2.1 Introduction:-

A computer network or data network is a telecommunications network that allows computers to exchange data. In computer networks, networked computing devices pass data to each other along data Connections. The connections (network links) between nodes are established using either cable media or wireless media. The best-known computer network is the internet.

Today, computer networks arc the core of modern communication. All modem aspects of the public switched telephone network (PSTN) are computer-controlled. Telephony increasingly runs over the Internet Protocol, although not necessarily the public Internet. The scope of communication has increased significantly in the past decade. This boom in communications would not have been possible without the progressively advancing computer network. Computer networks, and the technologies that make communication between networked computers possible, continue to drive computer hardware, software, and peripherals industries. The expansion of related industries is mirrored by growth in the numbers and types of people using networks, from the researcher to the home user.

Network computer devices that originate, route and terminate the data are called network nodes. Nodes can include hosts such as personal computers, phones, servers as well as networking hardware. Two such devices arc said to be networked together when one device is able to exchange information with the other device, whether or not they have a direct connection to each other.

Computer networks support applications such as access to the World Wide Web, shared use of application and storage servers, printers, and fax machines, and use of email and instant messaging applications. Computer networks differ in the physical media used to transmit their signals, the communications protocols to organize network traffic, the network's size, topology and organizational intent [1][3].

2.2 Network protocol:-

Defines are rules and conventions for communication between networks devices. Protocols for computer networking all generally use packet switching techniques to send and receive messages in the form of packets.

Network protocols include mechanisms for devices to identify and make connections with each other, as well as formatting rules that special how data is packaged into messages sent and received. Some protocols also Support message acknowledgement and data compression designed for reliable and/or high-performance network communication. Hundreds of different computer network protocols have been developed each designed for specific purposes and environment [4].

2.3 Network links:-

The communication media used to link devices to form a computer network include electrical cable, optical fiber and radio waves. In the OSI model, these are defined at layers 1 and 2- the physical layer and the data link layer.

A widely adopted family of communication media used in local area network (LAN) technology is collectively known as Ethernet. The media and protocol standards that enable communication between networked devices over Ethernet are defined by IEEE 802.3. Ethernet transmit data over both copper and fiber cables. Wireless LAN standards use radio waves, or others use infrared signals as a transmission medium. Power line communication uses a building's power cabling to transmit data [5].

2.4 Network devices:-

A part from the physical communications media described above, networks comprise additional basic system building blocks, such as network interface controller (NICs), repeaters, hubs, bridges, switches, routers, modems, and firewalls.

2.4.1 Router:

A router is a device that forwards data packets along networks. A router is connected to at least two networks, commonly two LANs or WANs or a LAN and its ISP's network Routers are located at gateways, the places where two or more networks connect, and are the critical device that keeps data flowing between networks and keep the networks connected to the Internet [6].

When data is sent between locations on one network or I from one network to a second network the data is always seen and directed to the correct location by the router. The router accomplishes this by using headers and forwarding tables to determine the best path for forwarding the data packets, and they also use protocols such as ICMP to communicate with each other and configure the best route between any two hosts.

The Internet itself is a global network connecting millions of computers and smaller networks — so you can see how crucial the role of a router is to our way of communicating and computing.

I Need a Router For most home users; they may want to set-up a LAN or WLAN and connect all computers to the Internet without having to pay a full broadband subscription service to their ISP for each computer on the network. In many instances, an ISP will allow you to use a router and connect multiple computers to a single Internet connection and pay a nominal fee for each additional computer sharing the connection This is when home users will want to look at smaller routers, often called broadband routers that enable two or more computers to share an Internet connection Within a business or organization, you may to connect multiple computers to the Internet. But also want to connect multiple private networks — and these are the types of functions a router is designed for [3][7].

2.5 Routing basic:-

Routing is used for taking a packet from one device and sending It through the network to another device on a different network. If your network has no routers, then you are not routing. Routers route traffic to all the networks in your internetwork to be able to route packets, a router must know, at a minimum, the following:

* Destination address.
* Neighbor routers from which it can learn about remote networks.
* Possible routes to all remote networks.
* The best route to each remote network.

The router learns about remote networks from neighbor routers or from an administrator. The router then builds a routing table that describes how to find the remote networks. If the network is directly connected, then the router already knows how to get to the network. If the networks are not attached, the router must learn how to get to the remote networks either static routing, which means that the administrator. Must hand-type all network locations into the routing table, or use dynamic routing [8].

2.5.1 Routing Metrics:

Routing algorithms have used many different metrics to determine the best route. Sophisticated routing algorithms can base route selection on multiple metrics, combining them in a single (hybrid) metric.

All the following metrics have been used:

- Path length
- Reliability
- Delay
- Bandwidth
- Load
- Communication cost

Path length is the most common routing metric. Some routing protocols allow network administrators to assign arbitrary costs to each network link. In this case, path length is the sum of the costs associated with each link traversed. Other routing protocols define hop count, a metric that specifies the number of passes through internetworking products, such as routers, that a packet must take en route from a source to a destination. Reliability, in the context of routing algorithms, refers to the dependability (usually described in terms of the bit-error rate) of each network link. Some network links might go down more often than others.

After a network fails, certain network links might be repaired more easily or more quickly than other links. Any reliability factors can be taken into account in the assignment of the reliability ratings, which are arbitrary numeric values usually assigned to network links by network administrators [9].

Routing delay refers to the length of time required to move a packet from source to destination through the internetwork. Delay depends on many factors, including the bandwidth of intermediate network links, the port queues at each router along the way, network congestion on all

intermediate network links, and the physical distance to be traveled. Because delay is a conglomeration of several important variables, it is a common and useful metric.

Bandwidth refers to the available traffic capacity of a link all other things being equal, an l0-Mhps Ethernet link would be preferable to a 64-Kbps leased line. Although bandwidth is a rating of the maximum attainable throughput on a link, routes through links with greater Bandwidth does not necessarily provide better routes than routes through slower links. For example, if a faster link is busier, the actual time required to send a packet to the destination could be greater [10].

Load refers to the degree to which a network resource, such as a router, is busy. Load can be calculated in a variety of ways including CPU utilization and packets processed per second. Monitoring these parameters on a continual basis can be resource-intensive itself.

Communication cost's another important metric, especially because some companies may not care about performance as much as they care about operating expenditures. Although line delay may be longer, they will send packets over their own lines rather than through the public lines that cost money for usage time [11].

2.5.2 Static Routing:

Static routing is the process of an administrator manually adding routes in each router's routing table. There are benefits and disadvantages to all routing processes.

Static routing has the following benefits:-

- No overhead on the router CPU.
- No bandwidth usage between routers.
- Security (because the administrator only allows routing to certain networks).

Static routing has the following disadvantages:-

- The administrator must really understand the internetwork and how each router is connected to configure the routes correctly.
- 1f one network is added to the internetwork, the administrator must add a route to it on all routers [12].

2.5.3 Default Routing:

Default routing is used to send packets with a remote destination network not in the routing table to the next hop router. You can only use default routing to configure a default route, you use wildcards in the network address instead of network information and mask by using a default route, and you can just create one static route entry instead. First, you must delete the existing static route entry instead. First, you must delete the existing static routes from the router, and then add the default route. Default routes: the ip classless command. All Cisco routers are glassful routers, which mean they expect a default subnet mask on each interface of the router. When a router receives a packet for a destination subnet not in the routing table, it will drop the packet by default if you are using default routing, you must use the ip classless command because no remote subnets will be in the routing table [8][13].

2.5.4 Dynamic Routing:

Dynamic routing is the process of using protocols to find and update routing tables on routers this is easier than static or default routing, but you use it at the expense of router CPU processes and bandwidth on the network links.

A routing protocol defines the set of rules used by a router when it communicates between neighbors routers. There are two types of routing protocols used in internetworks:

Interior Gateway Protocol (IGP) and Exterior Gateway Protocol (EGP). IGP routing protocols are used to exchange routing information with routers in the same autonomous system (AS). An AS is a collection of networks under a common administrative domain. EGPs arc used to communicate between Asses [14].

2.6 Distance vector & Link state:

The distance-vector routing protocols use a distance to a remote network to find the best path each time a packet goes through a router, it’s called a hop. The route with the least number of hops to the network is determined to be the best route. The distance-vector routing algorithm passes complete routing tables to neighbor routers.

The neighbor routers then combine the received routing table with their own routing tables to Complete the internetwork map this is called routing by rumor, because a router receiving an update from a neighbor router believes the information about remote networks without actually finding out for itself: It is possible to have a network that has multiple links to the same remote network. If that is the case, the administrative distance is first checked. If the administrative distance is the same, it will have to use other metrics to determine the best path to use to that remote network [15].

RIP uses only hop count to determine the best path to an internetwork. If RIP finds more than one link to the same remote network with the same hop count, it will automatically perform a round-robin load balance. RIP can however, a problem with this type of routing metric arises when the two a remote network are different bandwidths but the same hop count perform load balancing for u in each routing table. Each router sends its complete routing table out each router has only the directly connected network stop six equal-cost link to each active interface on the router. The routing table of each router I When the routers are converging, no data is passed. That's why fast convergence time is a plus. One of the problems with RIP, in fact, is its slow convergence time includes the network number, exit interface, and hop count to the network [16].

Typically called shortest path first, the routers each create three separate tables. One of these tables keeps track of directly attached neighbors, one determines the topology of the entire internetwork, and one is used for the routing table. Link-state routers know more about the internetwork than any distance-vector routing protocol. An example of a IP routing protocol that is completely link state is OSPF.

Uses aspects of distance vector and link state, for example, EIGRP. There is no set way of configuring routing protocols for use with every business. This is a task that is performed on a case-by-case basis. However, if you understand how the different routing protocols work, you can make good business decisions. This course and equivalent exam only cover distance- vector routing protocols and theory [11][14].

2.7 Routing Information Protocol (RIP):-

RIP it is the dynamic routing protocol being used in the practical networks to propagate network topology information to the neighboring routers. The RIP allows that routers update their routing tables at programmable intervals, generally every 30 seconds.

RIP is a true distance-vector routing protocol it sends the complete routing table out to all active interfaces eve30 seconds. RIP only uses hop count to determine the best way to a remote network, but it has a maximum allowable hop count of 15, meaning that 16 is deemed unreachable. RIP works well in small networks, but it is inefficient on large networks with slow WAN links or on networks with large number routers installed [17]

RIP version 1 uses only classful routing, which means that all devices in the network must use the same subnet mask. This is because RIP version 1 does not send updates with subnet mask information in tow. RIP version 2 provides what is called prefix routing and does send subnet mask information with the route updates this is called classless.

Rip version 1 Distance Vector and Default Metric Hop Count and Administrative Distance 120 and Hop Count Limit 15 and Convergence Slow and Update timers 30 seconds and Updates Full table and Algorithm Bellman-Ford and Update Address Broadcast and Port UDP Port.

Rip version 2 Distance Vector and Default Metric Hop Count and Administrative Distance 120 and Hop Count Limit 15 and Convergence Slow and Update timers 30 seconds and Updates Full Table and Algorithm Bellman Ford and Update Address 224.0.0.9 and Port UDP port.

Characteristic RIP is Distance vector routing protocol, and It metric is the number of jumps and The maximum number of jumps is 15 and One updates every 30 seconds and it selects the fastest route for the packages and It generates great amount of traffic of network with updates.

The main is that The RIP allows fifteen as maximum limit for the number of jumps through which data can be sent, The network destiny is considered unreachable if there are more than fifteen jumps router and routers that use RIP is that Constantly they are connected with routers neighboring to update his tables of routing, generating therefore a great amount of network traffic Nevertheless, the RIP continues being very popular and it is Continued implementing widely [17].

2.7.1 Routing Information Protocol Timers:

RIP uses three different kinds of timers to regulate its performance Route update timer sets the interval (typically 30 seconds) between periodic routing updates, in which the router sends a complete copy of its routing table out to all neighbors.

Route invalid timer determines the length of time that must expire (90 seconds) before a router determines that a route has become invalid. It will come to this conclusion if it hasn't heard any updates about a particular route for that period. When that happens, the router will send out updates to all its neighbors letting them know that the route is invalid [18].

Route flush timer sets the time between a route becoming invalid and its removal from the routing table (240 seconds). Before it is removed from the table, the router notifies its neighbors of that route's impending doom. The value of the route invalid timer must be less than that of the route flush timer. This is to provide the router with enough time to tell its neighbors about the invalid route before the routing table is updated [18]

2.8 Open shortest path first (OSPF):-

In 1988, the group: Internet Engineers Task Force (IETF) began to develop a new protocol of routing that it would replace to protocol RIP. Then development the Open Shortest Path First protocol (OSPF). Protocol OSPF proposes the use of shorter and accessible routes by the construction of a map of the network and data base maintenance with information on local and neighboring systems, this way he is able to calculate the metric for each route, and then the shorter routing routes are chosen.

OSPF characteristics are fast detection of changes in the topology and very fast reestablishment of routes without loops, and Low overload, use updates about changes on routes, and Division of traffic by several equivalent routes, and Routing according type of service, and Use of multi-send in local area networks, and Subnet and Super- net mask Authentication.

2.8.1 Open Short Path First Cost

The path cost of an interface in OSPF is called metric that indicates standard value such as speed. The cost of an interface is calculated on the basis of bandwidth in equation (1). Cost is inversely proportional to the bandwidth. Higher bandwidth is attained with a lower cost.

$$\text{Cost} = \frac{10^8}{\text{Bandwidth in bps}} \longrightarrow (1)$$

Where the value of 10^8 is 100000000 in bps is called reference bandwidth based on by default [9] [18].

2.8.2 Shortest Path First (SPF) Algorithm

OSPF is a link state routing protocol that uses a shortest path first algorithm to calculate the least cost path to all known destinations. Dijkstra algorithm is used for calculating the shortest path. Several procedures of this algorithm are given [10]:

- For any change in the routing information, a link state advertisement is generated by a router. This advertisement provides all link states on that particular router with information.
- All routers exchange LSAs by flooding. The link state update is received by each router and preserves a copy of link state database in it. This link state update propagates to all other routers.
- After creation of database of each router, routers start calculating shortest path tree to the destinations. In order to find the least cost path, the router uses Dijkstra algorithm.
- If any changes occurred in the OSPF network such as link cost, new network being added or deleted, Dijkstra algorithm is recalculated to find the least cost path.

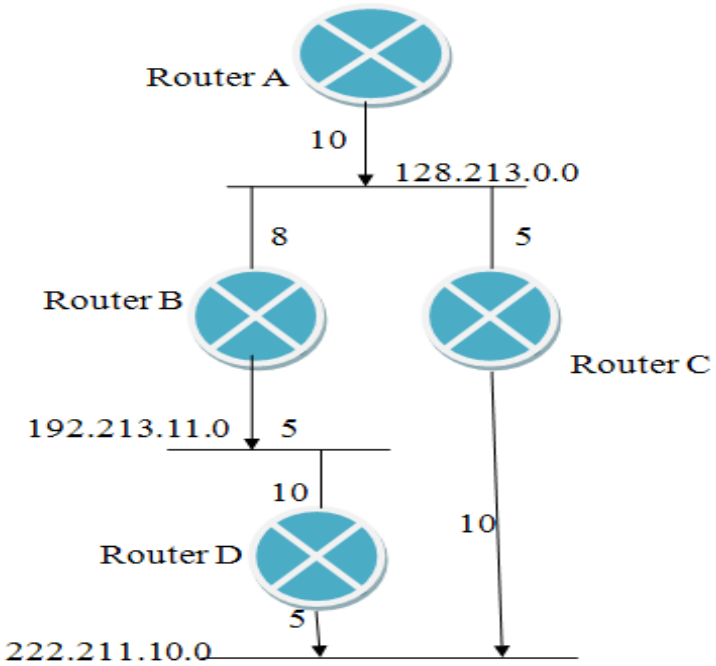

Figure (2.1) Network cost

Every router uses this algorithm at the root of the tree in order to find the shortest path on the basis of cost to reach the destinations. Figure (2.1) shows a network diagram that is indicated with the interface cost to find out the shortest path [19].

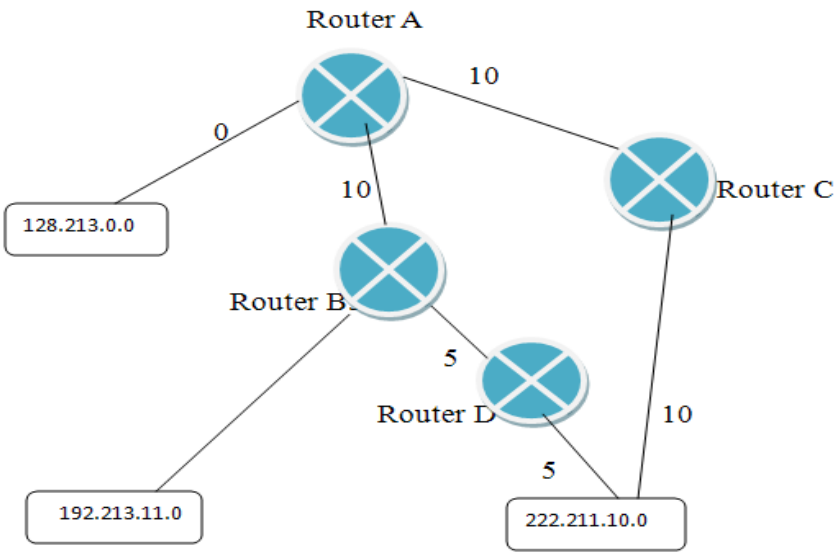

Figure (2.2) shortest path trees

2.8.3 Open Short Path First Convergence

Consider the network in Figure (2.3) running OSPF. Assume the link between Router3 and Router5 fails. Router3 detects link failure and sends LSA to Router2 and Router4. Since a change in the network is detected traffic forwarding is suspended. Router2 and Router4 updates their topology database, copies the LSA and flood their neighbors. By flooding LSA all devices in the network have topological awareness. A new routing table is generated by all routers by running Dijkstra algorithm. The traffic is now forwarded via Router4.

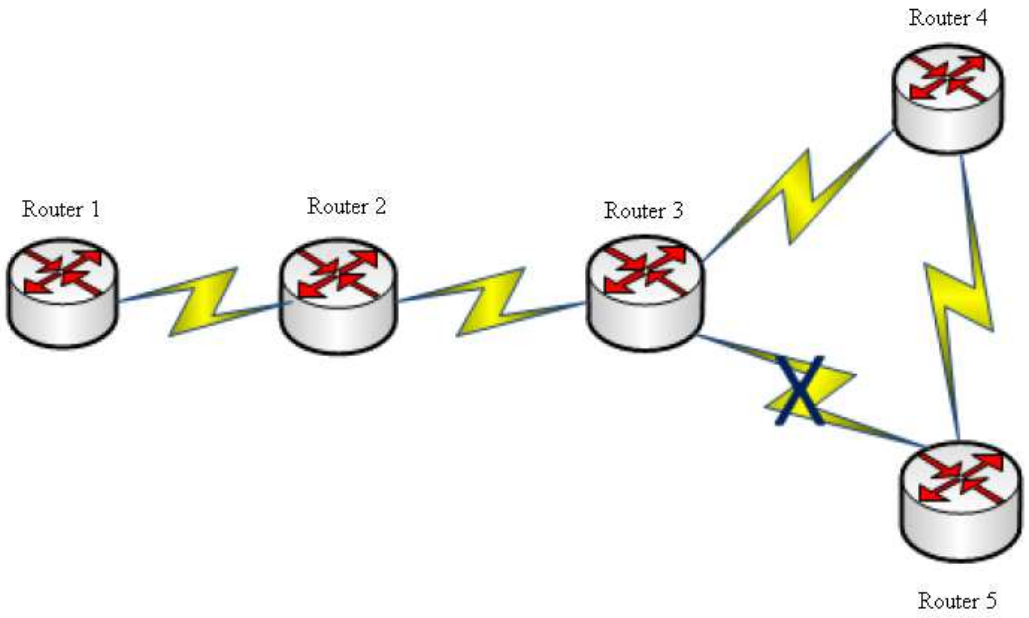

Figure (2.3) OSPF Network

2.8.4 Advantages and Disadvantages of OSPF

The advantages of OSPF are:

- OSPF is not a Cisco proprietary protocol.
- If any changes occur in the network it updates fast.
- OSPF minimizes the routes and reduces the size of routing table by configuring area.
- Low bandwidth utilization.
- Multiple routes are supported.
- Support variable length subnet masking.
- It is suitable for large network.

Disadvantages of OSPF are:

- Difficult to configure.
- Link state scaling problem.
- More memory requirement

2.9 Enhanced Interior Gateway Routing Protocol (EIGRP):-

EIGRP is an enhanced version of IGRP (Interior Gateway Routing Protocol), an obsolete routing protocol that was developed by Cisco. EIGRP is an advanced distance-vector protocol that implements some characteristics similar to those of link-state protocols. Some Cisco documentation refers to EIGRP as a hybrid protocol. EIGRP advertises its routing table to its neighbors as distance vector protocols do, however it uses the hello protocol and forms neighbor relationships similar to link-state protocols. EIGRP sends partial updates when a metric or the topology on the network changes. It does not send full routing-table updates in periodic fashion as distance-vector protocols do. EIGRP is a classless protocol that permits the use of VLSMs (Variable Length Subnet Masks) and supports CIDR (Classless inter-Domain Routing) for a scalable allocation of IP addresses [19].

EIGRP uses the metrics like bandwidth, delay, reliability, load, and MTU in making its routing decisions .The default metrics used are bandwidth and delay. For a more granular level of control, EIGRP multiplies each of the metrics by 256 before performing the calculation of the composite metric. EIGRP has been designed to make much better use of bandwidth and to allow routers to have a much better awareness of neighboring routers. Instead of sending its entire routing table out at

regular intervals an EIGRP router sends out only partial updates, and even then, only when a route changes. This makes a better use of the Network bandwidth An EIGRP router also has a more complete view of the network than a tidal distance vector protocol as it not only maintains its own routing table, but also keeps a copy of the routing tables of neighboring routers. When an EIGRP router cannot find a route to a network based on all the information it currently has, it sends out a query to other routers, which is propagated until a route is found [19].

2.9.1 Enhanced Interior Gateway Routing Protocol Features:

In a well- designed network, EIGRP scales well and provides extremely quick convergence times with minimal network traffic some of the features of EIGRP are as follows:

EIGRP has rapid convergence times for changes in the network topology. In some situations convergence can be almost Instantaneous EIGRP uses DUAL to achieve rapid convergence a router that runs EIGRP stores backup routes for destinations when they are available so that it can quickly adapt to alternate routes. If no appropriate route or backup route exists in the local routing table. EIGRP queries its neighbors to discover an alternate route. These queries are propagated until an alternate route is found [11].

EIGRP has low usage of network resources during normal operation; only hello packets arc transmitted on a stable network. Like other link-state routing protocols, EIGRP uses EIGRP hello packets to establish relationships with neighboring EIGRP routers. Each router builds a neighbor table from the hello packets that it receives from adjacent EIGRP routers. EIGRP does not send periodic routing updates like IGRP does. When a change was occurs, routing table changes are only propagated, not the entire routing table. When changes are only propagated the bandwidth required for EIGRP packets is minimized, which reduces the load that the routing protocol itself places on the network.

EIGRP supports automatic (Classful) route summarization at major network boundaries as the default. However, unlike other glassful routing protocols, such as IGRP and RIP, manual route summarization can be configured on arbitrary network boundaries to reduce the size of the routing table [11] [10].

2.9.2 Packet Enhanced Interior Gateway Routing Protocol Types:

Like OSPF, EIGRP relies on different packet types to maintain its tables and establish relationsh1ps with neighbor route EIGRP uses the following live types of packets [20]:

- Hello
- Acknowledgment
- Update
- Query

2.9.3 Enhanced Interior Gateway Routing Protocol Metrics

With the use of total delay and the minimum link bandwidth, it is possible to determine the routing metrics in EIGRP. Composite metrics, which consists of bandwidth, reliability, delay, and load, are considered to be used for the purpose of calculating the preferred path to the networks in equation (2). The EIGRP routing update takes the hop count into account though EIGRP does not include hop count as a component of composite metrics. The total delay and the minimum bandwidth metrics can be achieved from values which are put together on interfaces and the formula used to compute the metric is followed [12] by:

$$256 \times \left[(K_1 + B_w + \frac{K_2 \times B_w}{256 - Load} + K_3 \times Delay)\right] \times \frac{K_5}{K_4 + Reliability} \longrightarrow (2)$$

For weights, the default values are:

$$K_1=1,\ K_2=0,\ K_3=1,\ K_4=0,\ K_5=0.$$

These default values efficiently trimming down the above formula to

$$256 \times (BW + Delay)$$

A significant and totally non-obvious fact is that if , then term

$$\frac{K_5}{K_4 + Reliability}$$ Is not used (i.e. taken as 1)

EIGRP uses calculate scale bandwidth is:

$$Bw = \frac{10^7}{B_n} \times 256$$

Where (B_n) is in kilobits per second and represents the minimum bandwidth on the interface to destination
BW = Bandwidth

2.9.4 Diffusion Update Algorithm

The Diffusion Update Algorithm (DUAL) uses some provisions and theories which has a significant role in loop-avoidance mechanism as follows [11]:

- **Feasible Distance (FD)**

The lowest cost needed to reach the destination is usually termed as the feasible distance for that specific destination.

- **Reported Distance (RD)**

A router has a cost for reaching the destination and it is denoted as reported distance.

- **Successor**

A successor is basically an adjacent router which determines the least-cost route to the destination network.

- **Feasible Successor (FS)**

FS is an adjacent router which is used to offer a loop free backup path to the destination by fulfilling the conditions of FC.

- **Feasible Condition (FC)**

After the condition of FD is met, FC is used in order to select the reasonable successor. The RD advertised by a router should be less than the FD to the same destination for fulfilling the condition.

In EIGRP, all route calculations are done by the DUAL. One of the tasks of DUAL comprises keeping a table, known as topology table, which includes all the entries found from the loop-free paths advertised by all routers. DUAL selects the best loop-free path (known as successor path) and second best loop free path (known as feasible path) from the topology table by using the distance information. It then saves this into the routing table. The neighbor of the least cost route to the destination is called a successor [20].

In case of having no loop-free path in the topology table, the re-calculation of the route must be done and then the DUAL inquire its neighbors. This occurs during re-calculation for searching a new successor. Although the re-calculation of the route does not seem to be processor-intensive, it may have an effect on the convergence time and

Consequently, it is useful for avoiding needless computations. In case of having any FS, DUAL is used for avoiding any needless re-computation. If we consider Figure (2.3), will be able to understand how the DUAL converges. This example aims at router K for the destination only. The cost of K (hops) coming from each router is presented in figure (2.3).

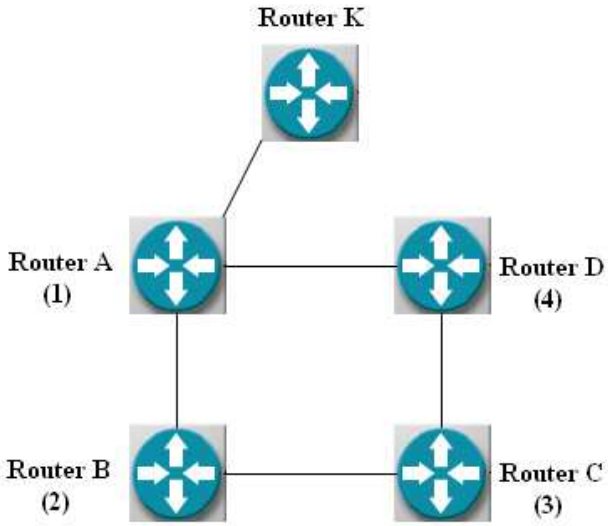

Figure (2.4): DUAL placed in the network

In Figure (2.4), the link from A to D fails. When the loss of the FS occurs, a message goes to the adjacent router sent by D. This is received by C. Then C determines if there is any FS. In case of having no FS, C needs to begin a new route calculation by entering the active state. The cost from router C to router K is 3 and the cost from router B to router K is 2. Hence it is possible for C to switch to B. There is no effect on router A and B for this change. Thus they have no contribution in finding the reasonable successor [12].

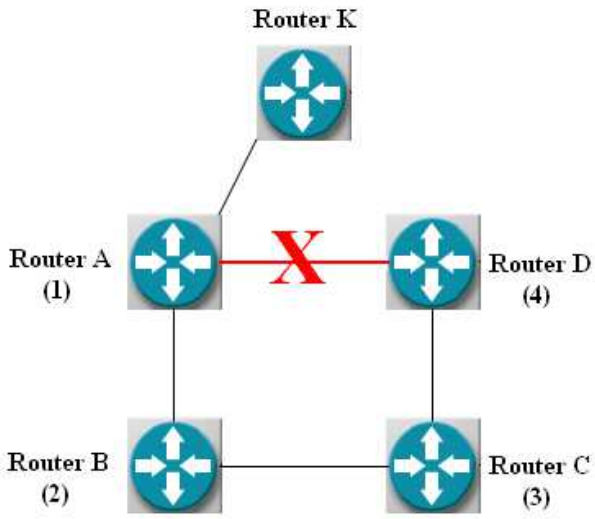

Figure (2.5): Failure link of network topology

2.9.5 Enhanced Interior Gateway Routing Protocol Convergence

Would assume in figure (2.3), that the link from Router3 and Router5 goes down and at the same time Router3 identifies the failure of the link. There is no FS present in the topology database and hence the role of Router3 is to be entered into the active convergence. Router4 and Router2, on the other hand, are the only neighbors to Router3. Given that, there is no availability of route with lower FD, and Router3 sends a message to both Router4 and Router2 for gaining a logical successor. Router2, for acknowledgement, replies to Router3 and indicates that there is no availability of successor. On the other hand, Router3 gets positive acknowledgement from Router4 and the FS with higher FD becomes available to Router3. The distance and new path is allowed by Router3 and then added to the routing table. Followed by Router2 and Router4 are sent an update about the higher metric. In the network, all the routers converge when the updates are reached to them [18] [21].

2.9.6 Advantages and Disadvantages of EIGRP

There are some advantages provides by EIGRP as follows:

- Easy to configure.
- Loop free routes are offered.
- It keeps a back up path in the network to get the destination.
- Multiple network layer protocols are included.
- EIGRP convergence time is low and it is responsible for the reduction of the bandwidth utilization.
- It can work with Variable Length Subnet Mask (VLSM) and Class Less Inter Domain Routing (CIDR).
- EIGRP also supports the routing update authentication.

Disadvantages of EIGRP are:

- Considered as Cisco proprietary routing protocol.
- Routers from other vendors are not able to utilize EIGRP.