# Analysis of Shortest Path Packet Tracing of Routers

A.K.M Fazlul Haque[1], Mahdi Roksana[2]
[1]Department of Electronics and Telecommunication Engineering,
[2]Department of Computer Science and Engineering
Daffodil International University
Email: akm_haque@yahoo.com, mahdi_roksana@yahoo.com

***Abstract***: *In this paper, the shortest path in a packet switched network has been analyzed. A router receives a packet from a network and passes it to another network calculating the shortest path. However, the packets of a network use different routing protocols. A routing protocol is a combination of rules and procedures that lets routers informs each other of changes. It allows routers to share whatever they know about their neighborhood. Routing protocols are used to continuously update the routing tables that are consulted for forwarding and routing. The primary contribution of this paper is a simulation method of displaying the packet traces which finds the shortest path to route the packet through its destination. The simulation has been done by using Packet Tracer 4.01 software that allows us to stop time in our network and examine traffic in detail.*

***Keywords:*** *Routing, Routing protocols, Shortest path, Packet Tracing.*

## 1. Introduction

Routing is defined as the task of moving data packets across a network from a source point to a destination point [1]. This usually involves two distinct phases – the first is to find the optimal routing paths, taking into account a set of rules and constraints; and the second is the actual transport of the data packets through the network via the previously established path. The critical phase of routing is to select the optimal routing path, due to the complexity and large dimension of network topologies and the very often large number of rules and constraints that have to be met. Source routed networks define its routing path tables at the ingress nodes, and for static source routed networks these paths remain unchanged unless reconfiguration is necessary by the addition or removal of nodes or links.

Routing metrics are a scoring system for routes a routing device knows. Metrics are calculated by routers to prioritize routes from best to worst. Routers use the metrics to select the best possible routes to a given destination. Metrics can include hop count (how many stops there are between here and the destination), media type (Serial, Ethernet, and SONET etc.), and availability (whether the machine is up or down) and several other factors including some set by the Network Administrator. A lower metric generally indicates a better route.

In a packet-switching network, a unique packet which causes a report of each stage of its progress to be sent to the network control center from each visited system element. Packet tracing is the process by which one can verify the path of a packet through the layers to its destination and a trace is a collection of packet records that contain a timestamp, high-level data link control (HDLC) information, and the first 40 bytes of the packet. Each trace only contains packets flowing in one direction of the link [2]. The duration of the trace depends on the storage space in the monitoring machine and on the link load. Common values for the storage space are 50GB, 100GB, 202GB and 336GB.

In this paper, a simulation has been done to find the shortest path that a packet takes to reach its destination. The routing protocols that are used to continuously update the routing tables are: Address Resolution Protocol (ARP) and Routing Information Protocol (RIP). The Internet Control Message Protocol (ICMP) is used by hosts and gateways to send notification of datagram problems back to the sender. First, the technical terms of these protocols are analyzed and then the shortest path packet tracing is verified by using Packet Tracer 4.01 simulation software.

## 2. Literary Survey of the Protocols

### 2.1 Address Resolution Protocol (ARP)

The Address Resolution Protocol (ARP) is used by hosts to map IP addresses onto Medium Access Control (MAC) link layer addresses [3, 4, 15]. The resulting address associations are used to direct packet delivery within the physical local network. Every packet in an IP network must be delivered to some interface in the local network. Those whose destination IP addresses are external to the local network (as determined by the subnet mask) are delivered to the subnet gateway. Those packets destined for internal network are delivered directly. Whether the destination address is local or gateway, the IP address must be mapped onto a MAC address. ARP resolution performs a distributed lookup via a simple broadcast request followed by a unicast response. The querying host sends the request to the local broadcast address. According to the protocol, only a host assigned to the requested address should reply with its local hardware address. This reply, containing both the requested IP address and associated MAC address, is sent via unicast to the querying host. The host caches the association, which expires and is evicted at a later time per some local policy. Once evicted, the host repeats the request, cache, and eventual ejection. While the cache hold time for a response is undefined in the protocol specification, many implementations set the expiration to approximately 20 minutes, with the option of resetting the expiry timer after each use [5]. Hosts implicitly trust the address associations residing in the ARP cache. If an adversary can influence these values, the host can be manipulated into sending packets to the wrong hardware address. The lack of authentication of address association data leaves hosts susceptible to reply spoofing and cache entry poisoning, commonly referred to as cache poisoning. In fact, freely available tools are designed to exploit these vulnerabilities [6]. Most IP protocol stacks are designed to ignore unsolicited ARP replies. However, this does little to prevent cache poisoning. An adversary can coerce a host into requesting a specific address by spoofing an ICMP (Internet Control Message Protocol) ping message. The spoofed message contains the targeted IP address, requiring the host to resolve the MAC address to reply. By carefully poisoning the cache and spoofing replies, an adversary can perform both Denial of Service (DoS) and Man in the Middle (MITM) attacks [7]. Such attacks were known even in 1989 [8], and they still exist today [9].

ARP is used in four cases of two hosts communicating:

a. When two hosts are on the same network and one desires to send a packet to the other
b. When two hosts are on different networks and must use a gateway/router to reach the other host
c. When a router needs to forward a packet for one host through another router
d. When a router needs to forward a packet from one host to the destination host on the same network

### 2.2 Routing Information Protocol (RIP)

Routing information protocol is a network routing protocol base on the Bellman-Ford (or distance vector) algorithm [10-12]. According to the RIP, a router will recode the connected routers in its routing table. When the destination of the packet is not in routing table, the router will deliver it to neighbor routers. In order to reduce the transmission cost, the router would periodic interchange routing table with other routers. The proposed mechanism is based on the concept of RIP to reduce the transmission overhead and request of server. The proposed mechanism is to let every entity maintain its own tables. These entities would interchange tables with other entities periodically. In this way, entities can deliver data to other entities without via server.

RIP uses a single routing metric (hop count) to measure the distance between the source and a destination network. Each hop in a path from source to destination is assigned a hop count value, which is typically 1. When a router receives a routing update that contains a new or changed destination network entry, the router adds 1 to the metric value indicated in the update and enters the network in the routing table. The IP address of the sender is used as the next hop.

#### 2.2.1 RIP Timers

RIP uses numerous timers to regulate its performance. These include a routing-update timer, a route-timeout timer, and a route-flush

timer. The routing-update timer clocks the interval between periodic routing updates. Generally, it is set to 30 seconds, with a small random amount of time added whenever the timer is reset. This is done to help prevent congestion, which could result from all routers simultaneously attempting to update their neighbors. Each routing table entry has a route-timeout timer associated with it. When the route-timeout timer expires, the route is marked invalid but is retained in the table until the route-flush timer expires.

## 2.3 Internet Control Message Protocol (ICMP)

The Internet Control Message Protocol (ICMP) is one of the core protocols of the Internet protocol suite. It is chiefly used by networked computers' operating systems to send error messages—indicating, for instance, that a requested service is not available or that a host or router could not be reached. ICMP differs in purpose from TCP and UDP in that it is usually *not* used directly by user network applications. One exception is the ping tool, which sends ICMP Echo Request messages (and receives Echo Response messages) to determine whether a host is reachable and how long packets take to get to and from that host [13].

### 2.3.1 The Ping Application

The "ping" program contains a client interface to ICMP [14]. It may be used by a user to verify an end-to-end Internet Path is operational. The ping program also collects performance statistics (i.e. the measured round trip time and the number of times the remote server fails to reply). Each time an ICMP echo reply message is received, the ping program displays a single line of text. The text printed by ping shows the received sequence number, and the measured round trip time (in milliseconds). Each ICMP Echo message contains a sequence number (starting at 0) that is incremented after each transmission, and a timestamp value indicating the transmission time.

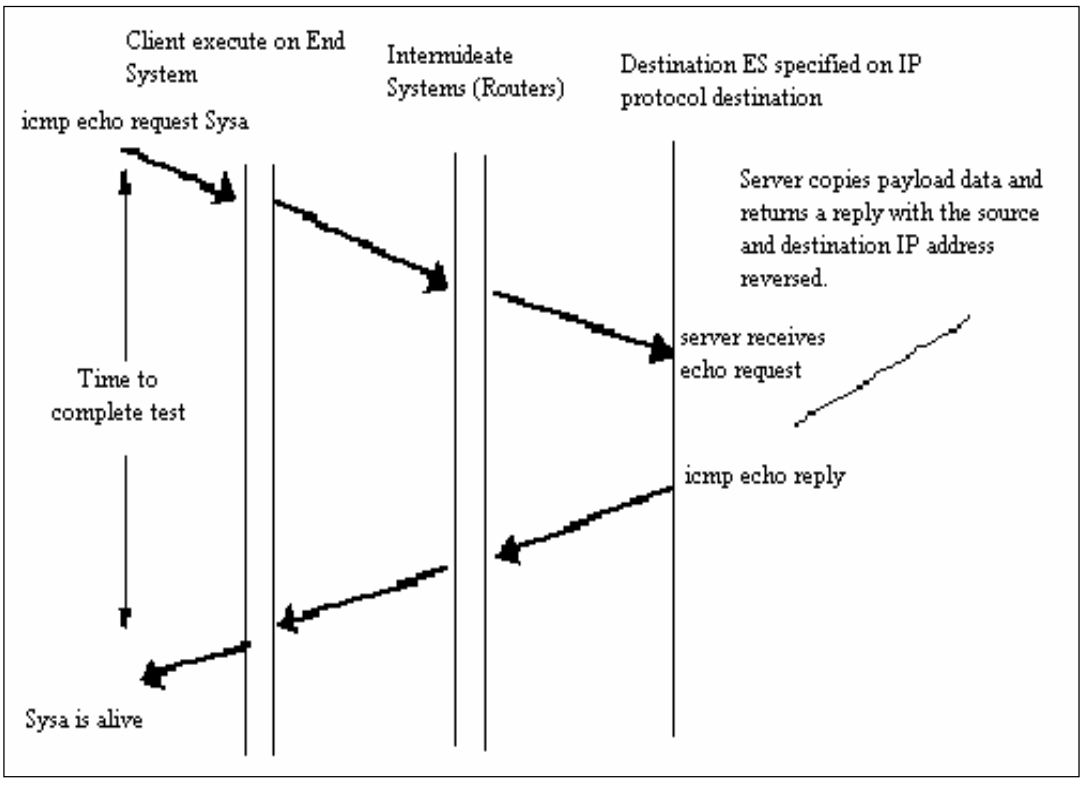


**Fig 1: Use of the ping program to test whether a particular computer ("Sysa") is operational.**

The operation of ICMP is illustrated in the frame transition diagram shown in Fig. 1. In this case there is only one Intermediate System (IS) (i.e. IP router). Two types of message are involved; the ECHO request (sent by the client) and the ECHO reply (the response by the server). Each message may contain some optional data. When data are sent by a server, the server returns the data in the reply, which is generated. ICMP packets are encapsulated in IP for transmission across an Internet. The problem with sending an ICMP Echo message [13] is that not all nodes on the Internet may necessarily respond to the 'ping'. Thus, the actual location of the node cannot be determined unless alternative methods are employed.

## 3. Simulation and Testing

In this section, we verify the improvement of our information based routing on the ability of achieving the shortest-path from a simulator, comparing with the best result. Routing is the main process to deliver packets. A router that handles a packet examines the destination address in the IP header, computes the next hop that will bring the packet one step closer to its destination, and delivers the packet to the next hop, where the process is repeated. To make this work, two things are needed. First, routing tables match destination addresses with next hops. Second, routing protocols determine the contents of these tables.

Case 1: Before starting the simulation, we first create a topology where Pc0 and Pc1 are connected with the serially connected routers (router 0 and router 1). To send a packet from Pc0 to Pc1, there is only one path. Fig. 2 and Fig. 3 show the echo packet and acknowledgement packet respectively at Pc0. The time required to reach the acknowledgement packet to Pc0 in 0.010s.

Case 2: In the second topology (shown in Fig. 4) we have disconnected router0 and router4 and connected another two routers (router1 and router3). Then we start the simulation mode. In this case, the ICMP packet is passing through router1 to reach its destination Pc1which is shown in Fig. 5. This time, the time required to send and receive ICMP packet is 0.014s (Fig. 6). Here we find that, the extra 0.004s is required because the packet has to travel more two hops than before.

Case 3: We connect router0 and router4 and add a PDU again at Pc0 as shown in Fig. 7, but this time another type of packet is created. This is the ARP packet. An ARP packet is created when the host or router does not have the hardware or MAC address of its next hop. The host will send an ARP request and also drop the ICMP packet. It does not buffer the packet and wait for the ARP reply to come back because that would cause a lot of performance drop if there are a lot of pending ARP entries. When the MAC address is available on the ARP table of the router, this table can be used as next time we add PDU on the same PC. In Fig. 7, we can see that the ARP table for Pc0 is empty. After getting the ARP reply packet as shown in Fig. 8, the table is filled up with the MAC address of the next hop i.e. 192.168.1.1 which is the IP address of router0.The ICMP packet is again created and forwarded. But when the packet reached to router4, it again creates an ARP packet for the same reason and gets the next hop MAC address.

Case 4: We create another scenario as shown in Fig. 9. This time the ICMP packet is being passed from network to network without any abstraction (Fig. 10 and 11). The main critical point that we are trying to focus throughout these cases is the route that the packet takes to reach its destination. The packet could pass through router1→ router3→ router4; where it needs 0.014s. But it chooses its route through router0 →router4 which takes only 0.010s to complete the ICMP echo and ICMP reply. This proves the shortest path selection during transmission.

Routers and switches send out CDP packets every 60 seconds regardless of what packets we have created. Each device configured for CDP sends periodic messages, known as advertisements, to a multicast address. The advertisements also contain time-to-live, or holdtime, information, which indicates the length of time a receiving device, should hold CDP information before discarding it. Each device also listens to the periodic CDP messages sent by others in order to learn about neighboring devices and determine when their interfaces to the media go up or down.

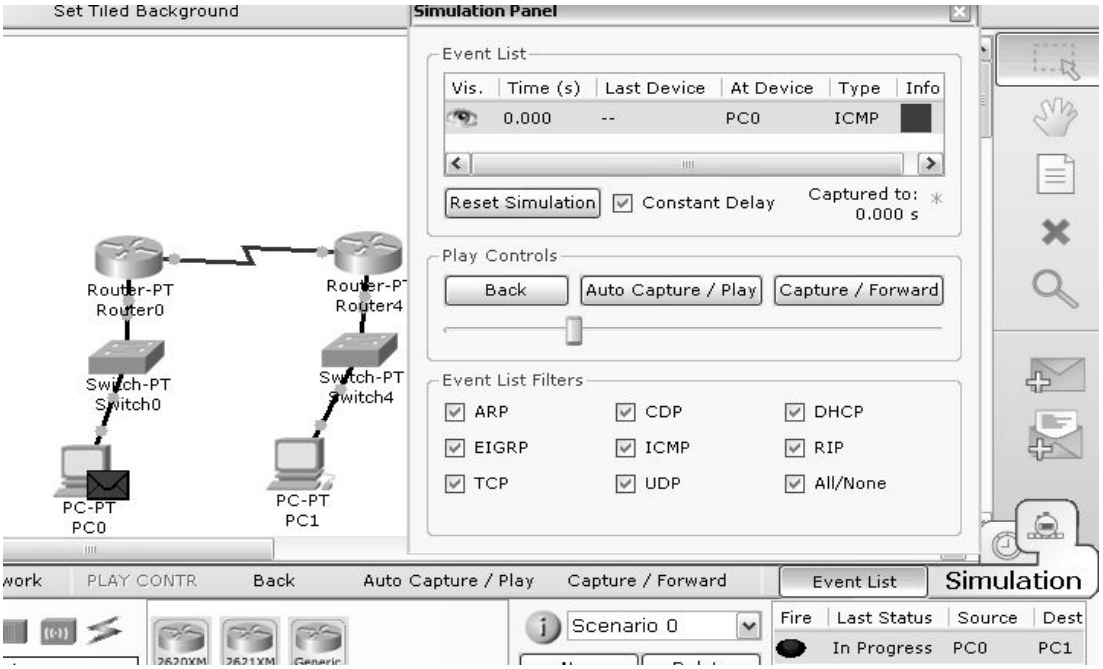


**Fig. 2: A simple PDU is added to PC0.**

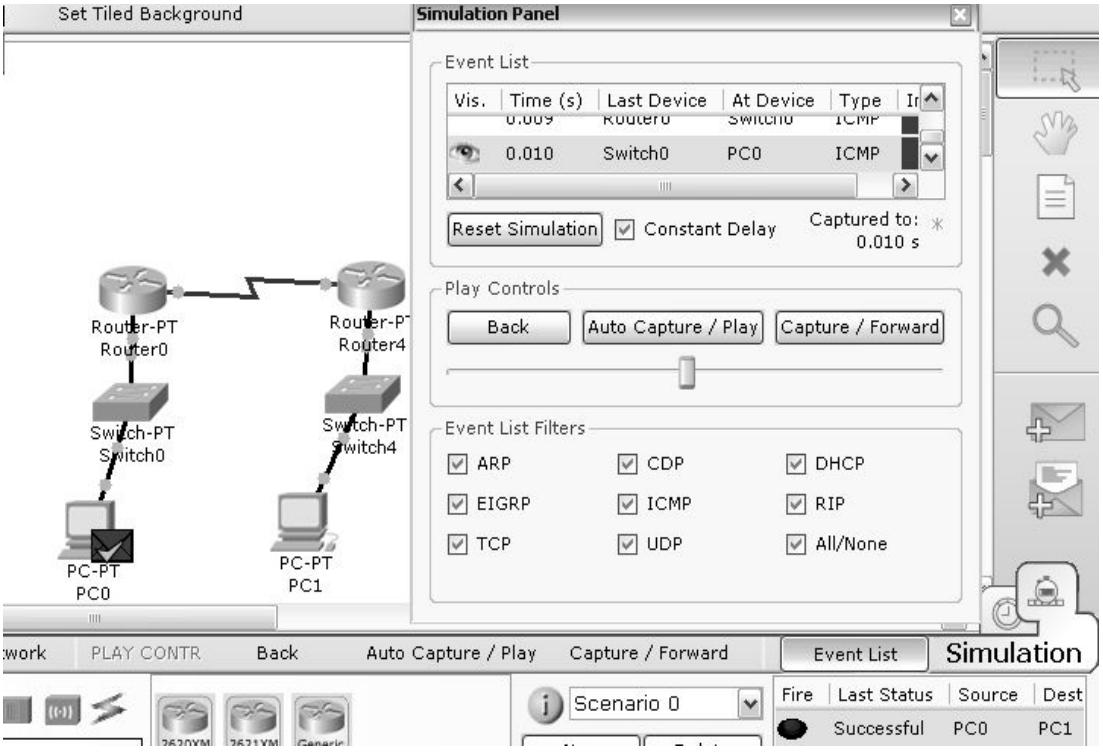


**Fig. 3: An acknowledgement packet is successfully received by PC0.**

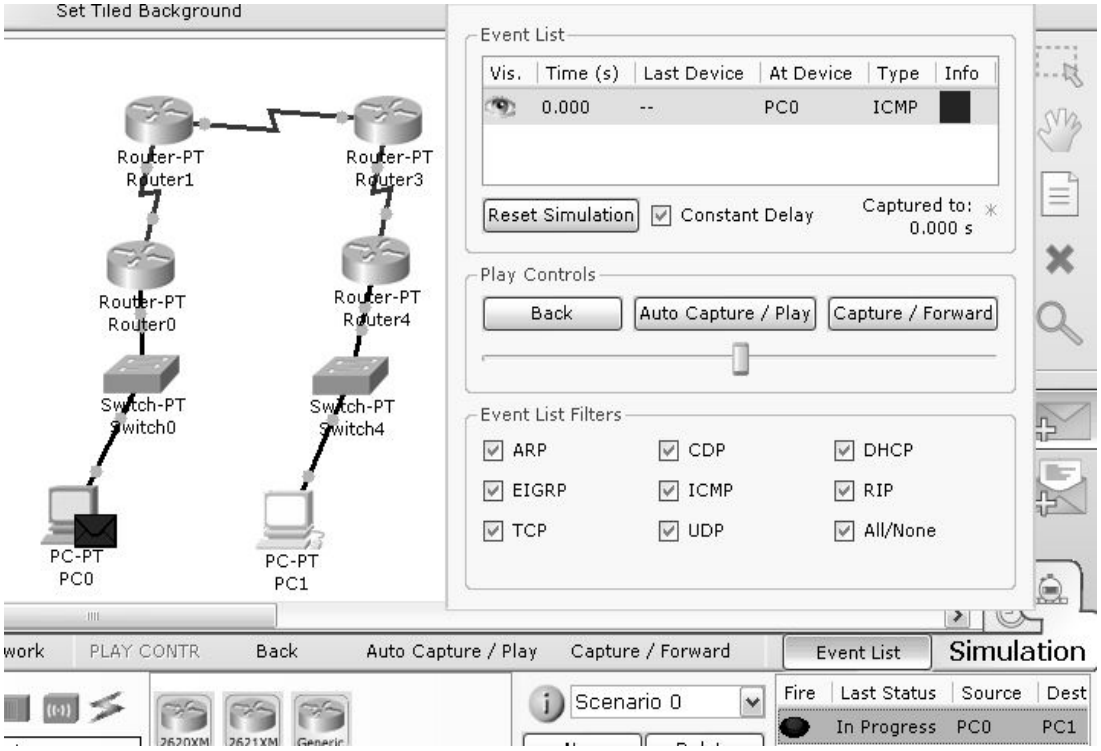


**Fig. 4: A simple PDU is added to PC0.**

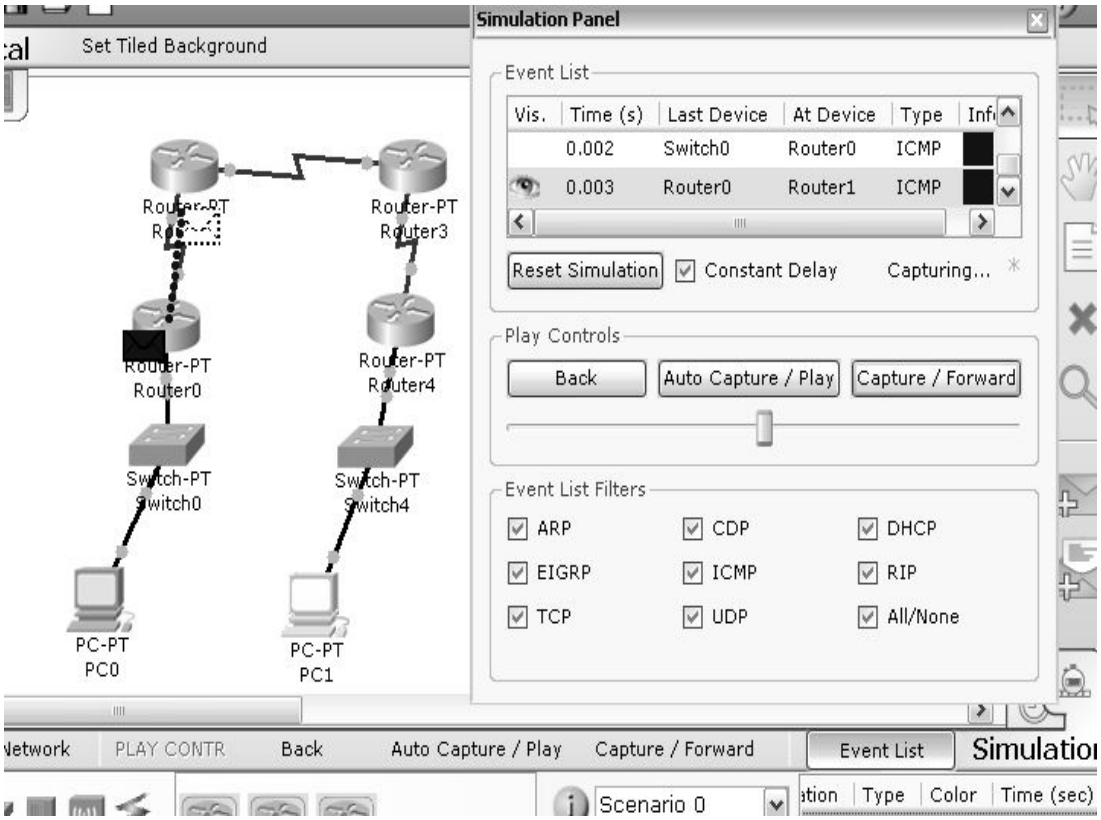


**Fig. 5: The packet is passing to router1 from router0.**

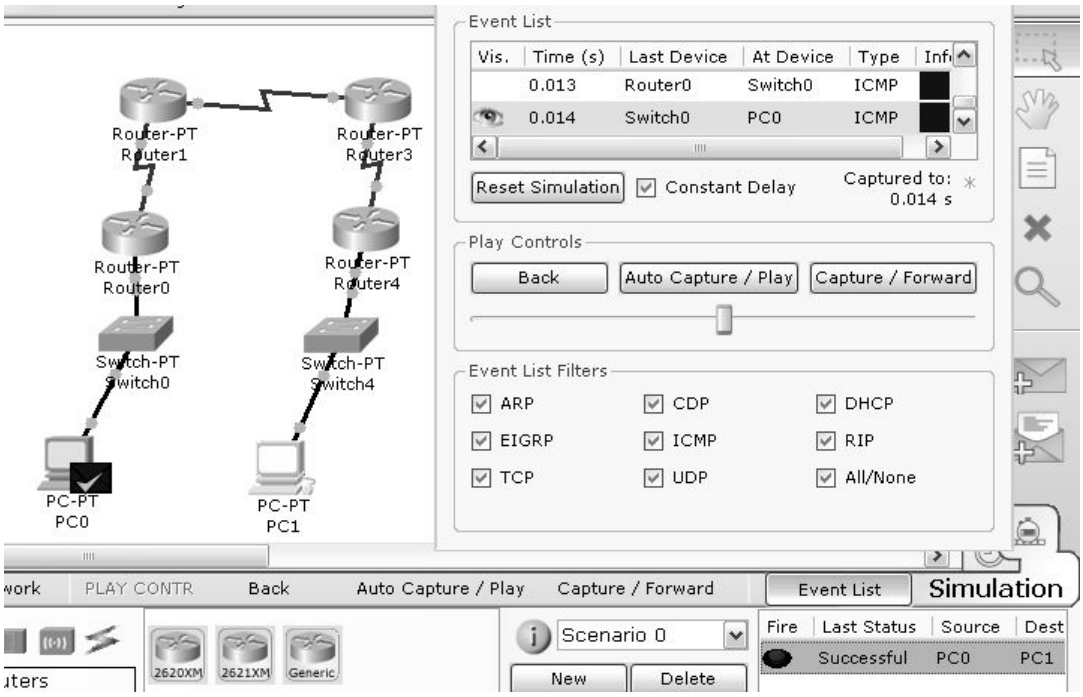


**Fig. 6: An acknowledgement packet is successfully received by PC0.**

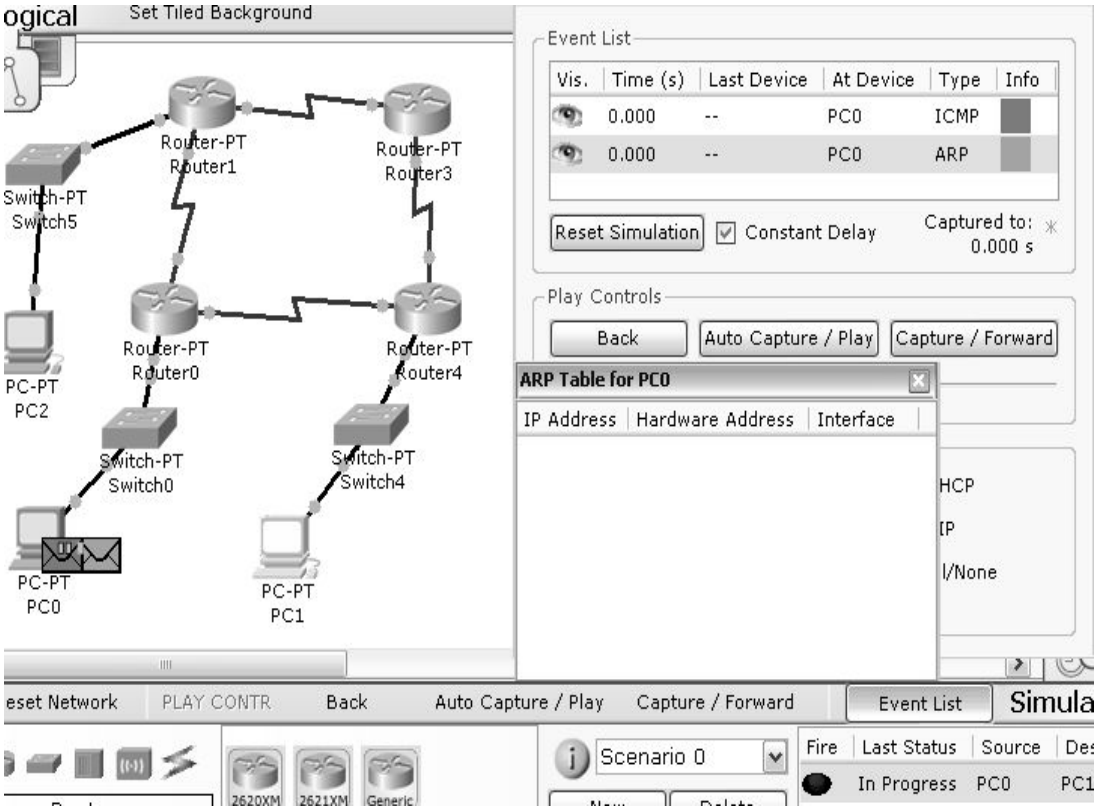


**Fig. 7: ARP packet is created and ICMP packet is discarded.**

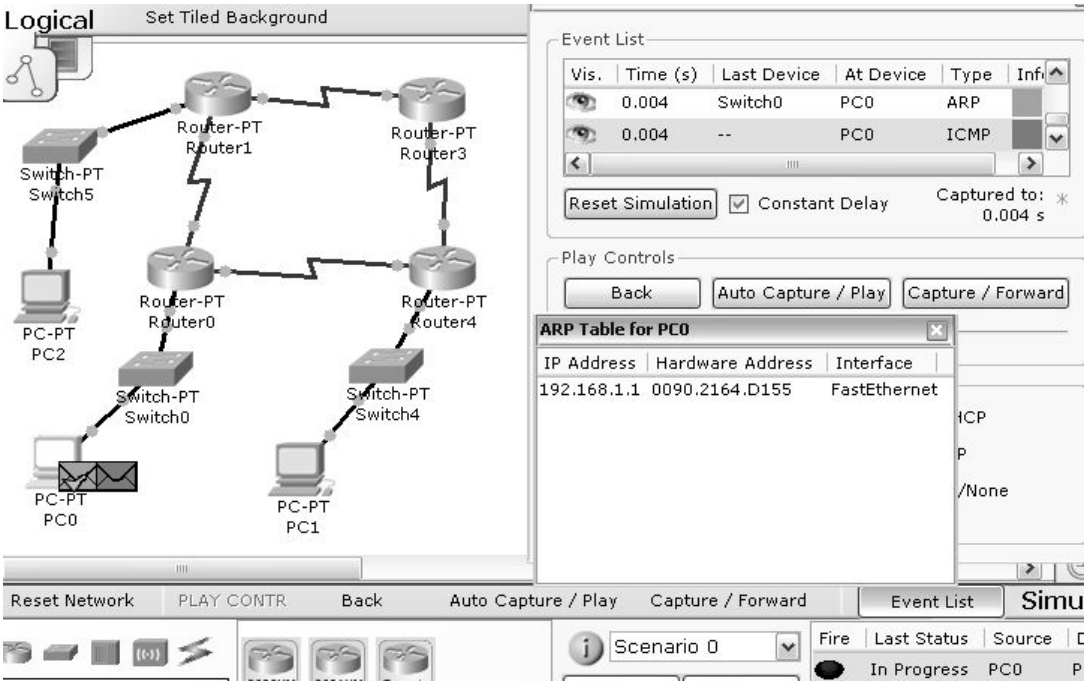


**Fig. 8: After receiving the ARP reply, ICMP packet is created.**

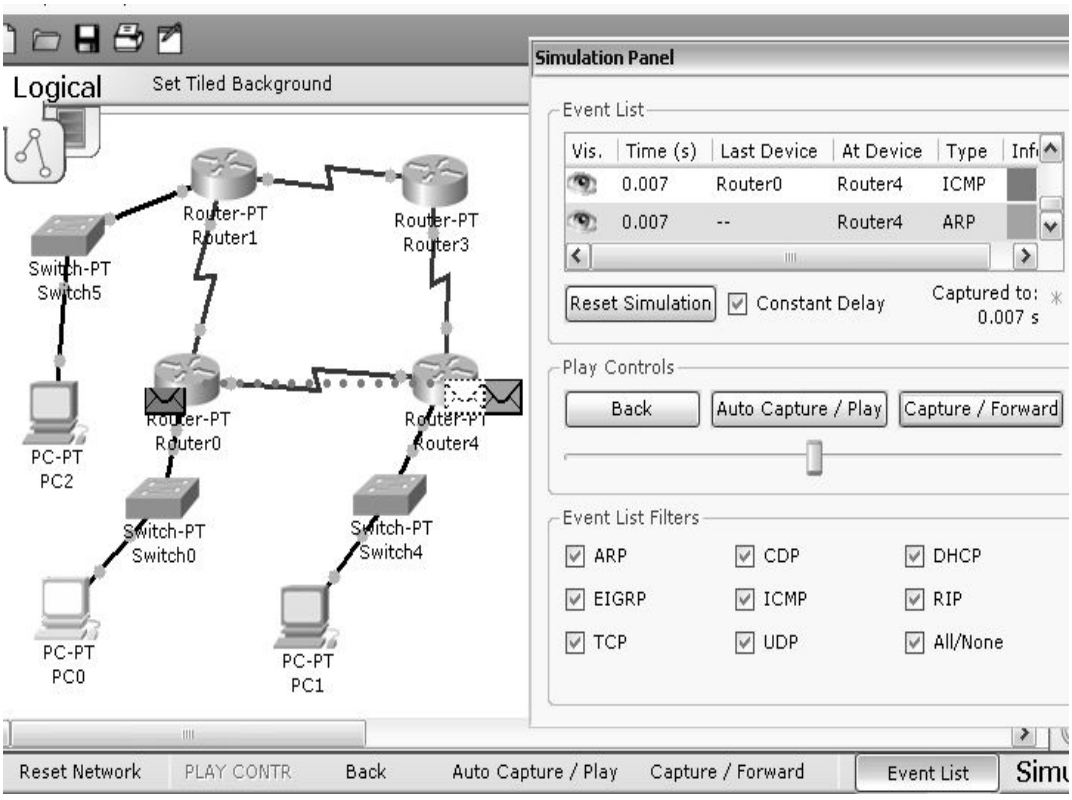


**Fig. 9: ICMP packet is passing to router4 from router0 and ARP packet is again created.**

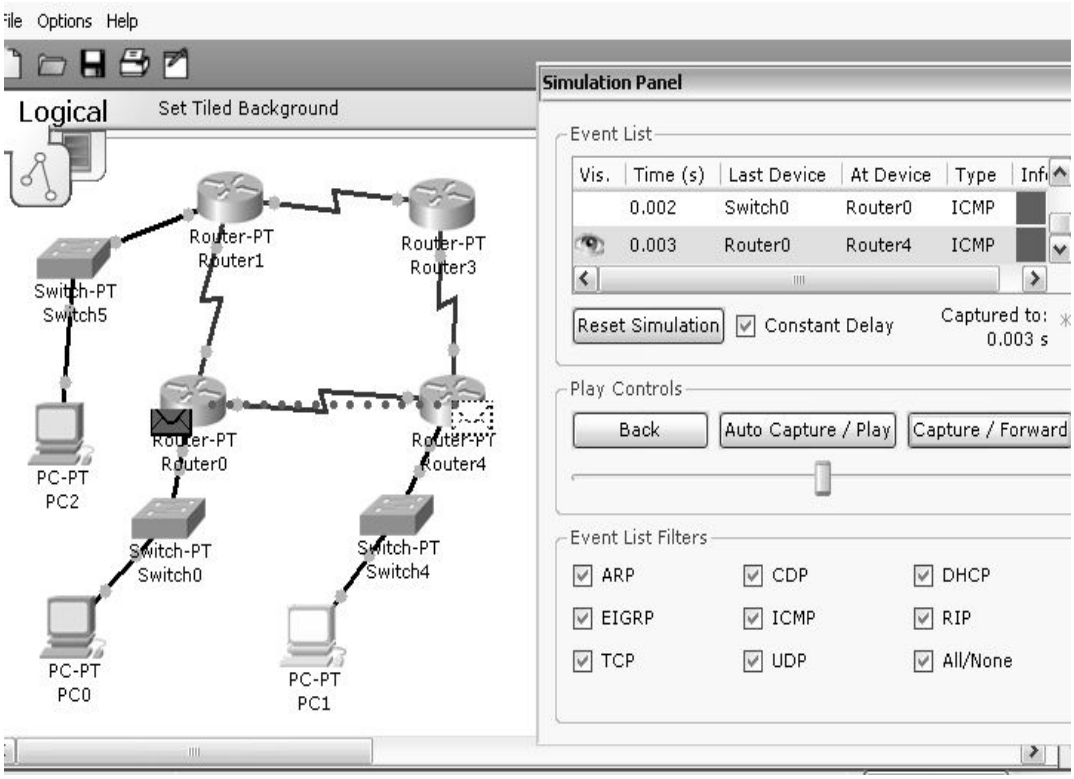


**Fig. 10: ICMP packet is passing to router4.**

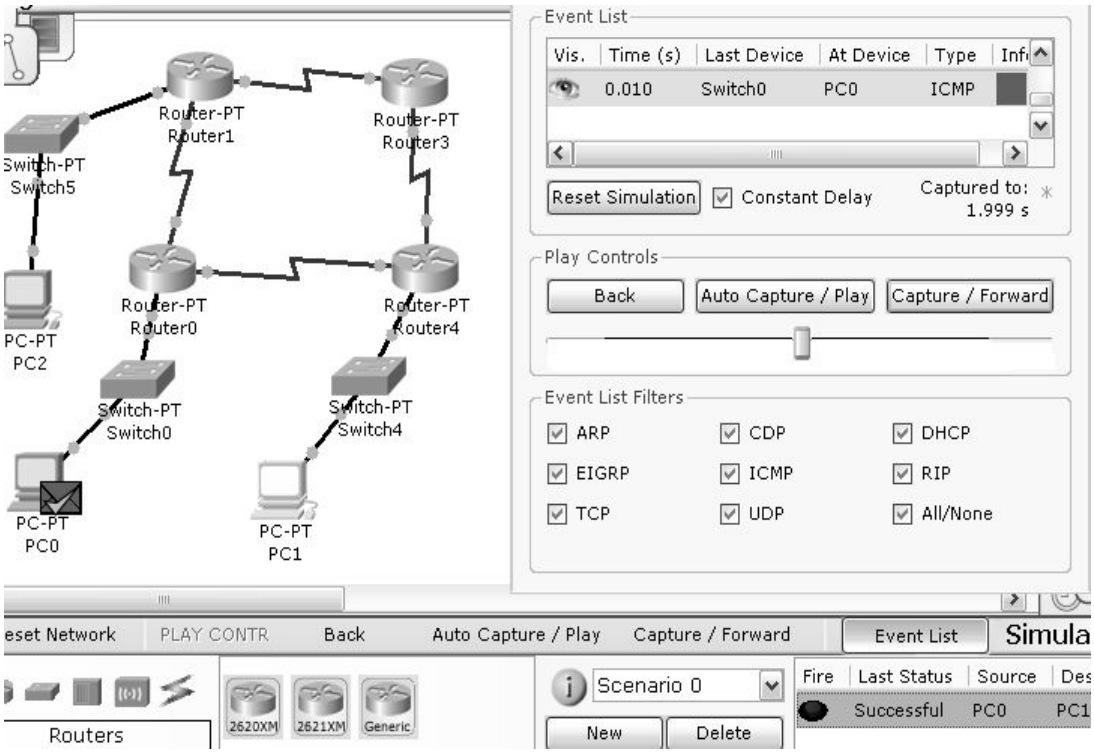


**Fig. 11: An ICMP acknowledgement packet is successfully received.**

## 4. Conclusion

The analysis of shortest path in a packet tracing mechanism is the common thread running through this paper. With a packet trace system we have monitored and displayed packet transferring in a telecommunication network, especially so that faults or errors in the network can be detected quickly and easily. It also allows us to find the shortest path for the router to transfer packet. In this paper, the routing protocols that have been analyzed are the formulas used by routers to determine the appropriate path onto which packet should be forwarded. The routing protocol also specifies how routers report changes and share information with the other routers in the network that they can reach. The changing conditions of the network can be dynamically adjusted by the routing protocols, otherwise all routing decisions have to be predetermined and remain static. Critical terms have been proved by using simulation software in this paper. A user interface has been used to input acceptable packet transfer characteristics. Packet transfer from network to network has been monitored at each step in the simulation which allows us to understand the trace route and find the shortest path in transmission.

## 5. References


[1] Nuno M. Garcia, Przemyslaw Lenkiewicz, Mário M. Freire, Paulo P. Monteiro, "On the Performance of Shortest Path Routing Algorithms for Modeling and Simulation of Static Source Routed Networks – an Extension to the Dijkstra Algorithm", Second International Conference on Systems and Networks Communications (ICSNC 2007).

[2] Applied Research Group, *IP Data Analysis; http:ipmon.sprintlabs.com/packstat/packetoverview.php*

[3] Wesam Lootah, William Enck, Patrick McDaniel, "Ticket-based Address Resolution protocol", 21st Annual Computer Security Applications Conference (ACSAC'05), Issue December 2005, pp. 106-116.

[4] D. C. Plummer. An ethernet address resolution protocol or converting network protocol addresses to 48.bit ethernet address for transmission on ethernet hardware. RFC 826, November 1982.

[5] D. Bruschi, A. Orgnaghi, and E. Rosti. S-arp: a secure address resolution protocol. 2003.

[6] D. Song. dsniff: a collection of tools for network auditing and penetration testing. http://www.monkey.org/ dugsong/dsniff, accessed May 2005.

[7] B. Fleck and J. Dimov. Wireless access points and arp poisoning: Wireless vulnerabilities that expose the wired network. http://downloads.securityfocus.com/library/arppoison.pdf.

[8] S. M. Bellovin. Security problems in the tcp/ip protocol suite. Computer Communications Review, 2(19):32–48, April 1989.

[9] S. M. Bellovin. A look back at "security problems in the tcp/ip protocol suite". In 20th Annual Computer Security Application Conference (ACSAC), pages 229–249, December 2004.

[10] Jui-Fa Chen, Wei-Chuan Lin, Hua-Sheng Bai, Shih-Yao Dai, "A Message Interchange Protocol Based on Routing Information Protocol in a Virtual World", 19th International Conference on Advanced Information Networking and Applications (AINA'05) Volume 2 (INA,, USW,, WAMIS,, and IPv6 papers), March 2005, pp. 377-384.

[11] G. Malkin, "RIP Version 2", RFC2453, November 1998, http://www.rfc-editor.org

[12] J. Hawkinson,"Guidelines for creation, selection, and registration of an Autonomous System (AS)".

[13] J. Postel, RFC 792, "Internet Control Message Protocol," *Internet Engineering Task Force*, Sept. 1981.

[14] ICMP, Internet Control Message Protocol, http://www.erg.abdn.ac.uk/users/gorry/course/inet-pages/icmp.html

[15] Forouzan**,** B. **"**Data Communication and Networking", (4th edition), McGraw Hill 2006.



A.K.M Fazlul Haque is an Assistant Professor in the Department of Electronics and Telecommunication Engineering, Daffodil International University. Currently he is pursuing his Ph.D. in the CSE Department of Jahangir Nagar University in the field of Telemedicine. Mr. Hague's areas of interest include Biomedical Engineering, Communication Engineering, Networking and Digital Signal Processing.