Routing protocol

1. INTRODUCTION 1. 1 What is Computer Network? The group of computers and devices linked bycommunicationchannels allowing users to share information, data, software and hardware with further users is meant to be computer network. Network protocols bound hardware as well as software components of network. Two or more computers are said to be in a network if and only if they are connected mutually and are able to commune. Computers are connected to a network by the use of all the ports i. e. , parallel ports, modem ports, Ethernet ports, serial ports, USB ports , fire wire ports and many more in one or more way.

But Ethernet port is the most broadly used ports for networking. Hosts, end stations or workstations are referred while talking about networks. Anything attached to the network including hubs, bridges, switches, routers, access points, firewalls, workstations, servers, mainframes, printers, scanners, copiers, fax machines and more are included under Host or end stations . Computers are connected in a network for sharing of software and hardware resources, information and data as well as smooth the progress of communication. 1. 2 TCP/IP Layered architecture

Fig: TCP/IP Layered architecture The following are the layers of the TCP/IP architecture: Application Layer: In the application layer Simple Mail Transfer Protocol (SMTP) and File Transfer Protocol (FTP) uses protocol for network communication. Application layer protocols are most frequently linked with client-server applications. Transport Layer: End-to-end message transfer capability, flow control, error control and fragmentation etc are provided by the transport layer. The transport layer ensures source to destination delivery of packets safely and reliably.

The service through which applications are connected together via the use of ports is provided by transport layer. Network Layer: Packets are logically transmitted over the entire network in the OSI's Network layer. Hosts addressing by assigning them an IP address and packet routing among multiple networks are handled in this layer. This layer is concerned with routing data; end to end message delivery etc. Interface Layer: The data exchange between the host and the network are monitored by the interface layer. The protocols for physical transmission of data is defined by Interface Layer . 1. 3 Autonomous System

IP networks and routers collection under the control of one entity representing a common routing policy is called an Autonomous System. Each AS have a unique AS number for use in routing. Each network is uniquely identified on the internet by ASN. IANA (Internet assigned Numbers authority) assign AS numbers and supply to Regional internet Registries (RIRs) in blocks. Autonomous System can be divided into three categories: Multihomed Autonomous System: Connections to more than one AS is maintained by a Multihomed AS. Stub autonomous System: Connection to only one other AS is Stub autonomous System.

Transit autonomous System: Connections through itself to separate networks are provided by Transit autonomous System. 1. 4 Routing The method of selecting paths in a network via which to send data is meant to be routing. The process of finding a pathway from a sender to a desired destination is also said to be routing. The telephone network, the internet and transport networks, etc perform routing. Network Layer of either TCP/IP layered model or the OSI (Open System interconnect) Reference model mainly carry out routing. The logically addressed packets are passed from their source to destination via intermediary nodes i. e. orwarding is directed by routing. Routing tasks are performed by routers. Routing and packet forwarding is performed by ordinary computers available with multiple network cards in a limited manner. Forwarding is directed by the routing process on the basis of routing tables where routing record to different network destinations are maintained. In order to have efficient routing, construction of routing table held in the routers' memory is most necessary thing. Only one network path are frequently used by routing algorithms at a time, but the use of multiple alternative paths is made possible by multi-path routing techniques.

Following are the types of routing delivery semantics: Unicast: A message is delivered to a single specified node by router. Fig: Unicasting Broadcast: A message is delivered to all nodes in the network by router. Fig: Broadcasting Multicast: A message is delivered to assembly of nodes that have expressed interest in getting the message by router. Fig: Multicasting Anycast: A message is delivered to any one out of a set of nodes, typically the one next to the source. Fig: anycasting 2. TYPES OF ROUTING Following are the types of Routing mechanisms. They are: Static Routing Dynamic Routing 2. Static Routing: The process by which routes can be manually entered into the routing table with the help of a configuration file which loads automatically as soon as router starts is called static routing. Network administrator, who configures the routes, can enter these routes as an option. Thus 'static' routes mean the routes that cannot be changed (except a person changes them) after their configuration. The simplest type of routing is static routing. In case of change of routing information often or configuration on a huge number of routing devices (router) it doesn’t work fine as it is a manual process.

The outages or down connections are not handled properly by static routing because manually configured route must be reconfigured physically in order to fix or renovate any lost connectivity. 2. 2 Dynamic Routing: Network destinations are discovered dynamically by means of software applications called Dynamic routing protocols. A routing table is created and managed by router in Dynamic Routing. Firstly, a router will 'learn' routes to the directly connected entire networks. It will then learn routes from other routers using the same routing protocol.

One or more best routes are selected from the list of routes for each and every network destination by router. 'Best route' information are distributed to other routers running the same routing protocol by Dynamic protocols, distributing the information on what networks it subsist and can be reached. This provide dynamic routing protocols the capability to get used to logical network topology changes, equipment failures or network outages 'on the fly'. 2. 3 Types of Dynamic Routing Distance-Vector Routing Paths are calculated using Bellman Ford Algorithm by a distance-vector routing protocol.

RIPv1 and 2 and IGRP (Interior Gateway Routing Protocol) are examples of distance-vector routing protocols. Earlier, distance vector protocols such as RIPv1 show classful behavior but newer distance vector protocols such as RIPv2 and Enhanced interior Gateway Routing Protocol (EIGRP) show signs of classless behavior. Distance-vector routing protocols • Easy and competent in small networks • Deprived convergence properties • Facilitate in the growth of more complex but more scalable link-state routing protocols for use in large networks. Periodic copies of a routing table are passed from router to router by distance vector routing algorithms. • Logical broadcast is the most commonly used addressing scheme. Periodic updates are sent by routers running a distance vector routing protocol even if there are no changes in the network. • Complete routing table is included under the periodic routing update in a pure distance vectorenvironment. • All known routes can be verified and changes can be made by getting a neighbor's complete routing table based on simplified information also called as " routing by rumor". Fig: Distance Vector Routing

Periodic routing updates are received from router A to router B in the figure. Distance vector metric (such as hop count) are added by Router B to each route learned from router A, rising the distance vector. Its own routing tables are passed to its neighbor, router C. This process occurs between directly connected neighbor routers in all directions. The chief purpose is to decide the top route to contain in the table when the routing table is updated by a routing protocol algorithm. Different routing metric is used to determine the best route by each distance vector routing protocol.

Metric value is generated for each path through network by the algorithm. Usually, the path is better if metric is smaller. Single characteristic of a path helps in calculation of metrics and combination of several path characteristics helps in calculation of more complex metrics. The most commonly used metrics used by distance vector routing protocols are: Hop Count: Packet's number of passages throughout the output port of one router Bandwidth: Link’s data capacity Delay: Time necessary to shift a packet from starting place to destination.

Load: work load on router or link. Reliability: each network link bit error rate Maximum Transmission Unit (MTU): the utmost message extent in octets satisfactory to all links on the path. Link-State Routing Packet-switched networks use link-state routing protocol for computer communications. OSPF and IS-IS are its examples. A topological database is built by the help of link-state routing that describes extra precise inter-network routes. Large networks use link state routing protocols and now used by most of the organization and ISP.

Router performs the link-state protocol in the network. A map of the connectivity of the network is constructed by every node in the form of graph showing node connection to other node is the basic concept of link-state routing. The best next hop is calculated by each node independently for every possible destination in the network. The routing table for the node is formed by the collection of best next hops. Fig: Link-State Routing To find out the shortest path from itself to every other node in the network an algorithm is run by each node independently over the map.

OSPF, EIGRP and Novell's NLSP (NetWare Link State Protocol) are the examples of link state routing protocol. IPX is only supported by Novell's NLSP. A partial map of the network is maintained by each router in this type of routing protocol. Link stateadvertisement(LSA) is flooded throughout the network when a network link changes state (up to down, or vice versa). The changes are noted and routes are re-computed by all the routers accordingly. Greater flexibility and sophistication are provided by Link State Routing protocols than the Distance Vector routing protocols.

Overall broadcast traffic is reduced and better decisions are made about routing by taking characteristics such as bandwidth, delay, reliability, and load into consideration, instead of taking their decisions only on hop count. 3. ROUTING ALGORITHMS 3. 1 Bellman-Ford Algorithm: • Also called as Label Correcting algorithm • Used for negative edge weight • Same as Dijkstra's algorithm • In order to maintain distance tables, this algorithm is used by router • Exchanging information with the neighboring nodes help to update information in the distance table • All nodes in the network is represented by the number of data in the table The directly attached neighbors are represented by the columns of table and all destinations in the network are represented by the row. • The number of hops, latency, the number of outgoing packets, etc. are measurements in this algorithm. 3. 2 Dijkstra’s Algorithm: • Edsger Dijkstra conceived Dijkstra's algorithm • Mostly used for routing • Is a graph search algorithm • The single-source shortest path problem for a graph is solved by this algorithm with non negative edge path costs • The shortest path tree is produced as a output • Helps in finding shortest route from one router to other A shortest-path pning tree having route to all possible destination is built by this algorithm for router • The router using the algorithm is the source of its shortest-path pning tree 4. ROUTING PROTOCOLS Routing protocol describe the way of communication between routers which helps in the selection of routes between any two nodes on a network. Usually, knowledge of immediate neighbors is known by each router. This information is shared by a routing protocol to have routers the knowledge of the network topology. Most commonly used Routing protocols are as follows: 4. RIP (Routing information Protocol) • dynamic inter-network routing protocol • used in private network • routes are automatically discovered • routing tables are built • a Distance-Vector routing protocol • uses Bellman-Ford algorithm • 15 hops are allowed with RIP • 180 sec is the hold down time • Full updates are transmitted every 30 sec by each RIP router • Works at network layer • Prevent routing loops • Hop limit • incorrect routing information are prevented from being propagated • easy configuration • no parameter required Two versions of RIP are as follows: RIPv1: • classful routing is used subnet information is not carried by periodic routing updates • no support for VLSM (variable length subnet masks) • Same network class have different sized subnet by the use of RIPv1 • No router authentication • Broadcast based and 15 is the maximum hop count A RIPv1 packet format is shown below: [pic]Fig: RIP packet format Command: determine whether the packet is a request or a response. A router send all or part of its routing table is asked by the request. Reply to a request or regular routing update means the response. Routing table entries are contained in responses. Version number: RIP version used is specified.

Potentially incompatible versions can be signaled by this field. Zero: RFC 1058 RIP doesn’t use this field; it was added to have backward compatibility provided to pre-standard varieties of RIP. Addressfamilyidentifier (AFI): The address family used is specified. Address-family identifier is contained in each entry to specify the category of address being particularized.
The AFI for IP is 2. Address: The IP address is particularized for the entry.

Metric: The number of inter-network hops traversed in the trip to the destination is indicated. 1 and 15 for an applicable route, or 16 for an unapproachable route. RIPv2: Developed in 1994 • Classless inter-Domain Routing (CIDR) is supported • Subnet information can be carried • Addition of MD5 authentication and Rudimentary plain text authentication for the security of routing updates. • Routing updates are multicast to 224. 0. 0. 9 • 15 is the maximum hop count A RIPv2 packet format is shown below: [pic] Fig: RIPv2 packet format Command: determine whether the packet is a request or a response. A router send all or part of its routing table is asked by the request. Reply to a request or regular routing update means the response. Routing table entries are contained in responses.

Version number: RIP version used is specified. Unused: Zero is the value set. Address-family identifier (AFI): The address family used is specified. Authentication information is contained in the remainder of the entry if the AFI for the initial entry is 0xFFFF in the message. At present, simple password is the only authentication type. Route tag: The methodology is provided for distinguishing between internal routes (learned by RIP) and external routes (learned from other protocols). IP address: IP address is particularized for the entry. Subnet mask: The subnet mask is contained for the entry.

No subnet mask has been particularized for the entry if this field is zero. Next hop: The IP address of the next hop is indicated to which packets for the entry should be forwarded. Metric: The number of inter-network hops traversed in the trip to the destination is indicated. 1 and 15 for an applicable route, or 16 for an unapproachable route. 4. 2 OSPF (Open

Shortest Path First) • A Link-State protocol • used for routing between routers belonging to a single autonomous system • link-statetechnologyis used • information about the direct connections and links is communicated between the routers Identical database is maintained by each OSPF router for the description of the autonomous System's topology • Calculation of a routing table by the construction of a shortest- path tree from this database. • Routes are quickly recalculated in the face of topological changes • equal-cost multi-path are supported • Authentication of all OSPF routing protocol exchanges • Designed for TCP/IP environment • routing updates authentication • IP multicast are utilized in sending/receiving the updates • routes IP packets based exclusively on the target IP address originate in the IP packet header Grouping of sets of networks • IP subnets are flexibly configured • Destination and mask is available to the route distributed by OSPF The following figure shows the packet format used by OSPF: [pic]Fig: OSPF packet format Version number: the OSPF version used is specified. Type: the OSPF packet type is identified as one of the following: Hello: neighbor relationships are established and maintained. Database description: the contents of the topological database are described. Link-state request: pieces of the topological database are requested from neighbor routers.

Link-state update: a link-state request packet is responded. Link-state acknowledgment: link-state update packets are acknowledged. Packet length: the packet length, the OSPF header is specified. Router ID: the source of the packet is identified. Area ID: The area of packet is identified. All OSPF packets are linked with a single area. Checksum: the complete packet contents are checked for any harm suffered in travel. Authentication type: the authentication type is contained. Authentication of all OSPF protocol exchanges. Configuration of the authentication type on per-area basis.

Authentication: authentication information is contained. Data: encapsulated upper-layer information is contained. 5. WORKING 5. 1 Distance Vector Routing: The following methods show the overall working of the Distance-Vector Routing: . There is no predefined route i. e. entire route for a particular destination is not known to any router. The port to send out a unicast packet is known by each router on the basis of destination address. Progressively the route is made and there is the formation of the route by the contribution of each router when it receives the packet.

The optimal tree is not predefined in DVRP actually. No routers have knowledge for making an optimal tree. Slowly and gradually the tree is made. The tree is formed as soon as a router receives a packet; it is forwarded by router through some of the ports, on the basis of source address. Other down-stream routers make the rest of the tree. The formation of the loops must be prevented by this protocol. Duplications are also prevented in order to make the entire network receive only one copy. In addition to this, the shortest path from source to the destination is the path travelled by a copy.

Inconsistencies occurring with Distance-Vector Routing: Incorrect routing entries are caused by slow inter-network convergence which may bring inconsistencies maintaining routing information. . The following example

describes how inconsistencies occur in Distance-Vector routing: The entire figure describes the inconsistencies occurring with Distance-Vector Routing. Defining a maximum to prevent count to infinity: . With this approach, the routing table update loop is permitted by routing protocol until the metric exceeds its maximum allowed value. Fig: Defining a maximum to prevent count to infinity 6 hops are defined as the maximum allowed value.
When the metric value exceeds 16 hops, we cannot reach network 10. 4. 0. 0 Routing Loops in Distance-Vector Routing: A routing loop is said to be occurred if two or more routers have false routing information representing that a applicable path to an unapproachable destination exists via other routers. Fig: Routing Loop Solutions to eliminate routing loops Split horizon: The information is not sent in the direction from where original information comes. The split horizon function is illustrated by the following figure

Fig: Split Horizon Route Poisoning: Routing loops are eliminated. The following figure provides an example of Route Poisoning: Fig: Route Poisoning In addition to split horizon, route poisoning and holddown timers, poison reverse, holddown timers and triggered updates are other methods to eliminate routing loops. 5. 2 Link-State Routing: The following methods show the overall working of Link-State Routing. Gathering of the neighbor information continuously. Router answering to this protocol are broadcasted the list of neighbor information, process known as flooding.

Soon, this information is distributed to all routers on the network. Flooding of the neighbor information in case of a (routing-significant) change in the network. The best path can be calculated to any host on any destination network as everything about the network is known by every router. 6. ADVANTAGES AND DISADVANTAGES Distance-Vector Routing Advantages of Distance-Vector Routing: • simple and flat network • No special hierarchical design is required. • Implementation of hub-and-spoke networks • No concern for worst-case convergence times in a network • less memory and processing power usage

Disadvantages of Distance-Vector Routing: • Incorrect routing entries create inconsistencies in maintaining the routing information • Rise of a condition count to infinity • Occurrence of a routing loop • Variable Length Subnet Masking (VLSM) or super netting is not supported • multi-vendor routing environment is not supported Link-State Routing Advantages of Link-State Routing: • Paths are chosen via network by the use of cost metrics • changes in the network topology are reported to all routers in the network quickly • fast convergence times • No occurrence of routing loops routing decisions are based on the most recent set of information • Link-State protocols use cost metrics to choose paths though the network. The cost metric reflects the capacity of the links on those paths. Disadvantages of Link-State Routing: • Topology database, an adjacency database, and a forwarding database is required. • a significant amount of memory is required in large or complex networks • significant amount of CPU power usage • need of a strict hierarchical network design to reduce significant amount of CPU power usage • network capability or performance is low to transport data . APPLICATION AREAS Distance-Vector Routing: • used in mobile, wireless and hoc networks (MANETs) • used for mobile ad hoc routing (Ad hoc On-Demand Distance Vector Routing) . Link-State

Routing: • used in larger, more complicated networks • Optimized Link State Routing Protocol (OLSR) designed for mobile, wireless and hoc networks 8. COMPARING DISTANCE-VECTOR AND LINK-STATE ROUTING STRATEGIES • Mostly, best path is determined by Distance Vector protocols, while bandwidth, delay, reliability and load are considered to make routing decision by Link-State protocols Distance Vector protocols are simple and efficient where as Link-State protocols are flexible and sophisticated • Routing information Protocol (RIP v1 and v2) and interior Gateway Routing Protocol (IGRP developed by Cisco) are Distance Vector protocols where as OSPF, EIGRP, Novell's NLSP (NetWare Link State Protocol) are Link-State protocols • Notion of a distance is not required in Distance Vector routing where as Link-State routing is based on minimizing some notion of distance • Uniform policies are not required at all routers in Distance Vector routing but uniform policy is required in Link-State routing Router have little knowledge about network topology in Distance Vector routing where as routing domain has excessive knowledge about topology information in Link-State routing 9. CONCLUSION Introduction, working, use, advantages and disadvantages of Distance-Vector and Link-State routing are explained in this project. Bellman ford and Dijkstra’s algorithm are also discussed. This project describes the popularity of Distance-Vector and Link-State routing because of their complex, sophisticated, flexible features in recent computer networking field..