UNIT–04
UNIT-04/LECTURE-01

Switching Techniques

Switching is a technique which is used in large network,large I mean those networks that contains large no. of node,wire,device etc.In this type of networks it is difficult to connect nodes point to point.So in this situation we used Switching Technique.In simple words Switching is a hardware or software device which create a connection between one or more than one device/node/computer.

Packet Switching

- Packet switching features delivery of variable bitrate data streams (sequences of packets) over a shared network which allocates transmission resources as needed using statistical multiplexing or dynamic bandwidth allocation techniques. When traversing network adapters, switches, routers, and other network nodes, packets are buffered and queued, resulting in variable delay and throughput depending on the network's capacity and the traffic load on the network.
- Packet switching contrasts with another principal networking paradigm, circuit switching, a method which sets up a limited number of dedicated connections of constant bit rate and constant delay between nodes for exclusive use during the communication session. In cases where traffic fees are charged (as opposed to flat rate), for example in cellular communication services, circuit switching is characterized by a fee per unit of connection time, even when no data is transferred, while packet switching is characterized by a fee per unit of information transmitted (characters, packets, messages)
- Packet mode communication may be utilized with or without intermediate forwarding nodes (packet switches or routers). Packets are normally forwarded by intermediate network nodes asynchronously using first-in, first-out buffering, but may be forwarded according to some scheduling discipline for fair queuing, traffic shaping, or for differentiated or guaranteed quality of service, such as weighted fair queuing or leaky bucket. In case of a shared physical medium (radio, 10BASE5 or thick Ethernet,), the packets may be delivered according to a multiple access scheme.
- Packet switching features delivery of variable bitrate data streams (sequences of packets) over a shared network which allocates transmission resources as needed using statistical multiplexing or dynamic bandwidth allocation techniques. When traversing network adapters, switches, routers, and other network nodes, packets are buffered and queued, resulting in variable delay and throughput depending on the network's capacity and the traffic load on the network.
- Packet switching contrasts with another principal networking paradigm, circuit switching, a method which sets up a limited number of dedicated connections of constant bit rate and constant delay between nodes for exclusive use during the communication session. In cases where traffic fees are charged (as opposed to flat

rate), for example in cellular communication services, circuit switching is characterized by a fee per unit of connection time, even when no data is transferred, while packet switching is characterized by a fee per unit of information transmitted (characters, packets, messages.

Circuit Switching

- Circuit switching is a methodology of implementing a telecommunications network in which two network nodes establish a dedicated communications channel (circuit) through the network before the nodes may communicate. The circuit guarantees the full bandwidth of the channel and remains connected for the duration of the communication session. The circuit functions as if the nodes were physically connected as with an electrical circuit.
- The defining example of a circuit-switched network is the early analog telephone network. When a call is made from one telephone to another, switches within the telephone exchanges create a continuous wire circuit between the two telephones, for as long as the call lasts.
- Circuit switching contrasts with packet switching which divides the data to be transmitted into packets transmitted through the network independently. In packet switching, instead of being dedicated to one communication session at a time, network links are shared by packets from multiple competing communication sessions, resulting in the loss of the quality of service guarantees that are provided by circuit switching.
- In circuit switching, the bit delay is constant during a connection, as opposed to packet switching, where packet queues may cause varying and potentially indefinitely long packet transfer delays. No circuit can be degraded by competing users because it is protected from use by other callers until the circuit is released and a new connection is set up. Even if no actual communication is taking place, the channel remains reserved and protected from competing users.
- Virtual circuit switching is a packet switching technology that emulates circuit switching, in the sense that the connection is established before any packets are transferred, and packets are delivered in order.
- While circuit switching is commonly used for connecting voice circuits, the concept of a dedicated path persisting between two communicating parties or nodes can be extended to signal content other than voice. Its advantage is that it provides for continuous transfer without the overhead associated with packets making maximal use of available bandwidth for that communication. Its disadvantage is that it can be relatively inefficient because unused capacity guaranteed to a connection cannot be used by other connections on the same network.

Hybrid Switching (RGPV Dec2012)

- Our new-generation Hybrid Switch Technology represents a major evolution. With full bandwidth for SDH and packet connections, it offers traffic switching in native formats and the deployment flexibility of non-blocking connectivity, using patent-pending technology.
- The new technology provides a bandwidth of 480Gb/s for both TDM circuits and packet connections, with the native-format traffic switching including native SDH cross-connecting,

free of circuit emulation penalties for TDM switching. Similarly, native packet switching is achieved without any stranded bandwidth.

- Non-blocking connectivity enables every input to connect to any output, while offering native multicast broadcast functionality, with Fujitsu's technology reducing the overall complexity of the system and increasing its throughput.

Single Bit Error And Burst Error

- When data is being transmitted from one machine to another, it may be possible that data become corrupted on its, way. Some of the bits may be altered, damaged or lost during transmission. Such a condition is known as error.
- The error may occur because of noise on line, attenuation and delay distortion. For reliable communication, it is important that errors are detected and corrected.

S.NO	RGPV QUESTIONS	Year	Marks
Q.1	Explain briefly about the hybrid switching technique	Dec2012	7
Q.2	Explain the packet switching technique.	Dec 2012	7
Q.3	What is circuit switching? Discuss how packet switching is better than circuit switching for communication.	Dec 2013	7

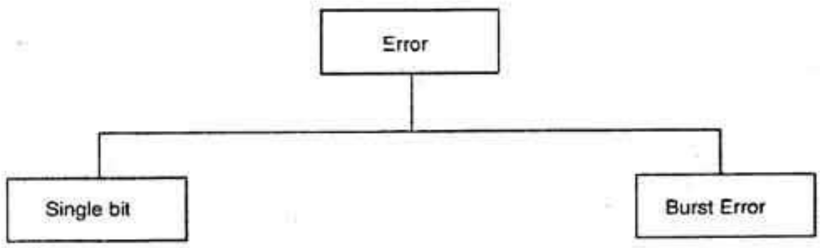
UNIT-04/LECTURE-02

Type of Errors (RGPV Dec2013)

There are two main types of errors in transmissions:

1 single bit error

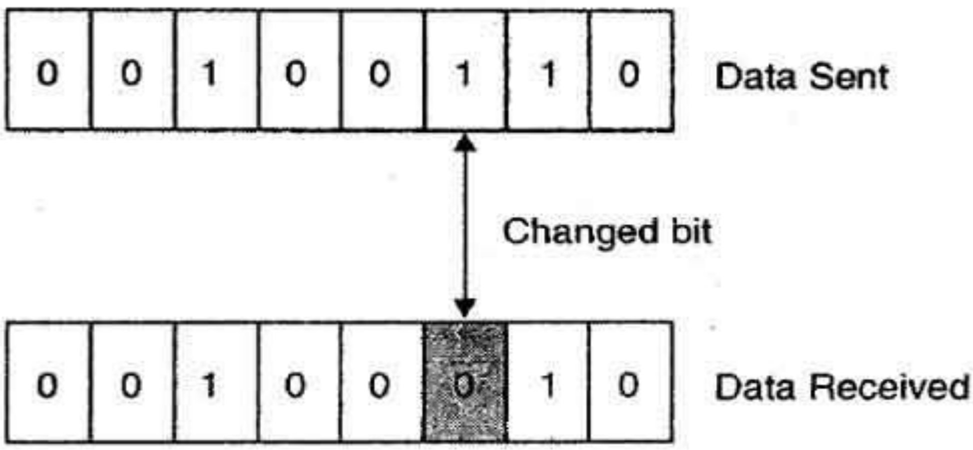
2 burst error



Types of errors

Single bit error:

- It means only one bit of data unit is changed from 1 to 0 or from 0 to 1 as shown in fig.

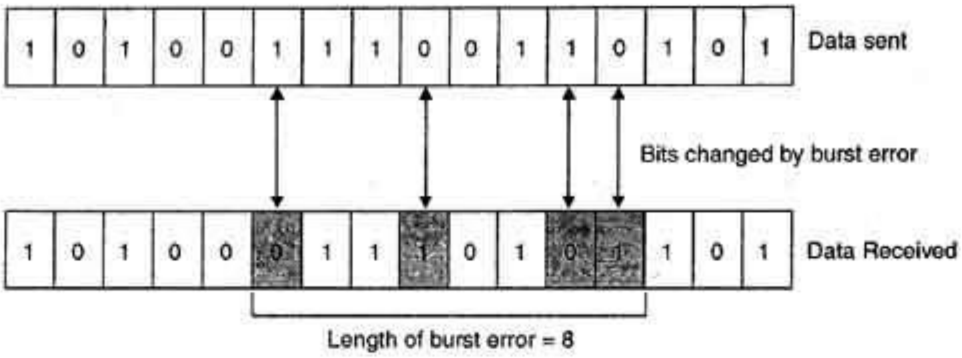


Single bit error

- Single bit error can happen in parallel transmission where all the data bits are transmitted using separate wires. Single bit errors are the least likely type of error in serial transmission.

Burst Error:

- It means two or more bits in data unit are changed from 1 to 0 from 0 to 1 as shown in fig.



Burst error

- In burst error, it is not necessary that only consecutive bits are changed. The length of burst error is measured from first changed bit to last changed bit. As shown in fig. length of burst error is 8, although some bits are unchanged in between. Burst error is most likely to occur in a serial transmission. The noise occurring for a longer duration affects multiple bits. The number of bits affected depends on the data rate & duration of noise. For e.g. if data rate is 1 kbps, a noise of 1/100 second can affect 10 bits.

Error Detection Schemes

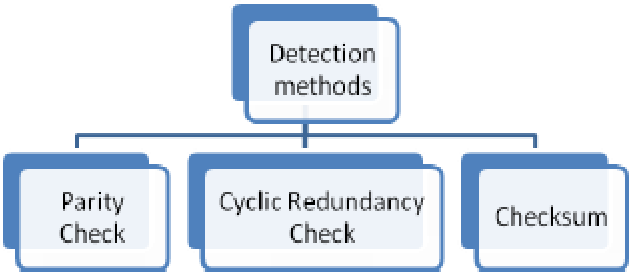
- Error detection is most commonly realized using a suitable hash function (or checksum algorithm). A hash function adds a fixed-length tag to a message, which enables receivers to verify the delivered message by recomputing the tag and comparing it with the one provided.
- There exists a vast variety of different hash function designs. However, some are of particularly widespread use because of either their simplicity or their suitability for detecting certain kinds of errors (e.g., the cyclic redundancy check's performance in detecting burst errors).
- Random-error-correcting codes based on minimum distance coding can provide a suitable alternative to hash functions when a strict guarantee on the minimum number of errors to be detected is desired. Repetition codes, described below, are special cases of error-correcting codes: although rather inefficient, they find applications for both error correction and detection due to their simplicity.

S.NO	RGPV QUESTIONS	Year	Marks
Q.1	Explain the types of error in data communication	Dec.2013	6

UNIT-04/LECTURE-03

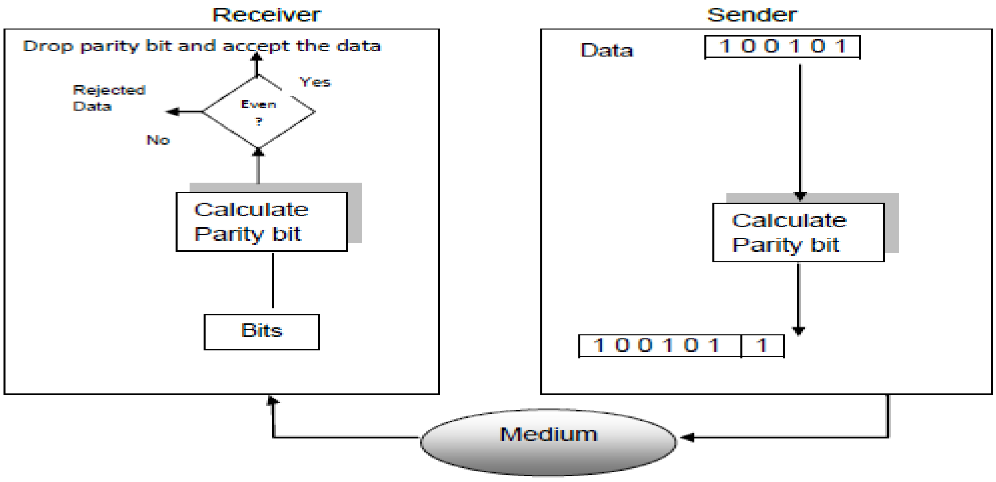
Error Detection (RGPV DEC-2013)

- Error detection is most commonly realized using a suitable hash function (or checksum algorithm). A hash function adds a fixed-length tag to a message, which enables receivers to verify the delivered message by recomputing the tag and comparing it with the one provided.
- There exists a vast variety of different hash function designs. However, some are of particularly widespread use because of either their simplicity or their suitability for detecting certain kinds of errors (e.g., the cyclic redundancy check's performance in detecting burst errors).
- Random-error-correcting codes based on minimum distance coding can provide a suitable alternative to hash functions when a strict guarantee on the minimum number of errors to be detected is desired. Repetition codes, described below, are special cases of error-correcting codes: although rather inefficient, they find applications for both error correction and detection due to their simplicity.



1.Parity Check:

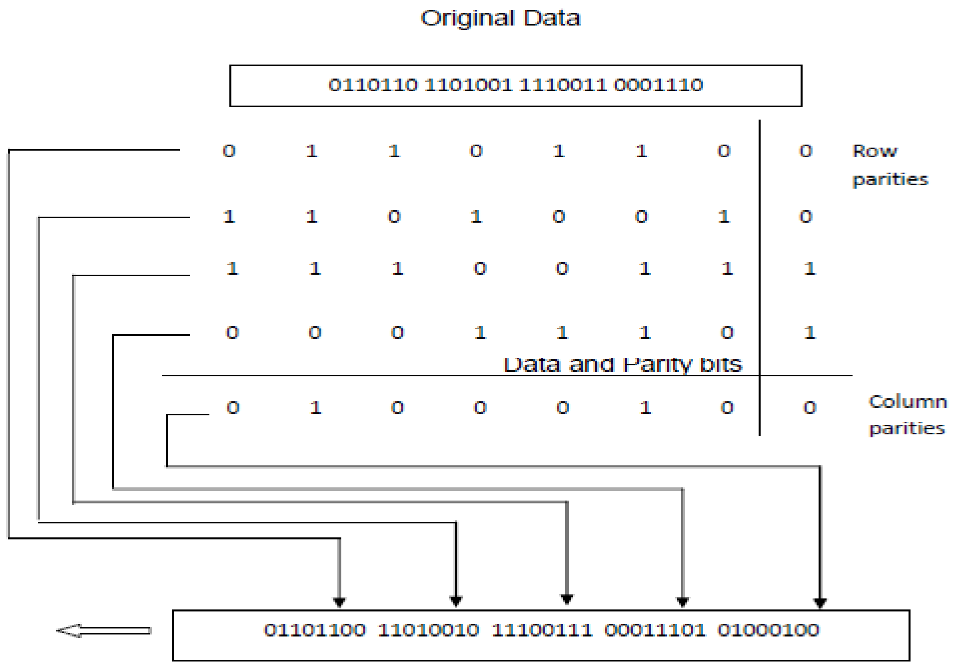
- In this technique, a redundant bit called a parity bit is addedto every data unit so that the total number of 1's in the unit(including the parity bit) becomes even (or odd). Following Figure shows this concept when transmit the binary data unit110101.



- Simple parity check can detect all single-bit errors. It can also detect burst errors as long as the total number of bits changed is odd. This method cannot detect errors where the total number of bits changed is even.

Two-Dimensional Parity Check:

- A better approach is the two dimensional parity checks. In this method, a block of bits is organized in a table (rows and columns). First we calculate the parity bit for each data unit. Then we organize them into a table. We then calculate the parity bit for each column and create a new row of 8 bits. Consider the following example; we have four data units to send. They are organized in the tabular form as shown below.



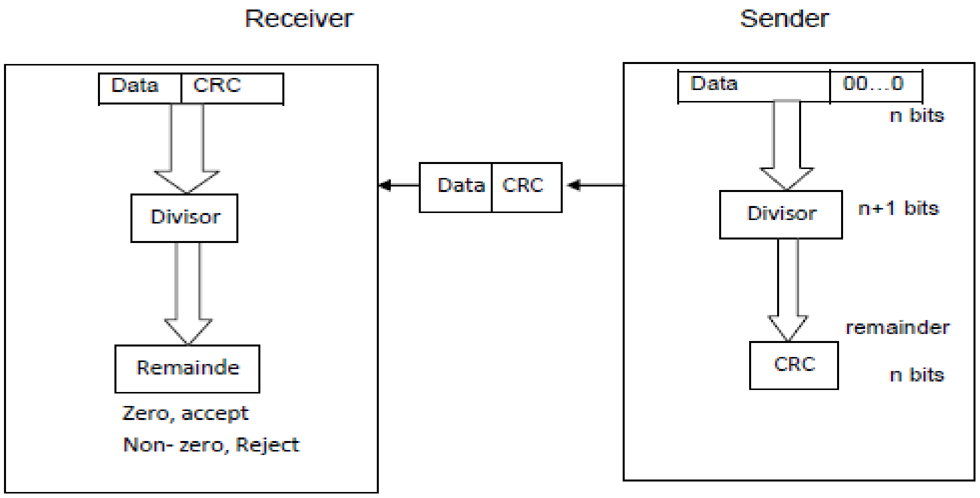
- We then calculate the parity bit for each column and create a new row of 8 bits; they are the parity bits for the whole block. Note that the first parity bit in the fifth row is calculated based on all first bits: the second parity bit is calculated based on all second bits: and so on. We then attach the 8 parity bits to the original data and send them to the receiver. Two-dimensional parity check increases the likelihood of detecting burst errors. A burst error of more than ‗n‘bits is also detected by this method with a very high probability.

2.Cyclic Redundancy Check (CRC)

- Most powerful of the redundancy checking techniques is the cyclic redundancy check (CRC). This method is based on the binary division. In CRC, the desired sequence of redundant bits are generated and is appended to the end of data unit. It is also called as CRC reminder. So that the resulting data unit becomes exactly divisible by a predetermined binary number.
- At its destination, the incoming data unit is divided by the same number. If at this step there is no remainder then the data unit is assumed to be correct and is therefore accepted.A remainder indicates that the data unit has been damaged in transit and therefore must be rejected. The redundancy bits used by CRC are derived by dividing the data unit by a predetermined divisor; the remainder is the CRC.To be valid, a CRC must have two qualities: It

must have exactly one less bit than the divisor, and appending it to the end of the data string must make the resulting bit sequence exactly divisible by the divisor.

The following figure shows the process:



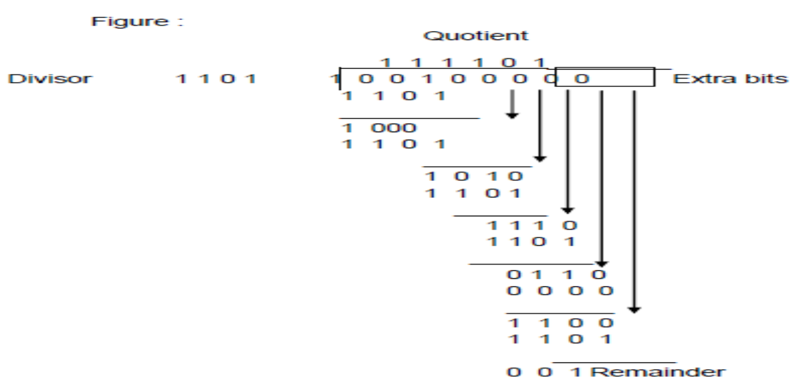
Step1: A string of 0's is appended to the data unit. It is n bits long. The number n is 1 less if-number of bits in the predetermined divisor which is n + 1 bits.

Step 2: The newly generated data unit is divided by the divisor, using a process called as binary division. The remainder resulting from this division is the CRC.

Step 3: the CRC of n bits derived in step 2 replaces the appended 0's at the data unit. Note that the CRC may consist of all 0's.

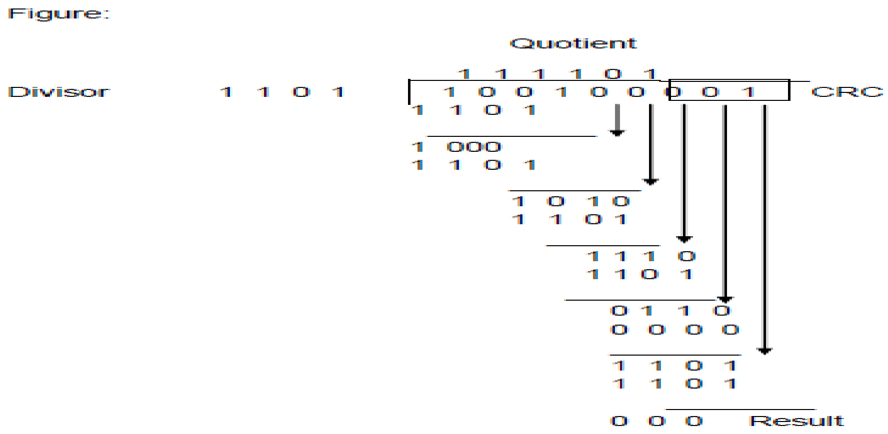
The data unit arrives at the receiver data first, followed by the CRC. The receiver treats the whole string as a unit and divides it by the same divisor that was used the CRC remainder. If the string arrives without error, the CRC checker yields a remainder of zero, the data unit passes. If the string has been changed in transit, the division yields zero remainder and the data unit does not pass.

Following figure shows the process of generating CRC reminder:



A CRC checker functions does exactly as the generator does. After receiving the data appended with the CRC, it does the samemodulo-2 division. If the remainder is all 0's, the CRC is dropped and the data is accepted: otherwise, the received stream of bits is discarded and data is resent.

Following Figure shows the same process of division in the receiver.



Performance: CRC is a very effective error detection method. If the divisor is chosen according to the previously mentioned rules, 1.CRC can detect all burst errors that affect an odd number of bits. 2.CRC can detect all burst errors of length less than or equal to the degree of the polynomial 3.CRC can detect, with a very high probability, burst errors of length greater than the degree of the polynomial.

3.Checksum

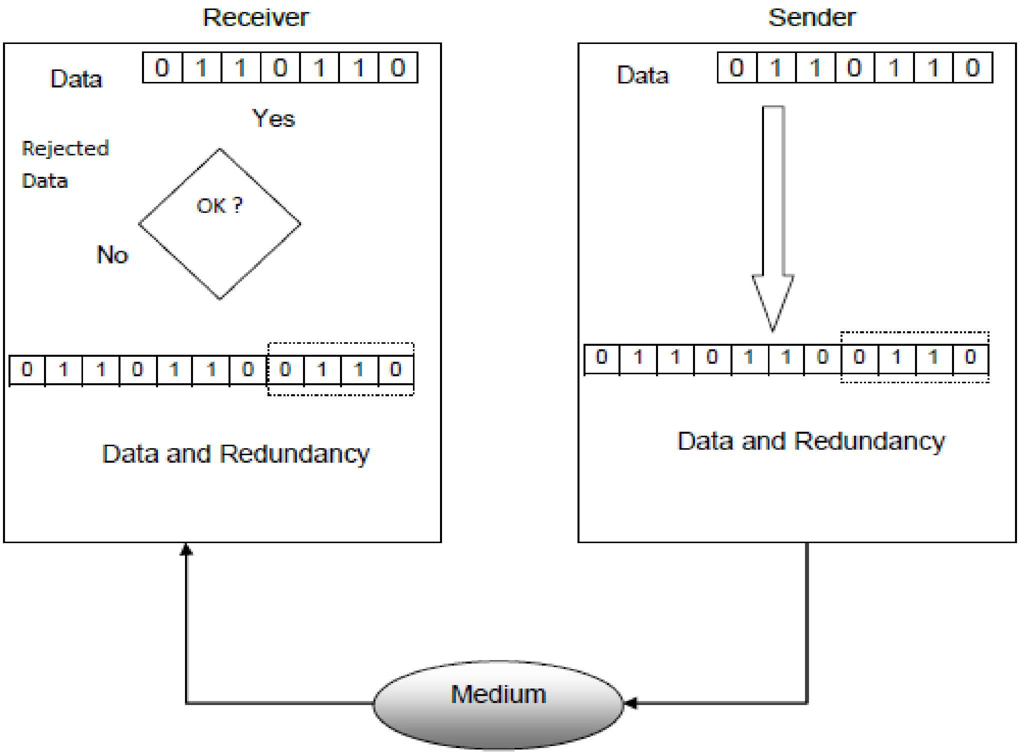
A checksum is fixed length data that is the result of performing certain operations on the data to be sent from sender to the receiver. The sender runs the appropriate checksum algorithm to compute the checksum of the data, appends it as a field in the packet that contains the data to be sent, as well as various headers. When the receiver receives the data, the receiver runs the same checksum algorithm to compute a fresh checksum. The receiver compares this freshly computed checksum with the checksum that was computed by the sender. If the two checksum matches, the receiver of the data is assured that the data has not changed during the transit

S.NO	RGPV QUESTIONS	Year	Marks
Q.1	Discuss briefly about redundancy checks	Dec 2013	4
Q.2	Explain error detection & error correction methods briefly.	Dec.2013	7

UNIT-04/LECTURE-04

Redudancy

- redudancy In order to detect and correct the errors in the data communication we add some extra bits to the original data. These extra bits are nothing but the redundant bits which will be removed by the receiver after receiving the data. Their presence allows the receiver to detect or correct corrupted bits. Instead of repeating the entire data stream, a short group of bits may be attached to the entire data stream.This technique is called redundancy because the extra bits are redundant to the information: they are discarded as soon as the accuracy of the transmission has been determined.



- There are different techniques used for transmission error detection and correction.

Error Correction methods:- (RGPV DEC-2013,DEC-2012)

Hamming Code:

- The Hamming code can be applied to data units of any length and uses the relationship between data and redundancy bits discussed above. For example, a 7-bit ASCII code requires 4 redundancy bits that can be added 10 the end of the data unit or interspersed with the original data bits. In following Figure,these bits are placed in positions 1, 2,4, and 8 (the positions in an 11-bit sequence that are powers of 2). For clarity in the examples below, we refer to these bits as r1, r2, r4, and r8.

11	10	9	8	7	6	5	4	3	2	1
d	d	d	*r8*	d	d	d	*r4*	d	*r2*	*r1*

In the Hamming code, each r bit is the parity bit for onecombination of data bits, is shown below:

r1 : bits 1,3,5,7,9,11
r2 : bits 2,3,6,7,10,11
r3 : bits 4,5,6,7
r4 : bits 8,9,10,11

r1will be assigned to these bits position:
11 9 7 5 3

d	d	d	*r8*	d	d	d	*r4*	d	*r2*	*r1*

1

r2will be assigned to these bits position:
11 10 7 6 3 2

d	d	d	*r8*	d	d	d	*r4*	d	*r2*	*r1*

r4will be assigned to these bits position:
7 6 5 4

d	d	d	*r8*	d	d	d	*r4*	d	*r2*	*r1*

r8will be assigned to these bits position:
11 10 9 8

d	d	d	*r8*	d	d	d	*r4*	d	*r2*	*r1*

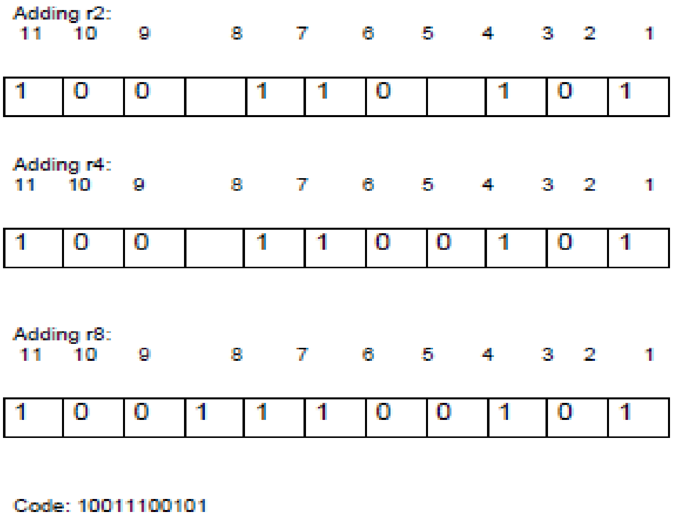
Now suppose we have 1001101 data to be sent, then the redundant bits are calculated by the following method:

Data is: 1 0 0 1 1 0 1

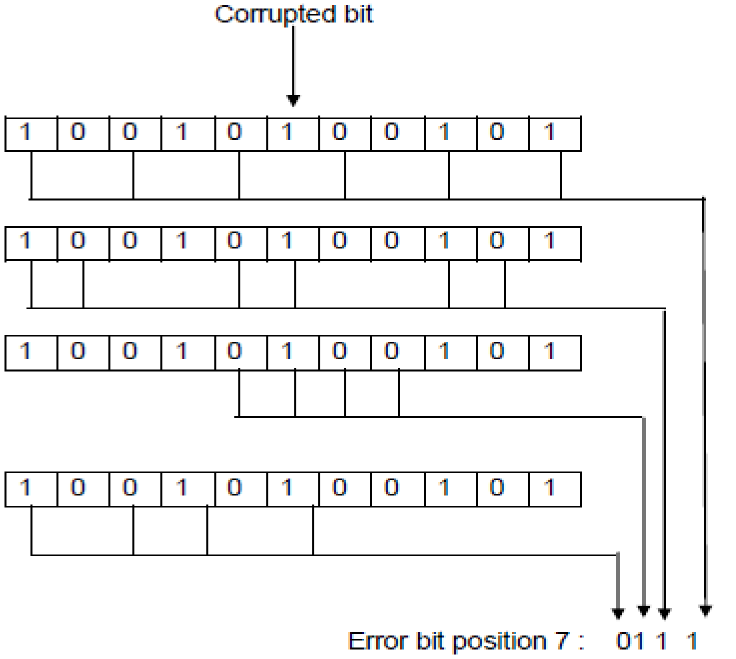
11	10	9	8	7	6	5	4	3	2	1
1	0	0		1	1	0		1		

Adding r1:

11	10	9	8	7	6	5	4	3	2	1
1	0	0		1	1	0		1		1



- Now imagine that by the time the above transmission is received, the number **7** bit has been changed from **1** to **0.**The receiver takes the transmission and recalculates 4 new parity bits, using the same sets of bits used by the sender plus the relevant parity r bit for each set (see following Fig.). Then it assembles the new parity values into a binary number in order of r position (r8 r4, r2, r1). In our example, this step gives us the binary number 0111 (7 in decimal), which is the precise location of the bit in error.



- Once the bit is identified, the receiver can reverse its value and correct the error. The beauty of the technique is that it can easily be implemented in hardware and the code is corrected before the receiver knows about it.

S.NO	RGPV QUESTIONS	Year	Marks
Q.1	Explain error detection & error correction methods briefly.	Dec.2013	7

UNIT-04/LECTURE-05

Integrated Services for Digital Network (ISDN) (RGPV Dec2012/Dec 2013)

Integrated Services for Digital Network (ISDN) is a set of communication standards for simultaneous digital transmission of voice, video, data, and other network services over the traditional circuits of the public switched telephone network. It was first defined in 1988 in the CCITT red book. Prior to ISDN, the telephone system was viewed as a way to transport voice, with some special services available for data. The key feature of ISDN is that it integrates speech and data on the same lines, adding features that were not available in the classic telephone system. There are several kinds of access interfaces to ISDN defined as Basic Rate Interface (BRI), Primary Rate Interface (PRI), Narrowband ISDN (N-ISDN), and Broadband ISDN (B-ISDN).

ISDN is a circuit-switched telephone network system, which also provides access to packet switched networks, designed to allow digital transmission of voice and data over ordinary telephone copper wires, resulting in potentially better voice quality than an analog phone can provide. It offers circuit-switched connections (for either voice or data), and packet-switched connections (for data), in increments of 64 kilobit/s. A major market application for ISDN in some countries is Internet access, where ISDN typically provides a maximum of 128 kbit/s in both upstream and downstream directions. Channel bonding can achieve a greater data rate; typically the ISDN B-channels of three or four BRIs (six to eight 64 kbit/s channels) are bonded.

ISDN should not be mistaken for its use with a specific protocol, such as Q.931 where as ISDN is employed as the network, data-link and physical layers in the context of the OSI model. In a broad sense ISDN can be considered a suite of digital services existing on layers 1, 2, and 3 of the OSI model. ISDN is designed to provide access to voice and data services simultaneously.

However, common use reduced ISDN to be limited to Q.931 and related protocols, which are a set of protocols for establishing and breaking circuit switched connections, and for advanced calling features for the user. They were introduced in 1986.

In a videoconference, ISDN provides simultaneous voice, video, and text transmission between individual desktop videoconferencing systems and group (room) videoconferencing systems

ISDN Interface

The entry level interface to ISDN is the Basic(s) Rate Interface (BRI), a 128 kbit/s service delivered over a pair of standard telephone copper wires. The 144 kbit/s payload rate is broken down into two 64 kbit/s bearer channels ('B' channels) and one 16 kbit/s signaling channel ('D' channel or data channel). This is sometimes referred to as 2B+D.

The interface specifies the following network interfaces:

- The U interface is a two-wire interface between the exchange and a network terminating unit, which is usually the demarcation point in non-North American networks.
- The T interface is a serial interface between a computing device and a terminal adapter, which is the digital equivalent of a modem.
- The S interface is a four-wire bus that ISDN consumer devices plug into; the S & T reference points are commonly implemented as a single interface labeled 'S/T' on an Network termination 1 (NT1).
- The R interface defines the point between a non-ISDN device and a terminal adapter (TA) which provides translation to and from such a device.

Primary Rate Interface

The other ISDN access available is the Primary Rate Interface (PRI), which is carried over an E1 (2048 kbit/s) in most parts of the world. An E1 is 30 'B' channels of 64 kbit/s, one 'D' channel of 64 kbit/s and a timing and alarm channel of 64 kbit/s.

In North America PRI service is delivered on one or more T1 carriers (often referred to as 23B+D) of 1544 kbit/s (24 channels). A PRI has 23 'B' channels and 1 'D' channel for signalling (Japan uses a circuit called a J1, which is similar to a T1). Inter-changeably but incorrectly, a PRI is referred to as T1 because it uses the T1 carrier format. A true T1 (commonly called "Analog T1" to avoid confusion) uses 24 channels of 64 kbit/s of in-band signaling. Each channel uses 56 kb for data and voice and 8 kb for signaling and messaging. PRI uses out of band signaling which provides the 23 B channels with clear 64 kb for voice and data and one 64 kb 'D' channel for signaling and messaging. In North America, Non-Facility Associated Signalling allows two or more PRIs to be controlled by a single D channel, and is sometimes called "23B+D + n*24B". D-channel backup allows for a second D channel in case the primary fails. NFAS is commonly used on a T3.

PRI-ISDN is popular throughout the world, especially for connecting PBXs to PSTN.

While the North American PSTN can use PRI or Analog T1 format from PBX to PBX, the POTS or BRI can be delivered to a business or residence. North American PSTN can connect from PBX to PBX via Analog T1, T3, PRI, OC3, etc.

Even though many network professionals use the term "ISDN" to refer to the lower-bandwidth BRI circuit, in North America BRI is relatively uncommon whilst PRI circuits serving PBXs are commonplace.

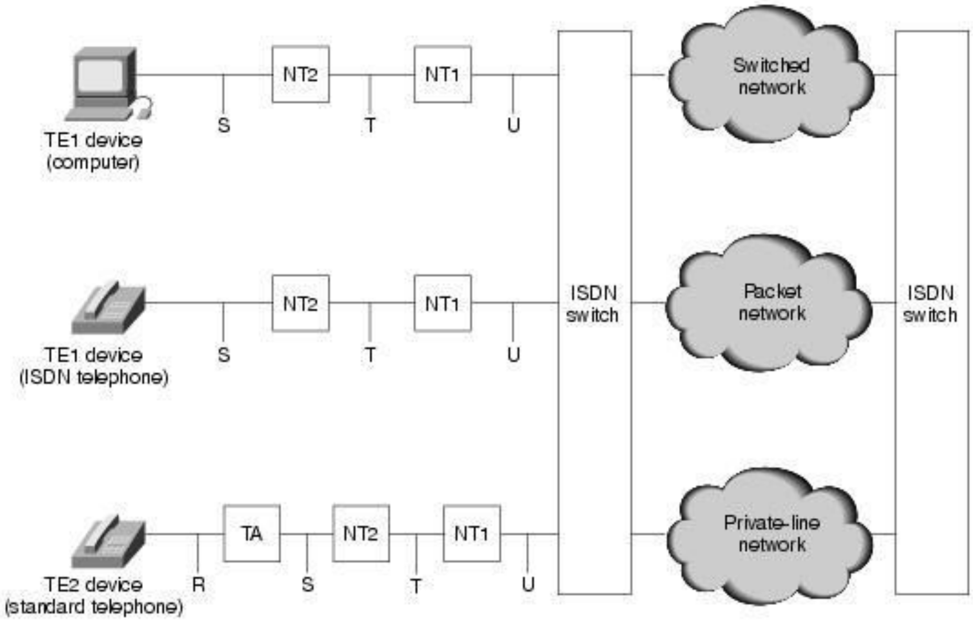
ISDN Devices

- ISDN devices include terminals, terminal adapters (TAs), network-termination devices, line-termination equipment, and exchange-termination equipment. ISDN terminals come in two types. Specialized ISDN terminals are referred to as terminal equipment type 1 (TE1). Non-ISDN terminals, such as DTE, that predate the ISDN standards are referred to as terminal equipment type 2 (TE2). TE1s connect to the ISDN network through a four-wire, twisted-pair digital link. TE2s connect to the ISDN network through a TA. The ISDN TA can be either a standalone device or a board inside the TE2. If the TE2 is implemented as a standalone device, it connects to the TA via a standard physical-layer interface. Examples include EIA/TIA-232-C (formerly RS-232-C), V.24, and V.35.

- Beyond the TE1 and TE2 devices, the next connection point in the ISDN network is the network termination type 1 (NT1) or network termination type 2 (NT2) device. These are network-termination devices that connect the four-wire subscriber wiring to the conventional two-wire local loop. In North America, the NT1 is a customer premises equipment (CPE) device. In most other parts of the world, the NT1 is part of the network provided by the carrier. The NT2 is a more complicated device that typically is found in digital private branch exchanges (PBXs) and that performs Layer 2 and 3 protocol functions and concentration services. An NT1/2 device also exists as a single device that combines the functions of an NT1 and an NT2.
- ISDN specifies a number of reference points that define logical interfaces between functional groups, such as TAs and NT1s. ISDN reference points include the following:

  - **R** - The reference point between non-ISDN equipment and a TA.
  - **S** - The reference point between user terminals and the NT2.
  - **T** - The reference point between NT1 and NT2 devices.
  - **U** - The reference point between NT1 devices and line-termination equipment in the carrier network. The U reference point is relevant only in North America, where the NT1 function is not provided by the carrier network.

- Figure: Sample ISDN Configuration Illustrates Relationships Between Devices and Reference Points illustrates a sample ISDN configuration and shows three devices attached to an ISDN switch at the central office. Two of these devices are ISDN-compatible, so they can be attached through an S reference point to NT2 devices. The third device (a standard, non-ISDN telephone) attaches through the reference point to a TA. Any of these devices also could attach to an NT1/2 device, which would replace both the NT1 and the NT2. In addition, although they are not shown, similar user stations are attached to the far-right ISDN switch.



- Figure: Sample ISDN Configuration Illustrates Relationships Between Devices and Reference Points

S.NO	RGPV QUESTIONS	Year	Marks
Q.1	What is ISDN.Discuss ISDN services and ISDN protocols	DEC2013 Dec 2012	7 7

UNIT-04/LECTURE-06

Services (RGPV Dec2013)

There are two types of services associated with ISDN:

- BRI
- PRI

ISDN BRI Service

- The ISDN Basic Rate Interface (BRI) service offers two B channels and one D channel (2B+D). BRI B-channel service operates at 64 kbps and is meant to carry user data; BRI D-channel service operates at 16 kbps and is meant to carry control and signaling information, although it can support user data transmission under certain circumstances. The D channel signaling protocol comprises Layers 1 through 3 of the OSI reference model. BRI also provides for framing control and other overhead, bringing its total bit rate to 192 kbps. The BRI physical layer specification is International Telecommunication Union-Telecommunications Standards Section (ITU-T) (formerly the Consultative Committee for International Telegraph and Telephone [CCITT]) I.430.

ISDN PRI Service

- ISDN Primary Rate Interface (PRI) service offers 23 B channels and 1 D channel in North America and Japan, yielding a total bit rate of 1.544 Mbps (the PRI D channel runs at 64 kbps). ISDN PRI in Europe, Australia, and other parts of the world provides 30 B channels plus one 64-kbps D channel and a total interface rate of 2.048 Mbps. The PRI physical layer specification is ITU-T I.431.

ISDN Specifications

- This section describes the various ISDN specifications for Layer 1, Layer 2, and Layer 3.

Layer 1

- ISDN physical layer (Layer 1) frame formats differ depending on whether the frame is outbound (from terminal to network) or inbound (from network to terminal). Both physical layer interfaces are shown in Figure: ISDN Physical Layer Frame Formats Differ Depending on Their Direction.
- The frames are 48 bits long, of which 36 bits represent data. The bits of an ISDN physical layer frame are used as follows:

- **F** - Provides synchronization
- **L** - Adjusts the average bit value

- **E** - Ensures contention resolution when several terminals on a passive bus contend for a channel
- **A** - Activates devices
- **S** - Is unassigned
- **B1**, **B2**, and **D** - Handle user data

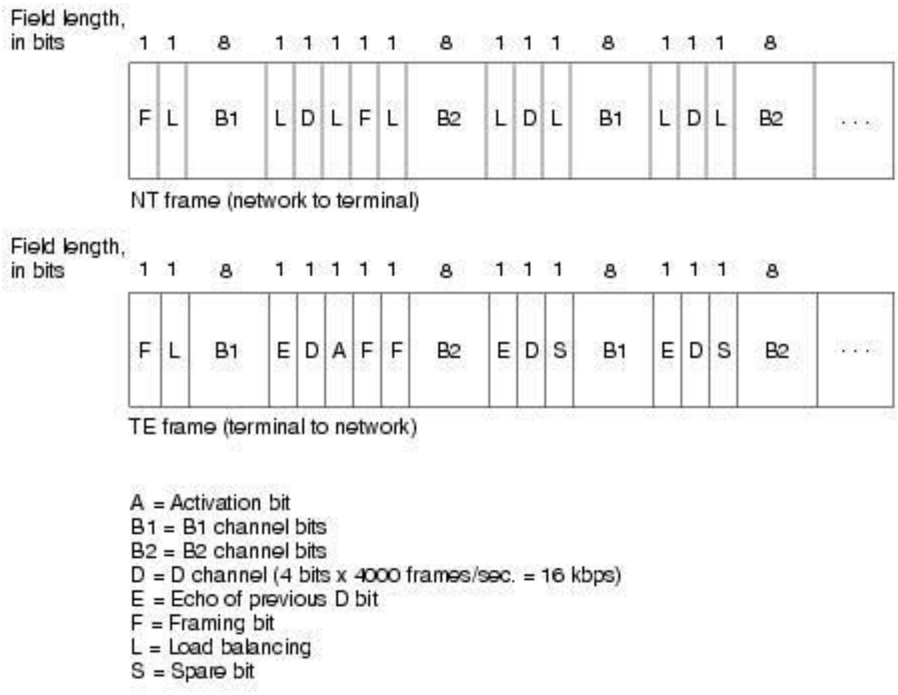


Figure: ISDN Physical Layer Frame Formats Differ Depending on Their Direction

- Multiple ISDN user devices can be physically attached to one circuit. In this configuration, collisions can result if two terminals transmit simultaneously. Therefore, ISDN provides features to determine link contention. When an NT receives a D bit from the TE, it echoes back the bit in the next E-bit position. The TE expects the next E bit to be the same as its last transmitted D bit.

- Terminals cannot transmit into the D channel unless they first detect a specific number of ones (indicating "no signal") corresponding to a pre-established priority. If the TE detects a bit in the echo (E) channel that is different from its D bits, it must stop transmitting immediately. This simple technique ensures that only one terminal can transmit its D message at one time. After successful D-message transmission, the terminal has its priority reduced by requiring it to detect more continuous ones before transmitting. Terminals cannot raise their priority until all other devices on the same line have had an opportunity to send a D message. Telephone connections have higher priority than all other services, and signaling information has a higher priority than nonsignaling information.

Layer 2

- Layer 2 of the ISDN signaling protocol is Link Access Procedure, D channel (LAPD). LAPD is similar to High-Level Data Link Control (HDLC) and Link Access Procedure, Balanced (LAPB). As the expansion of the LAPD acronym indicates, this layer is used across the D channel to ensure that control and signaling information flows and is received properly. The LAPD frame format (see Figure: LAPD Frame Format Is Similar to That of HDLC and LAPB)is very similar to that of HDLC; like HDLC, LAPD uses supervisory, information, and unnumbered frames. The LAPD protocol is formally specified in ITU-T Q.920 and ITU-T Q.921.

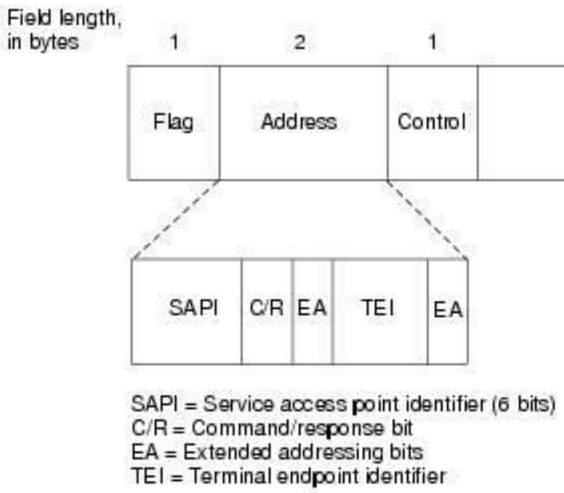


Figure: LAPD Frame Format Is Similar to That of HDLC and LAPB

- The LAPD Flag and Control fields are identical to those of HDLC. The LAPD Address field can be either 1 or 2 bytes long. If the extended address bit of the first byte is set, the address is 1 byte; if it is not set, the address is 2 bytes. The first Address-field byte contains the service access point identifier (SAPI), which identifies the portal at which LAPD services are provided to Layer 3. The C/R bit indicates whether the frame contains a command or a response. The Terminal Endpoint Identifier (TEI) field identifies either a single terminal or multiple terminals. A TEI of all ones indicates a broadcast.

S.NO	RGPV QUESTIONS	Year	Marks
Q.1	What is ISDN. Discuss ISDN services	Dec 2013	7

UNIT-04/LECTURE-07

Layer 3

- Two Layer 3 specifications are used for ISDN signaling: ITU-T (formerly CCITT) I.450 (also known as ITU-T Q.930) and ITU-T I.451 (also known as ITU-T Q.931). Together, these protocols support user-to-user, circuit-switched, and packet-switched connections. A variety of call-establishment, call-termination, information, and miscellaneous messages are specified, including SETUP, CONNECT, RELEASE, USER INFORMATION, CANCEL, STATUS, and DISCONNECT. These messages are functionally similar to those provided by the X.25 protocol.

Figure: An ISDN Circuit-Switched Call Moves Through Various Stages to Its Destination, from ITU-T I.451, shows the typical stages of an ISDN circuit-switched call.

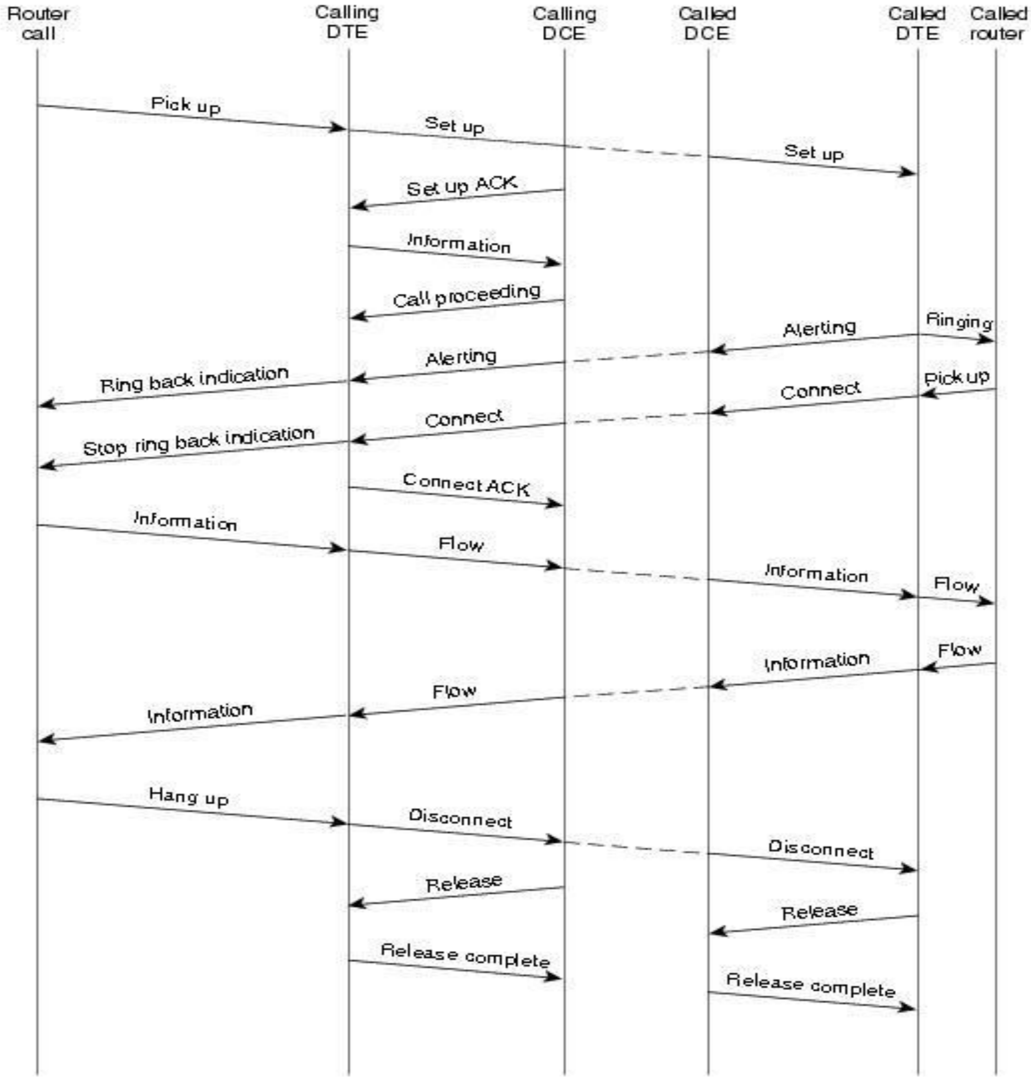


Figure: An ISDN Circuit-Switched Call Moves Through Various Stages to Its Destination

- ISDN is comprised of digital telephony and data-transport services offered by regional telephone carriers. ISDN involves the digitization of the telephone network to transmit voice, data, text, graphics, music, video, and other source material over existing telephone wires.
- ISDN devices include the following:

- Terminals
- Terminal adapters (TAs)
- Network-termination devices
- Line-termination equipment
- Exchange-termination equipment

- The ISDN specification references specific connection points that define logical interfaces between devices.
- ISDN uses the following two types of services:

- Basic Rate Interface (BRI, which offers two B channels and one D channel (2B+D)
- Primary Rate Interface (PRI), which offers 23 B channels and 1 D channel in North America and Japan, and 30 B channels and 1 D channel in Europe and Australia

- ISDN runs on the bottom three layers of the OSI reference model, and each layer uses a different specification to transmit data.

- Terminal Adapter (TA) - Converter device that converts standard electrical signals into the form used by ISDN - allows non-ISDN devices to operate on an ISDN network.
- Terminal Equipment Type 1 (TE1) - Compatible with the ISDN network. Example:Telephones, personal computers, fax machine or videoconferencing machine.
- Terminal Equipment Type 2 (TE2) - Not compatible with the ISDN network. Example: Analog phone or modem, requires a TA (TE2 connects to TA).
- Network termination type 1 & 2 (NT1 and NT2) - A small connection box that physically connects the customer site to the telco local loop, provides a four-wire connection to the customer site and a two-wire connection to the network (PRI – CSU/DSU).

Protocols

- ISDN User Part (ISUP)
- DSS1 (ETSI "Euro-ISDN", also used in many non-European countries)
- DSS2 (Digital Subscriber Signalling System No. 2)
- ETS 300 specification at ETSI

- NI-1 (US National ISDN Phase 1)
- NI-2 (US National ISDN Phase 2)
- 4ESS (Lucent 4ESS specific protocol defined in AT&T TR 41459)

- INS-NET 64/1500 (Japanese national/NTT carrier-specific protocol)
- DACS used in the UK by British Telecom it uses non standard D channel signalling for

pair gain

- QSIG
- Remote Operations Service Element protocol (ROSE)
- Q.931

- FTZ 1 TR 6 (obsolete German national protocol)
- TS.013/TS.014 (obsolete Australian national protocol)
- VN2/VN3/VN4 (obsolete French national protocols)

Specifications defining the physical layer and part of the data link layers of ISDN:

- ISDN BRI: ITU-T I.430.
- ISDN PRI: ITU-T I.431.

From the point of view of the OSI architecture, an ISDN line has a stack of three protocols

- physical layer
- data link layer
- network layer (the ISDN protocol, properly)[

ISDN services (RGPV Dec2013)

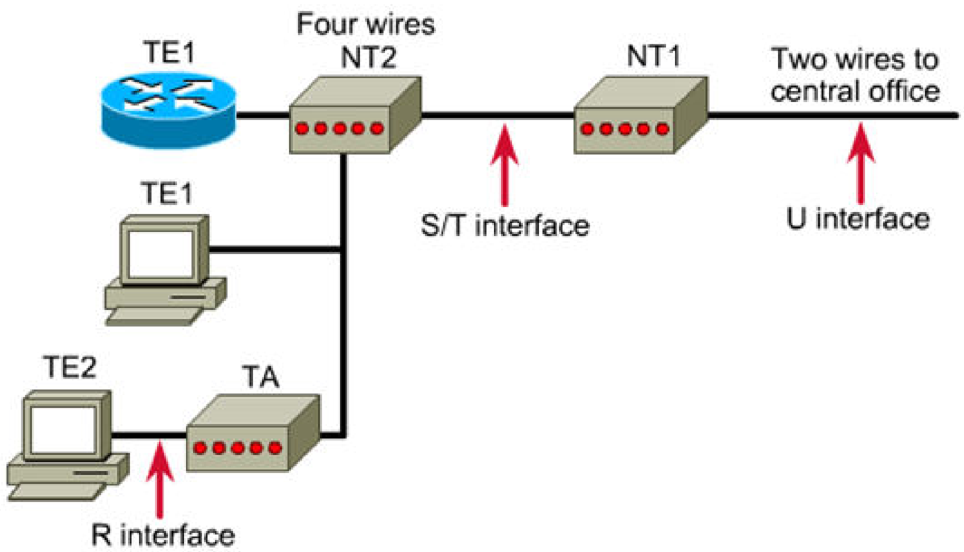
- Basic Rate Interface (BRI)
  - Two 64 Kbps B channels, one 16 Kbps D channel, and 48 Kbps worth of framing and synchronization.
  - Available data bandwidth: 128 Kbps (2 x 64 Kbps)
  - User bandwidth: 144 Kbps (128 Kbps + a 16 Kbps D channel)
  - Total line capacity: 192 Kbps (144 Kbps + 48 Kbps framing)
- Each B channel can be used for separate applications
  - Such as Internet and Voice
- Allows individual B channels to be aggregated together into a Multilink channel
- Primary Rate Interface (PRI)
  - A PRI connection can assign various 64 Kbps channels to both ISDN and analog modem connections
  - North America and Japan – PRI service has 23 64 Kbps B channels, one 64 Kbps D channel, and 8 Kbps of synchronization and framing for a total bit rate of up to 1.544 Mbps (same as T1)
  - Europe, Australia, and other parts of the world – PRI service has 30 64 Kbps B channels, one 64 Kbps D channel, and 64 Kbps of framing and synchronization for a total bit rate of up to 2.048 Mbps (same as E1)
- Each B channel to be used for separate applications including voice, data and Internet
- Multiple B channels can be Multilinked together

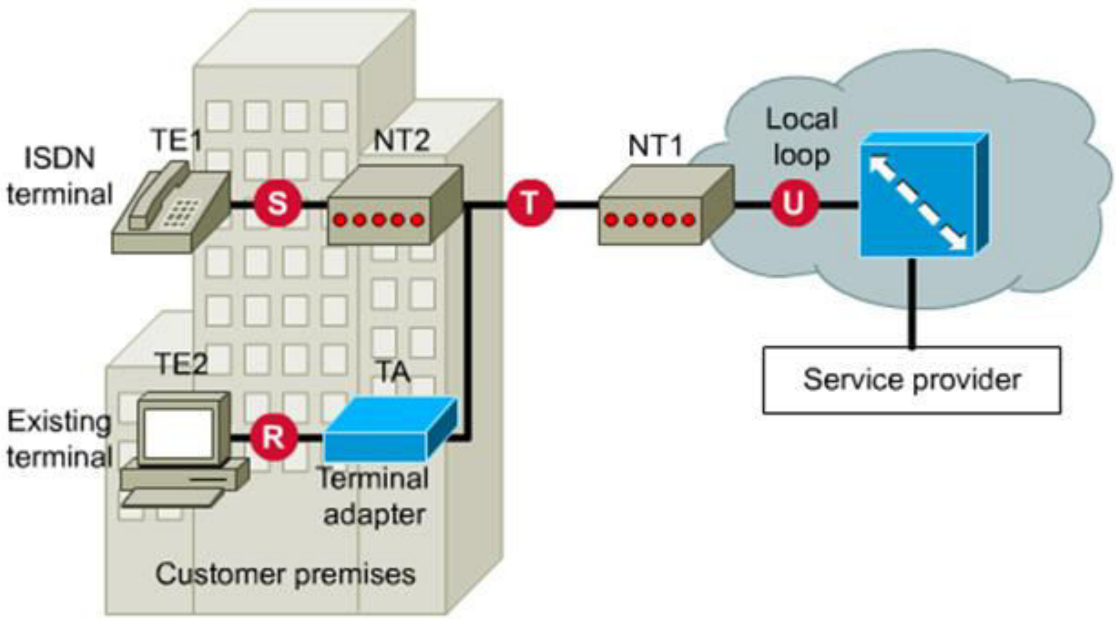
S.NO	RGPV QUESTION	YEAR	MARKS
Q.1	Discuss ISDN services and ISDN protocols	DEC 2013	7

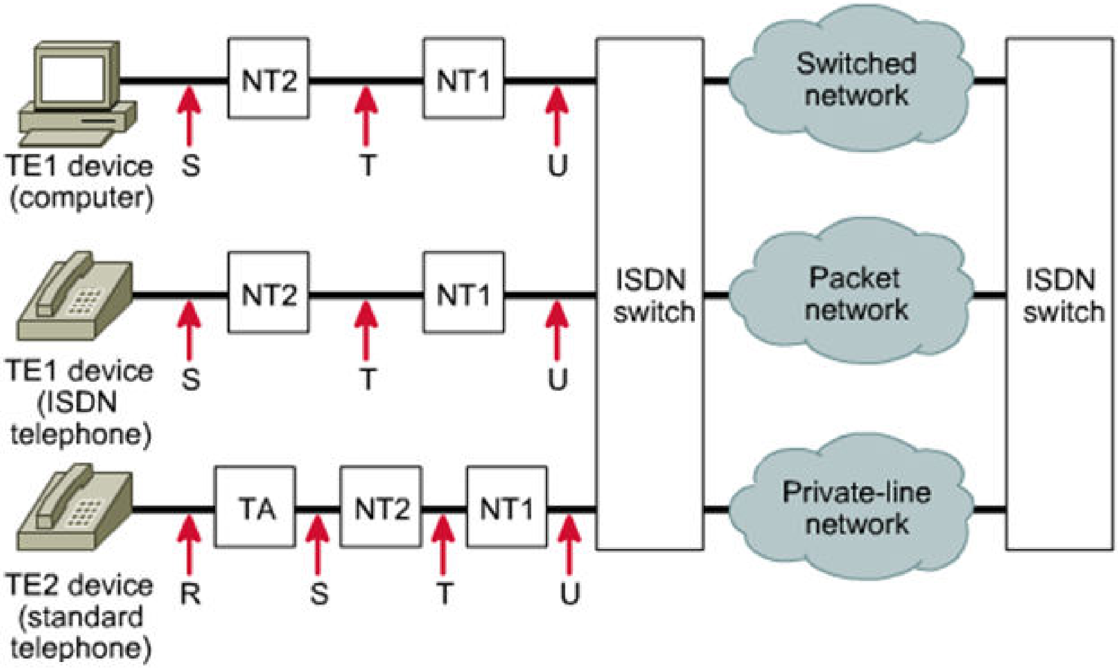
UNIT-04/LECTURE-08

ISDN refrence points

- U - Two wire cable that connects the customer's equipment to the telecommunications provider
- R - Point between non-ISDN equipment (TE2) and the TA
- S - Four-wire cable from TE1 or TA to the NT1 or NT2
- T - Point between NT1 and NT2







- The ISDN Physical Layer
- The ISDN Data Link Layer
- The ISDN Network Layer

Physical layer ISDN protocols

- – BRI (ITU-T I.430) / PRI (ITU-T I.431)
    - Defines two ISDN physical layer frame formats
        - – Inbound (local exchange to ISDN customer)
        - – Outbound (ISDN customer to local exchange)
- Data link layer ISDN protocols
    - – LAPD signaling protocol (ITU-T Q.920 for BRI and Q.921 for PRI) for transmitting control and signaling information over the D channel
        - LAPD frame format similar to ISO HDLC frame format
- Network layer ISDN protocols
    - – ITU-T I.930 and ITU-T Q.931 defines switching and signaling methods using the D channel.

UNIT-04/LECTURE-09
UNIT-04/LECTURE-10