A NOVEL IMPLEMENTATION OF A BACKUP SERVER TO MANAGE PPPOE CONNECTIONS IN A PROVIDER NETWORK INFRASTRUCTURE

Miroslav SVÍTEK[**], Eugen ŠLAPAK[*], Gabriel BUGÁR[**]
[*]Department of Computers and Informatics, Faculty of Electrical Engineering and Informatics,
Technical University of Košice, Letná 9, 042 00 Košice, Slovak Republic, E-mail: eugen.slapak@tuke.sk
[**]Department of Electronics and Multimedia Communications, Faculty of Electrical Engineering and Informatics,
Technical University of Košice, Němcovej 32, 040 01 Košice, Slovak Republic,
Tel. +421 55 602 2808, E-mail: gabriel.bugar@tuke.sk

ABSTRACT

Since a number of different users are sharing the same physical connection to the remote service provider, a way is needed to keep track of which user traffic should go to and which user should be billed. PPPoE provides for each user-remote site session to learn each other's network addresses. PPPoE has the advantage that neither the telephone company nor the Internet service provider (ISP) needs to provide any special support. Unlike dialup connections, DSL and cable modem connections are "always on." Significance of presented work is describing function and issues of PPPoE connection as an important part of implementation solution in case of managing user connections in an Internet service provider network. Mainly, we focus on one of the most important and least discussed problem of PPPoE – the backup server implementation with the ability to back up any element in the connected network to increase the resilience of the entire system.

Keywords: *PPPoE, backup server, RADIUS server, network security*

1. INTRODUCTION

The Point-to-Point over Ethernet (PPPoE) is a network protocol for encapsulating PPP frames inside Ethernet frame. PPPoE combines Ethernet and PPP, to provide an authenticated method of assigning IP addresses to client systems. At system initialization, the PPPoE client establishes a session with the access concentrator by exchanging a series of packets. Once the session is established, a PPP link is set up, which includes authentication using Password Authentication protocol (PAP). Once the PPP session is established, each packet is encapsulated in the PPPoE and PPP headers [1].

Sooner or later in every networking infrastructure will be a realization that there is nothing more important than backing up the whole system's configuration. Days, or even months of hard work can disappear in a matter of seconds. That's why it is so important to always take the measures to prevent this from happening. Performing backups often is important but also testing them can be invaluable because there is need to make sure that you can rely on them when needed [2], [3].

The aim of this work is a comprehensive implementation of a new backup system to manage subscriber connections within the existing network infrastructure of an internet service provider (ISP). One of most widely used Internet connection is the point-to-point protocol over Ethernet (PPPoE) technology. We studied the available options/solutions [4], [5], [6], [7], that could be used to solve this problem to design a useful implementation, which includes detailed knowledge of the products currently used in the computer network market. The main reason for opening the issue was the imperfection of the currently used PPPoE solutions by providers. These often results in a quality degradation of the provided services [8]. The goal was to find a stable solution with high performance to meet customer requirements, as well as possible price savings when changing the current solution.

The remainder of this paper is organized as follows. Section 2 provides an overview of the PPPoE protocol functionality as well as description of parameters and appropriate hardware resources. Section 3 describes the current state of the problematic and choice of solutions. Section IV explains in details the proposed implementation of the backup server, but also complex description of used technologies and systems in relation to direct practical implementation of the chosen solution. Section V concludes the paper.

2. POINT-TO-POINT PROTOCOL OVER ETHERNET

PPPoE combines the capabilities of the point-to-point protocol, which is mostly used in broadband networks with the Ethernet protocol working on the data link layer of ISO OSI model, thus allowing the ability to connect clients using a concentrator (as used in xDSL technologies). With PPPoE, operators can control access and operations of subscriber connections together with managing a large number of connections at one network point. The basic principle of PPPoE is shown in Fig. 1.

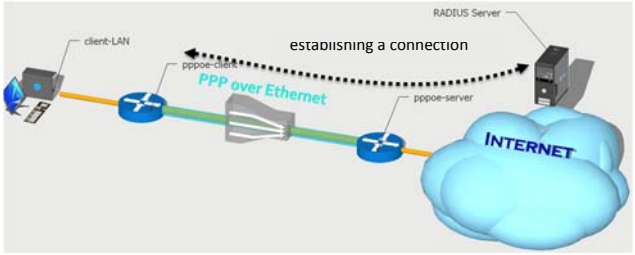

Fig. 1 PPPoE connection principle

To use PPPoE, it is necessary to initialize a PPPoE connection, PPP packets encapsulate in an Ethernet frame and set up the subscriber device as a PPPoE client. To use a PPPoE connection, each connection must know the physical address of the PPPoE server and establish a unique connection during the *PPPoE Discovery* and *PPPoE Session* stages. In these two stages, the client searches for the PPPoE server by using a physical address to create a relevant connection between the client and the server.

During the PPPoE Discovery stage, the client does not look for the path to the final device by using its routing information, but it tries to find a PPPoE server that concentrates all PPPoE connections in the network infrastructure. This process is a kind of client-server communication between the subscriber and the service provider. Even if there are several PPPoE servers in the network, the communication is governed by the response rule of the first server, which becomes its partner, unless the client's policy is specifically set up otherwise.

When the Discovery stage is done, the next stage is the PPPoE Session. This stage tries to establish a connection based on the received information during a standard PPP protocol included with the header in the Ethernet frame. Since the maximum Ethernet frame size is 1500 MTUs, within the information contained in the PPPoE connection header, the maximum size for a PPPoE connection is limited to 1492 MTUs.

2.1. Appropriate hardware resources

One of the most important part of the implementation is the convenient choice of the system core that the PPPoE router will represent. Analysis of useful compositions and methods for the calculation of the system control is evaluated according to the detailed documents for use in a provider network infrastructure.

To ensure collision-free operation of the system, the full functionality is required and it includes following points, that should be fulfilled:

- establish connection with PAP, CHAP, MS-CHAP authentication,
- possibility to use RADIUS server,
- option to add a backup RADIUS server,
- 10Gbps master node throughput in both directions,
- The ability to back up the main router with the same type of device,
- possibility to record connection and disconnection time,
- assign IP addresses from a fixed range,
- maximum number of routed IP prefixes,
- connection to the MPLS network of the operator.

When selecting the hardware, it is necessary to take into account the possible future increase in transmission capacity, the number of tunnels created or a possible solution change. As the computer networking industry is one of the fastest growing industries in the world, it is important that the infrastructure is ready for growth in overall data traffic and service quality. The statistics of the largest Slovak peering center SIX, it shows that the total data traffic in Slovakia has changed significantly in the last 10 years. In September 2008, the aggregate operation of the center was at 10 Gbps, while in 2018 it was worth 200 Gbps. In a detailed comparison, one can notice a huge increase between 2016 and 2018, when data traffic doubled from 100 Gbps to the already mentioned 200 Gbps. Data from 2019 is not yet complete, but the current data traffic ceiling was 253.4 Gbps in January 2020.

The four largest manufacturers of networking components on the market that we were currently considered to use are: Cisco systems, Juniper networks, HUAWEI and MikroTik. The above mentioned criteria was served as a basis for comparison of selected manufacturers' products with a short description of differences, evaluation of advantages and disadvantages, comparison of price and other parameters. After a detailed analysis of all the devices, we summarized the findings in the table 1.

Vendor	Model	U	Bw	Tunnels	Cons	Price
Cisco	ASR1001	1U	1Gbps	8000	500W	8000€
Juniper	ACX2200	1U	1Gbps	7000	200W	8775€
Huawei	AR3200	3U	4Gbps	10000	350W	7000€
MikroTik	CCR1036	1U	8Gbps	5000	73W	900€

Tab. 1 Comparison of suitable router models for PPPoE practical implementation developed by different vendors

After cross comparing analyzed parameters of considered devices, we decided to use router CCR1036 designed by MikroTik in the practical implementation, so the winner of the table 1 based on considered provided features.

3. ANALYSIS OF THE STATE OF THE ISSUE

3.1. Current implementation

Currently widely used solution of Internet service providers is built on a platform of Cisco systems. Most commonly used device model is the Cisco ASR 900 Series (simple diagram of current solutions shown in Figure 2).

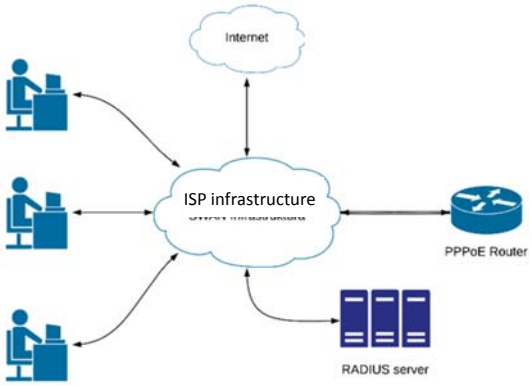

Fig. 2 Current solution diagram of Internet Service Provides

The subscribers are connected directly to the company network, then they are authenticated using the entered data containing the connection name, user login and password. The router processes and validates requests against a RADIUS (Remote Authentication Dial In User Service) server with return values such as: connection permission, associated connection speed. The RADIUS server is an AAA protocol (authentication, authorization and accounting) and it also solves the functionality of a competitive

connection so that it is not possible to connect multiple subscribers under one access data. Editing user profiles and access data is solved in the CRM system (Customer Relationship Management), which stores the parameters in a local private database. Using the MySQL function, the RADIUS server reads the values from the database and stores them in its memory. The solution has some drawbacks that make it vulnerable to possible connection failures that will be resolved in the upcoming implementation due to the added configuration.

The current implementation shortcomings are caused by the router's direct access to the RADIUS server without any backup. In a problem state of the RADIUS server itself, whether by a power failure, a software failure, or a connection failure with the router, the router loses the possibility of user authentication, resulting in the subscriber's inability to connect to the operator's network and the associated connection failure. Connections authenticated prior to server downtime will not work until after the connection expires when the subscriber connection authenticates again. Another serious disadvantage is the lack of backup on the router side, which is particularly serious due to the complete loss of functionality of the entire system and the associated loss of all subscriber connections.

The implementation works by assigning dynamic IP addresses to each active connection without translation, which causes a large number of necessary IP addresses to run smoothly throughout the system. If the number of IP addresses is exhausted from the available range, the router will stop sending replies to new subscriber connections.

3.2. Proposed implementation

The proposed implementation addresses these functional deficiencies in a more sophisticated way, as can be seen in Figure 3. It is based on the direct connection of the backup RADIUS server to the PPPoE router CCR1036, while the primary one is still connected to the network. Since the RADIUS backup accurately copies the primary server data, they are labeled under one device in the diagram. It follows from the above scheme that the number of routers itself has increased compared to the original implementation to avoid the possibility of a router failure itself, which has already been mentioned as a system failure.

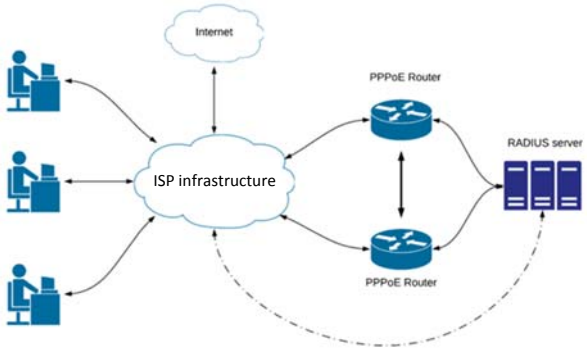

Fig. 3 Proposed solution diagram of Internet Service Provides

Using the user manager functionality, it is possible to obtain a backup RADIUS server that will be active only during the unavailability of the primary server. However, it will copy information from the primary server at fixed time intervals throughout its lifetime so that all functionality can be automatically redirected to the backup server without any loss of time or unavailability of connection authentication. The primary RADIUS server data loading process remains unchanged.

This implementation is complemented by the possibility of assigning private IP addresses to avoid the problem of exhaustion of range addresses. The possibility of assigning public IP addresses is also presented for comparison purposes.

4. DESIGN AND IMPLEMENTATION OF A BACKUP SERVER

To ensure the functioning of the whole system, it is important to correct the initial setup of the system. This section describes the process of setting up the main interface, which can be referred to as the Input/Output gateway to the Internet, the routing setting, and the password setting process.

Assignment of IP addresses in the address space is simple, it is necessary to know the IP address and the interface for which it is intended. It is entered in the form of IP address / subnet mask, from which the device itself calculates the network address. The next step is to add routing to guarantee network-wide traffic. In this option we can also choose to verify the state of the default gateway. Address 0.0.0.0/0 is the default address in the routing table. This ensures that the entire traffic is routed through the sfp-plus1 exit gate (Fig. 4).

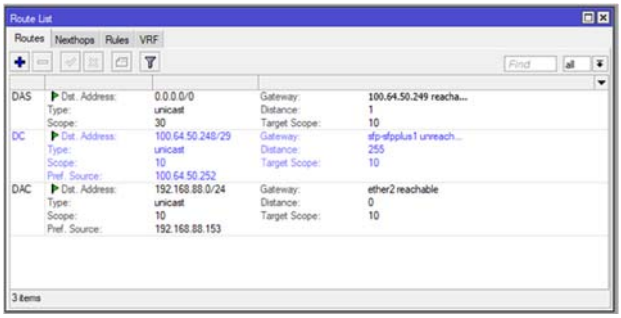

Fig. 4 The routing table initial setup overview

For security purposes, it is necessary to change the device access password. After saving, the device automatically blocks all administrator connections. You need to sign in again with a new password. An optional feature is to turn off the display, which many administrators turn off first.

Authentication of the subscriber using the RADIUS server must be done in several steps. The first one is the configuration of the service in the PPP window, where it is needed to add a new service with a name, select interface and expiration value, which we set to 3600 seconds, i.e. one hour. Authentication methods we chose all, since they do not affect the performance, but we gain by supporting a higher number of devices. It is also important to add a RADIUS server to the RADIUS list so we get a direct connection to the server.

Assignment of IP addresses we discussed in the description of the problem as a problem that can be effectively resolved immediately in two ways; first one by

using dynamic allocation of public addresses or vice versa private addresses. However, when assigning private addresses, we must take into account address translation options that are limited by the maximum number of port translations (mostly it is 65536 port numbers). Considering the standard of a maximum of 500 connections per user, it is possible to translate approximately 130 private addresses to one public address. In order to maintain the highest performance, a range of 128 IP addresses per public IP address will be translated with scalability to another range.

Since the router assigns IP addresses from the original selected range, each additional range must extend the previous one. To avoid the possibility of a high number of connections and depleted ranges, we will add the range of 2000 addresses, to make a reserve available when needed. For translation, it is necessary to add NAT functionality in the Firewall settings.

When the address range is ready for use, we will return to the PPPoE server to add a PPP profile containing IP address and connection limit data. We add the range which we used in the previous point, the DNS server addresses, and set the base limit to 100/100Mbps. If we did not set the basic limit, there could be a case in which the user would have unlimited speed when connected.

In the case of a solution based on the assignment of public IP addresses, we would do the same, but to the extent we would enter the public IP addresses and write them in the profile. However, NAT translation would not be solved.

Setting the speed profile is handled directly by the router, which limits the tunnel capacity to the desired value. The value is obtained from the RADIUS server in the format of download / upload speed in Mbps. Since the value obtained from the RADIUS server will be evaluated as NULL, it is necessary to create a profile directly in the router for each used profile. The easiest way to do this is to use the following command: *[admin @ MikroTik] / ppp profile> add name = 50/10 rate-limit = 50000/10000* to create a 50/10Mbps profile. By analogy, the formation is continued up to the desired number. Subsequently, the existing record in the router is used for authentication.

4.1. PPPoE router backup

In the case of the PPPoE router backup solution, it should be noted that the PPPoE server backup itself is not defined in any standard. Failover methods used in normal functionality cannot be used because there is no protocol that two PPPoE servers can communicate with. At this point, we began to think about the possibility of using timing alternatively. If two identical devices were used for the same purpose in the same network, they would not fulfill their functionality and would create conflicts. However, if we achieve a time resolution of the responses of each router, one of them will always solve the request faster than the other, the subsequent response of the other router will be unanswered. This functionality can be achieved suspiciously simply by setting the response delay on one of the routers in the PADO Delay block.

Adding a delay of 5ms results in a second device response delayed by this value. The logical question, however, is how do we guarantee load balancing if it is obvious that router 1 will always answer the request? The answer is the load characteristics of the device itself. As the overall data throughput of the device decreases, its response to requests increases. This is primarily due to the preference of data traffic over the processing of additional requests such as authentication, logging, sending e-mails, etc. As a result, when the number of connections of the first router increases, its response to connection requests exceeds 5ms, and this request is processed by the second router. By simply adding a delay on one device, we was able to achieve the equilibrium power distribution functionality between the two routers while creating a router backup.

Router response delay does not affect connection speed, only initial user authentication, which usually lasts in seconds. Very important is that both routers must have different configurations including device name, IP address, public address ranges used, and so on.

4.2. Extended functionality - Implementing security in the system

Since the PPPoE protocol itself is prone to two security threats, we have tried to eliminate their impact on MikroTik itself. These are attempts to reveal the password for a random user menu and a concentrated attack on router resources or even a DoS attack.

To eliminate the possibility of an infinite login attempt, we also implemented directly in the primary and backup RADIUS server. The number of attempts is fixed at 10, after which access is blocked for a minute.

DoS attacks are very popular nowadays due to their effectiveness and the possibility of systems malfunctioning. MikroTik does not contain such functionality, but after we studied the criteria for preventing attacks using scripts, we found and implemented such a solution as computationally demanding. This could burden the router, which would reduce performance. Since the traffic in the city of Košice is directed through the Bratislava node, we investigated the possibility of implementing an existing solution. We ask a local operator, an ISP in Kosice to provide us a developed system to block attempts from DDoS attacks, so we assigned a router name to the system and our solution was not short of important performance. When we deploy our solution in the operator's network we have prepared a platform background with a total of 10 test subscribers where our configured routers tried to connect in one moment. The test was successful, but we still waiting for the deployment of the solution in full system operation because of verification and review of the whole our implementation within the company policy and the final decision of the operation department.

During the work in the operator’s environment we met two strange cases of functioning. The first specific case was a new connection that has not yet created a speed profile in the operator's database. In this case, the speed profile is set to 10/10Mbps, which must also be added to the system otherwise the connection will not be answered. The second case was a problem with clients that were needed a static public IP address. After a few configuration attempts, we found that this ca be solved just with assigning of a fixed IP address to the Remote Access value in the profile that downloaded the router from the RADIUS server.

5. CONCLUSIONS

5.1. Systems comparison

In an overall comparison of the two systems (current and proposed solution), we would raise the total cost of implementation along with the performance increase. If we compare the price of a Cisco systems device for less than 10.000 € with a competing product from MikroTik for less than 1.000 €, we get an excellent price / performance ratio with added critical measures to prevent downtime.

5.2. Obtained enhanced functionality

The use of private IP addresses in the proposed implementation provides the possibility of reusability of currently allocated IP address ranges in other projects. While customers will lose functionality as DDNS because they no longer have a public, although dynamic, IP address, getting a large number of IP addresses is a constant benefit for the operator because of the overall number of IP addresses being limited across the Internet. Currently, it is no longer possible to purchase additional IP addresses, because they already have all their owners. The transition to IPv6 is an ongoing process, but it still has a huge way to go.

Another huge benefit value is the functionality of the backup server itself. Using the functionality developed by MikroTik, we was able to eliminate the risk of authentication server failure. The original intent of copying the values has proven to be time consuming and the hardware resources of the router itself have been realized, which makes me find a faster and more efficient method for acquiring subscriber data.

The added functionality certainly includes a conceptual simple backup system for the router itself in the network, thanks to which I achieved a backup of the primary device with power distribution to two physical devices, which of course may not be finite and in case of large.

5.3. Utilization of future implementation

Since PPPoE can be used with multiple types of connections, it is certainly a plus to have a functional solution for deploying the protocol, for example on WiFi networks, or the increasingly popular method of connecting PON subscribers, from connections with an Ethernet interface and a limited length of 100 meters.

Thanks to its almost universal implementation, it can be used in any operator network in the country, thus ensuring the great potential of the presented solution in the future.

In solving the presented PPPoE implementation we provided detailed knowledge of the issue of connecting participants using PPPoE protocol. From this knowledge we have tried to prepare a functional implementation that would benefit not only the individual or group, but also any enthusiast dedicated to computer networks. we managed to almost completely eliminate the possibility of a drop-out of the subscriber connection, which represents a significant improvement over the original implementation. Within the scope of enlargement, we would consider extending the solution to multiple locations within our country and thus be able to compare the possibility of using separate smaller systems or a concentrated central system for connection management in the territory of the country, as we see great potential in the possibilities and utilization of the implementation.

ACKNOWLEDGMENTS

This research was supported by the by the Slovak Research and Development Agency, project number APVV-18-0214 and APVV-18-0368.

REFERENCES

[1] PRASETYO, E. – HAMZAH, A. – SUTANTA, E.: Analisa Quality Of Service (Qos) Kinerja Point To Point Protocol Over Ethernet (Pppoe) Dan Point To Point Tunneling Protocol (Pptp). Jurnal JARKOM Vol. 2016, 4.1.

[2] DU, P. et al.: Design and Implementation of 10Gbps Software PPPoE Router for IoT Smart Home Network. IEICE Transactions on Communications, 2019.

[3] HU, T. – QIAN, G.: Packet Processing Method in PPPoE Authentication Process and Relevant Device. U.S. Patent Application No. 15/795,835, 2018.

[4] OWENS, C. B.: System and method for provisioning broadband service in a PPPoE network using DTMF communication. U. S. Patent No. 7,079,527, 2006.

[5] MAMAKOS, L. et al.: A method for transmitting PPP over Ethernet (PPPoE). RFC2516, Feb, 1999.

[6] YUSKO, J. – HAGLUND, K.: Intelligent PPPoE initialization. U.S. Patent Application No. 10/065,393, 2004.

[7] BERRY, B. et al.: PPP over Ethernet (PPPoE) extensions for credit flow and link metrics. IETF, RFC 5578, 2010.

[8] LIU, F. et al.: On the security of PPPoE network. Security and Communication Networks, 2012, 5.10: 1159-1168.

Received April 2, 2020, accepted June 5, 2020

BIOGRAPHIES

Miroslav Svítek is the student at the Department of Electronics and Multimedia Communications, Faculty of Electrical Engineering and Informatics, Technical University of Košice. His research interests include His research interests include data analysis and modelling network infrastructures, theory and simulation of complex systems, and solutions of optimization problems.

Eugen Šlapak is the PhD. student at the Department of Computers and Informatics, Faculty of Electrical Engineering and Informatics, Technical University of Košice. His research interests include real-time spectrum trading schemes, modelling of network complexity and real time mobility.

Gabriel Bugár is a Research Assistant at the Department of Electronics and Multimedia Communications, Faculty of Electrical Engineering and Informatics, Technical University of Kosice, Slovakia. His research interests include cognitive networks, image processing, security and E-learning.