

Computer Networks

Assignment

Solution

Q1. Find Network address, broadcast address, subnet mask and usable IP range for 182.168.5.54/22.

Solution:

Expressing 182.168.5.54 in binary gives:

10110110.10101000.00000101.00110110

Finding network address:

The network address is obtained by taking the leftmost 22 bits from the above host address as it is and making the rest all 0s. Network address in binary

10110110.10101000.00000100.00000000

Network address in decimal becomes 182.168.4.0/22

Finding broadcast address

The broadcast address is obtained by taking the network address and replacing the rightmost 10 (32 - 22) bits by 1s. Broadcast address in binary

10110110.10101000.00000111.11111111

Broadcast address in decimal becomes 182.168.7.255/22

Finding subnet mask

The subnet mask in binary contains 22 1s followed by 10 0s, making a 32 bit number

11111111.11111111.11111100.00000000

In decimal: 255.255.252.0

Finding useable IP range

The usable IP range excluding the network and broadcast address is

First: 10110110.10101000.00000100.00000001 = 182.168.4.1/22

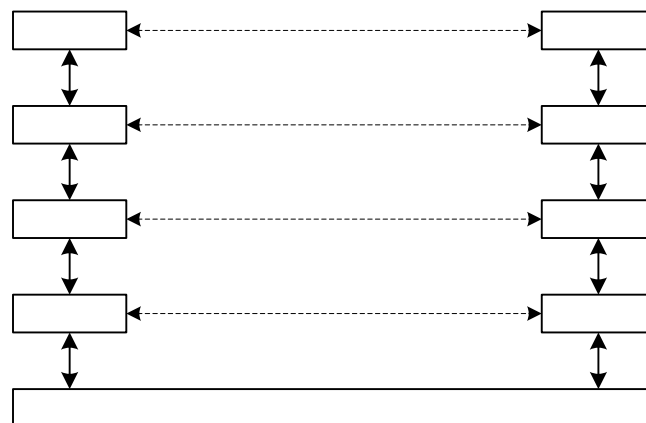
Last: 10110110.10101000.00000111.11111110 = 182.168.7.254/22

The number of hosts will be $2^{10} - 2 = 1022$.

Q2. Discuss about interface and services in layer architecture. Why layer architecture is important?

Answer:

In layered network architecture there are a set of layers and protocols. The layers are organized as a stack, with each one built upon the one below it. A layered architecture with four layers is shown in following figure.



Each layer defines a family of functions distinct from those of the other layers. By defining and localizing functionality in this fashion, the designers created an architecture that is both comprehensive and flexible.

Interfaces

There is a well defined interface between each pair of adjacent layers that make it possible for the data to pass down through the layers at the sending host and back up through the same set of layers at the receiving host. Each interface defines the information, operation and services a layer must provide

for the layer above it. Well-defined interface and layer functions provide greater modularity to a network. As long as a layer provides the expected services to the layers above it the implementation can be replaced by a completely different one.

Services

Within a host each layer calls upon the services of the layer just below it. For example, Layer 3 uses the service provided by layer 2 and provides its own services for layer 4. Between machines, layer x on one communicates with the corresponding layer x on another machine. This communication is governed by agreed rules of services called protocols. In reality no data are directly transferred from layer x on one machine to the same layer on another machine. Instead, each layer passed data and control information to the layer immediately below it, until the lowest layer is reached. Below layer 1 is the physical medium through which actual communication occur.

Importance of layered architecture

1. Layering reduces the design complexity.

It enables peer process abstraction which makes the unmanageable task of designing the complete network possible to be broken into several smaller manageable design problems, that is, the design of individual layers.

2. Provision of localized services strengthens modularity.

Each layer offers certain services to the higher layers and thus shields those layers from the details of how the offered services are actually implemented. Interfaces on all machines in a network need not be the same, provided that each machine correctly uses all the protocols.

3. They allow complete interoperability between incompatible systems

By defining the complete layered network model with all the interface details, the services and the protocols it is possible to ensure interoperability among various systems. There can be a seamless operation

without considering the operating system or the computer hardware. For example, the OSI model has been developed with this aim.

4. Hardware and software vendor independence.

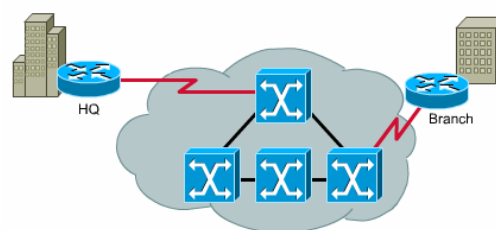
As long as correct layer functionality is ensured a network can be set up using products from different vendors and still the operation is guaranteed. For example, repeaters, hubs in the physical layer and web-browsers in the application layer.

Q3. Explain Frame Relay network and its working with PVC and SVC.

Answer:

Frame Relay is a virtual-circuit wide-area network. It is connection-oriented network with no error control and no flow control. Therefore, packets are always delivered in the same order they were sent. It does not have a retransmission policy if a frame is damaged which is simply dropped. Frame relay was designed in this way to provide fast transmission capability for more reliable media and for those protocols that have flow and error control at the higher layers. Like any other connection-oriented systems, Frame Relay involves three phases, namely, connection establishment phase, data transmission phase and connection termination phase. Frame Relay is used for interconnecting LANs at multiple company offices, and can also be used as a backbone network.

A Frame Relay network may be considered as a cloud that consists of switches, and customer nodes. The switch acts as DCE¹ and the customer equipment works as DTE². A virtual circuit is established between the DTE and corresponding DCE. A virtual circuit is identified by a DLCI (Data Link Connection Identifier) number. On a given physical channel, there cannot be two DLCIs which are identical.



© Cisco Systems, Inc. 2000

¹ Data Communications Equipment

² Data Terminal Equipment

Figure Basic Frame Relay configuration

Some of the important features of Frame Relay network are:

1. It operates at a higher speed than X.25 at 1.544 Mbit/s or higher.
2. It operates in just the physical and data link layer.
3. It has error detection at the data link layer only.
4. It allows bursty data.
5. Frame size is 9000 bytes.
6. It is less expensive than other traditional WANs.

Permanent Virtual Circuit (PVC) and Switched Virtual Circuit (SVC)

In PVC, a permanent connection is established between two distant hosts that communicate frequently, and the process involves recording corresponding table entry for all the switches by the administrator. An outgoing DLCI is given to the source and an incoming DLCI is given to the destination. One of the drawbacks of PVC is that it is costly because the connection needs to be kept connected all the time even when it is idle. Another drawback is that separate PVC is needed if a hosts needs to be connected to multiple hosts.

In a SVC, a temporary connection is established between the two distant hosts whenever data transfer is required, that is dynamically and is soon disconnected when the job is done. Thus SVC overcomes the shortcomings of the PVC. In an SVC three steps are required: (1) establish a connection, (2) transfer data and (3) terminate the connection. Setting up a connection will involve adding an entry for the virtual circuit in the switches.

Q4. Differentiate between random and slotted ALOHA with their efficiency.

Answer:

The difference between pure and slotted ALOHA may be stated in the following points.

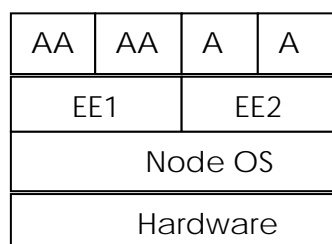
Pure ALOHA	Slotted ALOHA
(1) Time is treated as continuous and frames can originate at any time.	(1) Time is divided into discrete slots into which each frame must fit.
(2) A station sends a frame whenever it has a frame to send.	(2) A station waits for the beginning of the next time slot if it wants to send a frame.
(3) It does not require global synchronization.	(3) It requires global time synchronization.
(4) The vulnerable time in which there is a possibility of collision is twice the frame time.	(4) The vulnerable time for slotted ALOHA is halved and is equal to a single frame time.
(5) Throughput, $S = G \cdot \exp(-2G)$	(5) Throughput, $S = G \cdot \exp(-G)$
where G = average number of frames generated by the system during one frame transmission time	
(6) Maximum throughput, $S_{\max} = 0.184$ at $G = 0.5$. If one frame is generated during two frame transmission time then 18.4% of these frames will reach their destination successfully.	(6) Maximum throughput, $S_{\max} = 0.368$ at $G = 1$. If one frame is generated during one frame transmission time then 36.8% of these frames will reach their destination successfully.

Q5. Explain active networking. Differentiate it with P2P and Client-Server networking.

Answer:

An active network is a network in which the nodes are programmed to perform custom operations on the messages that pass through the node. For example, a node could be programmed or customized to handle packets on an individual user basis or to handle multicast packets differently than other packets. Active network approaches are expected to be especially important in networks of mobile users. Smart packets will use a special self-describing language that allows new kinds of information to be carried within a packet and operated on by a node. The architecture to implement an active network is composed of an execution environment that can execute active packets and a node operating system capable of supporting one or more execution environments. It also consists of active hardware, capable of routing or switching as well as executing code within active packets. Network processors are one means of implementing active networking concepts. Active networks have also been implemented as overlay networks.

Active network are cool. It can be at least as secure as legacy network. Data and algorithm in active network are mutable and fluid. It has faster hardware, more fully utilized. It enables more flexible networks. It minimizes global agreement overhead. It enables on-to-fly experimentation . it enables faster development of new services.



Active Network Framework

- The EE (execution environment) is a sandbox execution environment for active packets.

- The AA (active application) is an application injected in the network via active packets that are executed on active nodes.
- The node OS (operating system) provides an interface for the EE to resources of the host active node.
- Primary focus is communication and not computation.
- Packet is unit of multiplexing.
- No assumptions about underlying forwarding technologies.

Active network differs from the traditional network architecture which seeks robustness and stability by attempting to remove complexity and the ability to change its fundamental operation from underlying network components.

P2P (Peer-to-Peer) Networking

P2P is a distributed network architecture which consists of devices known as peers that share their own resources (disk storage, processing power or network bandwidth) directly, without the need for central server. Peer-to-peer is popular for file sharing on the Internet. Peer-to-peer systems often implement an Application Layer overlay network on top of the native or physical network topology.

Client-Server Networking

A client-server network consists of a number of devices called clients who acquire services from the relatively powerful devices called servers. Client devices are typically PCs or mobile devices with network software applications installed. Server device typically stores files, databases and applications like Web sites. The client-server model can be used on the Internet as well as local area networks (LANs). Examples of client-server systems on the Internet include Web browsers and Web servers, FTP clients and servers, and DNS.

6. Discuss about the concept and components involved in socket Programming.

Answer:

A socket represents a single connection between exactly two pieces of software and so multiple sockets are required in a client-server or distributed systems. Sockets are bidirectional, so data can be sent and received at both ends of the connection. Sockets provide an interface for programming networks at the transport layer. Network communication using Sockets is similar to performing file I/O. A socket is an endpoint of a two-way communication link between two programs running on the network. The source and destination IP address, and the port numbers constitute a network socket. Socket-based communication is independent of a programming language used for implementing it, thus C or C++ or Java can be used for socket programming. Programmers can access sockets using code libraries packaged with the operating system. There are several libraries that implement standard application programming interfaces (APIs). For example, the Berkeley Socket Library for UNIX and Windows Sockets (Winsock) library for Microsoft Windows.

A server program runs on a specific computer and has a socket at a specific port. The server listens to the socket for a client to make a connection request. The server then accepts the connection. Upon acceptance, the server gets a new socket at a different port so that it can continue to listen to other connection requests while serving the connected client. For example, Web browsers on the Internet know to use port 80 as the default for socket communications with Web servers.

Socket interfaces can be divided into three categories.

1. *Stream socket*: It implements connection-oriented semantics and requires that the two communicating parties first establish a socket connection, after which any data passed through that connection will be guaranteed to arrive in the same order in which it was sent. E.g. TCP (Transmission Control Protocol)
2. *Datagram sockets*: It is connection-less in which the sender simply sends datagram as needed and waits for the receiver to respond. Messages can be lost in transmission or received out of order. E.g. UDP (User Datagram Protocol)
3. *Raw socket*: It bypasses the library's built-in support for standard protocols and is used for custom low-level protocol development. E.g. IP (Internet Protocol)