УДК 654

БАБИЙЧУК Т. В.
ОБЕСПЕЧЕНИЕ БЕЗОПАСНОСТИ ПЕРЕДАЧИ ИНФОРМАЦИИ В MPLS СЕТЯХ

Бабийчук Тарас Владимирович
студент, Национальный Технический Университет Украины
«Киевский политехнический институт»
E-mail: rasmon777@gmail.com

Аннотация. *В данной статье автор излагает краткие сведения о технологии MPLS. Автором статьи приведены и проанализированы варианты обеспечения безопасности в сети MPLS. Сделаны выводы о целесообразности использования данной технологии.*

Ключевые слова: *MPLS, Безопасность.*

BABIICHUK T. V.
ENSURING THE SAFETY INFORMATION TRANSMISSION IN MPLS NETWORKS

Babiichuk Taras Vladimirovich
student, National Technical University of Ukraine
«Kyiv Polytechnic Institute»
E-mail: rasmon777@gmail.com

Abstract. *In this article, the author presents a summary of the MPLS technology. The author of the article shown and analyzed options for ensuring security in the MPLS network. Conclusions about the feasibility of this technology have done.*

Keywords: *MPLS, Security.*

Introduction. It is impossible without a transmitting or telephone connection today. Making a call or a message transmission signal is converted into a compressed data packet. Further there is a transfer of data packets over packet switched networks, in particular, IP networks. And as the number of network attacks is growing every year, we need an effective tool to protect our information. The high degree of the information security in the IP-telephony can be achieved using a multi-protocol label switching technology (MPLS).

Materials and methods. MPLS technology for transmitting packets uses so-called "tags". The block of the data of 32 bits size is added to the subject. Most of it is 20 bits long "tag", essentially a label, on the basis of which the decision of the further package movement is made.

Transmission principle. When the IP-packet from PC1 enters the MPLS network the first router put a label. Then this package goes to the point of destination, and each router changes the next one label to another. Leaving the network MPLS label is removed and transferred as a purely IP-packet as it was at the beginning (Fig. 1).

This is the basic principle of MPLS - routers commute packages on labels, without looking into the MPLS packet. The first router adds the label, the last one deletes [1].

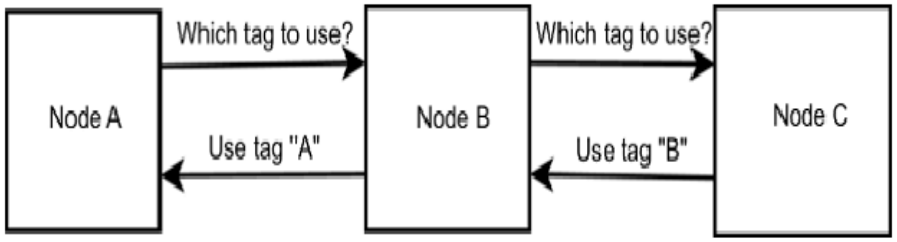

Fig. 1 Exchange tags

Discussions. Only two devices in the network know what package is and where it came from at a time. Thus the probability that the package will not be intercepted is increasing. If the package has been intercepted, the use of MPLS will quickly limit the network segment where the hacking occurred, thus it will enable the hot fix problems.

Also, the enterprises, relied on MPLS have to encrypt their data before it leaves their site. It would solve the issue of the encryption absence abilities within the MPLS network [2].

Conclusion. Taking into account all this factors I may rich the conclusion that using MPLS technology for the information security will reduce the probability of packet capture, and will quickly find network bottlenecks and eliminate it.

Список литературы

1. Сети для самых маленьких. Часть десятая. Базовый MPLS // habrahabr URL: https://habrahabr.ru/post/246425/

2. MPLS Security Is MPLS Secure? // rcrwireless URL: http://www.rcrwireless.com/20140513/wireless/mpls-security

References

1. Network for the little ones. Part Six. Basic MPLS // habrahabr URL: https://habrahabr.ru/post/246425/

2. MPLS Security Is MPLS Secure? // rcrwireless URL: http://www.rcrwireless.com/20140513/wireless/mpls-security

РЕЦЕНЗЕНТ

Правило Валерий Владимирович – *доцент кафедры ИТМ НТУУ «КПИ», кандидат технических наук, доцент*.