PHYSICAL SECURING OF AN OPTICAL RING NETWORK BY USING THE REDUNDANCY

Andreea-Gabriela COJOCARU, Marian ALEXANDRU

Transylvania University, Brasov, Romania (gabrielaandreea25@yahoo.com, marian.alexandru@unitbv.ro)

DOI: 10.19062/1842-9238.2017.15.1.9

Abstract: *A voice communication testing through a ring topology based on fiber optics is presented in this paper. The data packets were forwarded to an alternate route, without call interruption, in case of physical link failure. The alternate route was chosen by Spanning Tree Protocol Loop Guard. The protocol is specific to the tree topology, and this study shows the accuracy of a ring topology. A small network was created to test the protocol's efficiency, but the solution should be implemented in complicated networks with high traffic.*

Keywords: *network, security, ring topology,spanning tree protocol, loop guard*

1. INTRODUCTION

The concept of telecommunication represents the transfer of information from an emission source to a power receiver via a link. To make the connections a physical environment can be used, like copper or fiber optic cables, or by means of wireless media such as radio links or infrared waves.

In a world surrounded by advanced technology systems, the most important attributes are efficiency and speed of transmission. However, there are various factors that prevent good communication such as failure of terminals, interruption of the line caused by third parties or redundancy factors like software overhead.

To ensure the network functions properly, it is being taken into account the safety devices on the network, especially for the transmission medium.

Over time, the size of a network has grown substantially, which resulted in the development of different configurations and new topologies.

There is no value in not having the information sent correctly via the network or having it being read by unauthorized individuals [2]. The latter consitutes a serious security breach.

Many network attacks are from the inside and because it is very difficult to keep a record of all entities and all operations that are used at a time, it is a hard task to manually manage a network, in an efficient way [3].

Complexity is cause by several factors, which may include geographical dispersion and involving several organizations to ensure the network integrity or safety. Other causes may includ the existence of devices and different operating systems, a large number of entities in the network, etc.

There are several network topologies from which, the ring and mesh are well suited for providing protection.

The ring topology distinctive mark is that all the nodes are connected in succession, and the last one is connected to the first node.

Each node receives the transmitted signal and forwards it to the next one from the loop, keeping a copy of the message, if it is intended. The message will be removed from the loop when it will return to the node from where it was sent. To control access to the network, a token is used, which means that the node that is bound to send the token further, is the only one that has the right to do so [1].

In case of system failure, the desired behavior is to not interrupt the cycle, therefore, each node has a passive bypass mechanism.

The data transmission inside a ring topology is circular and the information is transferred between devices in a single way. So, each device from that ring is like a repeater. It become a receiver for the node, from which it receives the message, and a signal transmitter for the node, where the message is being sent [5].

An important advantage of this method is that each node sends data only when it receives an available token. This way, the number of colisions is reduced. Even if new devices are being added, each one has the same resources access type - the network performance will still be better than the bus topology. More than this, there is no need for a network server to control the connexions between devices.

The ring topology has some disadvantages, like the transmission of data packets is being done through all devices which have their sources and destinations connected. If a port is inactive, it affects the entire network. Also, the network is strictly dependent on the network cable that connects different components.

For that situations when a link is interrupted, there are implemented protocols which switch the traffic automatically. This way, the data transfer is able to be continued. One of the most known protocols for the switching traffic is STP (Spanning Tree Protocol).

STP is a link management protocol between components which take part of OSI layer 2 (Open System Interconnection). This protocol generates alternative routes preventing the loop links and it creates links between terminals by choosing the route with the lowest cost [6].

The protocol defines a tree with a root switch and links without loops. If a network link is interrupted and an alternative route is available, then the traffic is transferred on the alternative link. To create this route, the algorithm takes into account the port priority and the cost between ports [4].

Additional configurations can be made for the spanning tree protocol, like the one for STP Loop Guard. The protocol efficiency is seen when the entire network is implemented. If the operating mode is PVST (Per VLAN Spanning-Tree), Loop Guard prevents the root or the alternate ports from becoming designated ports when an unidirectional link is interrupted, and the spanning-tree doesn’t send BPDUs (Bridge Protocol Data Unis) on this ports [7]. If the chosen mode is MST (Multiple Spanning Tree Protocol), and the port is blocked by Loop Guard in all MST instances, BPDUs are not sent on nonboundary ports. If there is a boundary port, Loop Guard blocks it in all MST instances [7].

Also, starting from STP, there are other automatic routing protocols involved and used in a ring topology like MSTP (Multiple Spanning Tree Protocol), RSTP (Rapid Spanning Tree Protocol) and REP (Resilient Ethernet Protocol).

2. COMMUNICATION SYSTEM SETUP AND TESTING

In this study, the voice communication was tested in a ring topology based on fiber optics.

In order to build the communication system, the next components were needed: 3 switches Cisco Catalyst 2950SX-24, 6 media converters StartBitCom, a console cable, UTP cables, optical fiber cable, 2 laptops as terminals and a virtual PBX (Private Branch eXchange).

Between terminals a VoIP (Voice Over IP) call was generated, which had to keep in touch when the fiber optic was interrupted intentionally. For these things to be possible, the Spanning Tree Protocol Loop Guard was used.

As it was mentioned before, the Loop Guard method prevents the alternate or root ports from becoming designated when a unidirectional connection is interrupted.

An advantage of STP is being able to be activated even the switch is working in the PVST or MSTP mode. Also, Loop Guard is working only with the ports which are considered point-to-point by STP [7].

The pair of media converters is able to convert an electrical signal from a FastEthernet port, of the source switch, into an optical signal and then convert it back into an electrical signal, to forward data to a FastEthernet port, of the target switch. One of this media converters was configured to have its transmission wavelength set to 1550nm and the reception wavelength set to 1310nm. The second media converter was set to send data on 1310nm and to receive data on 1550nm.

For the switch configuration a console cable was needed. The terminal used in this study, didn't have a serial interface. In this case, a USB to RS232 DB9 serial adapter cable was used.

In the Fig. 1 the media converters for the 2nd switch are presented. The black cable connects the first switch to a media converter and the gray cable connects the third switch to the other media converter.

In figure the Fig. 2 the network structure is presented. The switches were connected with the media converters and the terminals through UTP (Unshielded Twisted Pair) cables. The media convertors (MC) were interconnected through optical fiber cable.

For testing the network, the Axon Virtual PBX Windows Software [8] and the Express Talk VoIP Softphone for Windows [9], both developed by NCS Software, were installed. The PBX software supports up to 64 lines and an unlimitted number of extensions. The chosen softphone is able to make audio and video calls.

(a) (b)

FIG. 1. a), b) Media convertors

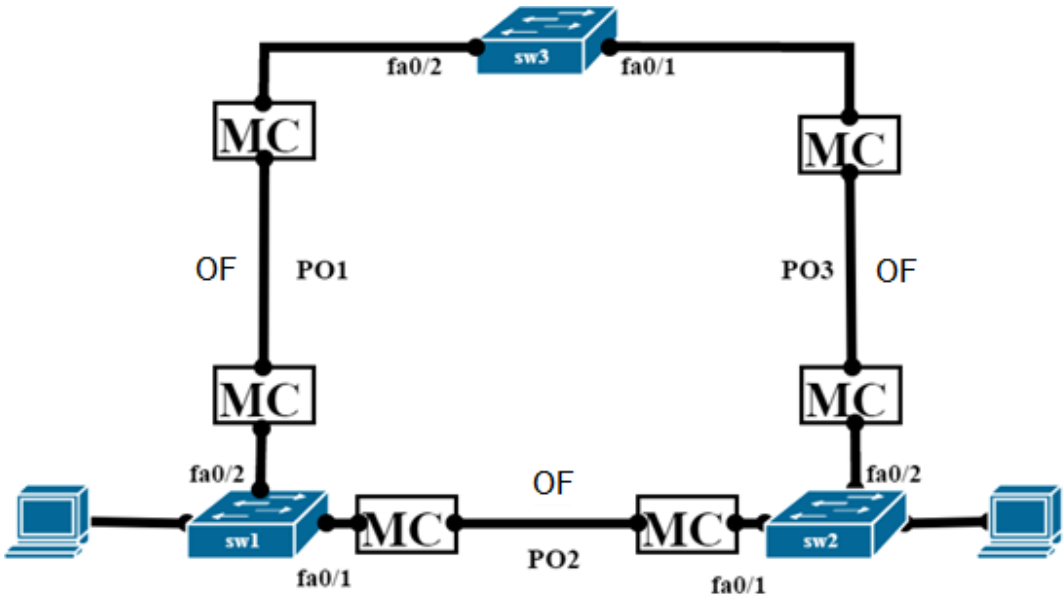


FIG. 2. Network connections

To clarify the test process, it is mentioned that one terminal is connected to the 1st switch and the other terminal is connected to the 2nd switch. Initially, the data traffic was carried out on the PO2 interface due to having the lowest cost. Also, the alternate route – composed from the PO1 and PO3 interfaces – had blocked ports not being able to transfer data through them.

The information was sent only through the port, which was connected with the terminal, and the ports which constituted the current link. Afterwards, a call was performed in order to ensure that the network was functioning under normal parameters.

The next step was to simulate a problem on the link by interrupting the optical fiber. The STP Loop Guard blocked the PO2 interface and the traffic was transferred on the alternate link. The root port channel became PO1 (in forwarding state). As it is presented in the Fig. 3, PO2 received the designation role (in „broken" state). This caused the „BKN*" message to appear next to the state section and the „P2P *LOOP_Inc" message next to the type section. This means that the PO2 is in a Loopguard inconsistence state.

During the experiment described above, the voice transmission had a short interrupt, but the call continued, as can be seen in the Fig. 4. That was possible because the data transfer was switched on the alternate link in about 1 second.

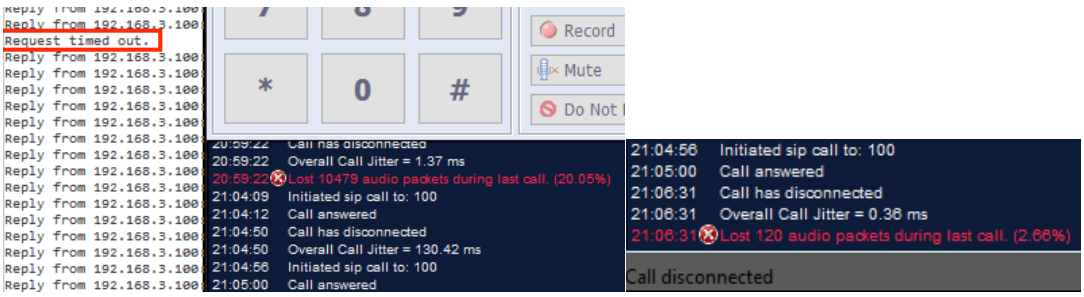
Once the network failure was fixed – by reconnecting the fiber optic cable to the media converter - the data traffic was forwarded back to the initial route, without losing data packets.

Even though the transfer was forwarded in a rapid way, there were still some data packets that were lost – the exact number may vary from case to case – because of the lack of connection and the implemented protocol reaction time.

In the same way the link between the 1st and 3rd switches or the link between the 2nd and 3rd switches can be interrupted. The implemented protocol will work in the same mode to bypass the failure.

```
sw1#sh spanning-tree active

MST00
  Spanning tree enabled protocol mstp
  Root ID     Priority    32768
              Address     0006.525e.54c0
              Cost        2016
              Port        66 (Port-channel2)
              Hello Time   1 sec  Max Age  6 sec  Forward Delay 15 sec

  Bridge ID   Priority    32768  (priority 32768 sys-id-ext 0)
              Address     000c.ce0a.ca00
              Hello Time   1 sec  Max Age  6 sec  Forward Delay 15 sec

Interface        Role Sts Cost      Prio.Nbr Type
---------------- ---- --- --------- -------- --------------------------------
Fa0/11           Desg FWD 200000    128.11   Edge P2p
Po1              Altn BLK 200000    128.65   P2p Bound(RSTP)
Po2              Root FWD 2016      128.66   P2p

sw1#
05:32:31: %SPANTREE-2-LOOPGUARD_BLOCK: Loop guard blocking port Port-channel2 on M
ST00.sh spanning-tree active

MST00
  Spanning tree enabled protocol mstp
  Root ID     Priority    32768
              Address     0006.525e.54c0
              Cost        200000
              Port        65 (Port-channel1)
              Hello Time   1 sec  Max Age  6 sec  Forward Delay 15 sec

  Bridge ID   Priority    32768  (priority 32768 sys-id-ext 0)
              Address     000c.ce0a.ca00
              Hello Time   1 sec  Max Age  6 sec  Forward Delay 15 sec

Interface        Role Sts Cost      Prio.Nbr Type
---------------- ---- --- --------- -------- --------------------------------
Fa0/11           Desg FWD 200000    128.11   Edge P2p
Po1              Root FWD 200000    128.65   P2p Bound(RSTP)
Po2              Desg BKN*2016      128.66   P2p *LOOP_Inc
```

FIG. 3. Messages during the connection interruption



(a) (b)

FIG. 4. Examples of connection interruption: a) a connection interruption with 10479 audio packets lost during a call; b) a connection interruption with 120 audio packets lost during a call

3. CONCLUSIONS

The purpose of this study was to demonstrate an optical ring network redundancy using the three Cisco Catalyst 2950 switches as core components. To forward data through the alternate link, the Spanning-Tree Protocol Loop Guard was used. For testing the connection, a VoIP call was generated – done through a virtual PBX and a softphone.

Applying the described method, during the experiment, generated good results: while the main route was interrupted, the traffic was forwarded to an alternate route created by STP taking into account the lowest cost. Although, during the call there were some voice packets that got lost, the call didn't stop.

Using the network redundancy, by routing the data packets through other links, the physical security was assured, also canceling the sabotage effects.

The main difficulty for implementing this experiment was to find out the best protocol to match our purpose and to set up the proper software on the devices used within the created network.

A small network was created to test the protocols efficiency, but the solution should be implemented in complicated networks with high traffic. Using VLANs (Virtual Local Area Network), optical fiber cables and network redundancy, for networks with a massive number of users, is beneficial for network operators. The focus is on being able to ensure service continuity, high availability and minimum downtime.

REFERENCES

[1] R. Horak, *Telecommunications and Data Communications Handbook*, 2007;
[2] M. Howard și S. Lipner, *The Security Development Lifecycle*, 2006;
[3] P. Holbrook și J. Reynolands, *Site Security Handbook*, 1991;
[4] W. Stallings, *Data and Computer Communications*, 9/E, Pearson Education, 2011;
[5] A. S. Tanenbaum, *Computer Networks*, 4/E, Prentice Hall, 2003;
[6] K. Dooley and I. J. Brown – o'Reilly, *Cisco IOS Cookbook*;
[7] *** *Catalyst 2950 and Catalyst 2955 Switch Software Configuration Guide*, Cisco IOS Release 12.1(20)EA2, 2004. Available at www.manualslib.com, accessed on 20 Jan. 2017;
[8] *** http://www.nch.com.au/pbx/, accessed on 16 Feb. 2017;
[9] *** http://www.nch.com.au/talk/, accessed on 16 Feb. 2017.