Secured LAN Network Topology of a Small Office with Redundancy

Uzmasaman Aejaz Chanderki

Trainee Engineer, Prasar Bharti, All India Radio, Mumbai.

***Abstract** - In today's time whether the office size is large or small security is must. Most of the offices compromise their security for some reason. Security as well as backup goes hand in hand. The proposed system is combination of a LAN network topology which will have security of the data flow using MD5 which strong yet pocket friendly cryptography method. The LAN network will also have a backup router which will act as standby when the active router goes down using Hot Standby Routing Protocol. This will provide interruption free work.*

Keywords- LAN network topology, Router, switch, MD5, backup protocol, HSRP.

1. INTRODUCTION

Small commercial offices also has their own confidential files that needs to protected but the data flow is in original which can be hacked and manipulated by anyone.

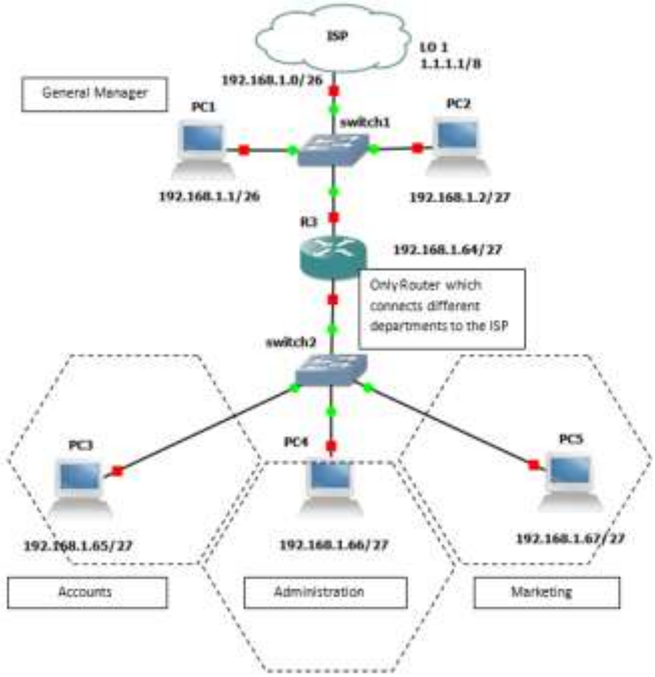


Fig: 1.1 Typical Topology of small office

With security backup is needed to assure that when the active router goes down by any reason it has a backup to have an interruption free work without any data loss. The proposed system is designed with a view of providing backup as well as security for a LAN network Topology The proposed system of small office network will have 4 departments for demonstration and ease purpose. The figure above shows the Network design without backup and security. The data flow is in its own format and Router 3 is backbone of the network which joins ISP and departments. It needs a standby Router when it turns down.

The security can be provided by doing encryption and decryption of end to end data using Message Digest 5 which is one of the strongest Cryptography methods. The hacker needs to spend & years to decode it which is not feasible for anyone. Implementation of MD5 is quite simple.

The redundancy is provided by a backup routing protocol known as HSPR which will run in background and check router status. If this Protocol didn't exist gateways needs to be added to each and every system which is again not possible in any way. The further section will discuss MD5, HSPR and its use in new system in great detail.

2. METHODOLOGY

Hot standby routing protocol is a Cisco proprietary. In this we have active and standby concept.

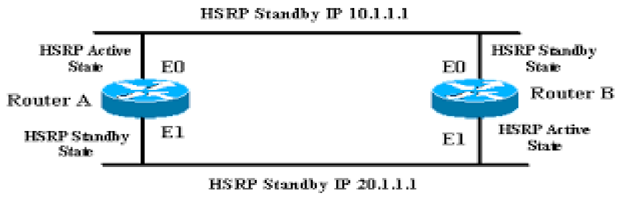


Fig: 2.1 HSRP

Whichever router is run first with HSRP command will be active other will be its standby. A virtual IP address is used as Gateway for all end users. The standby router comes to know that active router is alive by a constant 'hello' sent every 3 seconds. If these 3 seconds are missed it will wait for another 10 seconds and turns itself into active router. The highest priority is checked in order to get the crown of 'active' router. The priority can be manipulated using few commands.

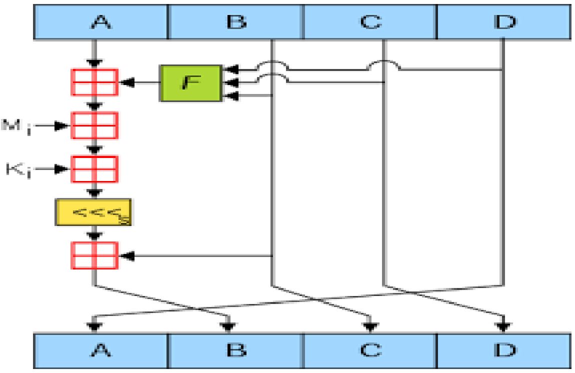


Fig: 2.2 Message Digest 5

The MD5 message-digest algorithm is a widely used hash function provides a 128-bit hash value. MD5 has been deprecated for uses other than as a non-cryptographic checksum to verify data integrity and detect unintentional data corruption.

3. PROPOSED SYSTEM

The designed topology is prototype with limited end devices for demo purpose. IP addresses taken are simple. The routers used are c3725 and switch is Ethernet switch. After basic IP addressing the routing protocol used is RIP version 2. Rip is run on all the protocols. In order to check if the routing protocol works fine we have pinged a loopback interface 1.1.1.1 created on ISP for testing purpose.

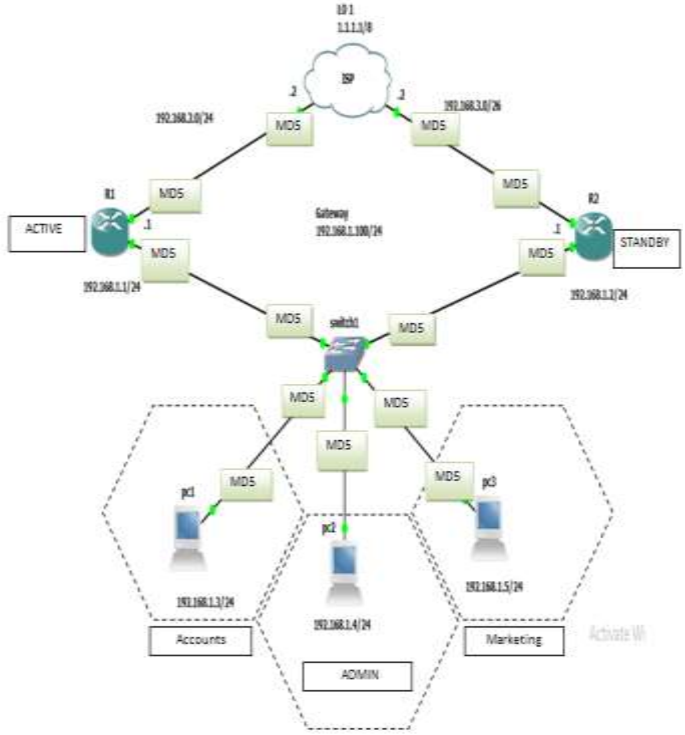


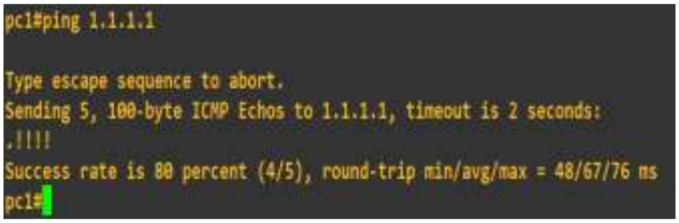
Fig: 3.1 The proposed network design

The data flow will be in form of MD5 format which will be decrypted at end user. There are two routers connected in between ISP and end user. They both will not be active but only 1 will be in force and other will be backup. HSRP protocol will be run on the interface facing end user on each of these routers.

4. RESULTS

A. HSPR

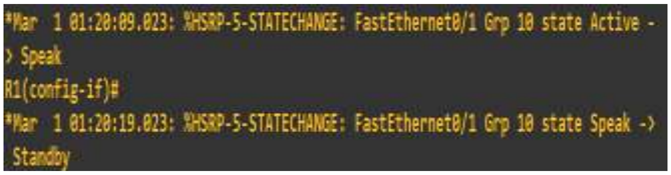
After doing basic IP addressing and setting up routing protocol 'ping' from PC1 to ISP Loopback interface is given to check data flow or path.



```
pc1#ping 1.1.1.1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 1.1.1.1, timeout is 2 seconds:
.!!!!
Success rate is 80 percent (4/5), round-trip min/avg/max = 48/67/76 ms
pc1#
```

Fig: 4.1 Testing from PC1 to Loopback

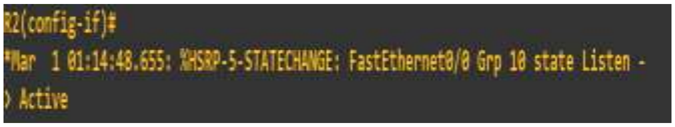
When the path is set all over topology HSPR needs to be set on router 1 and 2 interfaces.



```
*Mar  1 01:20:09.023: %HSRP-5-STATECHANGE: FastEthernet0/1 Grp 10 state Active -
> Speak
R1(config-if)#
*Mar  1 01:20:19.023: %HSRP-5-STATECHANGE: FastEthernet0/1 Grp 10 state Speak ->
 Standby
```

Fig: 4.2 Logs

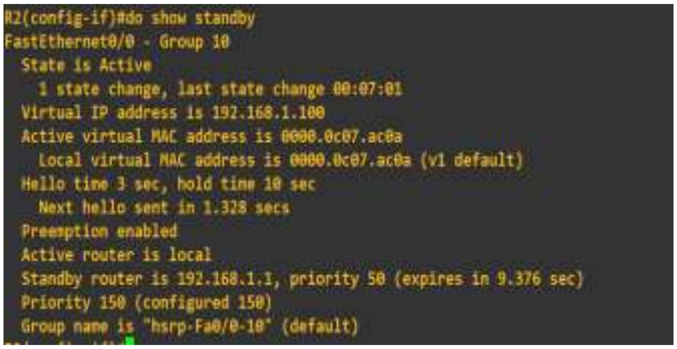
As soon as HSRP commands are given to the first router it consider himself as active one but as soon as router 2 comes in race highest priority wins. Here router 1 has lesser priority than router 2 so it is a standby router.



```
R2(config-if)#
*Mar  1 01:14:48.655: %HSRP-5-STATECHANGE: FastEthernet0/0 Grp 10 state Listen -
> Active
```

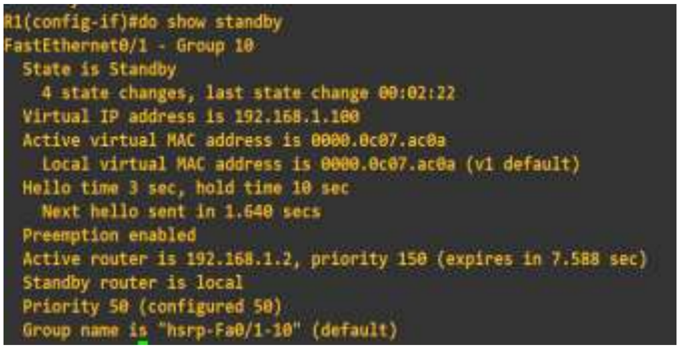
Fig: 4.3 Logs

In order to check the status of the routers there is a verification command 'show standby'.



```
R2(config-if)#do show standby
FastEthernet0/0 - Group 10
  State is Active
    1 state change, last state change 00:07:01
  Virtual IP address is 192.168.1.100
  Active virtual MAC address is 0000.0c07.ac0a
    Local virtual MAC address is 0000.0c07.ac0a (v1 default)
  Hello time 3 sec, hold time 10 sec
    Next hello sent in 1.328 secs
  Preemption enabled
  Active router is local
  Standby router is 192.168.1.1, priority 50 (expires in 9.376 sec)
  Priority 150 (configured 150)
  Group name is "hsrp-Fa0/0-10" (default)
```

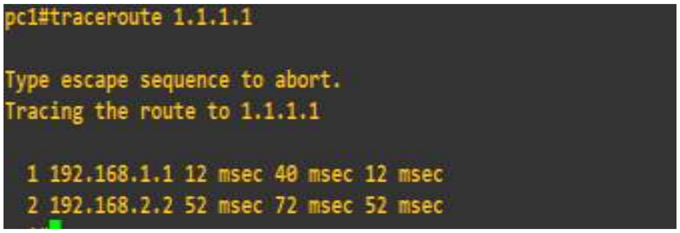
Fig 4.4 Router 2 verification



```
R1(config-if)#do show standby
FastEthernet0/1 - Group 10
  State is Standby
    4 state changes, last state change 00:02:22
  Virtual IP address is 192.168.1.100
  Active virtual MAC address is 0000.0c07.ac0a
    Local virtual MAC address is 0000.0c07.ac0a (v1 default)
  Hello time 3 sec, hold time 10 sec
    Next hello sent in 1.640 secs
  Preemption enabled
  Active router is 192.168.1.2, priority 150 (expires in 7.588 sec)
  Standby router is local
  Priority 50 (configured 50)
  Group name is "hsrp-Fa0/1-10" (default)
```

Fig: 4.5 Router 1 verification.

This will show every detail likes priority, hell timer, MAC address so on.

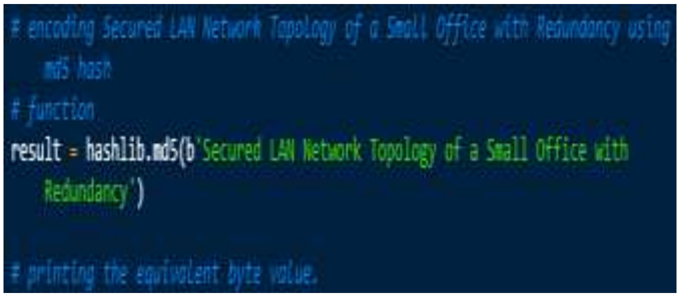


```
pc1#traceroute 1.1.1.1

Type escape sequence to abort.
Tracing the route to 1.1.1.1

  1 192.168.1.1 12 msec 40 msec 12 msec
  2 192.168.2.2 52 msec 72 msec 52 msec
```

Fig: 4.6 Data Flow Path

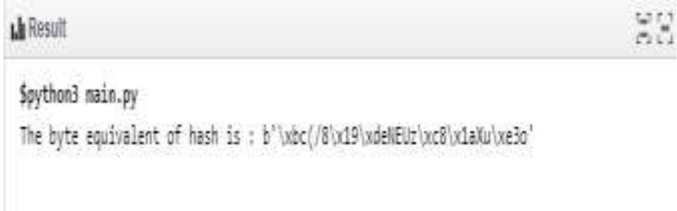
B. MD5 python

Implementing MD5 using Python 3.



```
# encoding Secured LAN Network Topology of a Small Office with Redundancy using
    md5 hash
# function
result = hashlib.md5(b'Secured LAN Network Topology of a Small Office with
    Redundancy')


# printing the equivalent byte value.
```

Fig: 4.7 Encrypting data using MD5



```
$python3 main.py
The byte equivalent of hash is : b'\xbc(/8\x19\xdeNEUz\xc8\x1aXu\xe3o'
```

Fig: 4.8 Encrypted data in MD5

5. CONCLUSION

This network topology can further be modified by using advance cryptography and using biometric and AI authentication. VRRP protocol can also be used whose timer is less and faster than HSRP. Active and standby Method can be avoided using Active-Active method which is provided by IGP Protocol to give even faster result. Authentication can be setup in individual routers and ports so that no one manipulates the commands in global mode.

REFERENCES

[1] R. Rivest. The MD5 Message-Digest Algorithm [rfc1321]

[2] Tao Xie and Dengguo Feng (30 May 2009). How to Find Weak Input Differences for MD5 Collision Attack.

[3] Rivest R L. The MD5 message digest algorithm [EB/OL].

[4] Xiaoyun Wang, Dengguo, k., m., m, H A V A L- 1 2 8 a n d R IP E M D] , Cryptology ePrint Archive Report 2004/199, 16 August 2004,

[5] J. Black, M. Cochran, T. Highland: A Study of the MD5 Attacks: Insights and Improvement, March 3, 2006

[6] Gray, Paul, Guide to IFPS (Interactive Financial Planning System), Second Edition, McGraw-Hill Book Company, New York, 1987.

[7] Welford, A. T., Reaction Times, University of Adelaide, Adelaide, Australia, 1980.

[8] Miller, L. H., "A Study In Man Machine Interaction", National Computer Conference, 1977.

[9] Barry H. and Sorkin, Robert D., Human Factors: Understanding People-System Relationships, John Wiley and Sons, 1983.

[10] Miller, Robert B., "Response Time in Man-Computer Conversational Transitions", AFIPS Conference Proceedings, Volume 33, Part 1, AFIPS Press, Montvale, New Jersey, 1968.

[11] Handbook of Perception and Human Performance, Volume 1, "Reaction Times and Speed-Accuracy Trade-off", John Wiley and Son's, 1986.

[12] Garrison, Ray H., Managerial Accounting, Fifth Edition, Business Publications, Inc., Plano, Texas.