INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH & DEVELOPMENT

ISSN: 2278 – 0211 (Online)

Multiple Routing Configurations For Fast Ip Network Recovery – Using Selective Repeat Automatic-Repeat-Request

Tanveer Fatima
MTech.,computer science
Associate Professor, DRK Institute of Science and Technology, Hyderabad, India
Laxman Vijay
MTech . computer science
academic scholar, DRK Institute of Science and Technology, Hyderabad, India
Chinta Santosh
Mtech . Computer Science
Research Scholar, DRK Institute Of Science And Technology, Hyderabad, India

Abstract:
Internet takes vital role in our communications infrastructure, due to slow convergence of routing protocols after network failure become a budding problem[1]. To assure fast recovery scheme from link and node failure in networks, recovery scheme called Multiple Routing Configuration (MRC)[3] has already been produced , which guarantees recovery in all single failure scenarios, using a mechanism to handle both link and node failures, and without knowing the root cause of the failure[2]. But it does not provide good acknowledgement protocol over the packets forwarded. In this paper, we propose a well enhanced SRARQ[4] protocol during data transmission in IP networks which supports fast retransmission of lost packet data for efficient result.

Key words: *Computer network reliability, protection, flow control, communication system fault tolerance.*

1.Introduction

1.1.Internet

The Internet (or internet)[5][6] is a global system of interconnected computer networks that use the standard Internet protocol suite (TCP/IP) to serve billions of users worldwide. It is a network of networks that consists of millions of private, public, academic, business, and government networks, of local to global scope, that are linked by a broad array of electronic, wireless and optical networking technologies. The Internet carries an extensive range of information resources and services, such as the inter-linked hypertext documents of the World Wide Web (WWW) and the infrastructure to support email. Internet is a short form of the technical term internetwork, the result of interconnecting computer networks with special gateways or routers. This can be known by seeing the figure (1) & figure (2) below.

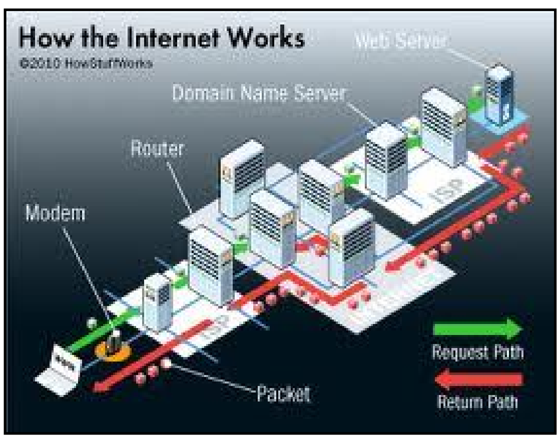

Figure 1

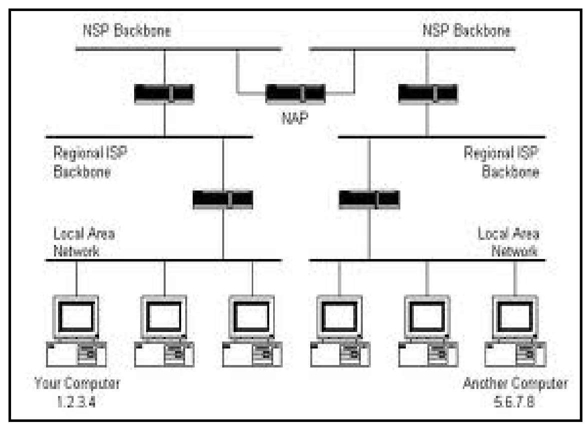

Figure 2

1.2.Dedicated Line

Telephone or cable communications link reserved for one use or for a specific user.

1.3.Router

Interconnecting device that transmits data between two or more networks by determining the best path for them.

1.4.Microwave Relay Station

Facility that receives and amplifies signals transmitted in the form of microwaves and relays them to another receiver.

1.5.Internet User

Person using the internet.

1.6.Modem

Device that converts digital signals into analog signals so that computers can communicate with each other over telephone lines.

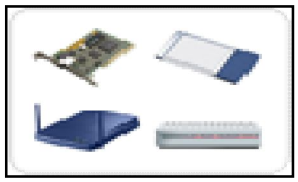

Figure 1

1.7.Telephone line

Linking of two off-site devices by cable within a telephone network.

1.8.Desktop Computer

Small workstation or microcomputer designed for stationary use.

1.9.e-mail software

software used to format, send and receive messages over the internet.

1.10.Browser

Software used to search and consult internet sites.

Figure 2

1.11.Submarine Line

Linking of off-site devices by underwater cable.

1.12.Cable Modem

Modem used to connect a computer to the internet over a cable line.

1.13.Cable Line

Linking of two off-site devices by cable within a cable network.

1.14.Access Server

Communications server that provides subscribers with remote connection to the internet.

1.15.Internet Service Provider

Company that is permanently connected to the internet; it provides individuals and organizations With access to various internet services.

1.16.Server

Computer that hosts various resources (including files, applications and database) and places then at the disposal of all the devices connected to the network.

1.17.Satellite Earth Station

Facility that transmits radio waves to a satellite and receives radio waves from a satellite.

1.18.Telecommunication Satellite

Satellite designed and placed into geostationary orbit to ensure long-range reception and transmission of signals in the form of radio waves.

2.Protocols

The Internet standards describe a framework known as the Internet protocol suite[7]. This is a model architecture that divides methods into a layered system of protocols (RFC 1122, RFC 1123). The layers correspond to the environment or scope in which their services operate. At the top is the application layer, the space for the application-specific networking methods used in software applications, e.g., a web browser program. Below this top layer, the transport layer connects applications on different hosts via the network (e.g., client–server model) with appropriate data exchange methods. Underlying these layers are the core networking technologies, consisting of two layers. The internet layer enables computers to identify and locate each other via Internet Protocol (IP) addresses, and allows them to connect to one another via intermediate (transit) networks. Last, at the bottom of the architecture, is a software layer, the link layer, that provides connectivity between hosts on the same local network link, such as a local area network (LAN) or a dial-up connection. The model, also known as TCP/IP, is designed to be independent of the underlying hardware, which the model therefore does not concern itself with in any detail. Other models have been developed, such as the Open Systems Interconnection (OSI) model, but they are not compatible in the details of description or implementation; many similarities exist and the TCP/IP protocols are usually included in the discussion of OSI networking.

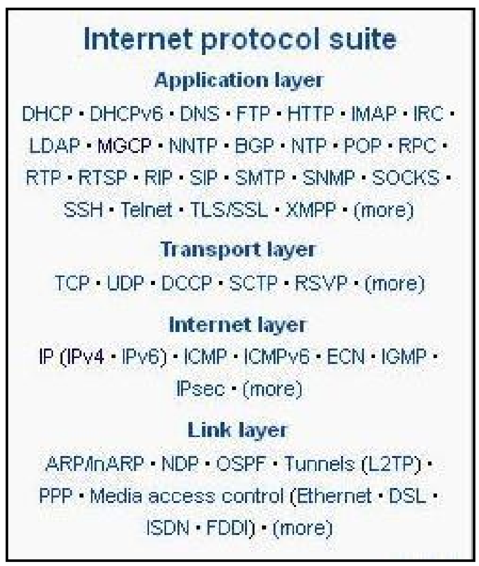

Figure 3

2.1.TCP vs. UDP

2.2.2.<u>Overview</u>

TCP (Transmission Control Protocol)[7] is the most commonly used protocol on the Internet. The reason for this is because TCP offers error correction. When the TCP protocol is used there is a "guaranteed delivery." This is due largely in part to a method called "flow control." Flow control determines when data needs to be re-sent, and stops the flow of data until previous packets are successfully transferred. This works because if a packet of data is sent, a collision may occur. When this happens, the client re-requests the packet from the server until the whole packet is complete and is identical to its original.

UDP (User Datagram Protocol)[7] is anther commonly used protocol on the Internet. However, UDP is never used to send important data such as WebPages, database information, etc; UDP is commonly used for streaming audio and video. Streaming media such as Windows Media audio files (.WMA), Real Player (.RM), and others use UDP because it offers speed! The reason UDP is faster than TCP is because there is no form of flow control or error correction. The data sent over the Internet is affected by collisions, and errors will be present. Remember that UDP is **only** concerned with speed. This is the main reason why streaming media is not high quality.

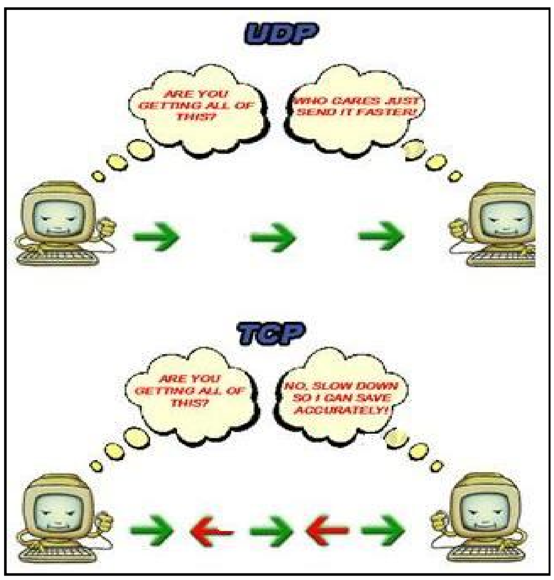

Figure 4

On the contrary, UDP has been implemented among some Trojan horse viruses. Hackers develop scripts and Trojans to run over UDP in order to mask their activities. UDP packets are also used in Doss (Denial of Service) attacks. It is important to know the difference between TCP port 80 and UDP port 80. If you don't know what ports are go here.

2.2.3.Frame Structure

As data moves along a network, various attributes are added to the file to create a frame. This process is called encapsulation. There are different methods of encapsulation depending on which protocol and topology are being used. As a result, the frame structure of these packets differs as well. The images below show both the TCP and UDP frame structures.

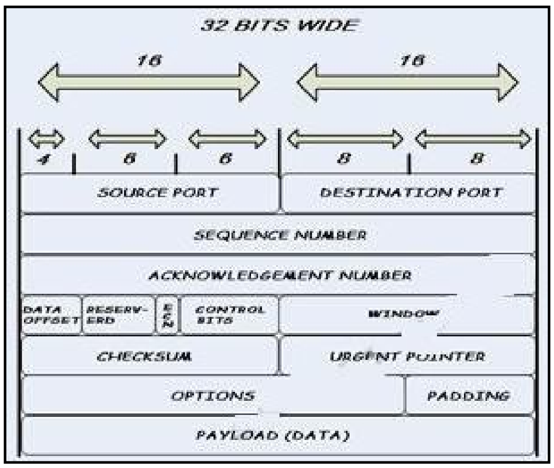

Figure 5 : TCP FRAME STRUCTURE

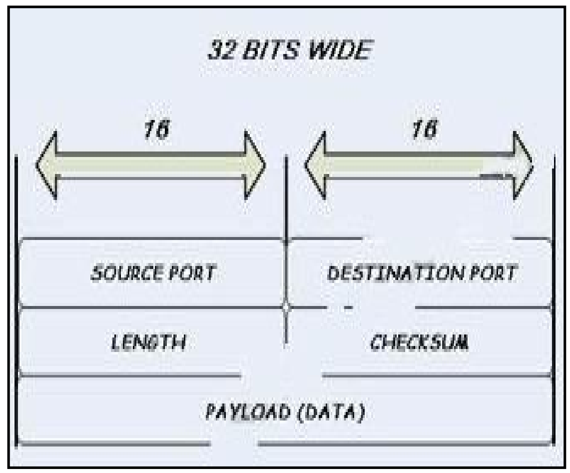

Figure 6: UDP FRAME STRUCTURE

The payload field contains the actually data. Notice that TCP has a more complex frame structure. This is largely due to the fact the TCP is a connection-oriented protocol. The extra fields are needed to ensure the "guaranteed delivery" offered by TCP.

In most networks, there are circumstances in which the externally offered load is larger than can be handled even with optimal routing. Then, if no measures are taken to restrict the entrance of traffic into the network, queue sizes at bottleneck links will grow and packet delays will increase, possibly violating maximum delay specifications. Furthermore, as queue sizes grow indefinitely, the buffer space at some nodes may be exhausted. When this happens, some of the packets arriving at these nodes will have to be discarded and later retransmitted, thereby wasting communication resources. As a result, a phenomenon similar to a highway traffic jam may occur whereby, as the offered load increases, the actual network throughput decreases while packet delay becomes excessive. It is thus necessary at times to prevent some of the offered traffic from entering the network to avoid this type of congestion. This is one of the main functions of flow control. But this flow control mechanism is not properly managed in the existing system of multiple routing configurations for fast IP network recovery. Why because, in MRC mechanism whenever a failure happens in the network it can generate an alternate link immediately by using preconfigured data and the packets are forwarded through that rout and continuous the network flow. As when the packet routes to other link when failures occurs, as that link also has its sufficient data packet to pass to the receiver as suddenly it comes makes more load therefore as it is using go-back-n technique if any data error occurs it rejects all frames and produce negative acknowledgement so that the sender must retransmit all the frames, but mean while the load suddenly which comes from other link when gets failed will also enter into in the queue to transmit to the user, as a receiver must quit all other data till it receives the error free data which leads to increase in queue size and makes congestion and may lose the data due to unproper flow control or another reason is that when the sender is running fast machine and receiver is on slow machine may lose the data. Therefore to prevent this proper flow control mechanism called SRARQ is incorporated which includes a feedback mechanism requesting transmitter a retransmission of only incorrect message block.

3.Srarq Overview

This powerful (i.e. SRARQ)[4] flow control mechanism is also sometimes necessary between two users for speed matching (i.e. for ensuring a fast transmitter does not overwhelm a slow receiver with more packets). Some others reserve the term “flow control” for this type of speed matching and use the term “congestion control” for regulating the packet population within the sub network. In this protocol receiver will have sufficient buffer space unlike go-back-n. If receiver receives any damages or error containing frame it will generates negative acknowledgement of that frame and it will stores correct frames in its buffer. When sender get negative acknowledgement of damaged or error containing frame its timer goes off after a certain time interval and it regenerate only the damaged frame. Thus there is less overhead in retransmission than in the case of go-back-n protocol.

3.1.Diagram

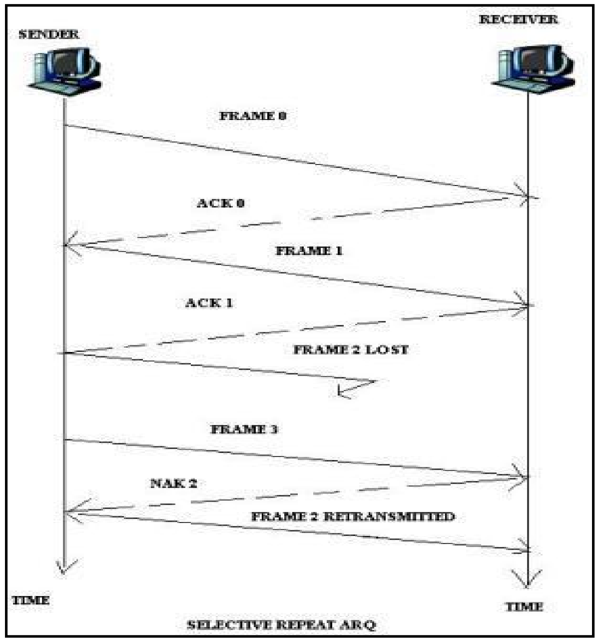

Figure 7: A sliding window protocol using selective repeat.

4.Algorithm

while (true) {

wait3for3event(&event); /* five possibilities: see event3type above */

switch(event) {

case network3layer3ready: /* accept, save, and transmit a new frame */

nbuffered = nbuffered + 1; /* expand the window */

from3network3layer(&out3buf[next3frame3to3send % NR3BUFS]); /* fetch new packet */

send3frame(data, next3frame3to3send, frame3expected, out3buf);/* transmit the frame */

inc(next3frame3to3send); /* advance upper window edge */

break;

case frame3arrival: /* a data or control frame has arrived */

from3physical3layer(&r); /* fetch incoming frame from physical layer */

if (r.kind == data) {

/* An undamaged frame has arrived. */

if ((r.seq != frame3expected) && no3nak)

send3frame(nak, 0, frame3expected, out3buf); else start3ack3timer();

```
if (between(frame3expected, r.seq, too3far) && (arrived[r.seq%NR3BUFS] == false)) {
/* Frames may be accepted in any order. */
arrived[r.seq % NR3BUFS] = true; /* mark buffer as full */
in3buf[r.seq % NR3BUFS] = r.info; /* insert data into buffer */
while (arrived[frame3expected % NR3BUFS]) {
/* Pass frames and advance window. */
to3network3layer(&in3buf[frame3expected % NR3BUFS]);
no3nak = true;
arrived[frame3expected % NR3BUFS] = false;
inc(frame3expected); /* advance lower edge of receiver's window */
inc(too3far); /* advance upper edge of receiver's window */
start3ack3timer(); /* to see if a separate ack is needed */
}
}
}
if((r.kind==nak) &&
between(ack3expected,(r.ack+1)%(MAX3SEQ+1),next3frame3to3send))
send3frame(data, (r.ack+1) % (MAX3SEQ + 1), frame3expected, out3buf);
while (between(ack3expected, r.ack, next3frame3to3send)) {
nbuffered = nbuffered − 1; /* handle piggybacked ack */
stop3timer(ack3expected % NR3BUFS); /* frame arrived intact */
inc(ack3expected); /* advance lower edge of sender's window */
}
break;
case cksum3err:
if (no3nak) send3frame(nak, 0, frame3expected, out3buf); /* damaged frame */
break;
case timeout:
send3frame(data, oldest3frame, frame3expected, out3buf); /* we timed out */
break;
case ack3timeout:
send3frame(ack,0,frame3expected, out3buf); /* ack timer expired; send ack */
}
if (nbuffered < NR3BUFS) enable3network3layer(); else disable3network3layer();
```

}

}

5.Main Objectives Of Srarq

- Selective repeat ARQ retransmits only the damaged or lost frames instead of sending multiple frames.
- Keeping average delay and buffer overflow at reasonable level.
- Maintain fairness between sessions and providing the requisite quality of service (QOS).
- The selective retransmission increases the efficiency of transmission and is more suitable for noisy channel.

6.Implementation

The implementation of SRARQ for network recovery mainly uses Two modules.

- Client Module 2. Sever Module
- Client
- This module is used to send the data to server through routers. It will provide user friendly interface to send the data to the required destination.
- Server
- It will receive the data send by the client which came from the active router. It can have any no. of clients.

7.Conclusion

We have presented SRARQ as an approach to achieve congestion control in ip-network. This SRARQ maintains a buffer space, to store all the correct frames in its buffer other than unlike go-back-n and generates negative acknowledgement of that only the damages or error containing frame. Which provides best flow control and efficient transmission of data.

8.Reference

1. D. D. Clark, “The design philosophy of theDARPAinternet protocols,” ACM SIGCOMM Comput. Commun. Rev., vol. 18, no. 4, pp. 106–114, Aug. 1988.
2. A. Markopoulou, G. Iannaccone, S. Bhattacharyya, C.-N. Chuah, and C. Diot, “Characterization of failures in an IP backbone network,” in Proc. IEEE INFOCOM, Mar. 2004, vol. 4, pp. 2307–2317.
3. Amund Kvalbein, Audun Fosselie Hansen, Tarik ˇ Ciˇcic, SteinGjessing and Olav Lysne “Multiple Routing Configuration For Fast IP Network Recovery” IEEE/ACM Transactions on networking, Vol. 17, No. 2, April 2009.
4. Automatic-repeat-request error-control schemes. Shu Lin, Costello, D. Miller, M. This paper appears in: Communications Magazine, IEEE Publication Date: Dec 1984.
5. B. Carpenter, “Architectural Principles of the Internet,” RFC 1958 (Informational), June 1996, updated by RFC 3439. [Online]. Available:http://www.ietf.org/rfc/rfc1958.txt.
6. Tommy Andre, Skancke nyquist, “Evaluating local proactive recovery schemes for ip networks” Master thesis.
7. Braden, R., Requirements for Internet Hosts { Communication Layers IETF Request for Comments: 1122, 1989.