (Explain Asymmetric key ciphers with appropriate examples and diagrams.)

উত্তর: সুইট অলান অলান (আইডেট, পাবলিক) কী ব্যবহার করে। এই প্রকার ক্লিন্ট এম এ সেভার রিসিভার এর পাবলিক কী দিয়ে মেসেজ এনক্রিপ্ট করে পাঠাবে, রিসিভার তার প্রাইভেট কী দিয়ে তার মেসেজ পাঠাবে। নিচের চিত্রে Alice Bob কে মেসেজ পাঠাবে, Bob এ পাবলিক কী দিয়ে মেসেজ এনক্রিপ্ট করে যাখানে পাঠাবে, Bob তার মেসেজ কে তার প্রাইভেট করে রিড করবে, পাবলিক কী দিয়ে করার জন্য অলান Public-Key Distribution Channel চালেন শালবে, message sent এর জন্য অলান unsecured চালেন শালবে

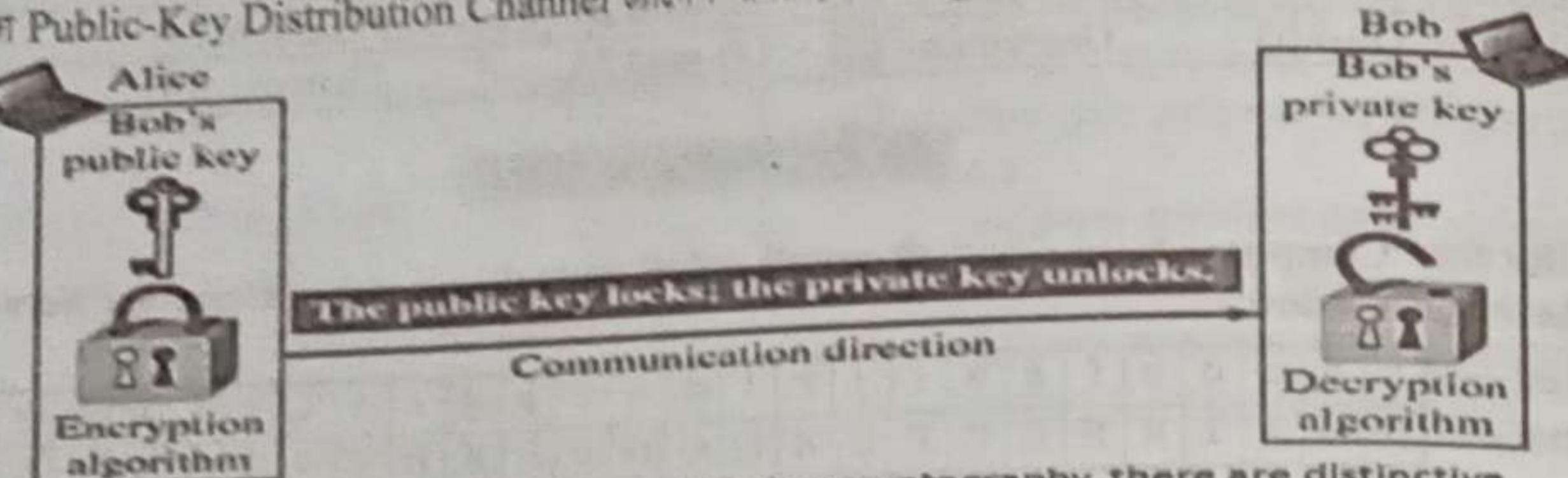


Figure: Locking and unlocking in asymmetric-key cryptosystem

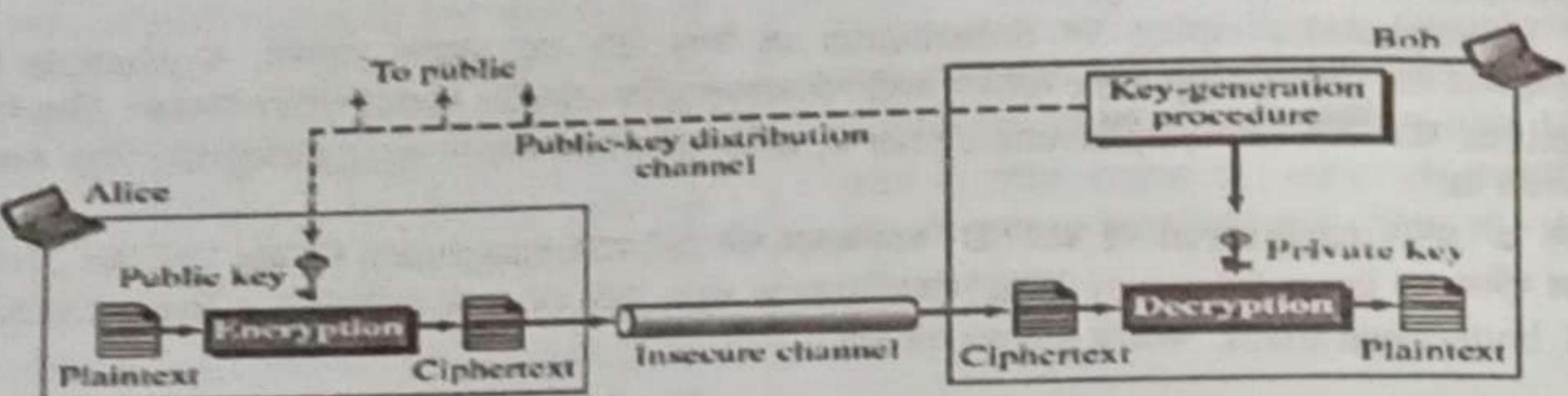


Figure: General idea of asymmetric-key cryptosystem

প্রশ্ন-১১) Message digest কি? এটি কিভাবে মেসেজের Integrity সংরক্ষণ করে? (What is Message Digest? How does it save/Store message integrity?)

উত্তর: Message Digest হচ্ছে একটি Cryptographic Hash Function, যা কিনা One Way Hashing Formula ব্যবহার করে Digits তৈরির মাধ্যমে একটি স্ট্রিং (String) ধৰণ করে। একটি ডাটার পরিবর্তন জনিত, মেসেজের কোন অংশের পুনরুৎসৃষ্টি করে। একটি ডকুমেন্ট সংরক্ষিত রাখা যাব ত্রিস্তুতি ব্যবহারের মাধ্যমে। যার ফলে ডকুমেন্টস এর কোন পরিবর্তন হয়না। একে ডকুমেন্ট এবং তাইসের Alice's ক্লিন্টিট সূচাকেই তুলনা (Compare) করা হয়। যদি দুটো একইরকম না হয়, তাহলে এর Alice's ক্লিন্টিট এবং সাইসের Alice's ক্লিন্টিট সূচাকেই তুলনা (Compare) করা হয়। যদি দুটো একইরকম না হয়, তাহলে ডকুমেন্ট এবং বিস্তারিতের সমতুল্য ইলেক্ট্রনিক Pair (যুগল) হচ্ছে মেসেজ এবং ডাইজেন্ট Pair (যুগল)। ডকুমেন্টস এর না। ডকুমেন্ট এবং বিস্তারিতের সমতুল্য ইলেক্ট্রনিক Pair (যুগল) হচ্ছে মেসেজ এবং ডাইজেন্ট Pair (যুগল)। মেসেজের ইন্টিগ্রিটি সংরক্ষিত রাখার জন্য Message Cryptographic Hash Function নামক এলগরিদম এর মধ্য দিয়ে মেসেজ Passed করা হয়। ইহা ফাংশন মেসেজের একটা কম্প্রেসড ইমেজ (Compressed Image) তৈরি করে যা ডাইজেন্ট (Digest) নামে পরিচিত এবং কিনা ক্লিন্ট হিসেবে ব্যবহৃত হয়।

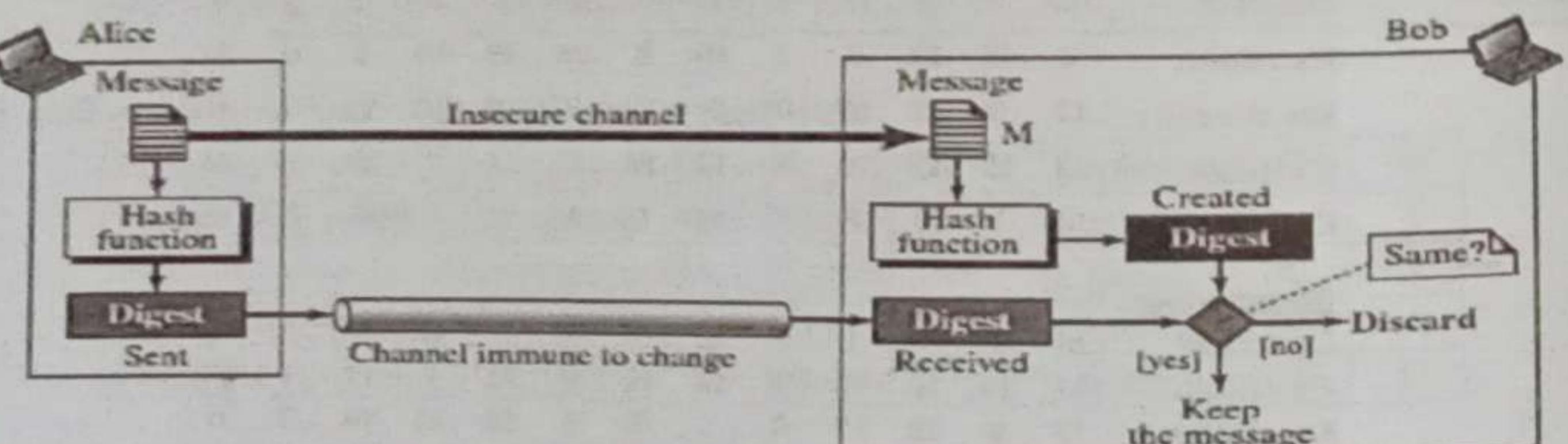


Figure: Message and digest

কোন ডকুমেন্টস বা মেসেজের ইন্টিগ্রিটি চেক করার জন্য Bob পুনরায় ক্লিন্টমাফিক হ্যাশ ফাংশন রাখ করে এবং নতুন ডাইজেন্ট ও পুরাতন ডাইজেন্ট এর সাথে তুলনা করে। যদি ডাইজেন্ট একই হয়, Bob নিশ্চিত হয় যে, অরিজিনাল মেসেজ এর কোন পরিবর্তন নাই।

প্রশ্ন-১২) হ্যাশ ও হ্যাশিং কাকে বলে? (What is Hash and Hashing?)

উত্তর: ক্রিপ্টোগ্রাফির উপরুক্তপূর্ব একটি বিষয় হচ্ছে হ্যাশ। হ্যাশ হচ্ছে কোনো ডাটার এনক্রিপ্টড স্ট্রিং ডাটা বা ডাটা সুরক্ষার জন্য ক্লিন্টমাফিক (Cryptography) এর একটি টেকনিক। আর কোনো ডাটাকে এনক্রিপ্ট করে হ্যাশ পরিণত করার প্রক্রিয়াকে হ্যাশিং (Hashing) বলা হয়। হ্যাশ ডিক্রিপ্ট করার কোনো কৌশল নেই। কারণ হ্যাশিং করা এনক্রিপ্টড ডাটা তথ্য হ্যাশকে মূল ডাটায় রূপান্বয় করার কোনো Key নেই। এক কথায়, কোনো কোনো ডাটাকে হ্যাশে এনক্রিপ্ট করা যায়, তবে ডিক্রিপ্ট করে মূল ডাটায় রূপান্বয় করা যায় না। হ্যাশিংয়ের মাধ্যমে গবেষণার উপরুক্তপূর্ব তথ্য, পাসওয়ার্ড, ক্রেডিট কার্ড নম্বর, সংবেদনশীল তথ্য ইত্যাদি এনক্রিপ্ট করা হয় যাতে কেউ তা সহজে বের করতে না পারে। বিভিন্ন প্রকার হ্যাশিং মেথডের মধ্যে MD4, MD5, SHA-1, SHA-2 ইত্যাদি উল্লেখযোগ্য।

হ্যাশিং পদ্ধতি ব্যবহার করে কোন ডাটাকে একবার হ্যাশ করে পরিবর্তন করা হলে তা আর মূল ডাটাটে রূপান্বয় করা সম্ভব না। কারণ হ্যাশ ফাংশন ব্যবহার করে যত বড় বা ছোট ইনপুটকে হ্যাশ করা হয়না কেন এটি সর্বসময় Fixed-Length Signature তৈরি করে। MD5 Algorithm ব্যবহার করলে যেকোন ইনপুটের জন্য 32 ক্যারেক্টোর আউটপুট পাওয়া যায় এবং SHA256 Algorithm ব্যবহার করলে যেকোন ইনপুটের জন্য 64 ক্যারেক্টোর আউটপুট পাওয়া যায়।

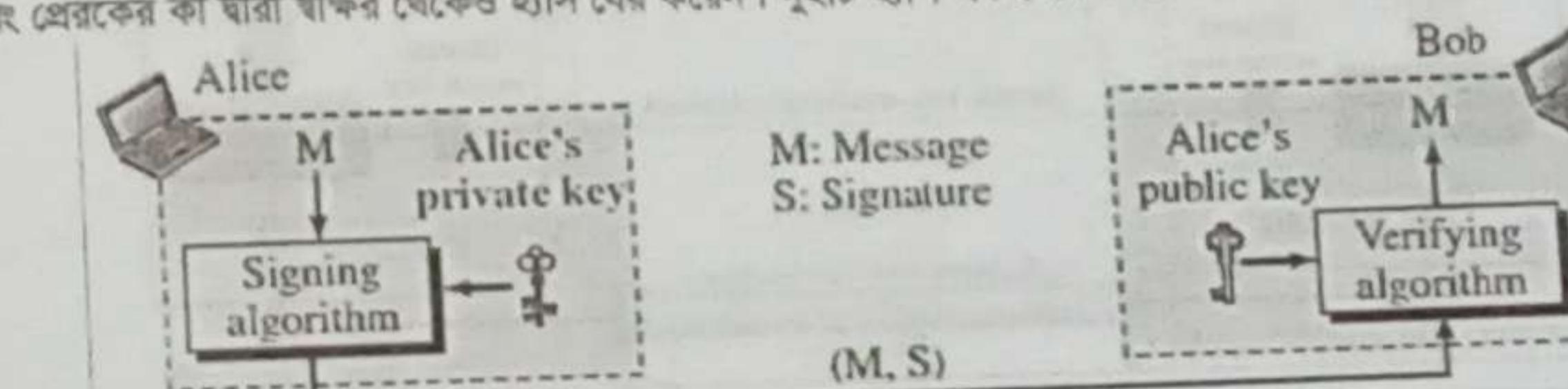
উদাহরণ: যদি "bitBox" এই শব্দটিকে যেকোনো একটি হ্যাশিং মেথডে এনক্রিপ্ট করা হয়। MD5 Algorithm ব্যবহার করে এটিকে এনক্রিপ্ট করলে হবে 2ad03abbc710b8fd8de4f8907c5171c। যা কিনা 32 ক্যারেক্টোর এর একটি স্ট্রিং। এখানে, 2ad03abbc710b8fd8de4f8907c5171c এটি হলো হ্যাশ আর bitBox শব্দটি হলো মূল ডাটা।

প্রশ্ন-১৩) ডিজিটাল সিগনচার প্রসেস বর্ণনা কর। কিভাবে এটা মেসেজ ইন্টেগ্রিটি ও অব্যবহৃতকেশন প্রদান করে? (Explain Digital Signature Process? How it gives Message integrity and Authentication?)

উত্তর: সাধারণত হস্তপ্রিয়ত কোন ব্যক্তিরকে জ্ঞান করে কোন প্রিন্টেড ডকুমেন্টে সংযুক্ত করার মাধ্যমে ধৰে নেওয়া হয় উক্ত ডকুমেন্ট যথাযথ প্রেরকের কাছ হতে উৎপন্ন হয়েছে। সত্যিকার অর্থে ইহা ডিজিটাল ব্যক্তির ইলেক্ট্রনিক মেসেজের মতো একই কার্য সম্পাদন করে। ডিজিটাল ব্যক্তির হলো একটি মেসেজ ডাইজেন্ট এর এনক্রিপ্টেড ভার্সন যা একটি মেসেজের সাথে একেরে সংযুক্ত থাকে। একটি মেসেজের সাথে একেরে সংযুক্ত থাকে। একটি মেসেজের সাথে একেরে সংযুক্ত থাকে।

- ✓ নিজের জন্য প্রাইভেট কী, যা দ্বারা ডিজিটাল ব্যক্তির সৃষ্টি করা হয়।
- ✓ স্বার্ব জন্য পাবলিক কী, যা দ্বারা ডিজিটাল ব্যক্তির যাচাই করা হয়।

একটি ডকুমেন্টে ডিজিটাল ব্যক্তির ব্যবহার পদ্ধতিতে যেকোন জালিয়াতি ধৰা সম্ভব এবং এ পদ্ধতিতে যথাযথ ব্যক্তি দ্বারা সুরক্ষিত হয়ে থাকে। প্রেরক যে দলিল পাঠাবে তা কম্পিউটারের প্রয়োগ ব্যবহার করে হ্যাশ তৈরি করে, তারপর তার গোপনীয় কী দিয়ে উক্ত হ্যাশটিকে যাচাই করা যায়। প্রেরক যে দলিল পাঠাবে তা কম্পিউটারের প্রয়োগ দ্বারা প্রাপ্ত দলিল প্রাপকের কাছে পাঠিয়ে দেওয়া হয়। প্রাপক কম্পিউটারের প্রয়োগ দ্বারা প্রাপ্ত দলিলকে হ্যাশে প্রেরণ করেন এবং প্রেরকের কী দ্বারা ব্যক্তির থেকেও হ্যাশ বের করেন। দুইটি হ্যাশ একই রকম হলে যাচাইকরণ নিশ্চিত হয়।



উদাহরণ ব্রহ্ম, এখানে Alice Bob কে মেসেজ পাঠাবে, Alice মেসেজ পাঠানোর সময় তার প্রাইভেট কী একটা সিগনচার জেনারেট করে এবং এরিজিনাল মেসেজ এর সাথে ইন্ট্রিয়েট করে পাঠাবে, Bob যখন রিসিভ করবে মেসেজটা Alice পাঠিয়েছে নাকি অন্য কেউ, সে Alice এর পাবলিক কী দ্বারা মেসেজকে ভেরিফাই করবে, যদি ভেরিফাই হয় তাহলে যে বুকে নিবে মেসেজটা Alice পাঠিয়েছে না হলে বুবাবে অন্য কেউ। এই ভাবে মেসেজ ইন্ট্রিয়েট আর অব্যবহৃতকেশন হয়ে থাকে।

প্রশ্ন-১৪) What is two factor authentications? Describe with example. (দ্বি-ক্ষেত্র বিশিষ্ট অব্যবহৃতকেশন কাকে বলে? উদাহরণসহ বর্ণনা কর।)

উত্তর: Two factor Authentication: অনলাইন জগতে এক এর অধিক বা বহুতর বিশিষ্ট সিকিউরিটি ব্যবহারকে Two factor Authentication (2FA) বা Multi-Factor Authentication (MFA) বলা হয়, আবার একে Two step Verification ও বলা হয়।

অর্থাৎ এই কম্পিউটারে সিস্টেমে আরোহণ পাওয়ার জন্য আপনার অনেকে সিকিউরিটি স্টেপ পার করতে হয়। উদাহরণ: দ্বি-ফ্যাক্টর অব্যবহৃতকেশন পদ্ধতিতে ব্যবহারকারীর নিরপেক্ষ হিসেবে দুটি ধৰ থাকে। এর মধ্যে প্রথম ধৰটিতে ব্যবহারকারী সচরাচর ব্যবহার করে এমন ফ্যাক্টর (পাসওয়ার্ড) থাকে। দ্বিতীয় ধৰটি হিসেবে লগ-ইন প্রক্রিয়াটি বৈধ বা অনুমোদন বা অ্যাকসেস পাওয়ার চোট। প্রায় অধিকাংশ ক্ষেত্রে প্রথম

ফার্মেটি পদ্ধতির বাস্তব নথি ব্যবহৃত হয়। হিটীর ফার্মেট হিসেবে কোনো সংস্থা, নথি বা অকরের মিলিত সেট বিভিন্ন উপায়ে ব্যবহারকারীর কাছে পাঠানো হয়। দ্রষ্টা হতে পারে মোবাইল নথিতে বা ইমেইল একাউন্টে নথির পাঠানো বা OTP (One Time Password) পাঠানো। সেই নথির বা OTP দিয়ে ব্যবহারকারী সংস্থার সিস্টেম বা সাইট এরেস করার অনুমতি পায়।



Figure: Two Factor authentication

প্রশ্ন-১৫) উপরুক্ত উদাহরণ ও ডায়াগ্রাম সহ সিমেট্রিক কী বর্ণনা করা? (Explain symmetric key with appropriate examples and diagrams.) [Lecturer, NTRCA-2015, NTRCA-2017]

উত্তর: Ciphers ব্যবহার করে গোপনীয়তা রক্ষা করা হয়। Ciphers দ্বারা ক্যাটাগরিতে বিভক্ত করা হয়।

- a) Symmetric Key Ciphers
- b) Asymmetric Key Ciphers

Symmetric Key Ciphers এনক্রিপশন ও ডিক্রিপশন করার জন্য Single key ব্যবহার করে। এনক্রিপশন ও ডিক্রিপশন আলগরিদম একে অপরের ইনভার্স।

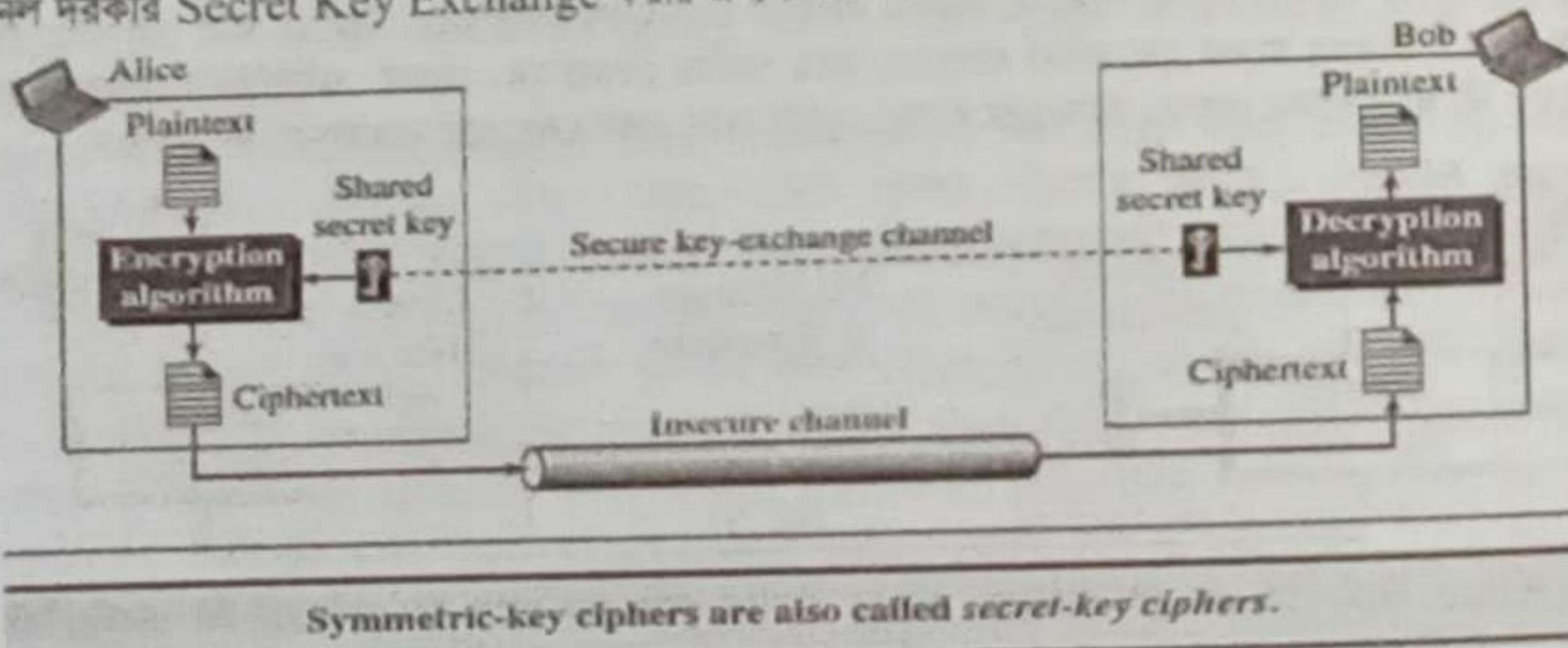
P হলি Plain text হয়, C যদি Cipher text হয় এবং K যদি key হয় তাহলে,

$$\text{Encryption: } C = E_k(P)$$

$$\text{Decryption: } P = D_k(C)$$

$$\text{অর্থাৎ } D_k(E_k(x)) = E_k(D_k(x)) = x.$$

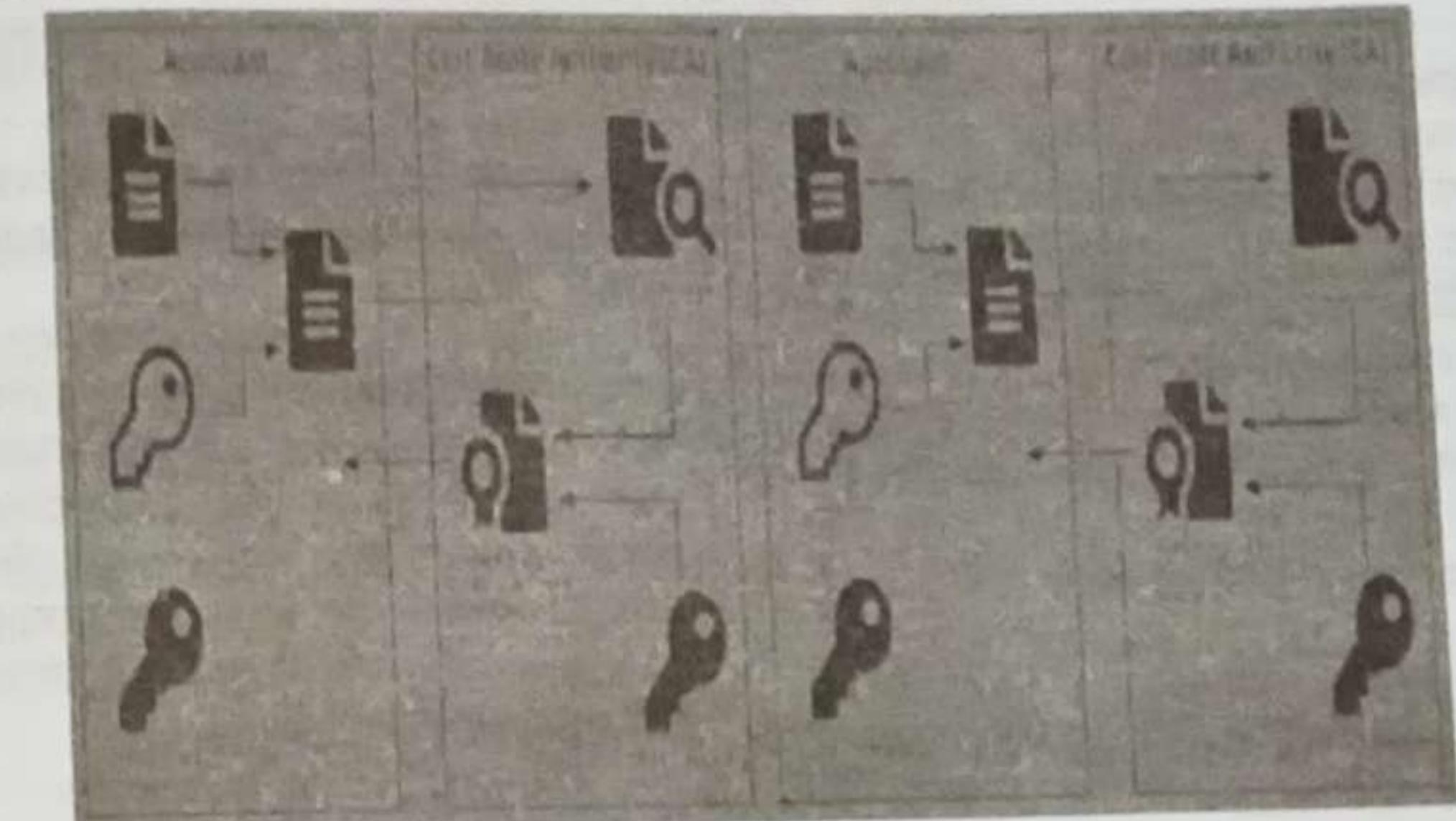
আমদের জেনে রাখা দরকার যে এনক্রিপশন টেকনিক যেন পারিলিক হয়, কিন্তু Shared key যেন গোপন রাখা হয়। এখানে Alice এর Bob এর আলাদা চ্যানেল দরকার Secret Key Exchange করার জন্য। তারা পারসোনাল Face to Face Secret key Exchange করে।



Symmetric-key ciphers are also called secret-key ciphers.

প্রশ্ন-১৬) Write down the purpose of Certification Authority (CA) in Digital Signature. (ডিজিটাল সিগনচার মধ্যে সার্টিফিকেট অধোবিটি(সি.এ) এর উদ্দেশ্য তালি লিখুন।) [SAE- Agriculture Ministry, BPSC-2021]

উত্তর: একটি Certificate Authority (CA), যা কখনো কখনো Certification Authority (CA) নামেও পরিচিত। ইহা এমন একটি কোম্পানি বা সংস্থা যা ডিজিটাল সিগনচার ব্যবহার করে Issue কৃত ইলেক্ট্রনিক ডকুমেন্ট এর মাধ্যমে কোন User এর পরিচয় বা আইডেন্টিটি দলি (যেমন: ওয়েবসাইট, ইমেইল ঠিকানা, সংস্থাতার বা স্থানীয় বাইক্সের) বৈধকরণের (Verification) কাজ করে তাকে ডিজিটাল সার্টিফিকেট দে।



একটা ডিজিটাল সার্টিফিকেট নিম্নোক্ত উদ্দেশ্য তালি নিয়ে কাজ করে:

(a) Authentication: এটি পূর্বে ইস্তুক্ত তথ্য ব্যবহার করে এন্টিটির পরিচয় যাচাই করে এরেস করার জন্য একটি সার্টিফিকেট প্রদান করে।

(b) Encryption: অনিয়ন্ত্রিত সেটওয়ার (যেমন ইন্টারনেট) তালিতে সুরক্ষিত যোগাযোগের জন্য বা তথ্য আদান প্রদানের জন্য এনক্রিপশন সুবিধা প্রদান করে।

(c) Integrity: তৃতীয় পক্ষ (Third Party) দ্বারা সার্টিফিকেটসহ সাইজ ডকুমেন্টের (Signed Document) কোনো প্রকারের ক্ষতি বা পরিবর্তন করা রোধ করে থাকে।

প্রশ্ন-১৭) Public Key Cryptography কীভাবে কাজ করে? (How to work Public key Cryptography?) [AME, Different Ministry, BPSC-2020]

উত্তর: Public Key Cryptography কে Asymmetric Cryptography ও বলা হয়। এটি একটি Cryptographic Technique। এটি Data encryption এবং decryption করার জন্য Private Key (গোপন) এবং Public Key (সরাসর জন্য উন্মুক্ত) নামে দুটি ভিন্ন ধরনের key ব্যবহার করে। এর ফলে, Internet এর মাধ্যমে এক Computer থেকে অন্য Computer এ নিরাপত্তার সাথে data আদান-প্রদান করতে পারে। এটি নিম্নোক্ত পদ্ধতিতে কাজ সম্পন্ন করে:

- a. Key Generation, b. Key Exchange, c. Encryption, d. Sending Encrypted data, e. Decryption

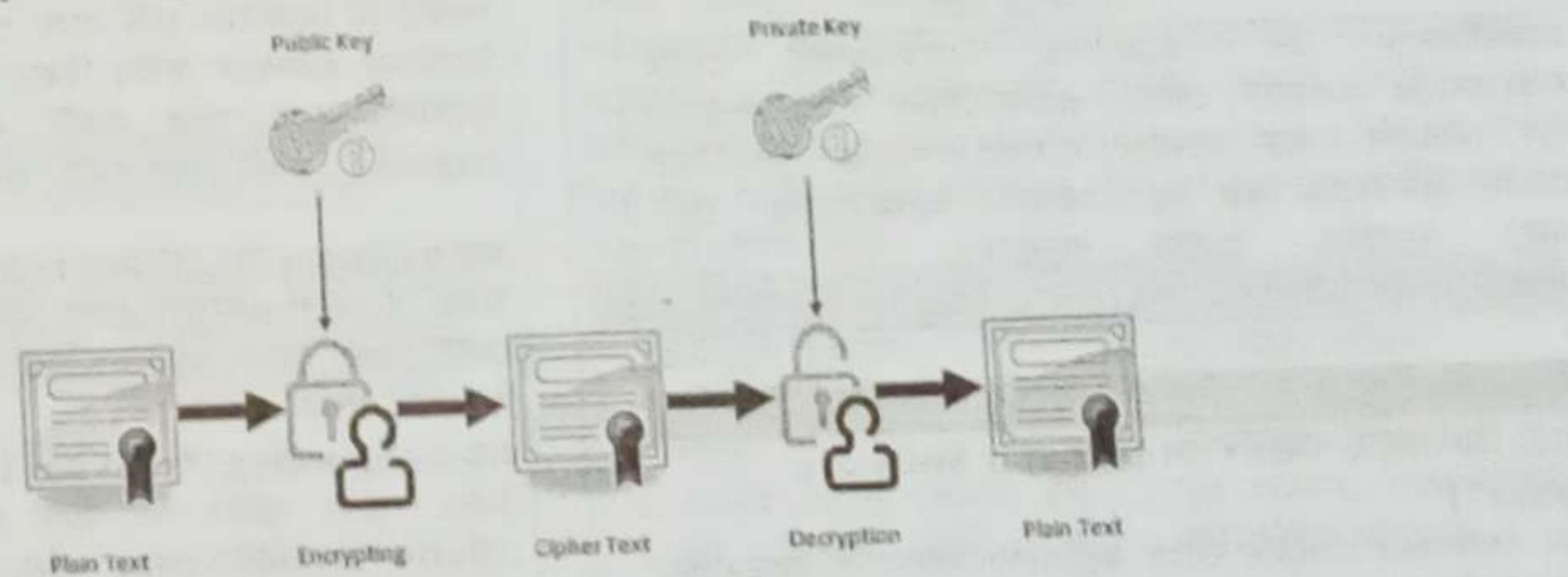


Figure: Public Key Cryptography Process

প্রশ্ন-১৮) State three purposes that are served by a digital signature. (ডিজিটাল সিগনচার এর দেওয়া সেবার মধ্যে তিনি উদ্দেশ্য লিখুন।) [AME, Different Ministry, BPSC-2020]

উত্তর: ডিজিটাল সিগনচার একটি সিগনচার ব্যবহার করার জন্য সিগনচারের বিকল্প হিসেবে Digital Fingerprint ব্যবহার করে। এই Fingerprint অথবা Coded Message ব্যবহারকারী এবং ডকুমেন্ট ভূত্যা ক্ষেত্রে Unique এবং ভূত্যকে একেরে সম্মত করে। একবার সিগনচার করার পর ডকুমেন্টটি যেকোন

ধরনের পরিবর্তন উক্ত সিগনচারকে বাতিল করে। ডিজিটাল স্বাক্ষর হল একটি মেসেজ ডাইজেন্টে'র এনক্রিপ্টেড ভার্সন যা একটি মেসেজ'র সাথে একত্রে সংযুক্ত থাকে। ডিজিটাল স্বাক্ষর তিনি বিভক্ত হয়ে আছে। অক্রিমতা, এবং সুরক্ষা। একটি নিরাপদ ডিজিটাল সিগনচার দুটি অংশ নিয়ে গঠিত:

- 1) নিজের জন্য গোপনীয় চাবি (প্রাইভেট কী), যা দ্বারা ডিজিটাল সিগনচার সৃষ্টি করা হয়।
- 2) সবার জন্য উন্মোচনের চাবি (পাবলিক কী), যা দ্বারা ডিজিটাল সিগনচার যাচাই করা হয়।

সাধারণত ডিস্টি বিশেষ উদ্দেশ্যে সকল হওয়ার জন্য সেচেলো কমিউনিকেশন করে।

Authentication: অপুনি এমন একটি প্রিম্য ঘার্ট পার্টিকে ব্যবহার করেছেন যেখন: সার্টিফিকেট অথোরিটি (Certificate Authority-CA) যা নির্মিত করে যে, আপনি নিজেই সর্বিকৃত হাতি।

Non-repudiation: এর অর্থ হল কেউই আপনার করতে পারে না করে। যারা এ হ্যাকিং করে তারা হচ্ছে হ্যাকার। মোবাইল কেন, প্লাটফর্ম বা বৈচারিক প্লাটফর্ম একাল করেছেন।

Message integrity: এটি অপুনি, ইলেক্ট্রনিক, OS বা সার্ভারকে দেখার যে ইয়ে ব্যক্তিগত হওয়ার পর থেকে কেনভেই ইহার পরিবর্তন করা হচ্ছে।

প্রশ্ন-১১) Authentication এবং Authorization এর মধ্যে পার্থক্য লিখুন। [41st BCS-Written-2020]

উত্তর: Authentication এবং Authorization এর মধ্যে পার্থক্য হল:

অ্যাথেন্টিকেশন (Authentication)	অ্যাথোরাইজেশন (Authorization)
কোন সিস্টেম আর্ডেস করার ক্ষেত্রে একজন ব্যবহারকারীর আইডেন্টিটি যাচাই করার প্রিম্যাকে অথেন্টিকেশন বলে।	কোন রিসোর্স আর্ডেস করার ক্ষেত্রে একজন ব্যবহারকারীর অধিকার ও অনুমতি যাচাই করার প্রিম্যাকে অথোরাইজেশন বলে।
ব্যবহারকারীর ক্রেতেনশিয়াল (Credential) (যেমন: পরিচয়, পাসওয়ার্ড, মোবাইল নং, ইমেইল ইত্যাদি) ভেরিফাই করে।	ব্যবহারকারীর অনুমতি ও অধিকার ভেরিফাই করে।
অথেন্টিকেশন সর্বপ্রথম ধাপে কাজে করে।	অথোরাইজেশন সাধারণত অথেন্টিকেশন এর পরের ধাপে কাজে করে।
অথেন্টিকেশন এর ক্ষেত্রে ব্যবহারকারীর পাসওয়ার্ড, সোপান পিন, মোবাইল নাম্বার, ইমেইল ইত্যাদি ডিটারমাইজ করা হয়। যেমন অনলাইন ব্যাকিং, ফেসবুক লগ ইন ইত্যাদি।	বহু ব্যবহারকারীর পাসওয়ার্ড ব্যবহারকারীদের অধিকার ও আর্ডেস সুবিধা দিয়ে থাকেন ব্যবহারকারীর শ্রেণী অনুসারে।

Computer Security

প্রশ্ন-১) সফটওয়্যার পাইরেসি কি? (What is Software Piracy?)

উত্তর: সফটওয়্যার পাইরেসি বলতে অনুমোদিত মালিক বা প্রক্রিয়াকারীর বিনা অনুমতিতে কোন সফটওয়্যার কপি করা, ব্যবহার করা, নিজের নামে বিতরণ করা কিম্বা কোন অকার পরিবর্তনের মাধ্যমে নিজের বলে জালিয়ে দেওয়া ইত্যাদি কার্যকরভাবে বৃদ্ধি করে।

প্রশ্ন-২) সাইবার ক্রাইম কি? (What is Cyber Crime?)

উত্তর: ইন্টারনেটকে কেন্দ্র করে যে সকল কম্পিউটার ভিত্তিক বা ভার্টুয়াল মেসেন্স ক্রাইম সংঘটিত হয় তাদেরকে বুঝায়।

প্রশ্ন-৩) সাইবার আক্রমণ কি? (What is Cyber Attack?)

উত্তর: সাইবার আক্রমণ এক ধরনের ইলেক্ট্রনিক আক্রমণ যাতে ক্রিয়েলালো ইন্টারনেটের মাধ্যমে অন্য কারও সিস্টেমে বিনা অনুমতিতে

প্রেরণ করে ফাইল, প্রোগ্রাম কিংবা হার্ডওয়ার ক্ষস বা ক্ষতি সহ করে।

প্রশ্ন-৪) হ্যাকিং কি? বিভিন্ন ধরার হ্যাকারের সঙ্গে দাও। (What is Hacking? Define different types of Hacker?)

উত্তর: সাধারণত হ্যাকিং একটি প্রক্রিয়া যার মাধ্যমে কেট কেন নে অনুমতি ব্যাপী করে একজন কম্পিউটার বা কম্পিউটার নেটওয়ার্কে অনুমতি ব্যাপী করে তারা হচ্ছে হ্যাকার। মোবাইল কেন, প্লাটফর্ম বা বৈচারিক প্লাটফর্ম এবং চিপিটল যা তার অনুমতি হচ্ছে ব্যবহার করলে তাও হ্যাকিং এর আওতার প্রতি হ্যাকারের সাধারণত এসব ইলেক্ট্রনিক যত্নের জন্য বের করে তা বিন্দু হ্যাক করে। হ্যাকারদের চিহ্নিত করা হয় Hat বা হুপি নিয়ে। তাঁর প্রকারের হ্যাকের রয়েছে: যথা:

1. Black hat hacker
2. Grey hat hacker
3. White hat hacker

Black hat hacker: একজন Black hat hacker যখন যে একটি সিকিউরিটি সিস্টেমের জন্য খুজে বের করে, তখন হ্রাস হওয়া কে নিজের বার্ষে কাজে লাগায়। অর্থাৎ এ সিস্টেমটি নিজের কর্তৃত নিয়ে নেবা ভাইরাস ছড়িয়ে দেওয়ার মাধ্যমে সিস্টেমটি নষ্ট করে।

Grey/Gray hat hacker: একজন Grey/Gray hat hacker যখন একটি সিকিউরিটি সিস্টেমের জন্য খুজে বের করে তার মত কাজ করে। সে ইচ্ছে করলে এ সিকিউরিটি সিস্টেমের সালিককে জন্ম জানাতে পারে অথবা তথ্য নিজের হ্যাক জন্য ব্যবহারও করতে পারে। বেশির ভাগ Hacker এ কাটারি মধ্যে পড়ে।

White hat hacker: একজন White hat hacker এটি সিকিউরিটি সিস্টেমের জন্য খুজে বের করে এবং এ সিকিউরিটি সিস্টেমের মালিককে জন্ম দিয়ে দ্রুত অবহিত করে। সিকিউরিটি সিস্টেমটি হতে পারে একটি কম্পিউটার, একটি কম্পিউটার এবং একটি গোপনীয়তা ক্ষেত্রে নিরাপত্তা সুযোগ নেয়। একটি কম্পিউটার ভাইরাসের মত এটিরও নিজেকে কোন প্রেমাণে যোগ করা প্রয়োজন হয় না। এগুলো সবসময় নেটওয়ার্কের কিছু ক্ষতি করে এমনকি ইন্টারনেট ব্যান্ডউইথ ও খরচ করে। কিন্তু ভাইরাস একটি কম্পিউটারের ফাইল নষ্ট করে বা আক্রমণ করে।

প্রশ্ন-৫) Spam কি? (What is Spam?)

উত্তর: ই-মেইল একটিটে প্রাই কিছু কিছু অচেনা ও অপ্রয়োজনীয় মেইল প্রাপ্তি ব্যাপী যা আমাদের বিরুদ্ধে ঘটায়। এই ধরনের ই-মেইল সাধারণত স্প্যাম মেইল বলে।

প্রশ্ন-৬) Spoofing কি? (What is Spoofing?)

উত্তর: স্পুফিং শব্দের অর্থ হলো প্রতারণা করা, যেকোন নেটওয়ার্ক সিকিউরিটির ক্ষেত্রে স্পুফিং হলো এমন একটি অভ্যন্তরীণ কম্পিউটারের ব্যবহৃত তথ্যের ক্ষতিসাধন, পরিবর্তন বা পোশনীয়তা ফাঁসের বিরুদ্ধে নিরাপত্তামূলক ব্যবহারকে কম্পিউটারের নিরাপত্তা বলে। সাইবার সিকিউরিটি এর প্রকারভেদ। যেমন:

- 1) Ransomware
- 2) Malware
- 3) Social engineering
- 4) Phishing

প্রশ্ন-৭) ফিশিং কি? (What is Phishing?)

উত্তর: Phishing বলতে প্রত্যাবর্তন মাধ্যমে কারো কাছ থেকে ব্যক্তিগত তথ্য, যেমন ব্যবহারকারীর নাম ও পাসওয়ার্ড, মেইল কর্তৃত তথ্য ইত্যাদি সংগ্রহ করাকে বোঝানো হয়ে থাকে। অভাবক্রমে এ পক্ষত্বিতে কোনো সুরক্ষিত ওয়েবসাইট সেবে মনুষের কাছ থেকে তথ্য চুরি করে থাকে। ইমেইল ও ইলেক্ট্রনিক মেসেজের মাধ্যমে স্পুফিং করা হয়ে থাকে। প্রত্যাক্রমের তাদের শিকারকে কেবলেকে

Computer Network and Security

যেকো নিয়ে তাদের ওয়েবসাইটটি নিয়ে যায়। এ ওয়েবসাইটটি সংশ্লিষ্ট ক্রিয়াকারীর ইমেইল, ব্যাক বা ফেডের কার্ডের অনলাইন ওয়েবসাইটের মেরামত করে থাকে। ব্যবহারকারীর সেটাকে অনলাইন সাইট তেরে নিজের তথ্য প্রদান করলে সেই তথ্য প্রত্যাক্রমের হাতে চলে যায়।

প্রশ্ন-৮) ভিশিং কি? (What is Vishing?)

উত্তর: মোবাইল, টেলিফোন, ইন্টারনেটভিত্তিক ভিশিং কোন বা অভিও ব্যবহার করে ফিশিং করার পদ্ধতি হয়।

প্রশ্ন-৯) ক্লাইমিকেশন কি? (What is Plagiarism?)

উত্তর: কোন ব্যক্তি বা প্রতিনিধির কোন সাহিত্য, গবেষণা বা সম্পাদনা কর্ম হ্রাস নকল বা আশীর্বক পরিবর্তন করে নিজের নামে প্রকাশ করাই হল Plagiarism।

প্রশ্ন-১০) What is Cracking? [Janata Bank-2015]

উত্তর: হ্যাকিং এবং ক্রাকিং একই জিনিস বিষ্ট ক্রাকিং করা হয় ব্যাপ উদ্দেশ্যে। However, cracking is generally less harmful than hacking.

প্রশ্ন-১১) Worms কি? (What is Worms?) [DoICT-BPSC-2014]

উত্তর: একটি কম্পিউটার ওয়ার্ম হল একটি যাদীন মালওয়ার কম্পিউটারের প্রেমাণে যা নিজেকে নকল করতে পারে তা অন্য কম্পিউটারে ছড়িয়ে পড়তে পারে। প্রায়শই এটি ছড়িয়ে পড়ার জন্য কম্পিউটারের নেটওয়ার্ক ব্যবহার করে এবং অন্য কম্পিউটারের নিরাপত্তা ব্যর্থার সুযোগ নেয়। একটি কম্পিউটারের ভাইরাসের মত এটিরও নিজেকে কোন প্রেমাণে যোগ করা প্রয়োজন হয় না। এগুলো সবসময় নেটওয়ার্কের কিছু ক্ষতি করে এমনকি ইন্টারনেট ব্যান্ডউইথ ও খরচ করে। কিন্তু ভাইরাস একটি কম্পিউটারের ফাইল নষ্ট করে বা আক্রমণ করে।

প্রশ্ন-১২) What is Cyber Security? (সাইবার সিকিউরিটি ককে বলে?) [Janata Bank-IT-17, Lecturer NTRCA-2011, NTRCA-2013, NTRCA-2014]

উত্তর: আকর্মিক দূর্বিনাজনিত কারণে বা অবাস্তুত ব্যক্তি কর্তৃক কম্পিউটারের ব্যবহৃত তথ্যের ক্ষতিসাধন, পরিবর্তন বা পোশনীয়তা ফাঁসের বিরুদ্ধে নিরাপত্তামূলক ব্যবহারকে কম্পিউটারের নিরাপত্তা বলে। সাইবার সিকিউরিটি এর প্রকারভেদ।

1. এটি ছান্নি ভাইরাস।
2. এটি মেমোরিতে ছান্নি হয়

২. হার্ডিং করার উদ্দেশ্য সহ অথবা অসহ দুই ধরনের হাতে পারে।	২. হার্ডিং তিনি ধরনের হাতে পারে। যোগাই হাত হার্ডিং, ব্ল্যাক হাত হার্ডিং এবং প্রে হাত হার্ডিং।
৩. হার্ডিং একটি পদ্ধতি বা প্রক্রিয়া।	৩. হার্ডিং বলতে কোনো বার্তা বা Group কে বৃক্ষার।

প্রশ্ন-১৭) আন্টিভাইরাস কি? (What is Antivirus?) [BKKB-17, DIP-14]

উত্তর: আন্টিভাইরাস (Antivirus) বলতে সাধারণভাবে কম্পিউটারের ভাইরাস রেখ করার জন্য ব্যবহৃত একধরনের প্রয়োগ যা কম্পিউটারের সংরক্ষণ এলাকা বা হার্ডডিউক বা মেমোরি বা ব্যবহারকারীদের যোগাযোগের মাধ্যম ব্যক্ত করতে পারে।

হাতে ভাইরাস সন্তোষক, প্রতিরোধ ও প্রতিকরণ করতে পারে।

করেক্টি আন্টিভাইরাস প্রয়োগের নাম নিচে দেয়া হল:

- ১. রিভ আন্টিভাইরাস
- ২. ক্যাম্পারাকি
- ৩. হ্যার্ডিং
- ৪. নরটন
- ৫. পিসিসিলিন
- ৬. এভিজি
- ৭. অ্যাভেন্ট
- ৮. পাড়া
- ৯. ইস্টেট

প্রশ্ন-১৮) ইন্টারনেটের মাধ্যমে সংঘটিত বা ইন্টারনেটে সংঘটিত ১০ টি আক্রমণের নাম লিখ? (Write the names of 10 attacks that took place on the internet or on the internet?) [Officer IT/ICT, Sonali and Janata Bank-2019]

উত্তর: ১০ টি আক্রমণের নাম:

- a) DOS and DDOS attacks
- b) Man-in-the-middle (MitM) attacks
- c) Password attack
- d) SQL injection attack
- e) Cross-site scripting (XSS) attack
- f) Birthday attack
- g) Malware attack
- h) Phishing and spear phishing attacks
- i) Drive-by attack
- j) Brute-force and dictionary network attacks

প্রশ্ন-১৯) Denial of Service (DoS), Distributed Denial of Service (DDoS) Attack কি? (What is the Denial of Service (DoS) and Distributed Denial of Service (DDoS) Attack?) [BCS-36]

উত্তর: Denial of Service Attack বা সেবা বাধাদারের আক্রমণ হলো কোনো কম্পিউটার সিস্টেমের কোনো সেবা বা সেবার (Service) প্রক্রিয়া ব্যবহারকারীদের বাধা দেয়ার একটি কৌশল। কোনো কম্পিউটার বা সিস্টেম বা ইন্টারনেট গৃহেক্সাইটে এই আক্রমণ

চলানোর মাধ্যমে এই সিস্টেম বা সাইটের যথাযথ কার্ডিঙক প্রতি, বা অনেক ক্ষেত্রে পুরোপুরি ব্যক্ত করে দেয়া হয়। এই আক্রমণের একটা বেশ জনপ্রিয় পদ্ধতি হলো বাইরে থেকে এই সাইটের সাথে যোগাযোগের জন্য অস্থায় বার্তা পাঠাতে হার্ডিং। এই বার্তা বিশ্বেল করতে করতে আরো বেশ করেক্ট বার্তা দিই পড়ে, তখন এই সিস্টেমটি আক্রমণকারীর পাঠানো বার্তা বিশ্বেলে থাকে, এবং প্রক্রিয়া ব্যবহারকারীরা থীর গতির সম্মতী হন।

Denial of Service আক্রমণের প্রধান দুটি মাধ্যম হলো-

- ১) ট্যার্ণেট করা কম্পিউটারকে রিসেপ্ট করে দেয়া, অথবা তার স্বীকৃতিসম্মতোকে ব্যবহার করে অন্যদের ব্যবহারের অধোগো করে দেয়।
- ২) আক্রমণের লক্ষ্য যে সিস্টেম বা সাইট, তার সাথে প্রক্রিয়া ব্যবহারকারীদের যোগাযোগের মাধ্যম ব্যক্ত করে দেয়া।

আর একধরিক ডিভাইস এবং একধরিক ইন্টারনেট থেকে Denial of Service Attack করা হলে তাকে Distributed Denial of Service (DDoS) Attack বলা হয়।

প্রশ্ন-২০) বিভিন্ন প্রকার নেটওয়ার্ক Attack সংক্ষেপে আলোচন কর (Discuss the different types of attacks?) [BCS-2017]

উত্তর: MAC Flooding: MAC Flooding নেটওয়ার্ক সংবচ্ছেয়ে সাধারণ আক্রমণ হল MAC Flooding attack। কম্পিউটার এর মত এটি নেটওয়ার্ক এর কোন হোস্ট কে স্বত্ত্ব আক্রমণ করে না। এটি নেটওয়ার্ক এর সুইচ এ আক্রমণ করে। এই একটি ম্যাক আড্রেস Table থাকে যাতে নেটওয়ার্ক এর হেড সুইচ এর কোন পোর্ট এর সাথে সংযুক্ত আছে তার ইনকর্ডেন তা MAC Flooding attack এর উদ্দেশ্য হলো এই MAC সুইচে আক্রেস করা। Attacker অনেকগুলো Eathernet হেড করার মাধ্যমে MAC Address Table এর জন্য কম্পিউটার মেমোরি consume করে, ফলে MAC আড্রেস টেবিল এ কোন নতুন আড্রেস আজড করা যায় না।

ARP Spoofing: ARP Spoofing attack এ Attacker এর MAC ARP Message Send করার মাধ্যমে Attacker এর MAC আড্রেসকে Network এর Legal User এর ip Address সাথে Linked করে দেয়।

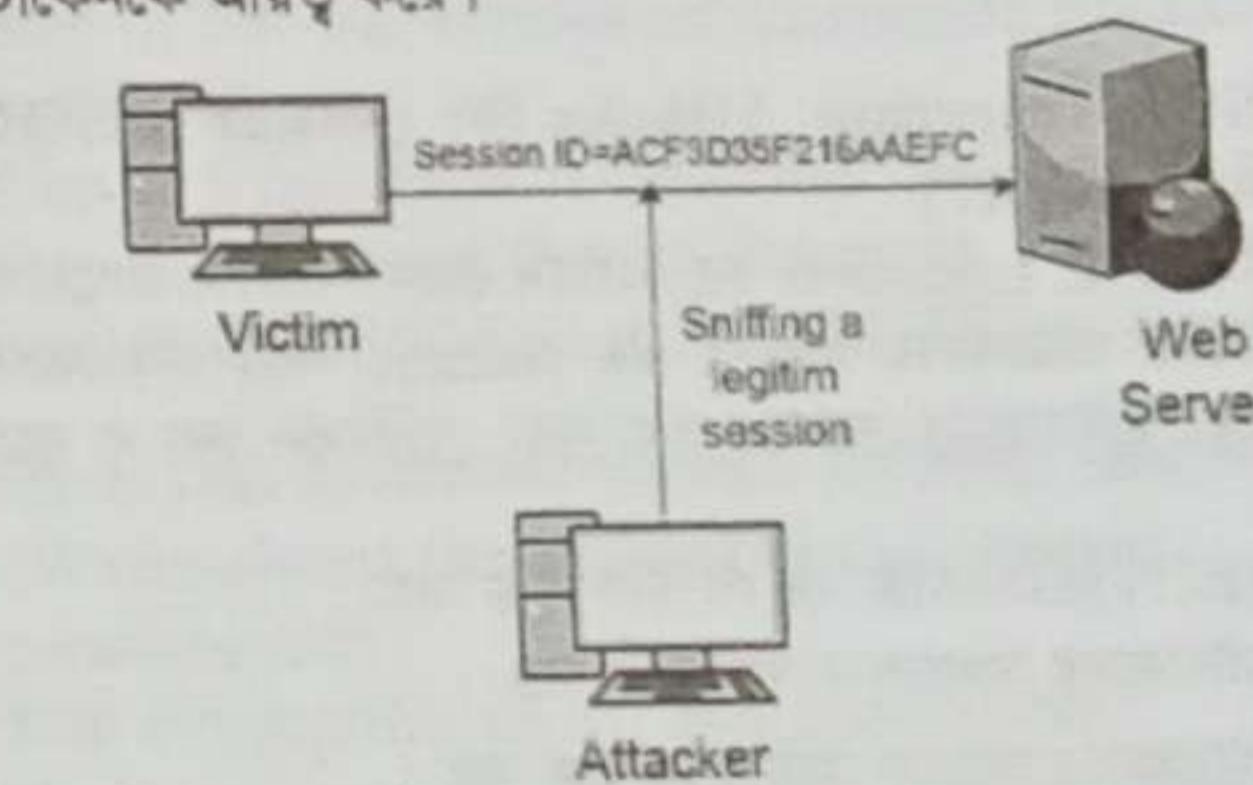
Packet Capturing (Packet Sniffing): এটি এমন ধরনের নেটওয়ার্ক আক্রমণ যেখানে আক্রমণকারী নেটওয়ার্ক এর মধ্যে প্রবাহিত Packet কে Capture করে, নেটওয়ার্ক এর মধ্যে প্রতি সাধারণ করতে পারে।

Password Attacks: এটি এমন এক ধরনের password-based attack যেখানে কোন computer user এর password হার্ডিং করার জন্য এটি ব্যবহার করা হয়। দুই ধরনের password attack আছে।

১. Directory based attack
২. Brute force attack

Port Scanning: কোন computer এ চলমান service এর TCP/UDP port scan করার মাধ্যমে access করে, চলমান service কে অচল করে দিতে পারে বা অন্য যেকোন ক্ষতি সাধন করতে পারে।

ওয়েব আক্রমণ। একে টিপিলি সেশন হাইজ্যাকিংও বলা হয়। এটি কম্পিউটার সেশনগুলির নীতির ভিত্তিতে কাজ করে। আক্রমণটি আক্রমণকারী একটি বৈধ সেশন আইডি চুরি করে যা সিস্টেমে প্রবেশ করতে এবং ডেটা পুনরুদ্ধার করতে প্রযোজ্য হয়। HTTP যোগাযোগে অনেকগুলি টিপিলি সংযোগ ব্যবহার করা হয় এবং যাতে প্রতিটি ব্যবহারকারীর সংযোগ স্লান্স করার জন্য সার্ভারের একটি পদ্ধতি প্রযোজ্য হয়। সর্বাধিক ব্যবহৃত পদ্ধতিটি প্রতিমা এবং তারপরে সার্ভার-ক্লাউডে প্রাইভেট জেডি ক্লাউডে একটি টোকেনেট URL এর মতো, কোন কৃতি হিসাবে HTTP অনুরোধের হেডারের অন্য অংশে বা এর বড়তে বিভিন্ন উপায়ে ব্যবহার করা যেতে পারে। আক্রমণটি ওয়েব সার্ভারে অননুমতি আরোপ পাওয়ার জন্য একটি বৈধ সেশন টোকেন চুরি বা পূর্বাভাস দিয়ে সেশন টোকেনকে আয়ত্ত করে।



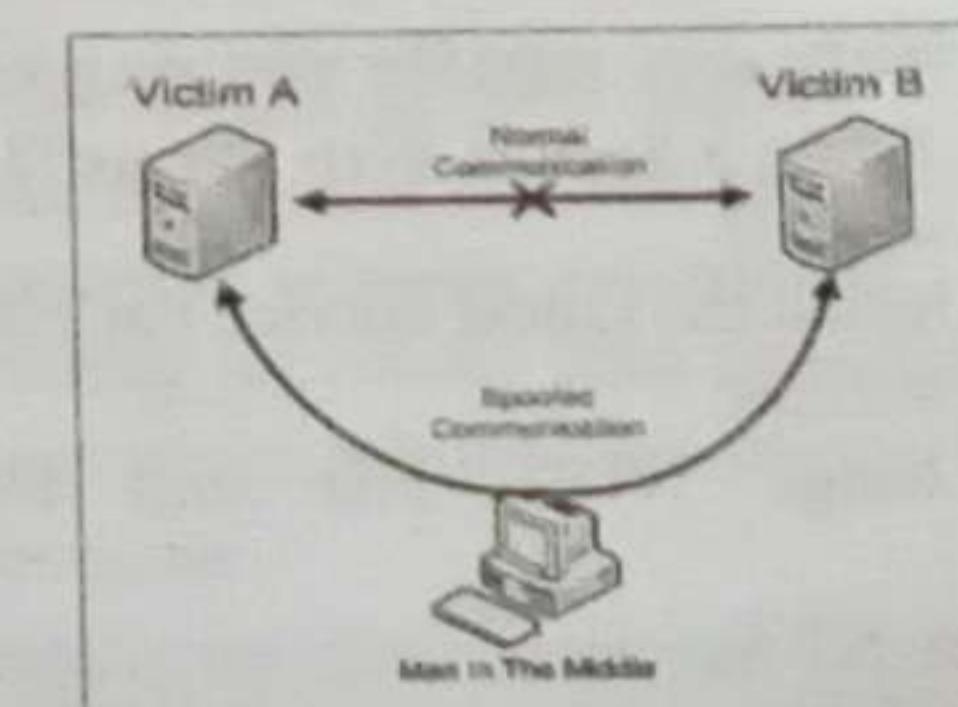
প্রশ্ন-২১) How to prevent the MAC Flooding Attack? (কীভাবে MAC Flooding Attack প্রতিরোধ করা যায়?)

উত্তর: The following are some of these methods:

- a) Port Security
- b) Authentication with AAA server
- c) Security measures to prevent ARP Spoofing or IP Spoofing
- d) Implement IEEE 802.1X suites

প্রশ্ন-২২) Brute force Attack কি? (What is Brute force Attack?) [BCS-36th Written]

উত্তর: Brute Force হলো এমন একটা পদ্ধতি যেখানে একজন হ্যাকার তার Victim এর সঠিক পাসওয়ার্ড পাওয়ার জন্য ভিত্তিমূলক তালিকা ডাটাবেজ থাকে। সেখান থেকে একের পর এক দিতে থাকে। এই পাসওয়ার্ডের তালিকা হ্যাকারগুলি বিভিন্নভাবে সংযোজ করে থাকে। ডিকশনারী এটাকের জন্য বিভিন্ন সফটওয়্যার পাওয়া যায়।



The Session Hijacking: [AP, Different Ministry-BPSC-2019] The Session Hijacking সেশন হাইজ্যাকিং এক ধরনের

প্রশ্ন-২৩) DHCP Starvation কী? সংক্ষেপে ব্যাখ্যা করুন। (What is DHCP Starvation? Explain shortly.) [AP, Different Ministry-BPSC-2019]

উত্তর: DHCP Starvation আক্রমণ এমন এক ধরনের ডেক্সের আক্রমণ যেখানে কোন আক্রমণকারী কিছু ছাইবেশী ম্যাক আড্রেস সহ প্রচুর পরিমাণে DHCP রিকুয়েস্টস প্রাক্টেট প্রদান করে। আক্রমণ সম্ভ

আইপি আর্ডেস গ্রাস করে। যাটাকার DHCP সার্ভারকে লক্ষ্য করে জাল বা অবিধি DHCP অনুরোধ ঘৰা সময় আইপি আর্ডেসগুলুকে DHCP সার্ভারে ব্যরাদ করে। এই আক্রমণে বৈধ নেটওর্ক ব্যবহারকারীদের পরিষেবায় সমস্যা হতে পারে।



Figure: DHCP Starvation

প্রশ্ন-২৮) SQL Injection Attacks কি? (What is SQL Injection Attack?)

উত্তর: একটি SQL Injection এর মাধ্যমে কোন আক্রমণ উপর্যোগী ওয়েব সার্ভারকে আক্রমণের মাধ্যমে এর Access নিয়ে নেয় যাতে করে এ সার্ভার ডাটাবেসের যেকোন তথ্য পড়া, পরিবর্তন করা বা মুছে দেয়া যায়।

SQL INJECTION ঘৰা যে যে কাজ করা যায়-

- ডাটাবেসের তথ্যকে এক্সেস করা যায়।
- ডাটাবেসের তথ্যকে মেডিফাই করা যায়।
- সাইটের লগইন এরিয়া বাইপাস করা যায়।
- SQL Server হ্যাক করা যায়।

প্রশ্ন-২৫) Cross-Site Scripting (XSS) ক্ষতিকারক কী বুঝায়? এর হাত থেকে রক্ষা পাওয়ার পদ্ধতি কোনো লিখন? (What is Cross-Site Scripting (XSS)? What are the methods to get rid of it?)

উত্তর: Cross-site Scripting হচ্ছে XSS এর পূর্ণরূপ। মূলত XSS হচ্ছে একটি কোড ইনজেকশন (Code Injection), যেটার সাহায্যে কোন ওয়েবসাইটে ক্ষতিকর কোড প্রবেশ করানো যায়। অর্থাৎ Cross Site Scripting (XSS) তখনই হয় যখন কোন ইউজার ম্যালিসিয়াস কোড কোন Website এ প্রবেশ করায়। যার কারণে Web Application এমন ভাবে কাজ করে যা তার করার কথা না। XSS Attacks অনেক জনপ্রিয় এবং অনেক বড় Website এর ঘৰা আক্রান্ত হয়েছে যার মাঝে FBI, CNN, Ebay, Apple, Microsoft, AOL রয়েছে। কিন্তু ওয়েবসাইট ফিচার XSS attack এর জন্য vulnerable। যেমন:

- Search Engines
- Login Forms
- Comment Fields

Cross-Site Scripting এর হাত থেকে রক্ষা পাওয়ার পদ্ধতি কোনো লিখন:

- Filter input on arrival.
- Encode data on output.
- Use appropriate response headers.
- Utilize a Content Security Policy.

- Validate User Input.
- Sanitize User Input.
- When Prevention Isn't Enough.

প্রশ্ন-২৬) Trojan Horses, Rogue Access Points Anarchists, Crackers কি? [DoICT- 2014]

উত্তর: **Trojan Horses:** Trojan হচ্ছে একটি প্রোগ্রাম যা অন্য প্রোগ্রামকে নষ্ট করে। এটিকে সবাই ভাইরাস নামেই জানে। **Trojan Horses** ব্যবহার করে অন্যান্য প্রোগ্রাম নষ্টের পাশা পাশা পাসওয়ার্ড অন্যান্য তথ্য হ্যাকারদের কাছে ব্যবহৃতভাবে পৌছিয়ে দেয়।

Rogue Access Points: কোন ওয়ারলেস নেটওর্কের প্রদেশ জ্ঞান হ্যাকারদের Rogue Access Points ব্যবহার করে।

Anarchists: Anarchists হচ্ছে এই সকল হ্যাকার যারা বিভিন্ন কম্পিউটার সিস্টেম বা অন্য কোন সিস্টেম কে জাল পাছন্দ করে। এরা যেকোন টার্গেটের সুযোগ খুঁজে কাজ করে।

Crackers: অনেক সময় ক্ষতিকারক হ্যাকার দের cracker নাম দেয়। খারাপ হ্যাকারাই Cracker। এদের পেশাই হচ্ছে বিভিন্ন পাসওয়ার্ড ভাঙ্গা এবং Trojan Horses তৈরি করা এবং অন্য ক্ষতিকারক Software তৈরি করা।

প্রশ্ন-২৭) ‘Cyber Vandalism’ কী? ব্যাখ্যা লিখন। (What is Cyber Vandalism? Explain it.) [Jnr. Instructor, Ministry of Technical Dept.-2019]

উত্তর: সাইবার ভেঙ্গলিজম হল ডিজিটাল আকারে ঘটে যাওয়া ক্ষতিকারক ধৰন। সাইবার ভ্যাঙ্গেলগুলি কোনও ওয়েবসাইটকে বিকৃত করা পারে, এমন ম্যালওয়্যার তৈরি করতে পারে যা Electronic Mail বা Element কে Damage করতে পারে যা এর Normal Utilization কে বাধা দেয়। এটি Cyberspace ব্যবহার করে Revenge, Destruction মূলক কাজ করে থাকে এবং বিভিন্ন উদ্দেশ্যমূলক ক্ষতিকারক তথ্য ছড়া।

উদাহরণ:

- ✓ Worms,viruses, Trojan horses, logic bombs, spam
- ✓ Website defacement
- ✓ Cyber stalking
- ✓ Cyber bullying
- ✓ Cyber spying

প্রশ্ন-২৮) একটি সিকিউর ওয়েব সার্ভার বিল্ড করার ধাপ কোনো লিখন। (Steps to Building a Secure Web Server?)

[Bangladesh Bank-2017]

উত্তর: Step 1: Install the Latest Service Pack and Applicable Hotfixes

Step 2: Change NTFS File and Director Permissions

Step 3: Secure NT Services

Step 4: Obsecure the Administrator Account

Step 5: Activate Screen Savers

Step 6: Protect the Registry

Step 7: Secure the Event Logs

Step 8: Hide the Name of the Last User

Step 9: Restrict Anonymous Network Access to the Registry

Step 10: Restrict Anonymous Lookup

Step 11: Remove Default Administrator Shares

Step 12: Perform System Audits

Step 13: Audit Base Objects

Step 14: Audit Privileges

Step 15: Disable Caching Logon Credentials

Step 16: Enable TCP/IP Filtering Security

- Keyboard patterns and swipes (i.e., 123456 or QWERTY)

প্রশ্ন-৩০) ই-মেইল কাকে বলে? অপ্রয়োজনীয় মেইল কিভাব এ প্রতিরোধ করা যায়? (What is e-mail? what are the step to prevent from unwanted mail?)

উত্তর: E-mail বা electronic mail এর সাহায্যে এক computer থেকে অন্য computer তথ্য আবান-প্রদান করা যায়।

6 Steps to get off mailing lists to STOP Junk Mail:

Step 1: Stop the Flow.

Step 2: No More Credit Card Solicitations.

Step 3: Put the Kibosh on Unwanted Phone Books and Catalogs.

Step 4: Contribute to Charities, Not Mailings.

Step 5: Stop Junk Promo Products.

Step 6: Get Off the List of ALL Direct Marketers.

প্রশ্ন-৩১) স্ট্রং বা শক্তিশালী পাসওয়ার্ড এর বৈশিষ্ট্য কোনো লিখন। (Write about the Properties of Strong passwords?)

উত্তর: Properties of Strong passwords:

- Be at least ten characters. Longer usually means better. If you choose your characters wisely, you can make stronger passwords using fewer characters.

- Include a mix of lower case and upper case letters. Upper case means capitalized. A character is any letter, number, or punctuation mark.

- Include at least one number

- Include at least one special character.

- Is not a dictionary word (even spelled backward). Dictionary words should be avoided. One of the first things cracking programs do is try "password". Shortly after they try "drowssap" (password spelled backward).

- Internet searches for any part of the password should not return any meaningful results.

- Do not use series like abc or 123 or 321.

- Avoid character substitution (like P@\$\$WORD) for dictionary words.

- This looks like a good password, but it's not: P@\$\$w0rd

প্রশ্ন-০২) Distinguish between phishing and pharming. Give examples to explain. (উদাহরণসহ ফিশিং ও ফার্মিং আটক এর মধ্যে পার্থক্য লিখুন।)

উত্তর: ফিশিং ও ফার্মিং আটক এর মধ্যে পার্থক্য:

উত্তর: Phishing: ফিশিং আটক হল একজনকর সোসাইল ইঞ্জিনিয়ারিং যা কিনা ব্যবহারকারীদের ধীরণা, মোশনেয়ার এবং ব্যক্তিগত তথ্য প্রকাশ করে দেওয়ার জন্য লক্ষ্য করে থাকে।

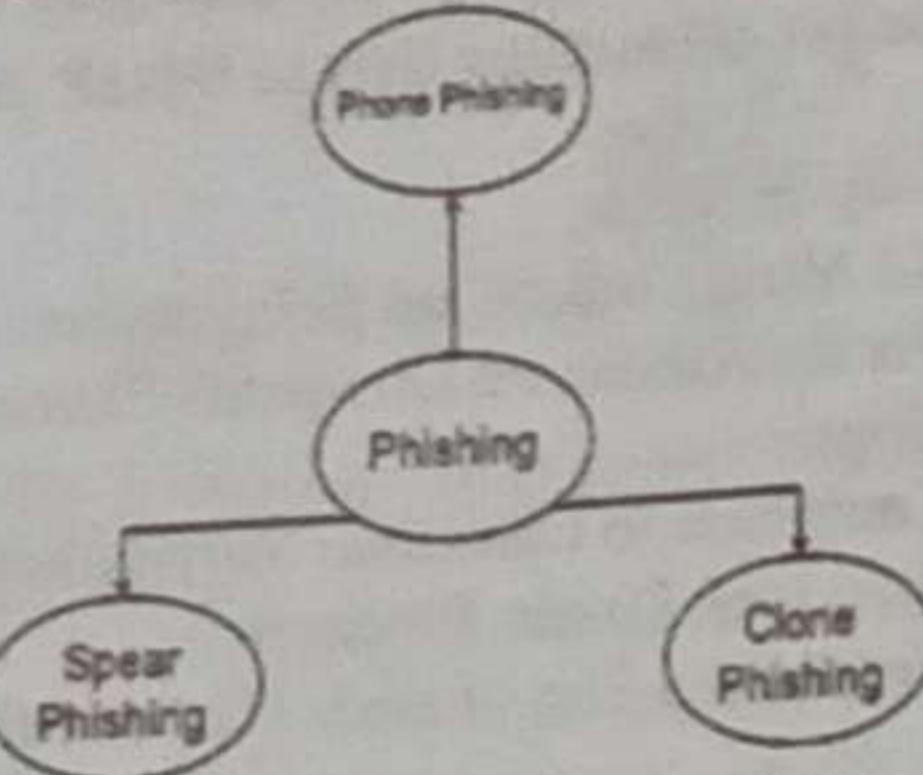


Figure: Architecture of Phishing

Pharming: ব্যবহারকারীদের ওয়েবসাইটে প্রবেশের চোট করে ব্যবহারকারীদের পরিচয়/তথ্য প্রাপ্তির জন্য কার্য আরও একটি এভেনিয়ু আটক বা কৌশল। কার্যরূপ ডিএলএল সার্ভার লেভেলের সাথে অপোস বা কম্প্যুটারে ইজ করে এবং যদি কেন ব্যবহারকারী একটি বৈধ ওয়েব সাইটের ঠিকানা সঠিকভাবে টাইপ করে তখন হৃতজোগীদের তুল বা নিখ্যা ওয়েবসাইটে যাওয়ার জন্য পুনর্নির্দেশ দিয়ে থাকে।

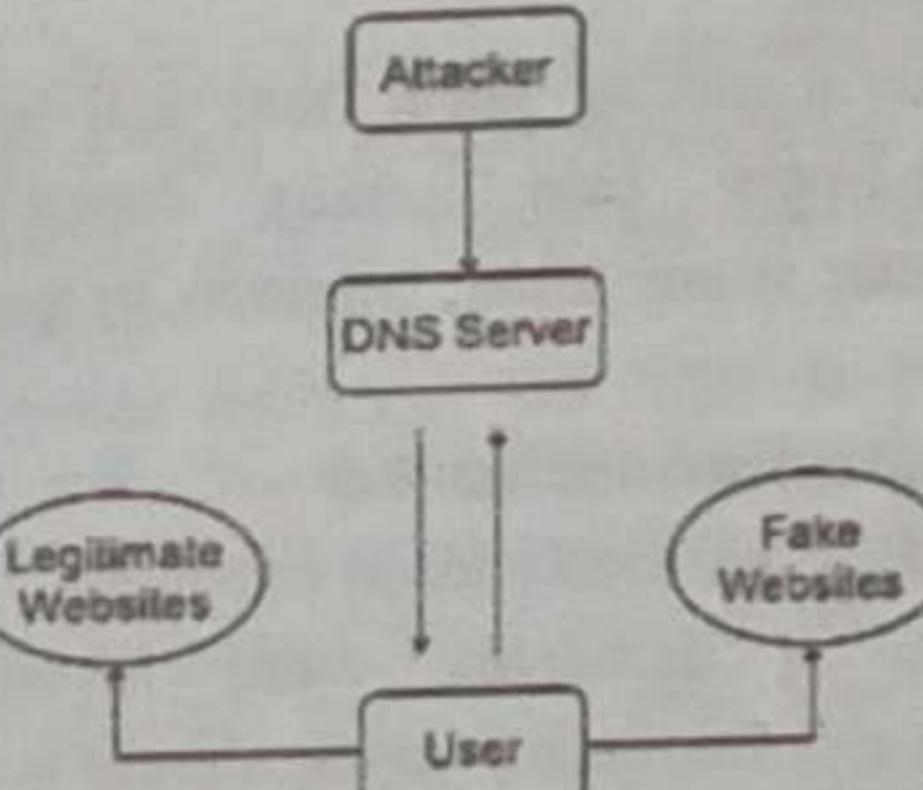


Figure: Architecture of Pharming

প্রশ্ন-০৩) The following table contains different types of security attacks. Now detected weather it is client side or server side attacks? [AME, MRA-BUET-2020]

Answer:

Attacks Name	Client Side or Server Side
Spoofing attack	(Example: Client Side)
Cross site scripting(XSS)	Client Side
Content Spoofing attack	Client Side
Session Fixation	Client Side

- v. Use anti-virus and email security
- vi. Trust the professionals
- vii. Firewall and Antivirus
- viii. Protect Data from Power Surges
- ix. Develop a Disaster Recovery Plan
- x. Keep Your Computer Dust-Free and Dry
- xi. Specify Access Levels
- xii. Work With IT Security Experts

প্রশ্ন-০৪) Differentiate among risk, threat and vulnerability. [AME, BB-2019]

উত্তর: Risk: Risk is defined as the potential for loss or damage of an asset when a threat exploits a vulnerability. Examples of risk include financial losses, loss of privacy, reputational damage, legal implications and even loss of life. Risk can also be defined as: Risk = Threat probability * potential loss / impact.

a) Threat: Anything that can exploit vulnerability, intentionally or accidentally and obtain damage or destroy an asset.

Common threats include things like:

- i. An activist tries to steal data from your website.
- ii. A fire starts in your data center
- iii. An administrator accidentally turns off your website AWS instance.
- iv. A flood hits your headquarters
- v. An insider tries to sell your corporate secrets to a competitor

b) Vulnerability: Vulnerability refers to weaknesses or gaps in a security program that can be exploited by threats to gain unauthorized access to an asset.

Common examples of vulnerabilities include:

- i. SQL injection
- ii. Cross site scripting (XSS)
- iii. Broken authentication and session management
- iv. Security misconfiguration
- v. Insecure cryptographic storage
- vi. Failure to restrict URL access
- vii. Insufficient transport layer protection
- viii. Insecure direct object references