

DEPARTMENT OF COMPUTER SCIENCE & ENGINEERING

LAB RECORD

Course Code : CS-604

Course : COMPUTER NETWORKING

Session :

Faculty Name :



Index

Sr. No.	Particulars
1	Time Table
2	University Scheme
3	Syllabus
4	List of Programs
5	List of Books & Websites
6	Important Viva Questions

UNIVERSITY SCHEME

Rajiv Gandhi Proudhogiki Vishwavidyalaya, Bhopal

B.E. VI Semester (Computer Science and Engineering)

Subject wise distribution of marks and corresponding credit (Grading System w.e.f-2012-13

S.No.	Subject Code	Subject Name & Title	Maximum Marks Allotted							Credits Allotted Subject wise	Total Credits	Remark		
			Theory Slot			Practical Slot			Total Marks					
			End Sem.	Mid Sem. MST (Two tests average)	Quiz, Assignment	End Sem	Term work							
							Lab work & sessional	Assignment/ quiz	Period per week					
L	T	P												
1	CS-601	Micro Processor and Interfacing	70	20	10	30	10	10	150	3	1	2	06	
2	CS-602	PPL	70	20	10	-	-	-	100	3	1	-	04	
3	CS-603	Software Engineering & Project managements	70	20	10	30	10	10	150	3	1	2	06	
4	CS-604	Computer Networking	70	20	10	30	10	10	150	3	1	2	06	
5	CS-605	Advance Computer Architecture(ACA)	70	20	10	-	-	-	100	3	1	-	04	
6	CS-606	Minor Project – I	-	-	-	30	10	10	50	0	0	2	02	
7	CS-607	Self study (Internal Assessment)	-	-	-	-	-	50	50	0	0	2	02	Grand Total
8.	CS-608	Seminar / Group Discussion (Internal Assessment)	-	-	-	-	-	50	50	0	0	2	02	
		Total	350	100	50	120	40	140	800	15	5	12	32	800

MST: Mid Semester Tests Taken at Least twice Per Semester

L: Lecture - T: Tutorial - P: Practical

UNIVERSITY SYLLABUS

RAJIV GANDHI PROUDYOGIKI VISHWAVIDYALAYA, BHOPAL

PROGRAMME: B.E. Computer Science & Engineering, VI Semester

Course: CS 604 Computer Networking

Branch: Computer Science & Engineering VI Semester.

UNIT-I

Computer Network: Definitions, goals, components, structure, Architecture, Classifications & types, Growth, Complexity and applications etc. Layered Architecture: Protocol hierarchy, Connection Oriented & Connectionless Services, Service primitive Design issues & its functionality. ISO-OSI Reference Model: Principle, Model, Descriptions of various layers and its comparison with TCP/IP. Network standardization. Examples of Networks: Telecommunication Network, Corporate Networks, Connection oriented network i.e., X.25, Frame relay & ATM, Wireless LAN 802.11, internet, Intranet, Extranet, SNA & DNA etc.

Unit II

Data Link Layer: Need, Services Provided, Framing & its methods, Flow Control, Error control. DLL Protocol: Elementary & Sliding Window. Piggybacking & Pipelining. Protocol verification: Finite State Machine Models & Petri net models. Example in Data Link Layers: HDLC & Internet. Comparison of BISYNC and HDLC Features. Bridges and layer-2 switches

Unit III

MAC Sub layer: Static & Dynamic channel allocation, Media access control for LAN & WAN. Classification of MAC Sub layer protocol, Study of various collisions, Collision free & limited contention protocol i.e., ALOHA: pure, slotted, CSMA, CSMA/CD, CSMA/CA, Bit Map, Binary count down, BRAP, MLMA, Adaptive tree walk & urn protocol etc. IEEE 802 standards for LAN & MAN & their comparison. Ethernet: Cabling, Binary exponentials algorithms, performance fast Ethernet, Gigabit Ethernet, FDDI. Wireless LANs, Broadband Wireless, Bluetooth: Architecture, Application & Layering.

UNIT – IV

Network Layer: Need, Services Provided, Design issues, Routing algorithms: Least Cost Routing algorithm, Dijkstra's algorithm, Bellman-ford algorithm, Hierarchical Routing, Broadcast Routing, Multicast Routing, Routing for mobile hosts, Routing in Ad Hoc Networks Routing Strategies, Congestion Control Algorithms: General Principles of Congestion control, Prevention Policies, Congestion Control in Virtual-Circuit Subnets, Congestion Control in Datagram subnets. IP protocol, IP Addresses, Comparative study of IPv4 & IPv6, Mobile IP.

Unit V

Processes to Processes Delivery – Transmission Control Protocol (TCP) – User Datagram Protocol, Data Traffic, Congestion Control and Quality of Service, Techniques to improve QOS, Integrated Services, and Differentiated Services. Network Security: Cryptography, Message Security, Digital Signature, User Authentication, Key Management, Security Protocols in Internet, DNS,SMTP, FTP, HTTP, WWW, Virtual Terminal Protocol, VoIP: Basic IP Telephone System, H.323 Characteristic & Layering, SIP Characteristics, Method & Sessions.

LIST OF EXPERIMENTS

Sr. No.	Name of Experiments
1	To study of different type of LAN and equipment devices
2	Study and verification of standard Network topologies i.e. Star, Bus, Ring etc.
3	LAN installations and their Configurations.
4	To implement various types of error correcting techniques.
5	To implement various types of framing methods.
6	To study of Tool Command Language (TCL).
7	Study and Installation of Standard Network Simulator: N.S-2, N.S-3.OpNet,QualNet etc
8	Study & Installation of ONE (Opportunistic Network Environment) Simulator for High Mobility Networks
9	Configure 802.11 WLAN
10	Implement & Simulate various types of routing algorithm.
11	Study & Simulation of MAC Protocols like Aloha, CSMA, CSMA/CD and CSMA/CA using Standard Network Simulators
12	Study of Application layer protocols- DNS, HTTP, HTTPS, FTP and TelNet.



EXPERIMENT NO. 1

Aim: To study various types of connectors.

1. Repeater
2. Hub
3. Switch
4. Bridge
5. Router
6. Gate Way

Apparatus Required

No software or hardware needed

Theory

1. **Repeater:** Functioning at Physical Layer. A repeater is an electronic device that receives a signal and retransmits it at a higher level and/or higher power, or onto the other side of an obstruction, so that the signal can cover longer distances. Repeaters have two ports, so cannot be used to connect for more than two devices.



2. **Hub:** An Ethernet hub, active hub, network hub, repeater hub, hub or concentrator is a device for connecting multiple twisted pair or fiber optic Ethernet devices together and making them act as a single network segment. Hubs work at the physical layer of the OSI model. The device is a form of multiport repeater. Repeater hubs also participate in collision detection, forwarding a jam signal to all ports if it



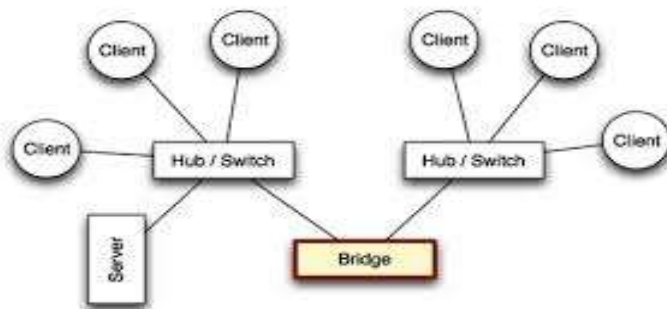
detects a collision.

3. **Switch:** A network switch or switching hub is a computer networking device that connects network segments. The term commonly refers to a network bridge that processes and routes data at the data link layer of the OSI model. Switch that additionally process data at the network layer are often referred to as
-

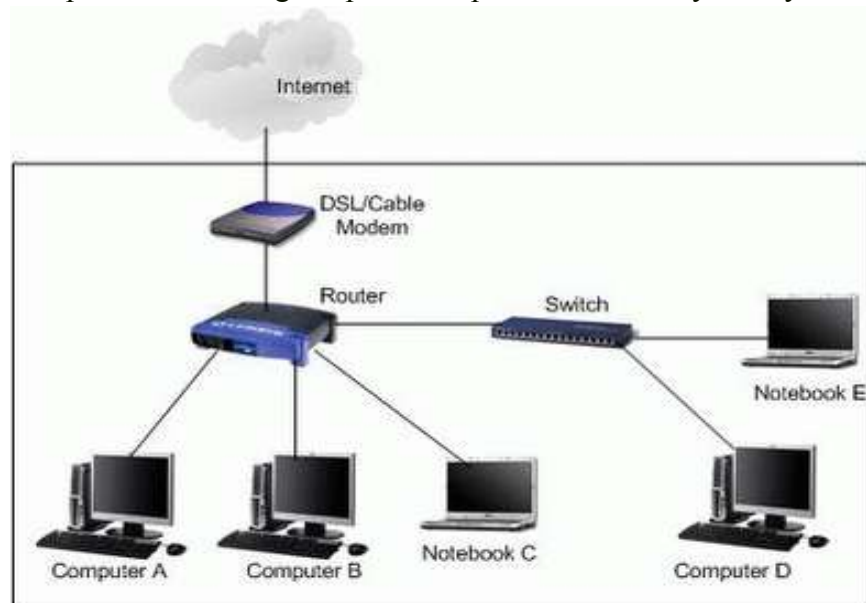


layer 3 switches or multilayer switches.

4. **Bridge:** A network bridge connects multiple network segments at the data link layer of the OSI model. In Ethernet networks, the term bridge formally means a device that behaves according to the IEEE 802.1 D standards. A bridge and switch are very much alike; a switch being a bridge with numerous ports. Switch of layer 2 switch is often used interchangeably with bridge. Bridges can analyze incoming data packets to determine if the bridge is able to send the given packet to another segment of the network.



5. **Router:** A router is an electronic device that interconnects two or more computer networks, and selectively interchanges packets of data between them. Each data packet contains address information that a router can use to determine if the source and destination are on the same network, or if the data packet must be transferred from one network to another. Where multiple routers are used in a large collection of interconnected networks, the routers exchange information about target system addresses, so that each router can build up a table showing the preferred paths between any two systems on the

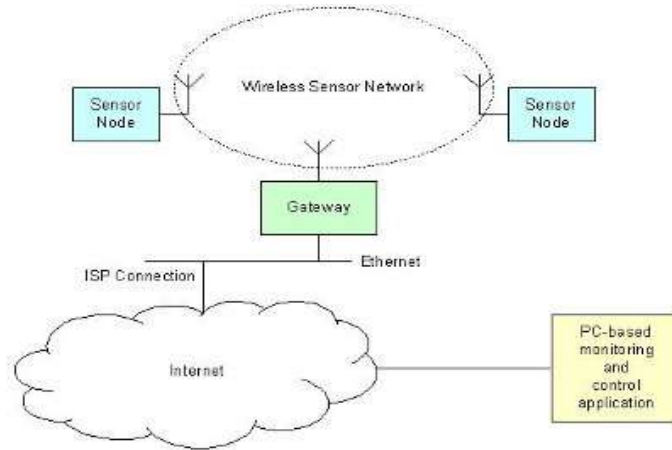


interconnected networks.

6. **Gate way:** In a communications network, a network node equipped for interfacing with another network that uses different protocols.

A gateway may contain devices such as protocol translators, impedance matching devices, rate converters, fault isolators, or signal translators as necessary to provide system interoperability. It also

requires the establishment of mutually acceptable administrative procedures between both networks. A protocol translation/mapping gateway interconnects networks with different network protocol technologies by performing the required protocol conversions.



Conclusions

Different Network Devices have been studied in detail.

Survey (Current Devices)

.....

.....

.....

.....

EXPERIMENT NO. 2

Aim: Study and verification of standard Network topologies i.e. Star, Bus, Ring etc.

Theory

Network topology is the arrangement of the various elements (links, nodes, etc.) of a computer or biological network. Essentially, it is the topological structure of a network, and may be depicted physically or logically. *Physical* topology refers to the placement of the network's various components, including device location and cable installation, while *logical* topology shows how data flows within a network, regardless of its physical design. Distances between nodes, physical interconnections, transmission rates, and/or signal types may differ between two networks, yet their topologies may be identical.

A good example is a local area network (LAN): Any given node in the LAN has one or more physical links to other devices in the network; graphically mapping these links results in a geometric shape that can be used to describe the physical topology of the network. Conversely, mapping the data flow between the components determines the logical topology of the network.

Topology

There are two basic categories of network topologies:

1. Physical topologies
2. Logical topologies

The shape of the cabling layout used to link devices is called the physical topology of the network. This refers to the layout of cabling, the locations of nodes, and the interconnections between the nodes and the cabling. The physical topology of a network is determined by the capabilities of the network access devices and media, the level of control or fault tolerance desired, and the cost associated with cabling or telecommunications circuits.

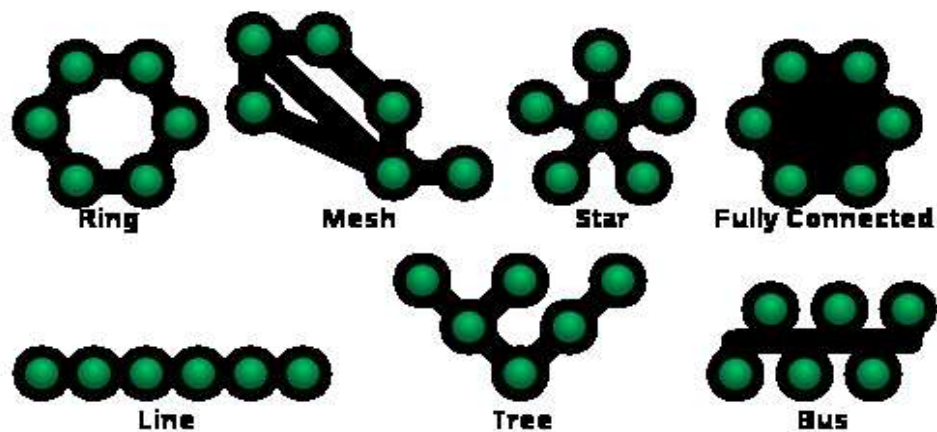
The logical topology, in contrast, is the way that the signals act on the network media, or the way that the data passes through the network from one device to the next without regard to the physical interconnection of the devices. A network's logical topology is not necessarily the same as its physical topology. For example, the original twisted pair Ethernet using repeater hubs was a logical bus topology with a physical star topology layout. Token Ring is a logical ring topology, but is wired a physical star from the Media Access Unit.

The logical classification of network topologies generally follows the same classifications as those in the physical classifications of network topologies but describes the path that the *data* takes between nodes being used as opposed to the actual *physical* connections between nodes. The logical topologies are generally determined by network protocols as opposed to being determined by the physical layout of cables, wires, and network devices or by the flow of the electrical signals, although in many cases the paths that the electrical signals take between nodes may closely match the logical flow of data, hence the convention of using the terms *logical topology* and *signal topology* interchangeably.

Logical topologies are often closely associated with Media Access Control methods and protocols. Logical topologies are able to be dynamically reconfigured by special types of equipment such as routers and switches.

The study of network topology recognizes eight basic topologies:

- Point-to-point
- Bus
- Star
- Ring or circular
- Mesh
- Tree
- Hybrid
- Daisy chain



Topology Structure of Campus

.....
.....
.....
.....

EXPERIMENT NO. 3

Aim: LAN installations and their Configurations.

Apparatus Required

Theory

Performance:

Perform the following steps as directed

Step 1: To make a Direct Cable connection

1. Click **Start**, click **Control Panel**, and then double-click **Network Connections**.
2. Under **Network Tasks**, click **Create a new connection**, and then click **next**.
3. Click **Set up an advanced connection**, and then click **next**.
4. Click **Connect directly to another computer**, and click **next**.
5. Choose the role this machine will play in the communication. If this computer has the information to which you need to gain access, click **Host**. If this computer will access information from the other computer, click **Guest**.

Step 2: To Set Up the Host Computer

1. Click the connection device that you want to use for this connection (a parallel or serial port, or an infrared port), and then click **Next**.
2. Grant access to the users who are allowed to connect by selecting the appropriate check boxes, and then click **Next**.
3. Click **Finish** to end the configuration process.

Step 3: to Set up the Guest Computer

1. Type a name to identify this connection, and then click **Next**.
2. Click the connection device that you want to use for this connection (a parallel or serial port, or an infrared port), and then click **Next**.
3. Decide whether this connection will be available for all users (click **Anyone's use**), or only for you (click **my use only**), and then click **Next**.
4. Click **Finish** to end the setup process

Step 4: To create Windows Workgroup

1. In Windows XP, right click on **My Computer**, select **System Properties**.
2. Select the **Computer Name** tab, click on **Change**.
3. Enter the appropriate **Computer name** and **Workgroup**.
4. Make sure that every computer on your home network references the same workgroup.

Step 5:

To Configure TCP/IP

To assign IP address, gateway, subnet mask, DNS

Step 6:

To create domain Bring all the PC of Lab under a network using workgroup or domain.

Create client and server

Result/ Conclusions

Windows workgroup is established and used for sharing and transferring data between physically connected PCs.

Lan Installation issues

.....

.....

.....

.....



EXPERIMENT NO. 4

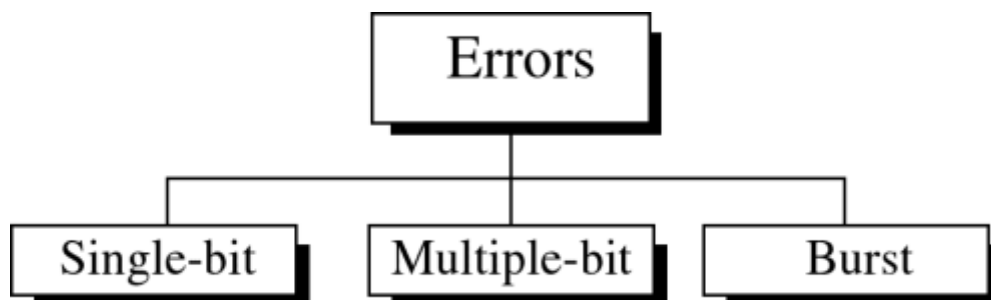
Aim: To implement various types of error correcting techniques.

Apparatus Required

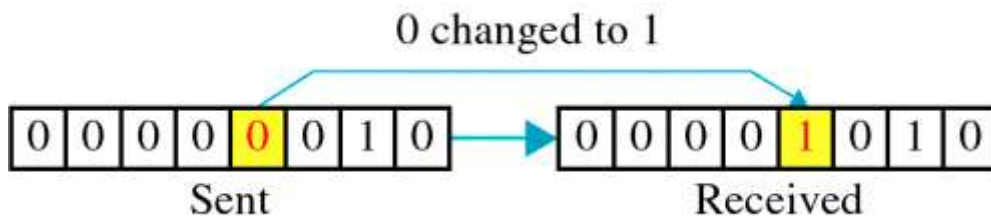
Theory

Error detection and correction are implemented either at the data link layer or the transport layer of the OSI model.

Types of Errors



Single-bit error

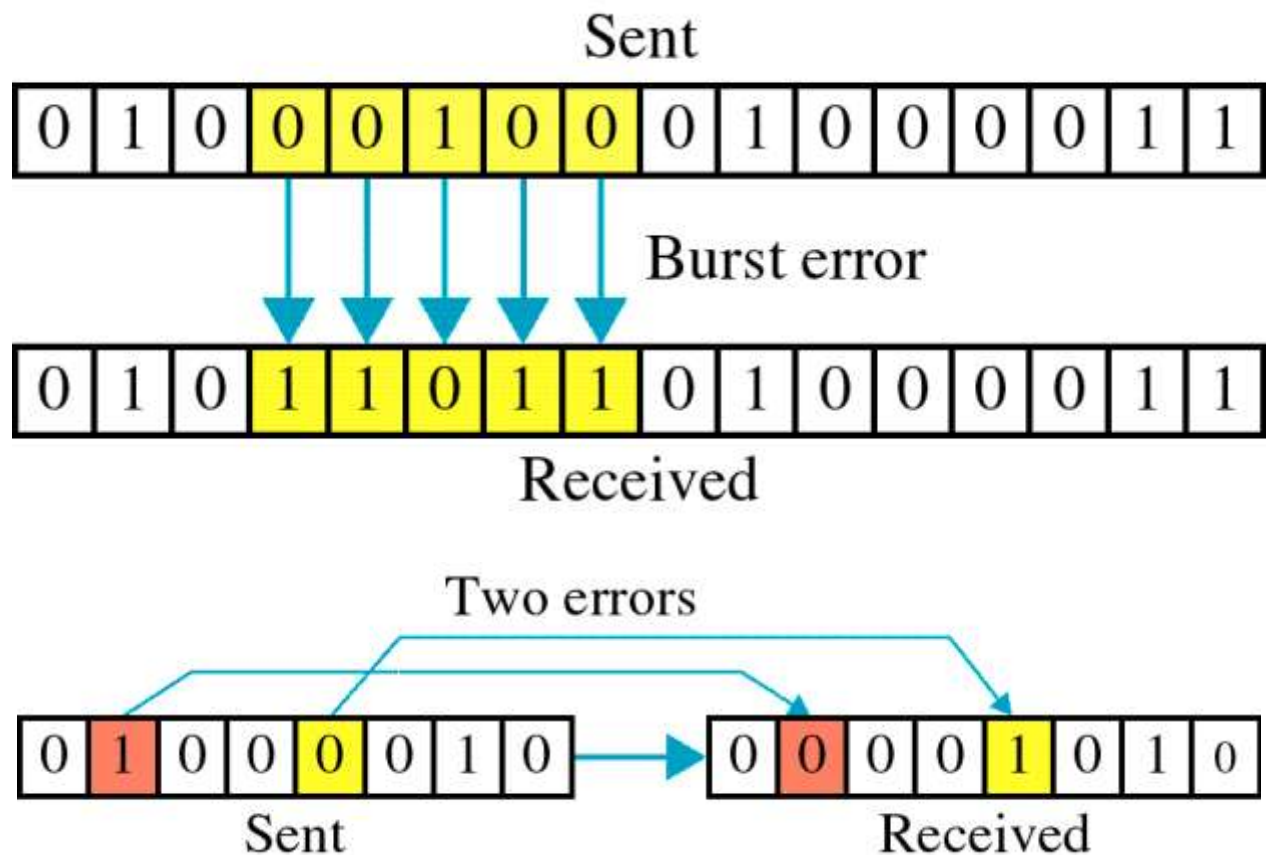


Single bit errors are the **least likely** type of errors in serial data transmission because the noise must have a very short duration which is very rare. However this kind of errors can happen in parallel transmission.

Example:

- ★ If data is sent at 1Mbps then each bit lasts only $1/1,000,000$ sec. or $1\ \mu\text{s}$.
- ★ For a single-bit error to occur, the noise must have a duration of only $1\ \mu\text{s}$, which is very rare.

Burst error



The term **burst error** means that two or more bits in the data unit have changed from 1 to 0 or from 0 to 1.

Burst errors do not necessarily mean that the errors occur in consecutive bits, the length of the burst is measured from the first corrupted bit to the last corrupted bit. Some bits in between may not have been corrupted.

Burst error is most likely to happen in serial transmission since the duration of noise is normally longer than the duration of a bit.

The number of bits affected depends on the data rate and duration of noise.

Example:

If data is sent at rate = 1Kbps then a noise of 1/100 sec can affect 10 bits. $(1/100 \times 1000)$

If same data is sent at rate = 1Mbps then a noise of 1/100 sec can affect 10,000 bits. $(1/100 \times 10^6)$

CYCLIC REDUNDANCY CHECK (CRC)

LOGIC:

1. Let r be the degree of $G(x)$. Append r zero bits to the low-order end of the frame. So it now contains $m+r$ bits and corresponds to the polynomial $x^2 m(x)$.
 2. Divide the bit string corresponding to $G(x)$ into the bit string corresponding to $x^2 m(x)$ using modulo-2 division.
 3. Subtract the remainder from the bit string corresponding to $x^2 m(x)$ using modulo-2 sub. The result is the check summed frame to be transmitted. We call it as a polynomial.
-

Implementation of Error Checking Techniques ()

.....

.....

.....

.....

EXPERIMENT NO. 5

Aim - To implement various types of framing methods.

- a) CHARACTER COUNT
- b) BIT STUFFING AND DE STUFFING
- c) CHARACTER STUFFING AND DE STUFFING

CHARACTER COUNT

Aim:Implementation of data link framing methods for counting characters in a given frame

LOGIC: The header in the given frame is by default first frame size including the first field data bits are counted and considered as the first frame and the next field contains the next frame size and so on.

PSEUDO CODE:

1. At the sender side the user is asked to enter the number of frames he want to transmit.
2. Depending upon the input, that much number of frames are taken as input from the user and stored in a 2 by 2 matrix.
3. The length of each frame is calculated and stored in a new array.
4. While out putting the frame, the length of each frame is added to the each frame and finally all the frames are appended and sent as a single string.
5. At the receiver side, the first number is treated as the length of the first frame and the string is extracted and displayed.
6. The next number is treated as the length of the next frame and so on.

At Sender:

INPUT:

Enter the number of frames you want to send: 2

Enter the frame: 1234

Enter the frame: 678

OUTPUT

The transmitted frame is: 512344678

At receiver:

INPUT:

Enter data 512344678

OUTPUT:

Frame sizes are: 5 4

Frames are:

Frame 1: 1234

Frame 2: 678

BIT STUFFING

AIM

Implementation of the data link framing methods for the bit stuffing in a frame.

LOGIC: Stuffing a 0 bit in a data frame in order to differentiate the header, trailer and data.

PSEUDO CODE: /* For given data */

1. a flag "01111110" is embedded at the starting and the ending of the data. /* stuffing of data */
2. if data bit is 1 increment count else count is zero.
3. If count is five store a zero bit after the five 1"s in the data array.
4. Repeat step 3 till the end of data. /* De stuffing of data */
5. If the data bit is 1 increment count else count is zero.
6. If the count is five and the next bit is zero then store the next bit after zero in the data array. /* transmit the data */
7. De stuffed data is transmitted without flags.

At sender:

INPUT:

Enter the string 1111110101

OUTPUT:

Transmitted data is: 01111110111111010101111110

Stuffed data is: 0111111011111101010101111110

At Receiver:

INPUT:

Enter the string 1111110101

OUTPUT:

De stuffed data is: 1111110101

CHARACTER STUFFING

AIM

Implementation of data link framing methods for character stuffing in a frame.

LOGIC: In a character data frame if a DLE is encountered between the data it is doubled and transmitted at the receiver side it is de stuffed and original data is obtained.

PSEUDO CODE: /* Defining DLE characters */

1. As the DLE characters are non-printable characters. The ASCII values of the printable characters like *, #, \$ are assigned to DLE, STX, ETX.

/*Stuffing the data */

2. If the ASCII value that is assigned to DLE occurs in the data array another DLE character is stuffed and stored in the array and transmitted along with starting and ending flags /* DE stuffing data */
 3. If the ASCII value of DLE occurs in the data array, the next bit is stored in to the array and transmitted without the flags.
-

4. Here whenever the program encounters characters like * the string DLE is added to the original string.

At Sender:

INPUT:

Enter Data r*gm

OUTPUT:

Stuffed data DLESTXrDLEDLEgmDLEETX

At receiver:

OUTPUT:

The message: r*gm

Coding

.....
.....
.....
.....

EXPERIMENT NO. 6

Aim - Study of Tool Command Language (Tcl)

Tcl (originally from "Tool Command Language", but conventionally spelled "Tcl" rather than "TCL"; pronounced as "tickle" or "tee-see-ell") is a scripting language created by John Ouster out. Originally "born out of frustration", according to the author, with programmers devising their own languages intended to be embedded into applications, Tcl gained acceptance on its own. It is commonly used for rapid prototyping, scripted applications, GUIs and testing. Tcl is used on embedded systems platforms, both in its full form and in several other small-footprint versions.

The combination of Tcl and the TkGUI toolkit is referred to as **Tcl/Tk**.

Features

Tcl's features include

- All operations are commands, including language structures. They are written in prefix notation.
- Commands are commonly variadic.
- Everything can be dynamically redefined and overridden.
- All data types can be manipulated as strings, including source code.
- Event-driven interface to sockets and files. Time-based and user-defined events are also possible.
- Variable visibility restricted to lexical (static) scope by default, but uplevel and upvar allowing process to interact with the enclosing functions' scopes.
- All commands defined by Tcl itself generate error messages on incorrect usage.
- Extensibility, via C, C++, Java, and Tcl.
- Interpreted language using byte code
- Full Unicode (3.1) support, first released 1999.
- Cross-platform: Windows API; UNIX, Linux, Macintosh, etc.
- Close integration with windowing (GUI) interface Tk.
- Multiple distribution mechanisms exist:
 - Full development version (e.g., Active State Tcl)
 - tclkit (kind of single-file runtime, only about 1 megabyte in size)
 - starpack (single-file executable of a script/program, derived from the tclkit technology)
 - FreewrapTCLSH turns TCL scripts into single-file binary executable programs.
 - BSD licenses, freely distributable source.

Tcl did not originally have object oriented (OO) syntax (8.6 provides an OO system in Tcl core), so OO functionality was provided by extension packages, such as incr Tcl and XOTcl. Even purely scripted OO packages exist, such as Snit and STOOOP (simple Tcl-only object-oriented programming).

Safe-Tcl is a subset of TCL that has restricted features. File system access is limited and arbitrary system commands are prevented from execution. It uses a dual interpreter model with the "untrusted interpreter" running code in an untrusted script. It was designed by Nathaniel Bornstein and Marshall Rose to include active messages in e-mail. Safe-Tcl can be included in e-mail when the *application/safe-Tcl* and *multipart/enabled-mail* are supported. The functionality of Safe-Tcl has since been incorporated as part of the standard Tcl/Tk releases.

Syntax and fundamental semantics

A Tcl script consists of several command invocations. A command invocation is a list of words separated by whitespace and terminated by a newline or semicolon.

```
word0 word1 word2 ... wordN
```

The first word is the name of a command, which is not built into the language, but which is in the library. The following words are arguments. So we have:

```
commandName argument1 argument2 ... argumentN
```

Practical example, using the *puts* command which outputs a string, adding a trailing newline, by default to the *stdout* channel:

```
puts"Hello, world!"
```

Variables and the results of other commands can be substituted inside strings too, such as in this example where we use *set* and *expr* to store a calculation result in a variable, and *puts* to print the result together with some explanatory text:

```
# Good style would put the expression (1+2+3+4+5, in this case) inside {curly braces}
```

```
set sum [expr1+2+3+4+5]
```

```
puts"The sum of the numbers 1..5 is $sum."
```

```
#expr function will be evaluated faster if curly braces are added on the equation.
```

```
set sum [expr{1+2+3+4+5}]
```

```
puts"The sum of the numbers 1..5 is $sum."
```

There is one basic construct (the command) and a set of simple substitution rules.

Formally, words are either written as-is, with double-quotes around them (allowing whitespace characters to be embedded), or with curly-brace characters around them, which suppresses all substitutions inside (except for backslash-newline elimination). In bare and double-quoted words, three types of substitution occur (once, in a single left-to-right scan through the word):

- **Command substitution** replaces the contents of balanced square brackets with the result of evaluating the script contained inside. For example, “[**expr 1+2+3**]” is replaced with the result of evaluating the contained expression (i.e. 6) since that's what the *expr* command does.
 - **Variable substitution** replaces a dollar-sign followed by the name of a variable with the contents of the variable. For example, “**\$foo**” is replaced with the contents of the variable called “foo”. The variable name may be surrounded in curly braces so as to delimit what is and isn't the variable name in otherwise ambiguous cases.
 - **Backslash substitution** replaces a backslash followed by a letter with another character. For example, “\n” is replaced with a newline.
-

From Tcl 8.5 onwards, any word may be prefixed by “{*}” to cause that word to be split apart into its constituent sub-words for the purposes of building the command invocation (similar to the “,@” sequence of Lisp's quasiquote feature).

As a consequence of these rules, the result of any command may be used as an argument to any other command. Also, there is no operator or command for string concatenation, as the language concatenates directly. Note that, unlike in Unix command shells, Tcl does not reparse any string unless explicitly directed to do so, which makes interactive use more cumbersome but scripted use more predictable (e.g. the presence of spaces in filenames does not cause difficulties).

The single equality sign (=) for example is not used at all, and the double equality sign (==) is the test for equality, and even then only in expression contexts such as the expr command or the first argument to if. (Both of those commands are just part of the standard library; they have no particularly special place in the library and can be replaced if so desired.)

The majority of Tcl commands, especially in the standard library, are variadic, and the proc (the constructor for scripted command procedures) allows one to define default values for unspecified arguments and a catch-all argument to allow the code to process arbitrary numbers of arguments.

Tcl is not statically typed: each variable may contain integers, floats, strings, lists, command names, dictionaries, or any other value; values are reinterpreted (subject to syntactic constraints) as other types on demand. However, values are immutable and operations that appear to change them actually just return a new value instead.

Coding

.....
.....
.....
.....



EXPERIMENT NO. 7

Study and Installation of Standard Network Simulator

In communication and computer network research, **network simulation** is a technique where a program models the behavior of a network either by calculating the interaction between the different network entities (hosts/routers, data links, packets, etc.) using mathematical formulas, or actually capturing and playing back observations from a production network. The behavior of the network and the various applications and services it supports can then be observed in a test lab; various attributes of the environment can also be modified in a controlled manner to assess how the network would behave under different conditions. When a simulation program is used in conjunction with live applications and services in order to observe end-to-end performance to the user desktop, this technique is also referred to as network emulation.

Network simulator

A **network simulator** is a piece of software or hardware that predicts the behavior of a network, without an actual network being present. A network simulator is a software program that imitates the working of a computer network. In simulators, the computer network is typically modeled with devices, traffic etc. and the performance is analyzed. Typically, users can then customize the simulator to fulfill their specific analysis needs. Simulators typically come with support for the most popular protocols in use today, such as WLAN, Wi-Max, UDP, and TCP.

Simulations

- Most of the commercial simulators are GUI driven, while some network simulators require input scripts or commands (network parameters). The network parameters describe the state of the network (node placement, existing links) and the events (data transmissions, link failures, etc.). An important output of simulations is the trace files. Trace files can document every event that occurred in the simulation and are used for analysis. Certain simulators have added functionality of capturing this type of data directly from a functioning production environment, at various times of the day, week, or month, in order to reflect average, worst-case, and best-case conditions. Network simulators can also provide other tools to facilitate visual analysis of trends and potential trouble spots.
 - Most network simulators use discrete event simulation, in which a list of pending "events" is stored, and those events are processed in order, with some events triggering future events—such as the event of the arrival of a packet at one node triggering the event of the arrival of that packet at a downstream node.
 - Some network simulation problems, notably those relying on queueing theory, are well suited to Markov chain simulations, in which no list of future events is maintained and the simulation consists of transiting between different system "states" in a memory less fashion. Markov chain simulation is typically faster but less accurate and flexible than detailed discrete event simulation. Some simulations are cyclic based simulations and these are faster as compared to event based simulations.
 - Simulation of networks can be a difficult task. For example, if congestion is high, then estimation of the average occupancy is challenging because of high variance. To estimate the likelihood of a buffer overflow in a network, the time required for an accurate answer can be extremely large. Specialized
-

techniques such as "control variants" and "importance sampling" have been developed to speed simulation.

Examples of network simulators

Examples of notable network simulation software are, ordered after how often they are mentioned in research papers:

1. ns2/ns3
2. OPNET
3. NetSim

1. NS (simulator)

Ns (from **network simulator**) is a name for series of discrete event network simulators, specifically **ns-1**, **ns-2** and **ns-3**. These simulators are used in the simulation of routing protocols, among others, and are heavily used in ad-hoc networking research, and support popular network protocols, offering simulation results for wired and wireless networks alike.

Design

Ns-3 is built using C++ and Python and scripting is available with either language. Split over 30 modules, features of ns-3 include:

- Callback-driven events
- Attribute system that manages default and per-object simulation values
- Helpers that allow using simpler API when configuring simulations

Workflow for ns

It includes four steps:

- Implement protocol models
- Setup simulation scenario, i.e. create Tcl file describing type of scenario, e.g. number of nodes, kind of agent working on nodes etc.
- Run simulation, i.e. Run the Tcl file
- Analyze simulation results, i.e. by GNU Awk and gnuplot

Components

- Ns, the simulator itself has Nam, the network animator to visualize ns (or other) output.
- Pre-processing component for Traffic and topology generators.
- Post-processing for Simple trace analysis, often in Awk, Perl, or Tcl.

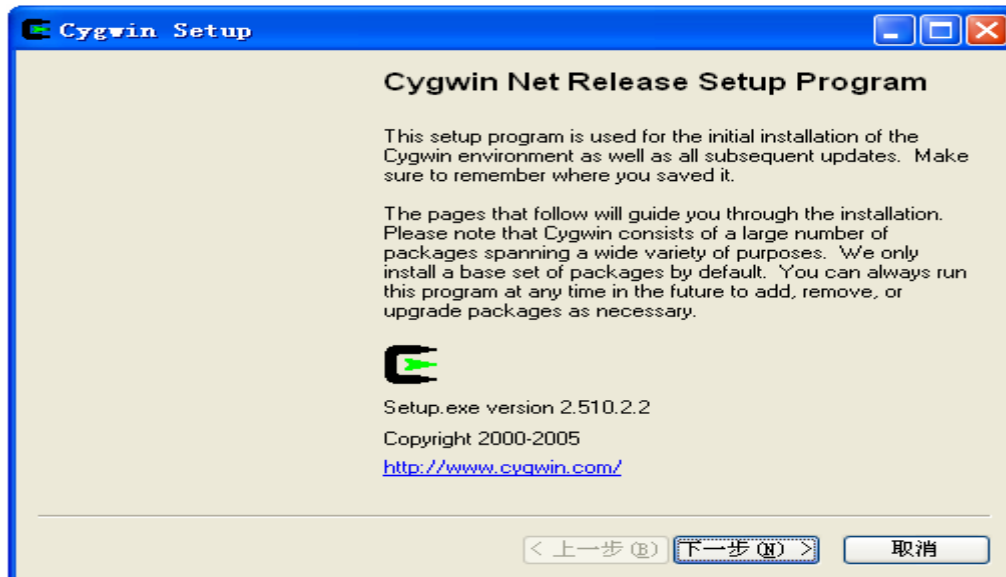
Installation of NS 2

1. Install CYGWIN

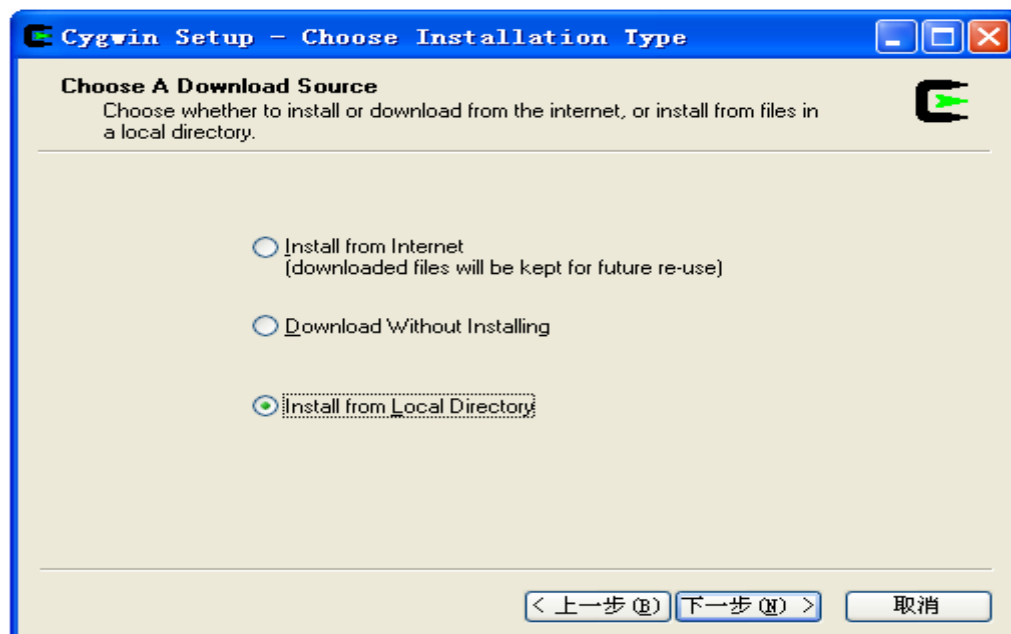
- Download zip file of ns2.29 (allinone) from:
-

<http://www.isi.edu/nsnam/dist/ns-allinone-2.29.2.tar.gz>

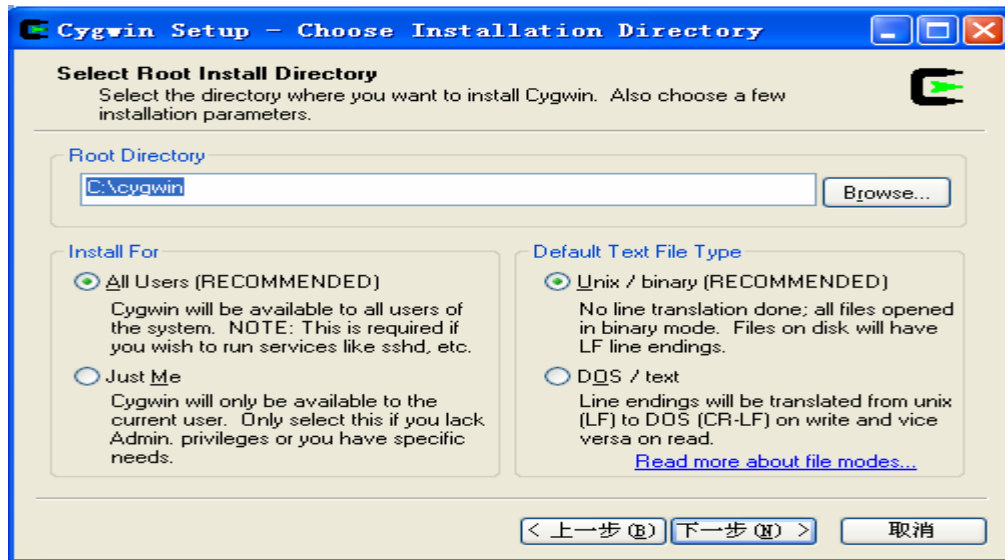
- Download cygwin setup.exe from www.cygwin.com
- Click on “cygwin.exe”.



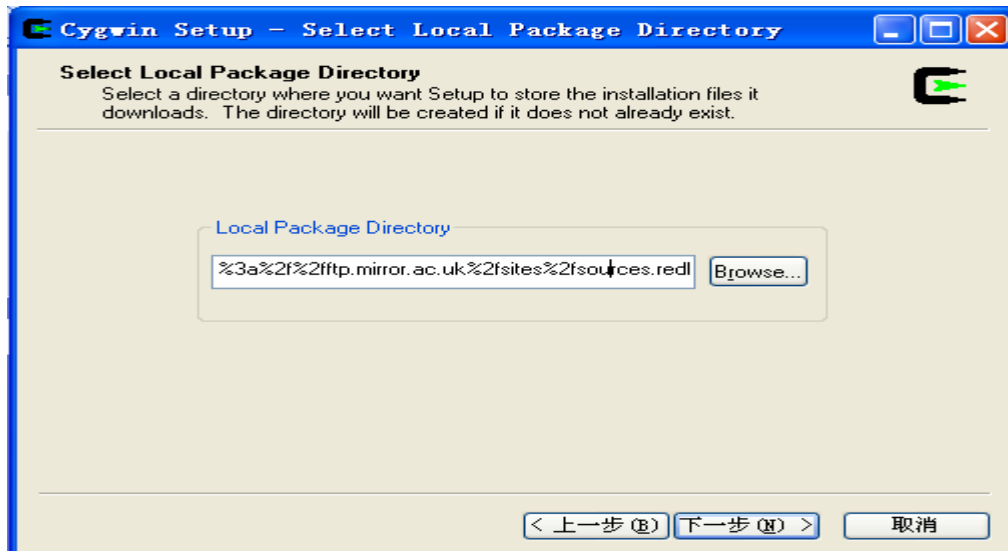
- Select “install local directory”



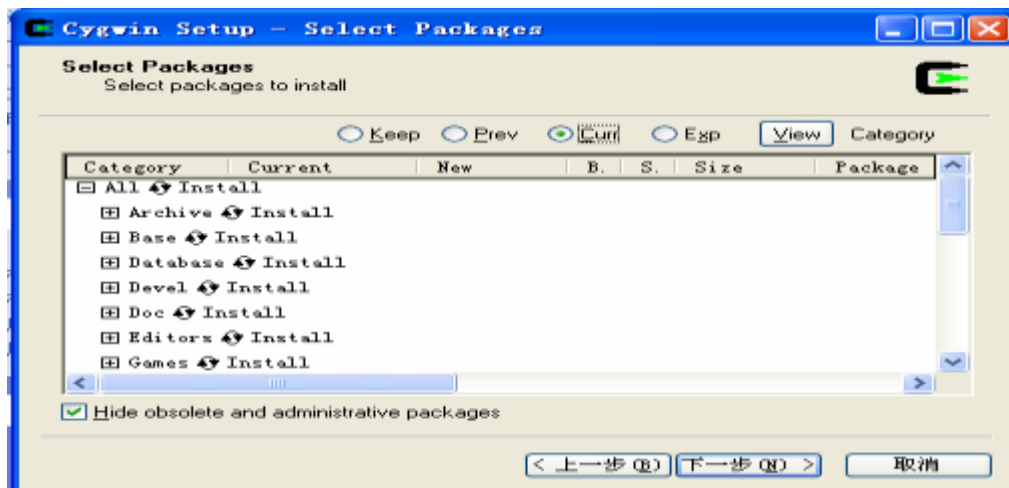
- Select browse for “cygwin” file (I selected as default).
-



- Install
“C:\NS2\NS-2.29 Install files\Cygwin
files\ftp%3a%2f%2ftp.mirror.ac.uk%2fsites%2fsources.redhat.com%2fftp%2fcygwin”

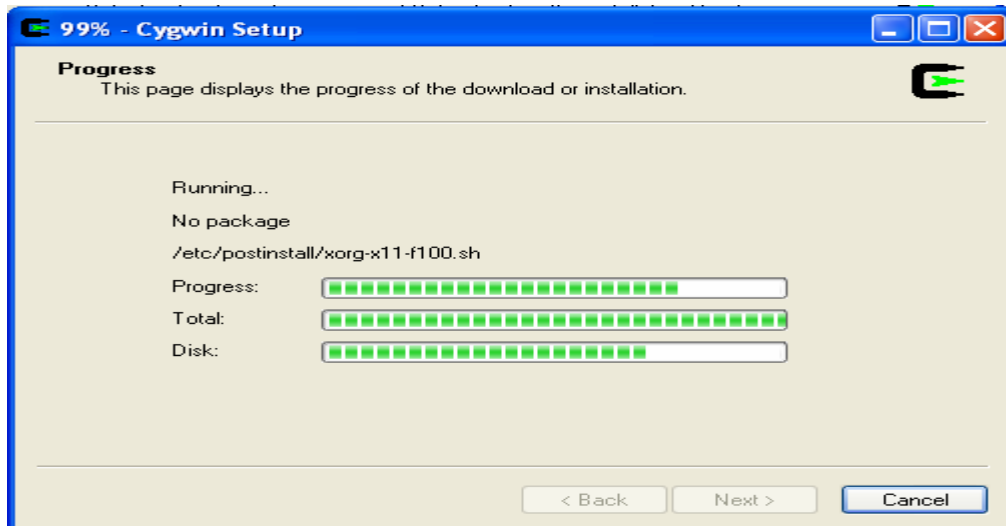


- Select to install all



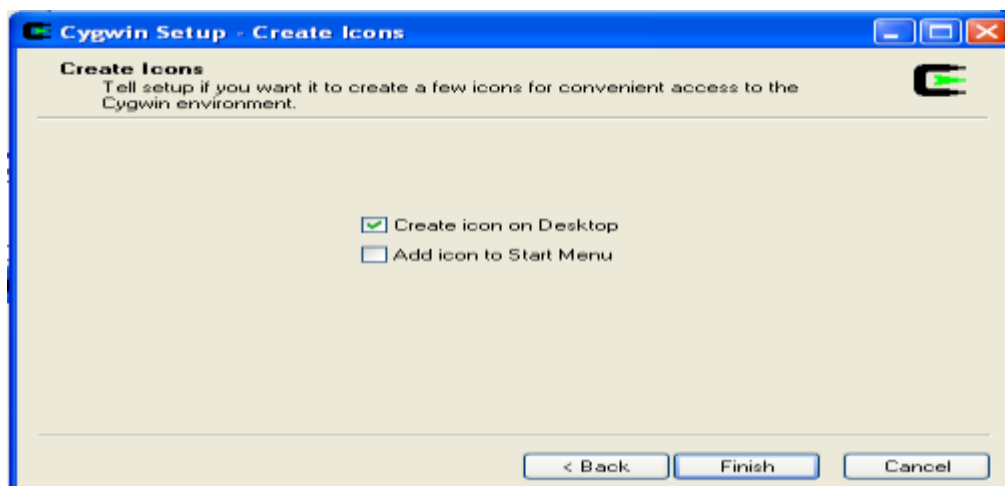
You can select “install”, “default”, “uninstall”, “install”, and “reinstall” behind the first line “all”. If we select “install”, then all sub items will be automatically selected. Otherwise you may lose some items.

- **Installing**



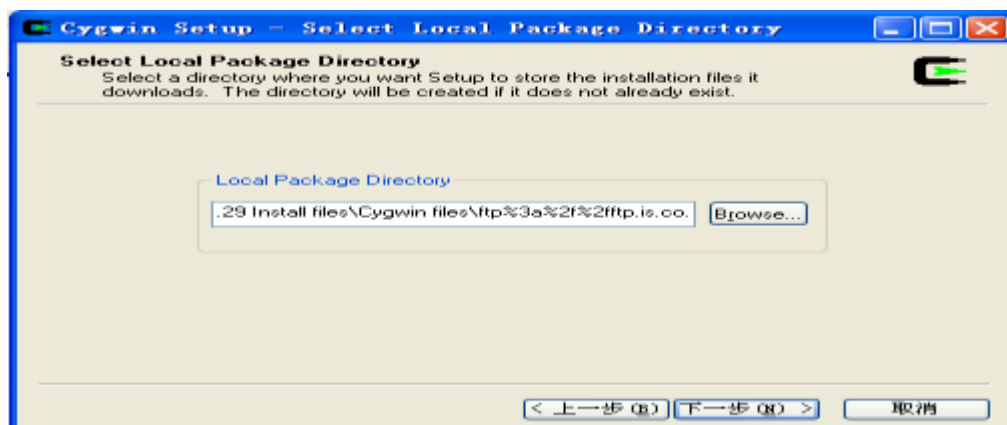
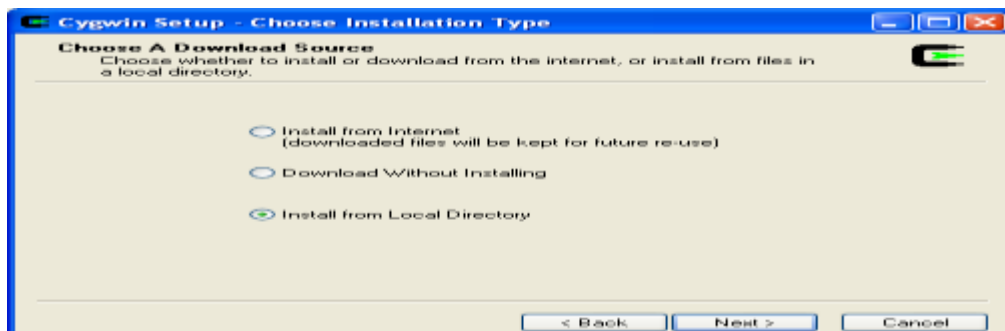
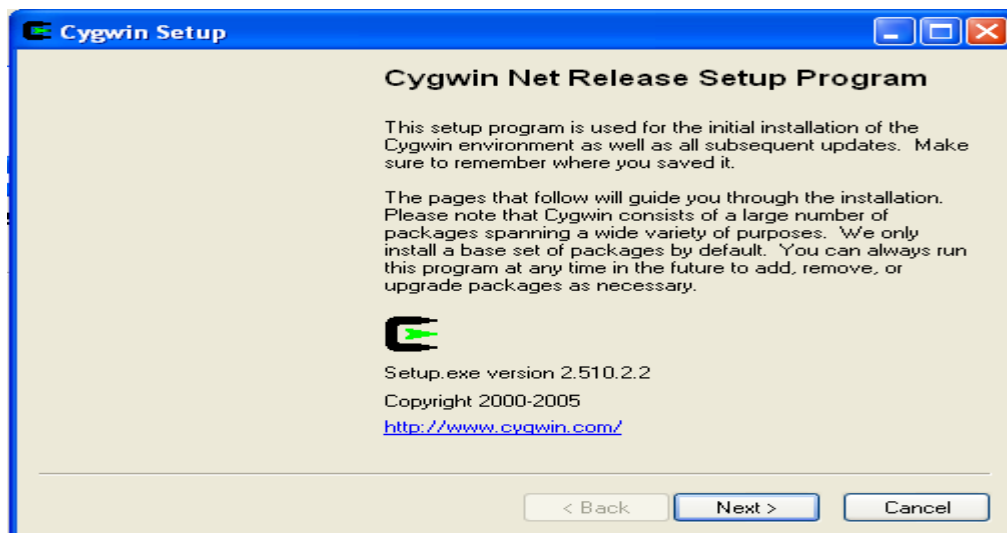
- **Finish in installing**

“ftp%3a%2f%2fftp.mirror.ac.uk%2fsites%2fsources.redhat.com%2fftp%2fcygwin”

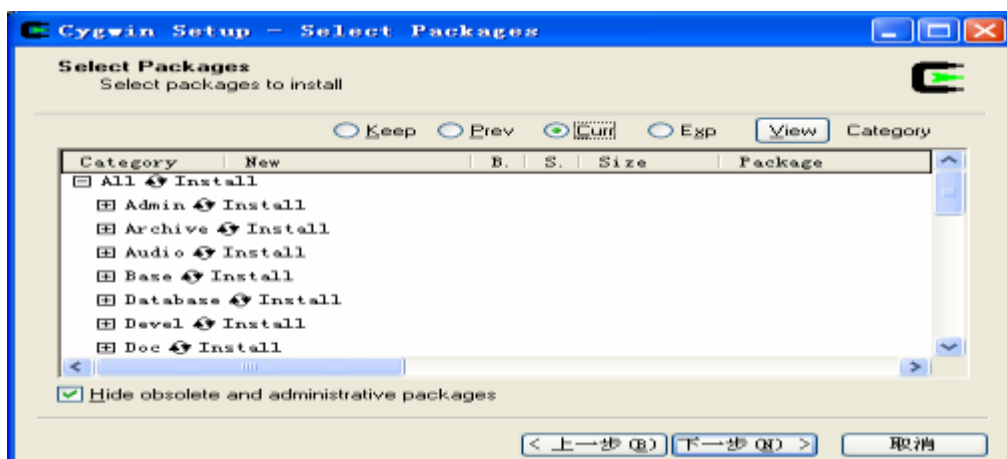


- **Install “Install**

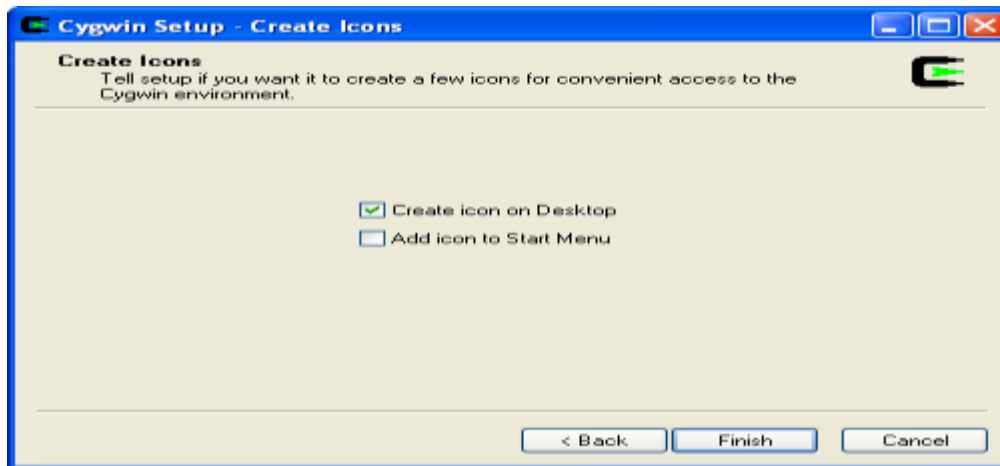
“C:\NS2\NS-2.29 Install files\Cygwin files \ ftp%3a%2f%2fftp.is.co.za%2fmirrors%2fcygwin”.



- Select to install all.

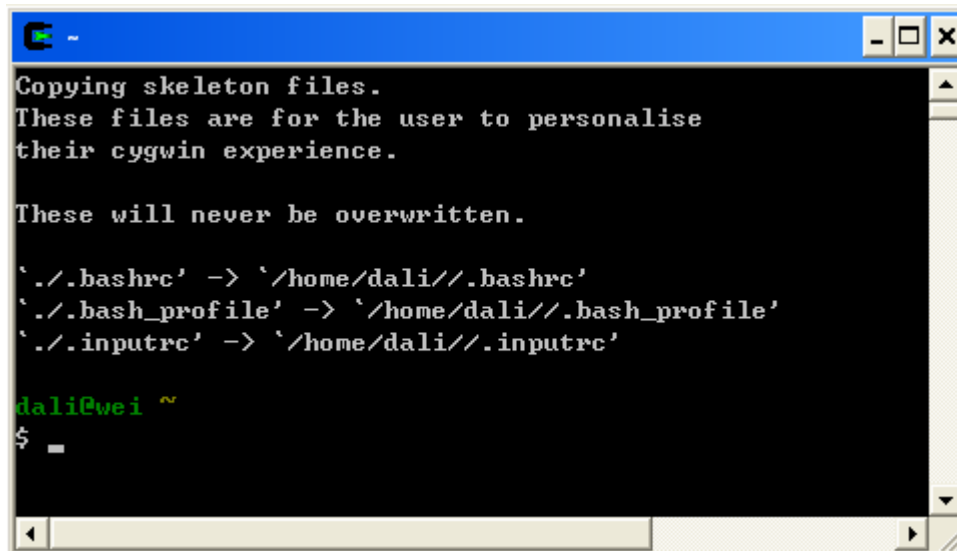


- Finish installing “ftp%3a%2f%2fftp.is.co.za%2fmirrors%2fcygwin”

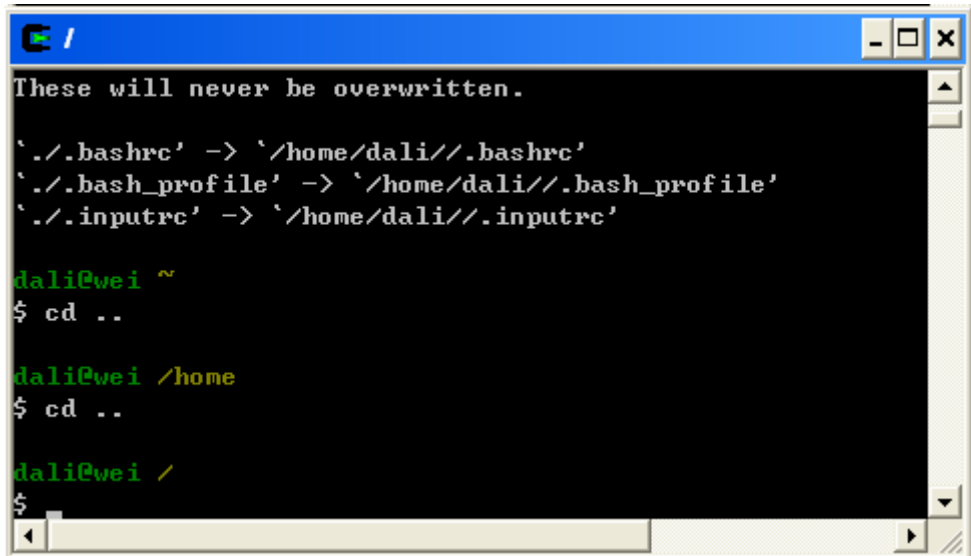


2. Install NS2

- a. Copy ns-allinone-2.29.2.tar to directory c:/cygwin/usr/local
- b. Unzip “ns-allinone-2.29.2.tar”
- c. Click on desktop icon “cygwin”



- d. Type “cd ..” to go to the upper folder (“cd” must be low case. And there is one space between “d” and “.”)



```

/
These will never be overwritten.

'./.bashrc' -> '/home/dali/./.bashrc'
'./.bash_profile' -> '/home/dali/./.bash_profile'
'./.inputrc' -> '/home/dali/./.inputrc'

dali@wei ~
$ cd ..

dali@wei /home
$ cd ..

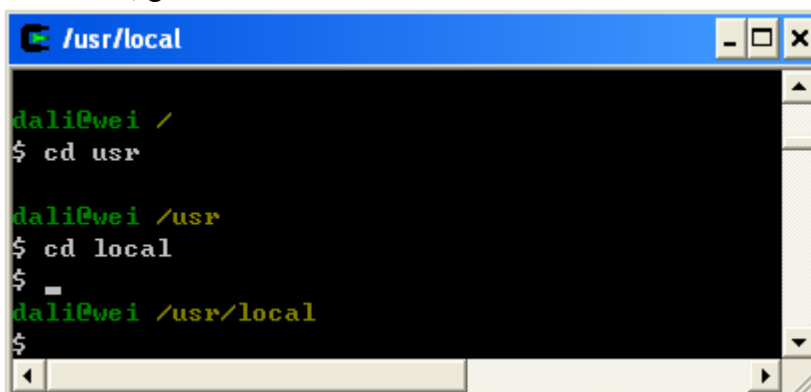
dali@wei /
$

```

e. Type “cd ..” again.

f. “cd usr”, go to folder “usr”

g. “cd local”, go to folder “local”



```

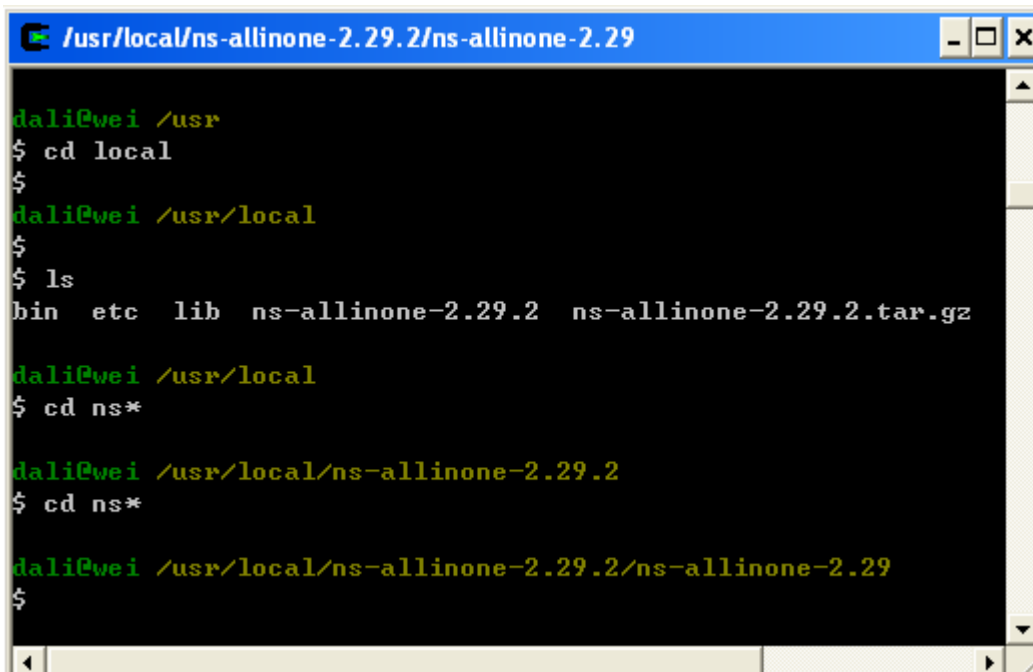
/usr/local

dali@wei /
$ cd usr

dali@wei /usr
$ cd local
$
dali@wei /usr/local
$

```

h. Find the “install.exe” file



```

/usr/local/ns-allinone-2.29.2/ns-allinone-2.29

dali@wei /usr
$ cd local
$
dali@wei /usr/local
$
$ ls
bin  etc  lib  ns-allinone-2.29.2  ns-allinone-2.29.2.tar.gz

dali@wei /usr/local
$ cd ns*

dali@wei /usr/local/ns-allinone-2.29.2
$ cd ns*

dali@wei /usr/local/ns-allinone-2.29.2/ns-allinone-2.29
$

```

```
/usr/local/ns-allinone-2.29.2/ns-allinone-2.29
dali@wei /usr/local/ns-allinone-2.29.2/ns-allinone-2.29
$ ls
$
README      install  otcl-1.11  tclcl-1.17  zlib-1.2.3
cweb        nam-1.11  sgb        tk8.4.11

dali@wei /usr/local/ns-allinone-2.29.2/ns-allinone-2.29
$
```

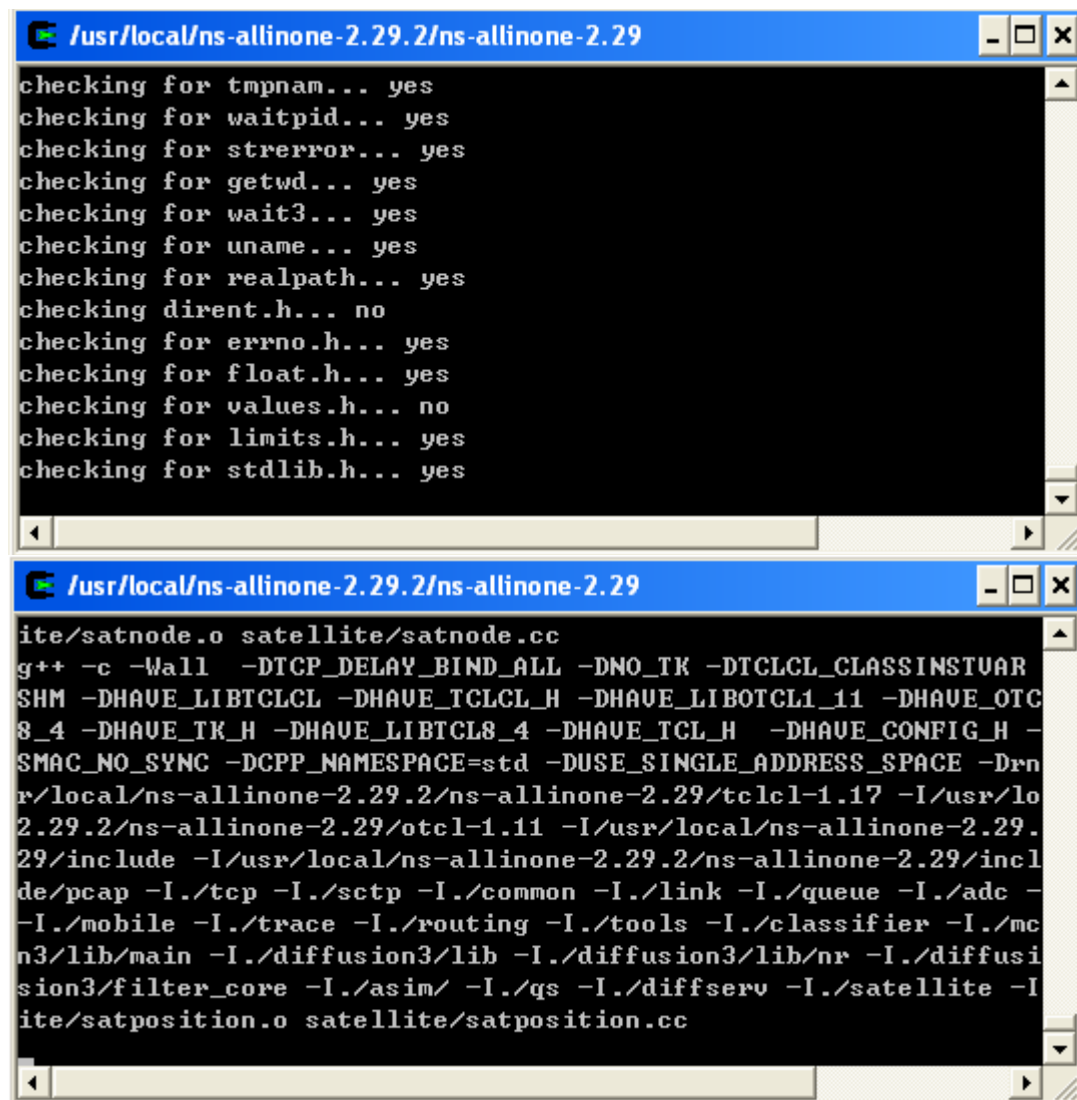
- i. Start to run the installation “./install” (Attention: After finish installing, some comments will come out. In my computer with celeron 2.66 CPU and 512 M Memory, this step took around 75 minutes.)

```
/usr/local/ns-allinone-2.29.2/ns-allinone-2.29
$ ls
INSTALL.WIN32  gt-itm    ns-2.29    tcl8.4.11  xgraph-12.1
README        install  otcl-1.11  tclcl-1.17  zlib-1.2.3
cweb          nam-1.11  sgb        tk8.4.11

dali@wei /usr/local/ns-allinone-2.29.2/ns-allinone-2.29
$ ./install
=====
* Testing for Cygwin environment
=====
Cygwin detected
Note: Cygwin install is still considered EXPERIMENTAL
Checking Cygwin version is >= 1.3.12... 1.5.19 (should be ok)

/usr/local/ns-allinone-2.29.2/ns-allinone-2.29
IBM USER@ibm-v5wfflqb2kx /usr/local/ns-allinone-2.29.2/ns-al
$ ./install
=====
* Testing for Cygwin environment
=====
Cygwin detected
Note: Cygwin install is still considered EXPERIMENTAL
```

- j. Installing



The image shows two terminal windows from the ns-allinone-2.29.2 directory. The top window displays the output of a configuration script, checking for various system headers and libraries. The bottom window shows the compilation command for the satellite components.

```
/usr/local/ns-allinone-2.29.2/ns-allinone-2.29
checking for tmpnam... yes
checking for waitpid... yes
checking for strerror... yes
checking for getwd... yes
checking for wait3... yes
checking for uname... yes
checking for realpath... yes
checking dirent.h... no
checking for errno.h... yes
checking for float.h... yes
checking for values.h... no
checking for limits.h... yes
checking for stdlib.h... yes

/usr/local/ns-allinone-2.29.2/ns-allinone-2.29
ite/satnode.o satellite/satnode.cc
g++ -c -Wall -DTCP_DELAY_BIND_ALL -DNO_TK -DTCLCL_CLASSINSTUAR
SHM -DHAVE_LIBTCLCL -DHAVE_TCLCL_H -DHAVE_LIBOTCL1_11 -DHAVE_OTC
8_4 -DHAVE_TK_H -DHAVE_LIBTCL8_4 -DHAVE_TCL_H -DHAVE_CONFIG_H -
SMAC_NO_SYNC -DCPP_NAMESPACE=std -DUSE_SINGLE_ADDRESS_SPACE -Dn
r/local/ns-allinone-2.29.2/ns-allinone-2.29/tclcl-1.17 -I/usr/lo
2.29.2/ns-allinone-2.29/otcl-1.11 -I/usr/local/ns-allinone-2.29.
29/include -I/usr/local/ns-allinone-2.29.2/ns-allinone-2.29/incl
de/pcap -I./tcp -I./sctp -I./common -I./link -I./queue -I./adc -
-I./mobile -I./trace -I./routing -I./tools -I./classifier -I./mc
n3/lib/main -I./diffusion3/lib -I./diffusion3/lib/nr -I./diffusi
sion3/filter_core -I./asim/ -I./qs -I./diffserv -I./satellite -I
ite/satposition.o satellite/satposition.cc
```

3. Configure system variables and library paths

- a. Installing is finished and the following window appears: **Make sure to copy all these contents.**

Please put `/usr/local/ns-allinone-2.29.2/ns-allinone-2.29/bin:/usr/local/ns-allinone-2.29.2/ns-allinone-2.29/tcl8.4.11/unix:/usr/local/ns-allinone-2.29.2/ns-allinone-2.29/tk8.4.11/unix` into your PATH environment; so that you'll be able to run `itm/tclsh/wish/xgraph`.

IMPORTANT NOTICES:

(1) You MUST put `/usr/local/ns-allinone-2.29.2/ns-allinone-2.29/otcl-1.11, /usr/local/ns-allinone-2.29.2/ns-allinone-2.29/lib,`

into your `LD_LIBRARY_PATH` environment variable.

If it complains about % libraries, add path to your % libraries into `LD_LIBRARY_PATH`.

If you are using `csh`, you can set it like:

`setenv LD_LIBRARY_PATH <paths>`

If you are using `sh`, you can set it like:

`export LD_LIBRARY_PATH=<paths>`

(2) You MUST put `/usr/local/ns-allinone-2.29.2/ns-allinone-2.29/tcl8.4.11/library` into your `TCL_LIBRARY` environmental

variable. Otherwise `ns/nam` will complain during startup.

(3) [OPTIONAL] To save disk space, you can now delete directories `tcl8.4.11` and `tk8.4.11`. They are now installed under `/usr/local/ns-allinone-2.29.2/ns-allinone-2.29/{bin,include,lib}`

After these steps, you can now run the ns validation suite with

`cd ns-2.29; ./validate`

For trouble shooting, please first read ns problems page

<http://www.isi.edu/nsnam/ns/ns-problems.html>. Also search the ns mailing list archive

for related posts.

`dali@wei /usr/local/ns-allinone-2.29.2/ns-allinone-2.29`

`$`

List of Books

SNo	TITLE	AUTHOR	PUBLISHER / EDITION	YEAR
1	Computer Networks	Tanenbaum A. S	Pearson Education.	2004
2	Data Communication & Networking	Behraj A Forouzan	McGraw-Hill	2006
3	Data Communications and Computer Networks	Prakash C. Gupta	PHI	2005

IMPORTANT VIVA QUESTION

1. Define Network?

A network is a set of devices connected by physical media links. A network is recursively a connection of two or more nodes by a physical link or two or more networks connected by one or more nodes.

2. What is a Link?

At the lowest level, a network can consist of two or more computers directly connected by some physical medium such as coaxial cable or optical fiber. Such a physical medium is called as Link.

3. What is a node?

A network can consist of two or more computers directly connected by some physical medium such as coaxial cable or optical fiber. Such a physical medium is called as Links and the computer it connects is called as Nodes.

4. What is a gateway or Router?

A node that is connected to two or more networks is commonly called as router or Gateway. It generally forwards message from one network to another.

5. What is point-point link?

If the physical links are limited to a pair of nodes it is said to be point-point link.

6. What is Multiple Access?

If the physical links are shared by more than two nodes, it is said to be Multiple Access.

7. Define Bandwidth and Latency?

Network performance is measured in Bandwidth (throughput) and Latency (Delay). Bandwidth of a network is given by the number of bits that can be transmitted over the network in a certain period of time. Latency corresponds to how long it takes a message to travel from one end of a network to the other. It is strictly measured in terms of time.

8. Define Routing?

The process of determining systematically how to forward messages toward the destination nodes based on its address is called routing.

9. What is a peer-peer process?

The processes on each machine that communicate at a given layer are called peer-peer process.

10. When a switch is said to be congested?

It is possible that a switch receives packets faster than the shared link can accommodate and stores in its memory, for an extended period of time, then the switch will eventually run out of buffer space, and some packets will have to be dropped and in this state is said to congested state.

11. Define the terms Unicasting, Multicasting and Broadcasting?

If the message is sent from a source to a single destination node, it is called Unicasting. If the message is sent to some subset of other nodes, it is called Multicasting. If the message is sent to all the nodes in the network it is called Broadcasting.

12. What is Multiplexing?

Multiplexing is the set of techniques that allows the simultaneous transmission of multiple signals across a single data link.

13. What is FDM?

FDM is an analog technique that can be applied when the bandwidth of a link is greater than the combined bandwidths of the signals to be transmitted.

14. What is WDM?

WDM is conceptually the same as FDM, except that the multiplexing and demultiplexing involve light signals transmitted through fiber optics channel.

15. What is TDM?

TDM is a digital process that can be applied when the data rate capacity of the transmission medium is greater than the data rate required by the sending and receiving devices.

16. What is Synchronous TDM?

In STDM, the multiplexer allocates exactly the same time slot to each device at all times, whether or not a device has anything to transmit.

17. List the layers of OSI

- a. Physical Layer
- b. Data Link Layer
- c. Network Layer
- d. Transport Layer
- e. Session Layer
- f. Presentation Layer
- g. Application Layer

18. Which layers are network support layers?

- a. Physical Layer
- b. Data link Layer and
- c. Network Layers

19. Which layers are user support layers?

- a. Session Layer
- b. Presentation Layer and
- c. Application Layer

20. Which layer links the network support layers and user support layers?

The Transport layer links the network support layers and user support layers.

21. What are the concerns of the Physical Layer?

Physical layer coordinates the functions required to transmit a bit stream over a physical medium.

- a. Physical characteristics of interfaces and media
- b. Representation of bits
- c. Data rate
- d. Synchronization of bits
- e. Line configuration
- f. Physical topology
- g. Transmission mode

22. What are the responsibilities of Data Link Layer?

The Data Link Layer transforms the physical layer, a raw transmission facility, to a reliable link and is responsible for node-to-node delivery.

- a. Framing
- b. Physical Addressing
- c. Flow Control
- d. Error Control
- e. Access Control

23. What are the responsibilities of Network Layer?

The Network Layer is responsible for the source-to-destination delivery of packet possibly across multiple networks (links).

- a. Logical Addressing
- b. Routing

24. What are the responsibilities of Transport Layer?

The Transport Layer is responsible for source-to-destination delivery of the entire message.

- a. Service-point Addressing
- b. Segmentation and reassembly
- c. Connection Control
- d. Flow Control
- e. Error Control

25. What are the responsibilities of Session Layer?

The Session layer is the network dialog Controller. It establishes, maintains and synchronizes the interaction between the communicating systems.

- a. Dialog control
- b. Synchronization

26. What are the responsibilities of Presentation Layer?

The Presentation layer is concerned with the syntax and semantics of the information exchanged between two systems.

- a. Translation
- b. Encryption
- c. Compression

27. What are the responsibilities of Application Layer?

The Application Layer enables the user, whether human or software, to access the network. It provides user interfaces and support for services such as e-mail, shared database management and other types of distributed information services.

- a. Network virtual Terminal
- b. File transfer, access and Management (FTAM)
- c. Mail services
- d. Directory Services

28. What are the two classes of hardware building blocks?

Nodes and Links.

29. What are the different link types used to build a computer network?

- a. Cables
- b. Leased Lines
- c. Last-Mile Links
- d. Wireless Links

30. What are the categories of Transmission media?

- a. Guided Media
 - i. Twisted - Pair cable
 - 1. Shielded TP
 - 2. Unshielded TP
 - ii. Coaxial Cable
 - iii. Fiber-optic cable
 - b. Unguided Media
-

- i. Terrestrial microwave
- ii. Satellite Communication

31. What are the types of errors?

a. Single-Bit error

In a single-bit error, only one bit in the data unit has changed

b. Burst Error

A Burst error means that two or more bits in the data have changed.

32. What is Error Detection? What are its methods?

Data can be corrupted during transmission. For reliable communication errors must be deducted and Corrected. Error Detection uses the concept of redundancy, which means adding extra bits for detecting errors at the destination. The common Error Detection methods are

- a. Vertical Redundancy Check (VRC)
- b. Longitudinal Redundancy Check (VRC)
- c. Cyclic Redundancy Check (VRC)
- d. Checksum

33. What is Redundancy?

The concept of including extra information in the transmission solely for the purpose of comparison. This technique is called redundancy.

34. What is VRC?

It is the most common and least expensive mechanism for Error Detection. In VRC, a parity bit is added to every data unit so that the total number of 1s becomes even for even parity. It can detect all single-bit errors. It can detect burst errors only if the total number of errors in each data unit is odd.

35. What is LRC?

In LRC, a block of bits is divided into rows and a redundant row of bits is added to the whole block. It can detect burst errors. If two bits in one data unit are damaged and bits in exactly the same positions in another data unit are also damaged, the LRC checker will not detect an error. In LRC a redundant data unit follows n data units.

36. What is CRC?

CRC, is the most powerful of the redundancy checking techniques, is based on binary division.

37. What is Checksum?

Checksum is used by the higher layer protocols (TCP/IP) for error detection

38. List the steps involved in creating the checksum.

- a. Divide the data into sections
- b. Add the sections together using 1's complement arithmetic
- c. Take the complement of the final sum, this is the checksum.

39. What are the Data link protocols?

Data link protocols are sets of specifications used to implement the data link layer. The categories of Data Link protocols are

- 1. Asynchronous Protocols
- 2. Synchronous Protocols
 - a. Character Oriented Protocols
 - b. Bit Oriented protocols

40. Compare Error Detection and Error Correction:

The correction of errors is more difficult than the detection. In error detection, checks only any error has occurred. In error correction, the exact number of bits that are corrupted and location in the message are known. The number of the errors and the size of the message are important factors.

41. What is Forward Error Correction?

Forward error correction is the process in which the receiver tries to guess the message by using redundant bits.

42. Define Retransmission?

Retransmission is a technique in which the receiver detects the occurrence of an error and asks the sender to resend the message. Resending is repeated until a message arrives that the receiver believes is error-free.

42. What are Data Words?

In block coding, we divide our message into blocks, each of k bits, called data words. The block coding process is one-to-one. The same data word is always encoded as the same codeword.

43. What are Code Words?

" r " redundant bits are added to each block to make the length $n = k + r$. The resulting n -bit blocks are called codewords. $2^n - 2^k$ codewords that are not used. These codewords are invalid or illegal.

44. What is a Linear Block Code?

A linear block code is a code in which the exclusive OR (addition modulo-2) of two valid codewords creates another valid codeword.

45. What are Cyclic Codes?

Cyclic codes are special linear block codes with one extra property. In a cyclic code, if a codeword is cyclically shifted (rotated), the result is another codeword.

46. Define Encoder?

A device or program that uses predefined algorithms to encode, or compress audio or video data for storage or transmission use. A circuit that is used to convert between digital video and analog video.

47. Define Decoder?

A device or program that translates encoded data into its original format (e.g. it decodes the data). The term is often used in reference to MPEG-2 video and sound data, which must be decoded before it is output.

48. What is framing?

Framing in the data link layer separates a message from one source to a destination, or from other messages to other destinations, by adding a sender address and a destination address. The destination address defines where the packet has to go and the sender address helps the recipient acknowledge the receipt.

49. What is Fixed Size Framing?

In fixed-size framing, there is no need for defining the boundaries of the frames. The size itself can be used as a delimiter.

50. Define Character Stuffing?

In byte stuffing (or character stuffing), a special byte is added to the data section of the frame when there is a character with the same pattern as the flag. The data section is stuffed with an extra byte. This byte is usually called the escape character (ESC), which has a predefined bit pattern. Whenever the receiver encounters the ESC character, it removes it from the data section and treats the next character as data, not a delimiting flag.

51. What is Bit Stuffing?

Bit stuffing is the process of adding one extra 0 whenever five consecutive 1s follow a 0 in the data, so that the receiver does not mistake the pattern 0111110 for a flag.

52. What is Flow Control?

Flow control refers to a set of procedures used to restrict the amount of data that the sender can send before waiting for acknowledgment.

53. What is Error Control?

Error control is both error detection and error correction. It allows the receiver to inform the sender of any frames lost or damaged in transmission and coordinates the retransmission of those frames by the sender. In the data link layer, the term error control refers primarily to methods of error detection and retransmission.

54. What Automatic Repeat Request (ARQ)?

Error control is both error detection and error correction. It allows the receiver to inform the sender of any frames lost or damaged in transmission and coordinates the retransmission of those frames by the sender. In the data link layer, the term error control refers primarily to methods of error detection and retransmission. Error control in the data link layer is often implemented simply: Any time an error is detected in an exchange, specified frames are retransmitted. This process is called automatic repeat request (ARQ).

55. What is Stop-and-Wait Protocol?

In Stop and wait protocol, sender sends one frame, waits until it receives confirmation from the receiver (okay to go ahead), and then sends the next frame.

56. What is Stop-and-Wait Automatic Repeat Request?

Error correction in Stop-and-Wait ARQ is done by keeping a copy of the sent frame and retransmitting of the frame when the timer expires.

57. What is usage of Sequence Number in Reliable Transmission?

The protocol specifies that frames need to be numbered. This is done by using sequence numbers. A field is added to the data frame to hold the sequence number of that frame. Since we want to minimize the frame size, the smallest range that provides unambiguous communication. The sequence numbers can wrap around.

58. What is Sliding Window?

The sliding window is an abstract concept that defines the range of sequence numbers that is the concern of the sender and receiver. In other words, the sender and receiver need to deal with only part of the possible sequence numbers.

59. What is Piggy Backing?

A technique called piggybacking is used to improve the efficiency of the bidirectional protocols. When a frame is carrying data from A to B, it can also carry control information about arrived (or lost) frames from B; when a frame is carrying data from B to A, it can also carry control information about the arrived (or lost) frames from A.

60. What are the two types of transmission technology available?

- (i) Broadcast and
- (ii) point-to-point

61. What is subnet?

A generic term for section of a large networks usually separated by a bridge or router.

62. Difference between the communication and transmission.

Transmission is a physical movement of information and concern issues like bit polarity, synchronization, clock etc.

Communication means the meaning full exchange of information between two communication media.

63. What are the possible ways of data exchange?

- (i) Simplex
- (ii) Half-duplex
- (iii) Full-duplex.

64. What is SAP?

Series of interface points that allow other computers to communicate with the other layers of network protocol stack.

65. What is Brouter?

Hybrid devices that combine the features of both bridges and routers.

66. What is cladding?

A layer of a glass surrounding the center fiber of glass inside a fiber-optic cable.

67. What is point-to-point protocol?

A communications protocol used to connect computers to remote networking services including Internet service providers.

68. How Gateway is different from Routers?

A gateway operates at the upper levels of the OSI model and translates information between two completely different network architectures or data formats.

69. What is attenuation?

The degeneration of a signal over distance on a network cable is called attenuation.

70. What is MAC address?

The address for a device as it is identified at the Media Access Control (MAC) layer in the network architecture. MAC address is usually stored in ROM on the network adapter card and is unique.

71. Difference between bit rate and baud rate.

Bit rate is the number of bits transmitted during one second whereas baud rate refers to the number of signal units per second that are required to represent those bits.

$$\text{baud rate} = (\text{bit rate} / N)$$

where N is no-of-bits represented by each signal shift.

72. What is Bandwidth?

Every line has an upper limit and a lower limit on the frequency of signals it can carry. This limited range is called the bandwidth.

73. What are the types of Transmission media?

Signals are usually transmitted over some transmission media that are broadly classified in to two categories.

a.) **Guided Media:** These are those that provide a conduit from one device to another that include twisted-pair, coaxial cable and fiber-optic cable. A signal traveling along any of these media is directed and is contained by the physical limits of the medium. Twisted-pair and coaxial cable use metallic that accept and transport signals in the form of electrical current. Optical fiber is a glass or plastic cable that accepts and transports signals in the form of light.

b.) **Unguided Media:** This is the wireless media that transport electromagnetic waves without using a physical conductor. Signals are broadcast either through air. This is done through radio communication, satellite communication and cellular telephony.

74. What is Project 802?

It is a project started by IEEE to set standards to enable intercommunication between equipment from a variety of manufacturers. It is a way for specifying functions of the physical layer, the data link layer and to some extent the network layer to allow for interconnectivity of major LAN protocols.

It consists of the following:

1. 802.1 is an internetworking standard for compatibility of different LANs and MANs across protocols.
2. 802.2 Logical link control (LLC) is the upper sublayer of the data link layer which is non-architecture-specific, that is remains the same for all IEEE-defined LANs.
3. Media access control (MAC) is the lower sublayer of the data link layer that contains some distinct modules each carrying proprietary information specific to the LAN product being used.

The modules are Ethernet LAN (802.3), Token ring LAN (802.4), Token bus LAN (802.5).

802.6 is distributed queue dual bus (DQDB) designed to be used in MANs.

75. What is Protocol Data Unit?

The data unit in the LLC level is called the protocol data unit (PDU). The PDU contains of four fields a destination service access point (DSAP), a source service access point (SSAP), a control field and an

information field. DSAP, SSAP are addresses used by the LLC to identify the protocol stacks on the receiving and sending machines that are generating and using the data. The control field specifies whether the PDU frame is a information frame (I - frame) or a supervisory frame (S - frame) or a unnumbered frame (U - frame).

76. What is the different type of networking / internetworking devices?

1. **Repeater:** Also called a regenerator, it is an electronic device that operates only at physical layer. It receives the signal in the network before it becomes weak, regenerates the original bit pattern and puts the refreshed copy back in to the link.
2. **Bridges:** These operate both in the physical and data link layers of LANs of same type. They divide a larger network in to smaller segments. They contain logic that allow them to keep the traffic for each segment separate and thus are repeaters that relay a frame only the side of the segment containing the intended recipient and control congestion.
3. **Routers:** They relay packets among multiple interconnected networks (i.e. LANs of different type). They operate in the physical, data link and network layers. They contain software that enable them to determine which of the several possible paths is the best for a particular transmission.
4. **Gateways:** They relay packets among networks that have different protocols (e.g. between a LAN and a WAN). They accept a packet formatted for one protocol and convert it to a packet formatted for another protocol before forwarding it. They operate in all seven layers of the OSI model.

77. What is ICMP?

ICMP is Internet Control Message Protocol, a network layer protocol of the TCP/IP suite used by hosts and gateways to send notification of datagram problems back to the sender. It uses the echo test / reply to test whether a destination is reachable and responding. It also handles both control and error messages.

78. What are the data units at different layers of the TCP / IP protocol suite?

The data unit created at the application layer is called a message, at the transport layer the data unit created is called either a segment or an user datagram, at the network layer the data unit created is called the datagram, at the data link layer the datagram is encapsulated in to a frame and finally transmitted as signals along the transmission media.

79. What is difference between ARP and RARP?

The address resolution protocol (ARP) is used to associate the 32 bit IP address with the 48 bit physical address, used by a host or a router to find the physical address of another host on its network by sending a ARP query packet that includes the IP address of the receiver.

The reverse address resolution protocol (RARP) allows a host to discover its Internet address when it knows only its physical address.

80. What is the minimum and maximum length of the header in the TCP segment and IP datagram?

The header should have a minimum length of 20 bytes and can have a maximum length of 60 bytes.

81. What is the range of addresses in the classes of internet addresses?

Class	A	-	0.0.0.0	-	127.255.255.255
Class	B	-	128.0.0.0	-	191.255.255.255
Class	C	-	192.0.0.0	-	223.255.255.255
Class	D	-	224.0.0.0	-	239.255.255.255
Class E - 240.0.0.0 - 247.255.255.255					

82. What is the difference between TFTP and FTP application layer protocols?

The Trivial File Transfer Protocol (TFTP) allows a local host to obtain files from a remote host but does not provide reliability or security. It uses the fundamental packet delivery services offered by UDP.

The File Transfer Protocol (FTP) is the standard mechanism provided by TCP / IP for copying a file from one host to another. It uses the services offer by TCP and so is reliable and secure. It establishes two connections (virtual circuits) between the hosts, one for data transfer and another for control information.

104. What are major types of networks and explain?

1. **Server-based network:** provide centralized control of network resources and rely on server computers to provide security and network administration
2. **Peer-to-peer network:** computers can act as both servers sharing resources and as clients using the resources.

83. What are the important topologies for networks?

1. **BUS topology:** In this each computer is directly connected to primary network cable in a single line. Advantages: Inexpensive, easy to install, simple to understand, easy to extend.
2. **STAR topology:** In this all computers are connected using a central hub. Advantages: Can be inexpensive, easy to install and reconfigure and easy to trouble shoot physical problems.
3. **RING topology:** In this all computers are connected in loop. Advantages: All computers have equal access to network media, installation can be simple, and signal does not degrade as much as in other topologies because each computer regenerates it.

84. What is mesh network?

A network in which there are multiple network links between computers to provide multiple paths for data to travel.

85. What is difference between baseband and broadband transmission?

In a baseband transmission, the entire bandwidth of the cable is consumed by a single signal. In broadband transmission, signals are sent on multiple frequencies, allowing multiple signals to be sent simultaneously.

86. Explain 5-4-3 rule?

In a Ethernet network, between any two points on the network ,there can be no more than five network segments or four repeaters, and of those five segments only three of segments can be populated.

87. What MAU?

In token Ring, hub is called Multistation Access Unit (MAU).

88. What is the difference between routable and non- routable protocols?

Routable protocols can work with a router and can be used to build large networks. Non-Routable protocols are designed to work on small, local networks and cannot be used with a router.

89. Why should you care about the OSI Reference Model?

It provides a framework for discussing network operations and design.

90. What is logical link control?

One of two sublayers of the data link layer of OSI reference model, as defined by the IEEE 802 standard. This sublayer is responsible for maintaining the link between computers when they are sending data across the physical network connection.

91. What is virtual channel?

Virtual channel is normally a connection from one source to one destination, although multicast connections are also permitted. The other name for virtual channel is virtual circuit.

92. What is virtual path?

Along any transmission path from a given source to a given destination, a group of virtual circuits can be grouped together into what is called path.

93. What is packet filter?

Packet filter is a standard router equipped with some extra functionality. The extra functionality allows every incoming or outgoing packet to be inspected. Packets meeting some criterion are forwarded normally. Those that fail the test are dropped.

94. What is multicast routing?

Sending a message to a group is called multicasting, and its routing algorithm is called multicast routing.

95. Expand IDEA.

IDEA stands for International Data Encryption Algorithm.

96. What is IGP (Interior Gateway Protocol)?

It is any routing protocol used within an autonomous system.

97. What is EGP (Exterior Gateway Protocol)?

It is the protocol the routers in neighboring autonomous systems use to identify the set of networks that can be reached within or via each autonomous system.

98. What is autonomous system?

It is a collection of routers under the control of a single administrative authority and that uses a common Interior Gateway Protocol.

99. What is BGP (Border Gateway Protocol)?

It is a protocol used to advertise the set of networks that can be reached within an autonomous system. BGP enables this information to be shared with the autonomous system. This is newer than EGP (Exterior Gateway Protocol).

100. What is Gateway-to-Gateway protocol?

It is a protocol formerly used to exchange routing information between Internet core routers.

101. What is NVT (Network Virtual Terminal)?

It is a set of rules defining a very simple virtual terminal interaction. The NVT is used in the start of a Telnet session.
