Technology of Encrypted Tunnels with Practical Usage

Ondrej Bures, Monika Borkovcova, and Petra Poulova

University of Hradec Kralove, Faculty of Informatics and Management,
Rokitanskeho 62, 500 03 Hradec Králové, Czech Republic
{ondrej.bures, monika.borkovcova,petra.poulova}@uhk.cz

Abstract. Searching for an effective solution and creating a functional and affordable option of linking internal network while maintaining existing services and technologies, which implies the convergence of not only data but voice networks as well, can best be done in the practical test. The article focuses on the professional performance of the resulting solution to a specific task. Subject to verification was unguaranteed type of Internet connection using encrypted IPSec (AES256) tunnels via Astaro technology. Verification was first conducted under conditions of test wiring outside the real operation, followed by performing and validating during real data and voice transmission. Based on tests and analyzes of data transfers and dropouts it was able to design a functional and secure connection. The analysis included an actual traffic with ICMP protocol responses evaluation. The proposed solution is usage maximization for small and medium-sized organizations as well as affordable and accessible way to secure all stations.

Keywords: broadband, secure tunnels, remote branch, network, internet, security

1 Introduction

Linking users with in-house computer networks is nowadays more and more commonplace. Development of information technologies and the growth of connected users sets greater demands on information security during data transfers over data connections. Ensuring the security of corporate computer networks is nowadays at a high level, but the safe use of ICT offsite has its own laws. Modern computer networks are becoming increasingly complex and without adequate network security they are not prepared to defend attacks from hackers. While network security is a continuous and ongoing process, security system still should be single, simple, powerful and proven. Complete security does not only mean attacks detecting but unconditional liquidating as well. Safety network problems may arise if there are weaknesses in technology, configuration or security policy. It should be matter of course to operate only with such security services that can be implemented in practice at the different layers of the communication protocol. As for testing the connection of a remote station to headquarters the technology Astaro SG + RED ensuring encrypted IPsec tunnels type (AES256) was used. Astaro RED SG + is a simple yet affordable way to secure remote offices within a few minutes and without any technical knowledge at the spot. The product integrates the VPN functionality and comprehensive security solutions. Astaro RED 1O works as a remote unit of Astaro Security Gateway (ASG) and requires no configuration on site. After connecting to the Internet unit registers itself to the central gate of ASG and connects with the central office via a VPN tunnel. Central Astaro SG provides central configuration for all RED devices and central DNS and DHCP. It also specifies a uniform security policy for all remote branch offices, including detailed reports of each of the remote offices without requiring additional reporting device. This device offers a new standard of security for remote offices, substantially eliminates investment into expensive hardware, thus significantly reduces the cost of connection and maintenance of remote sites. Since the whole issue is technically extensive, this paper focuses on selected areas of technical solutions [8, 10].

2 Description of Tested Connection

Connection of remote location to headquarters via unguaranteed transmission environment was solved by using asymmetric public Internet connection service via xDSL with transmission speed towards the user (downstream) of 8Mbps and uplink (upstream) of 512kbps.

Type specification of verified connection Astaro SG + RED:
Security Gateway (SG) is being installed in the central communication node while it provides a complete set of security applications, such as firewall, VPN, IPS and antivirus. The terminal Remote Ethernet Device (RED) is mounted on the side of remote location and provides an application of centralized parameters and security policies. In terms of safety is technology which uses IPsec AES256 algorithm encrypted communication tunnels NATO standard. In the Czech republic is the Astaro technology routinely used for several years by financial institutions, which can be supported by the vendor‘s references. From a security standpoint is S-GW not operating as a router, which would be routing data flow to all directions that are not explicitly prohibited. S-GW acts as a firewall, which transmits data flows only with appropriate parameters, only if they are explicitly permitted. Other traffic does not pass through S-GW. This is an example of another aspect that improves safety parameters for communication via public communications environment. Astaro technology allows prioritization of data streams inside the generated tunnel. Given the need to comply with existing services, this feature was used in tests for voice traffic prioritization. Original remote branch connection to the headquarters is possible because of Vanguard / Frame Relay technology providing data and voice services [3, 4].

3 Practical Test of the Unguaranteed Internet Type of Connection Using Encrypted IPsec Tunnels (AES256) via Astaro / Sophos Technology

Verifying remote station’s connection to a central hub took place while maintaining existing services and with existing technology usage maximization, Several ways of both data and voice traffic connection has been tested.

3.1 Types of Tested Setups in Terms of Data Traffic

Option 1 - L2–RED + router

Remote station is established in terms of voice and data network around the L2 layer in a way of appropriate VLAN for both data and voice. End router is attached to the corporate network through multi-VRF or full Multiprotocol Label Switching (MPLS). MultiVRF mode regards VLAN set of data, which are meant and appropriate for the remote office. In the case of the full MPLS regards one data VLAN which belongs to a given remote station. Gateway for end PC is provided locally and Astaro is in so called ”bridged mode”. In case of larger number of connected remote offices, each has to be provided with its own set of data VLAN [7].

Option 2 - L3–RED gateway

The remote station is connected in terms of data and voice networks around the L3 layer. RED provides a gateway for the local LAN segment and voice traffic. Astaro is in so called “routing mode”. Provided VLAN networks propagates only to a corresponding remote station. This option is more suitable for connecting small remote stations and it was verified in real operation.

3.2 Types of Tested Setups in Terms of Voice Traffic

Option 1 – Voices over Vanguard/SoTCP

Voice traffic setup is using the existing equipment Vanguard6455 established by the SoTCP protocol and Ethernet environment on Vanguard7310 in a central location. Vanguard7310 is connected to a regional PBX Alcatel 4400 by E1 trunk. Vanguard6455 at the remote location provides a voice gateway function for the small PBX Panasonic KXT6/16 equipped with connected phones and fax. Voice connection between the Vanguard device and PBX remained in the original engagement and is realized through analog FXS ports and CO input ports in existing PBX. In Fig.1 it is apparent that

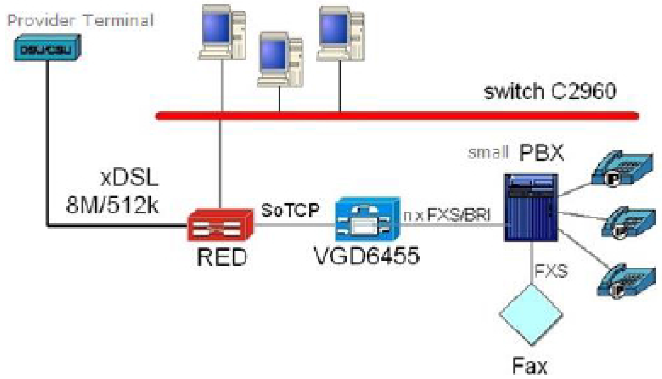


Fig. 1. Option 2 - Voice over IP PBX

a voice technology remained in the original engagement, which would eventually lead to migration of the network to the Ethernet environment which would minimize costs of technology renewal or at least delay the complete replacement of the whole technology. Due to the change in the type of environment from Frame Relay to Ethernet environment it was only necessary to make a change in Vanguard 6455 configuration [4].

Option 2 – Voices over IP and H.323

The setup is based on Voice IP technology Innovaphone using IP24 equipment which contains 4 FXS ports and like Vanguard it provides voice gateway function for a small local PBX equipped with connected telephones and fax, as shown in Fig. 2. In the setup there is also used IP305, which has registered testing IP phone IP110. In the tested configuration are both IP24 and IP305 established using the H.323 protocol on central IP6000, which is connected to the regional PBX Alcatel 4400 by E1 trunk. As for continuity in departmental voice network it is also possible in this case to use the existing central Vanguard device and H.323 protocol. This connection didn't appear to be successful because of the failing transmission of fax traffic.

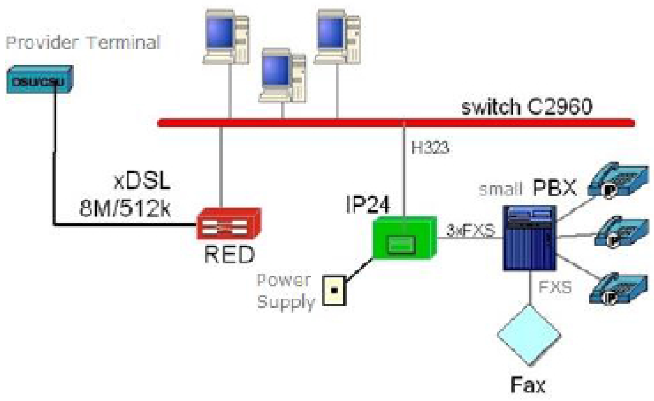


Fig. 2. Option 1 - Voice over VGD/SoTCP

Innovaphone products (IP24, IP305 a IP110) are used to enable implementation of IP telephony and to build IP phone system. IP phones resemble a traditional phone. They allow users to connect with other users. They receive voice, convert it to IP data stream and send it to a destination where the data stream is again converted back to voice. The task of the gateway is to convert IP data stream that carries the voice and signaling data to the physical media of a certain type and vice versa. Connection to PSTN serves as an example for gateway practical use. Gateway can as well offer services of PBX. In contrast to that the adapter is used to connect analog devices but cannot serve as a PBX. If the IP phone is trying to establish a call, it is necessary to determine where the target is located. If the called party is an IP telephone that is part of the same system, it is necessary to know its IP address. If the called party is located in the external network (e.g. PSTN) gateway has to be correctly identified in order to forward the call. In order of PBX to be able to control every call it has to be aware of all phones and gateways. Therefore, they have to be registered. PBX – the control panel is not equipment, but software that is present on the most of the gates and is activated by proper license. All Innovaphone devices support H.323 and SIP protocols [1].

3.3 Description of Used Innovaphone Products

IP6000 is one of the VoIP gateways of Innovaphone product line with the ISDN PRI interface. IP6000 Gateway acts as an intermediary between traditional telephone networks and the world of IP telephony (SIP / H.323). On the side of the telephone network, it is able to connect it up to two PRI ports. Innovaphone licensing model allows the use of only the necessary number of the ports and voice channels so as to achieve maximum equipment cost savings and effective use of ISDN connections. The unit itself is optimized for stable, secure, long-term and trouble-free operation even in harsh operating conditions. It is the reason for not moving any movable parts and the operating system is primarily designed and optimized for the telephone traffic. The operating system is fully developed by Innovaphone and contains no standard system components. IP305 –while using this VoIP gateway with ISDN BRI interface we can achieve connection of a standard telephone network (PSTN) with the world of IP telephony, but also it can be used as Innovaphone VoIP PBX for up to 50 registered users. IP305 interface consists of two ISDN BRI ports and two Ethernet ports, which can be connected into two separate networks. Gateway between networks can direct traffic or to route telephone calls to separate networks of various VoIP providers. Free Ethernet port can also be used for system administration only [9].

IP24 – this VoIP adapter has four analog FXS ports, which can be used in order to connect any standard analog devices. By using this adapter we can connect standard analog devices with the VoIP environment, including Innovaphone VoIP PBX. All analog ports support T.38 protocol, which is the ITU standard for the reliable faxing transmission over IP network. IP24 adapter can be powered by an external source or via the Ethernet port that meets the standard PoE. IP110 - this IP device is the basic product line of Innovaphone company and supports both SIP and H323 protocols. The device is equipped seven-lined display, which enables you to see all the statuses of the phone while allowing easy and quick orientation during operation. In this basic series four programmable function keys with indicator light are included. They can be used for speed dialing or for direct access to certain functions Innovaphone PBX. The device is one of the popular models, mostly because of its reliability [5, 9].

H.323 (Packet-based multimedia communications systems) covers the whole group of protocols designed to carry not only voice but also multimedia data in their entirety, and it is defined by the International Telecommunication Union (ITU). H.323 protocol defines components Terminal, Gateway and MCU. Terminal – usually HW or SW phone, a special type of terminal can be even considered as a voicemail system. Gateway – a device which enables bidirectional communication with other communication devices in the network (e.g. ISDN, analog phone network or other H.323 network). Gate formally is established of ”Media Gateway Controller” (MGC, call signalization controller) and ”Media Gateway” (MG, routing audio / video streams). MGC and MG are

typically a single physical device, otherwise we speak about decomposed gate. Conference unit (MCU) – again formally divided into Multipoint Controller (MC, controller of the conference call signalization) and Multipoint Processor (MP, multimedia channels maintenance, audio mixing, etc.).
Gatekeeper – optional entity that provides addresses translation and traffic control in H.323 network. H.323 standard is often criticized for its imperfections, the complexity and size. While H.323 is suboptimal, yet it is suitable for communication between VoIP gateways [5].

3.4 Validation Under Test Setup Among Real Operation

Verification was first conducted under conditions of test wiring outside real operation. It was necessary to test all variants of connection and thus eliminate possible errors when connecting technology. This will avoid possible unwanted outages real operation.

Connection specifications as following. Astaro RED is connected to the Internet over xDSL 8Mbps/512kbps. All options are tested according to 3.1. All options are functional, but appear to influence unguaranteed connection that experienced packet loss in percentage units over time. Fax verification has been done in two ways. First way was that the device was initially connected to the terminal device Vanguard6455 via an analogue card FXS. Vanguard6455 communicated with the central device Vanguard7310 using SoTCP protocol. During the second possible way of verification fax traffic over loan facility Innovaphone IP24 was tested. Fax was connected to the ending VoIP gateway IP PBX Innovaphone IP24 via a four-port analog FXS card, which was communicating with IP PBX innovaphone IP6000 at the centeral by using protocol H.323. There was no fault during each way of functionality of the fax traffic verification.

3.5 Verification of the Remote's Station Actual Operation

Verification of real operation started by reconnecting the remote location's existing connection, where leased line type LLnet 512Mbps using technology Vanguard / Frame Relay was used. The new connection was realized using the services of a public Internet ADSL 8Mbps / 512kbps, without guaranteed bandwidth availability or a degree of aggregation of the Astaro technology - configured according to the section 3.1. The first two days of testing conducted by the L2-RED + router option. The following eight days of testing were according to the L3-RED gateway option which has lower requirements on hardware of the remote station, yet allows local gateway function for end computers. The involvement of voice at the remote branch office was during the first of two days validated during the operation of the Vanguard6455 device and the SoTCP protocol. Existing small PBX Panasonic KXT6 / 16 with connected branches and fax was connected via the analog FXS card with the Vanguard6455 device. Following eight days served for verification of IP telephony using voice gateway through IP PBX Innovaphone IP24 with four ports output FXS analog card, which established connection with the existing small Panasonic KXT6 / 16 PBX and a fax. It was also fitted with a small IP PBX Innovaphone IP305 with registered IP110 IP phone for communication between technicians. Specification of the test environment was chosen to be readily comparable with the operating parameters (level of service) of the current connection type LLnet and to match the expected configuration of Astaro technology in terms of end location solution. During the test period data, voice and fax traffic was evaluated by the end user without any remarks. Due to the irregular connection use by the end user, it was necessary to verify the quality of the connection and the services quantitatively with generated traffic.

3.6 Description of the Original Setup Using Frame Relay

Vanguard devices form a complete product line of data multifunction devices intended to create a packet network keeping together voice and data signals and to interconnect networks of LAN and WAN levels and telephone networks. Hardware and software modularity of individual devices and the amount of supported protocols allows you to create such networks that guarantee the possibility of further development if needed. Vanguard 6455 device is an existing technology that is fully functional on the remote station and is connected to the central Vanguard 7310 via the Frame Relay environment. Variability of this technology could be used to connect it with the Ethernet environment through secure tunnels using Astaro using SoTCP protocol. Vanguard 6455 router is primarily designed for use in regional points of the network. The device provides a cost-effective support for voice, fax and mixed data transfer protocols over IP, Frame Relay, X.25, ISDN, ATM or Nx64 T1 / E1 services. Vanguard can be extended by various daughter cards.Daughter cards' supported expansion ports are 6 FXS ports, FXO ports 3, 3 ISDN S0 port, 6 E & M ports, port 2 E1 (G.703) with 30 channels. Tested branch was equipped with the original wiring of X.21 interface connected to the modem of the provider and over Frame Relay to the central central point Vangurad 7310 via E1 interfaces. Vanguard 6455 at the end point separates the data connection from the voice traffic and via the second X.21 interface device it is connected to the router, which routes data to the switch, where connections of the end user's PC lead to. End point Vanguard is equipped with dual port FXS card, which is connected to the local PBX Panasonic KX-T612. Vanguard 7310 router is designed for use in central connection points, allowing us to connect child nodes to existing LAN and WAN networks and telephony technologies that enable their interconnection. The basic unit (5 card slots, 128MB SDRAM, 2X 16 megabytes Flash), supplemented by cards 8 port Serial Card, 8 port T1 / E1 card and CPU Central Processor Unit.

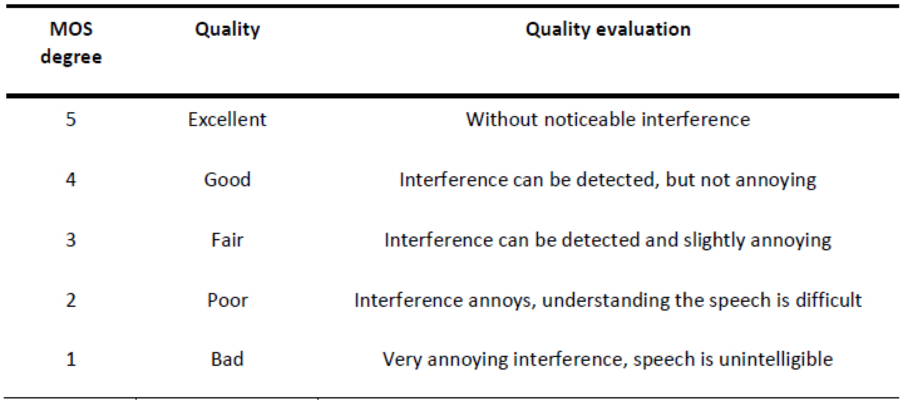
4 Evaluation and Analysis of Performed Tests - Data Transfers and Dropouts

Verification and testing was done not only in real traffic, but - as mentioned in the previous chapter - it was necessary to create the generated traffic between remote offices and a central connection. Whether any data has been safely delivered and what was real and potential loss rate generated by the operation was found based on responses of ICMP protocol. This protocol is used to send various error messages during transmission of IP protocol and does not make any packet repairs. ICMP Echo Request and Replay is a pair of ICMP Echo messages, which are used by ping tool for testing availability of stations and network nodes. Echo Request requirement is being dispatched to verify availability of the station. Echo Replay is the answer to the request.

4.1 Verification of the Real and the Generated Traffic with ICMP Protocol Responses Evaluation

This chapter describes the specification of verification. Generated traffic was created by both ways transmission of 1GB file in both directions of the remote station - headquarters and headquarters - remote station using FTP and TFTP servers and clients. Availability test of data transmission services in the Intranet (corporate network) between the ICMP and headquarters (PC FTP server headquarters) - remote station (notebook in a data network) and vice versa. The number of test packets in each series: 300 (packet size 100B, 1000B, 1600B – corresponds with mail communication). Test of transmission services for voice availability - ICMP between PC (DPA522) at headquarters (notebook in voice network of remote station and vice versa). 100B packet size corresponds to the typical voice traffic. Subjective call quality during the measurement was evaluated as well. Traffic was detected at the interface of Astaro Security Gateway towards the internal voice network at data and voice VLAN. Subjective evaluation of voice quality was carried out simultaneously with voice communications with employees at a remote office during ICMP responses authentication. Quality assessment is based on the established voice quality scale by the MOS parameter (Mean Opinion Score) - an estimate of the quality and speech intelligibility for the listener. MOS value is based on the subjective assessment of quality of the sample on a scale ranging from 5 to 1, as shown in the following Table.

Table 1. MOS range values



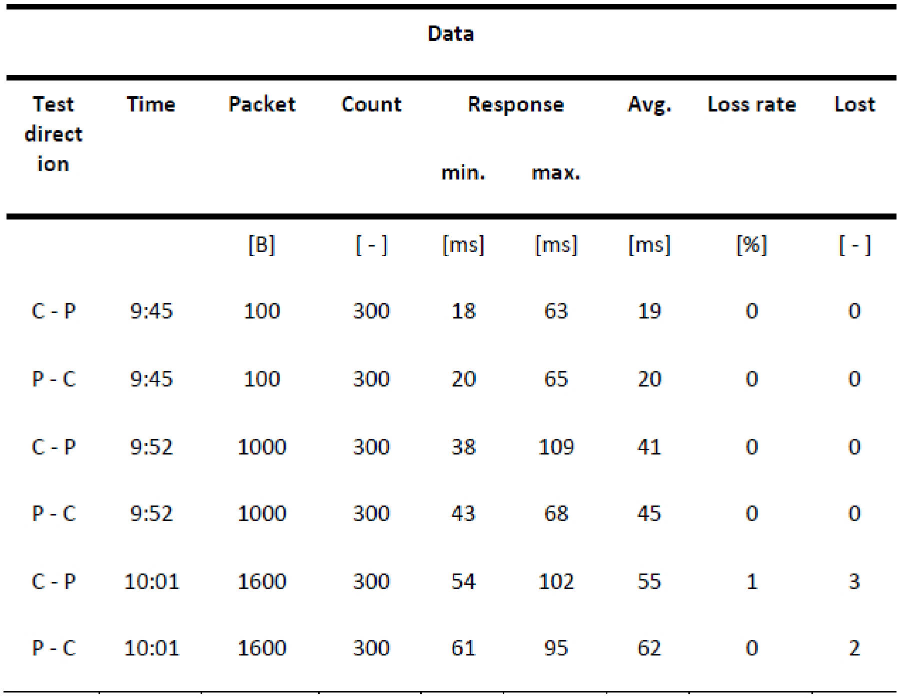
MOS degree	Quality	Quality evaluation
5	Excellent	Without noticeable interference
4	Good	Interference can be detected, but not annoying
3	Fair	Interference can be detected and slightly annoying
2	Poor	Interference annoys, understanding the speech is difficult
1	Bad	Very annoying interference, speech is unintelligible

Subjective assessment is based on students' assessment based on their perception and satisfaction with the call. Fax at the end point is connected to the analog local branch PBX Panasonic KXT616 which was established from analog CO trunk port to an IP PBX Innovaphone IP305 / IP24 via its analog FXS port and from here with H.323 protocol to the IP PBX Innovaphone IP6000, which is engaged in the headquarters, and from there into internal corporate voice network ITS by E1 trunk. Several fax machines are involved in ITS for tests performed from a remote location and vice versa.

ICMP Responses

Results of ICMP responses were transferred into Tables according to outbound specifications authentication. Divided measurements were carried out for real and generated traffic both with data load and voice traffic at a remote office and Security Gateway (SG) in the central communication node. The following test results show only realistic traffic between branch (P) and headquarters (C). Load was created by both ways transmission of large 1GB file (in both directions P-C and C-P) using FTP and TFTP servers and clients [2].

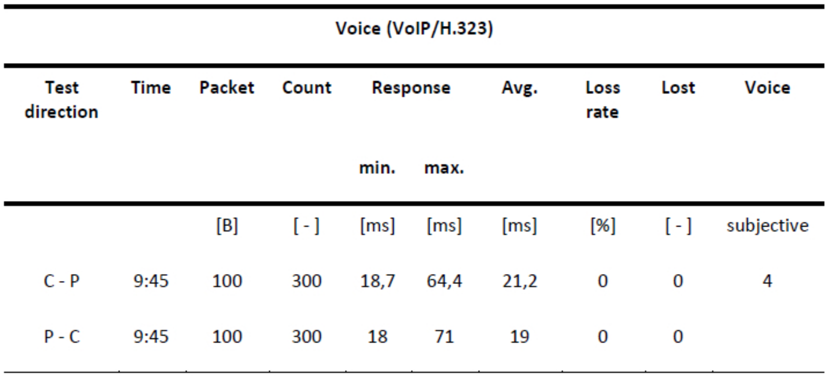
Table 2. Without load



Data								
Test direction	Time	Packet	Count	Response		Avg.	Loss rate	Lost
				min.	max.			
		[B]	[-]	[ms]	[ms]	[ms]	[%]	[-]
C - P	9:45	100	300	18	63	19	0	0
P - C	9:45	100	300	20	65	20	0	0
C - P	9:52	1000	300	38	109	41	0	0
P - C	9:52	1000	300	43	68	45	0	0
C - P	10:01	1600	300	54	102	55	1	3
P - C	10:01	1600	300	61	95	62	0	2

Test for availability of voice transmission service: ping between the PC522 in the headquarters (C) and a laptop in the voice network affiliates (P), and vice versa - the size of the packet 100B corresponds to typical voice traffic. Ping syntax[packet length, the number of packets], #ping 10.192.xxx.yyy -l 100 -n 300.

Table 3. Voice check test

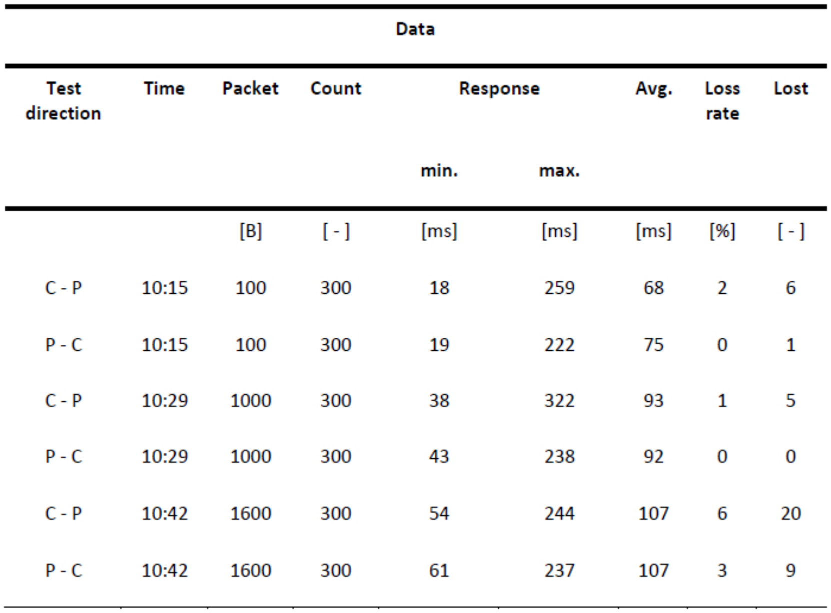


Voice (VoIP/H.323)

Test direction	Time	Packet	Count	Response		Avg.	Loss rate	Lost	Voice
				min.	max.				
		[B]	[-]	[ms]	[ms]	[ms]	[%]	[-]	subjective
C - P	9:45	100	300	18,7	64,4	21,2	0	0	4
P - C	9:45	100	300	18	71	19	0	0	

The following test results show the real and generated traffic between branch (P) and headquarters (C). Test for data transmission services availability (intranet): ping between PC FTP server at headquarters and in the notebook in data network of remote office and vice versa - (packet size 100B, 1000B, 1600B / corresponds to the mail app).

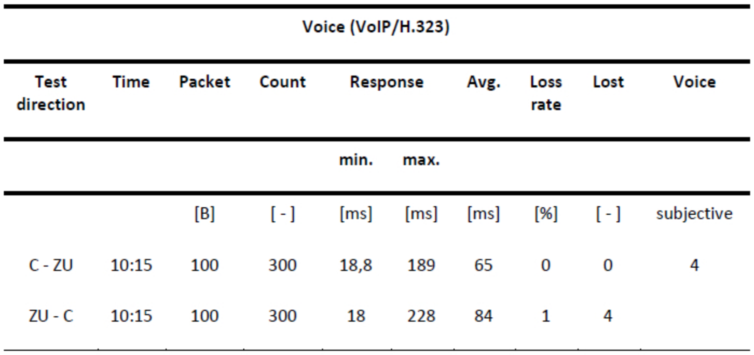
Table 4. Generated traffic



Data

Test direction	Time	Packet	Count	Response		Avg.	Loss rate	Lost
				min.	max.			
		[B]	[-]	[ms]	[ms]	[ms]	[%]	[-]
C - P	10:15	100	300	18	259	68	2	6
P - C	10:15	100	300	19	222	75	0	1
C - P	10:29	1000	300	38	322	93	1	5
P - C	10:29	1000	300	43	238	92	0	0
C - P	10:42	1600	300	54	244	107	6	20
P - C	10:42	1600	300	61	237	107	3	9

Table 5. Voice check test



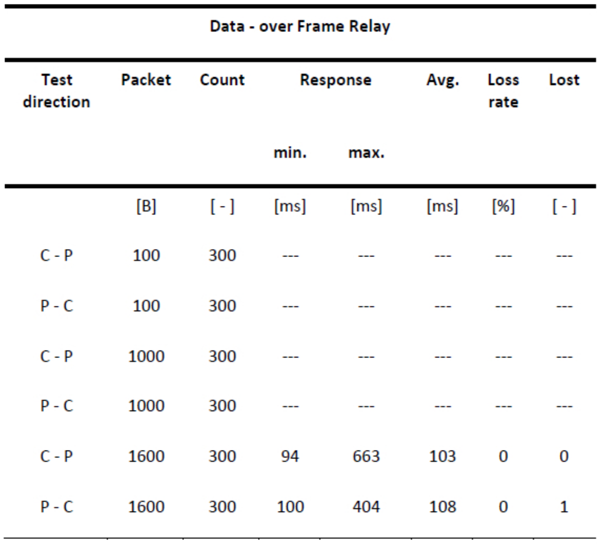
Voice (VoIP/H.323)									
Test direction	Time	Packet	Count	Response		Avg.	Loss rate	Lost	Voice
				min.	max.				
		[B]	[-]	[ms]	[ms]	[ms]	[%]	[-]	subjective
C - ZU	10:15	100	300	18,8	189	65	0	0	4
ZU - C	10:15	100	300	18	228	84	1	4	

Voice traffic testing was performed in the same way as in the previous test. The only difference was that generated traffic was added to the real one

ICMP Responses of the Original Circuit

As for comparison remote station LLnet connection, measurement of necessary scope was then performed. Real traffic over In order to be able to compare connection over Frame Relay it was necessary to transfer existing LLnet 512 kbps interfaces through Vanguard / Frame Relay as described in chapter 2.5. The results of the measurement are only of real traffic between branch (P) and center (C). Traffic load was created by transmitting 1GB file (in both directions P-C and C-P) using FTP and TFTP servers and clients.

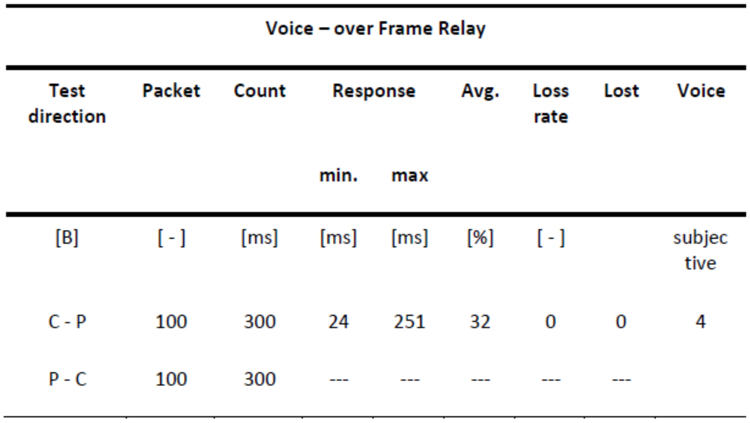
Table 6. Without load operation over Frame Relay



Data - over Frame Relay							
Test direction	Packet	Count	Response		Avg.	Loss rate	Lost
			min.	max.			
	[B]	[-]	[ms]	[ms]	[ms]	[%]	[-]
C - P	100	300	---	---	---	---	---
P - C	100	300	---	---	---	---	---
C - P	1000	300	---	---	---	---	---
P - C	1000	300	---	---	---	---	---
C - P	1600	300	94	663	103	0	0
P - C	1600	300	100	404	108	0	1

Voices transmission services availability test was conducted only in the direction headquarters (C) to the branch (P): ping between PC522 at headquarters and Vanguard 6455 at the remote office with packet size of 100B which corresponds with the typical voice traffic.

Table 7. Voice transmission test over FR

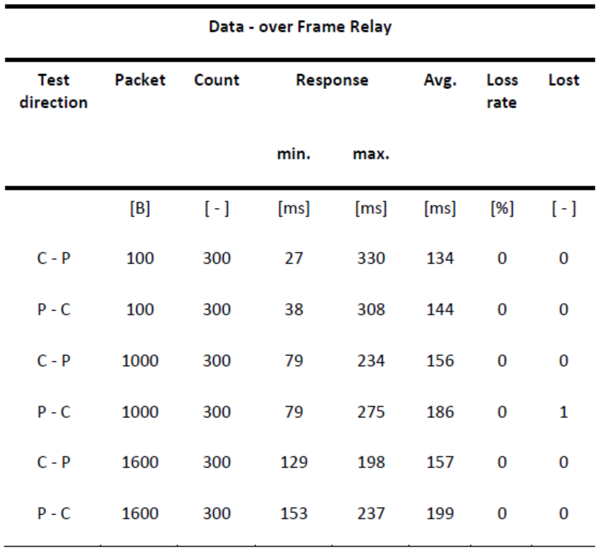


Voice – over Frame Relay

Test direction	Packet	Count	Response		Avg.	Loss rate	Lost	Voice
			min.	max				
[B]	[-]	[ms]	[ms]	[ms]	[%]	[-]		subjective
C - P	100	300	24	251	32	0	0	4
P - C	100	300	---	---	---	---	---	

Following test results show the real and generated traffic over Frame Relay between branch (P) and headquarters (C). Data transmission services (intranet) availability test: ping between PC FTP server at headquarters and the notebook located in data network at the remote office and vice versa - (packet size 100B, 1000B, 1600B / corresponds to the mail app).

Table 8. Generated traffic over Frame Relay

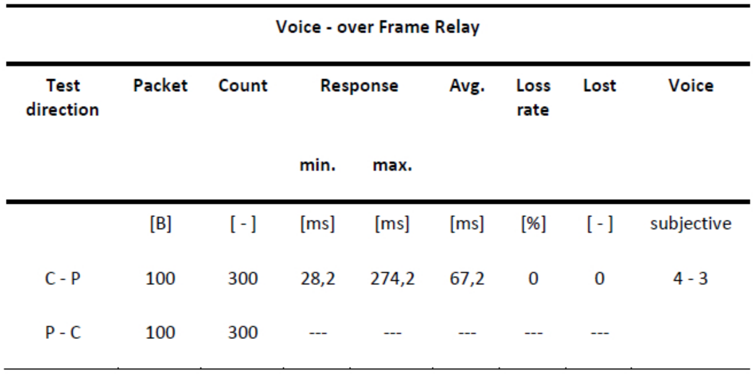


Data - over Frame Relay

Test direction	Packet	Count	Response		Avg.	Loss rate	Lost
			min.	max.			
	[B]	[-]	[ms]	[ms]	[ms]	[%]	[-]
C - P	100	300	27	330	134	0	0
P - C	100	300	38	308	144	0	0
C - P	1000	300	79	234	156	0	0
P - C	1000	300	79	275	186	0	1
C - P	1600	300	129	198	157	0	0
P - C	1600	300	153	237	199	0	0

Voice traffic availability test was conducted in the same way as in the previous test without load operation through Frame Relay. The only difference was that generated traffic was added to the real one.

Table 9. Test of voice traffic over Frame Relay



Voice - over Frame Relay

Test direction	Packet	Count	Response		Avg.	Loss rate	Lost	Voice
			min.	max.				
	[B]	[-]	[ms]	[ms]	[ms]	[%]	[-]	subjective
C - P	100	300	28,2	274,2	67,2	0	0	4 - 3
P - C	100	300	---	---	---	---	---	

Responses evaluation for an existing connection over Frame Relay was performed in the selected range. AS to be compared - see Table 10 with the values recorded only for large packets 1600B. See Tables 11 and 13 for the values only in the direction C - P. Based on the values obtained from both load and no load it is obvious that traffic is carried over a guaranteed symmetric and even with the generated traffic, loss rate was 0% without any significant differences of responses of the both directions.

4.2 Tests Evaluation

During the ten days test period in the real operation there were no flaws reported. Reviewing the operation here was influenced by the irregular use of connection by the end user depending on the course of work of the remote station, where the real traffic was typically generated by only one or two desktop computers. From a technical point of view the test results of ICMP responses met the expectations, the fluctuating quality of unguaranteed connection affects the packet loss. However, in terms of voice traffic no voice quality decrease was noticed thanks prioritization of data flows set within the IPSec tunnel. Fax traffic during the H.323 configuration against IP 6000 assessed after the test operation as ”without fault”. To ensure the fax gateway to the central site it is not necessary to apply IP PBX Innovaphone IP6000, it is enough to more affordable solution such as Innovaphone IP302 / IP305. Comparison of IMCP unguaranteed connection responses with existing solution with LLnet showed similar parameters, except for the acceptable packet loss, which is treated for data traffic from the level of the highest application layer. The results indicate that for connecting remote stations that generate more traffic by connecting multiple active PC workstations with a higher volume of voice traffic it is more likely to recommend better Internet connection with guaranteed bandwidth and availability, eventually with symmetrical zone. Tests regarding technical conditions showed the expected profitability of this data and voice services [6, 10]

5 Conclusion

Finding a suitable and optimal solution, which resulted from the requiring a cheaper way of connecting remote offices to departmental telecommunications network while maintaining existing levels of service so that it can maintain the existing technology that has included the voice and data convergence was fulfilled in the matter of a specific task. Based on the request suitable and safe solution for connecting remote stations via unguaranteed internet technology in Astaro (Sophos) has been found. Solving a specific task is based on the results of practical examination and testing. Based on the test results we managed to find more cost effective solution which also appears to be an economic implementation of Astaro technology by the form of virtualized Security Gateway. There may be concern about ensuring the security of transmitted data during transmission, especially in public administration or in the various security forces. We cannot deny possibility of breaking codes of encrypted tunnels and the eventual loss of valuable information. The objective of the testing was not the attempt to break the security. Nevertheless, we can assume that there is no reason for concerns thanks to the presence of encrypted IPsec tunnels (AES256) between the center and the remote station that meet NATO standards. It provides us with a simple question: ‘Who can say nowadays that this transfer is completely safe’? Safety risk can be found everywhere, especially in the human factor. Based on the analysis and performed tests it was able to design a functional and secure connection, which is a good solution for small and medium-sized organizations which need link remote offices with headquarters, ensure fast Internet connection and also the one which represents affordable and accessible way to provide all stations. Better Internet connection should be considered as well, particularly with guaranteed bandwidth and availability.

References

1. Horalek, J., Sobeslav, V.: Analysis of communication protocols for smart metering. ARPN Journal of Engineering and Applied Sciences, 10 (3), pp. 1438–1446 (2015)
2. Horalek, J., Sobeslav, V.: Data-networking aspects of power substation automation. International Conference on Communication and Management in Technological Innovation and Academic Globalization - Proceedings, pp. 147–153 (2010)
3. Quirem, S., Lee, B.K.: AES decryption using warp-synchronous programming. IEEE 31st International Performance Computing and Communications Conference, IPCCC 2012, art. No. 6407714, pp. 203–204 (2012)
4. Pavlik, J., Komarek, A., Sobeslav, V., Horalek, J.: Gateway redundancy protocols CINTI 2014 - 15th IEEE International Symposium on Computational Intelligence and Informatics, Proceedings, art. No. 7028719, pp. 459–464 (2014)
5. Rattal, S., Badri, A., Moughit, M.: A new wireless VoIP signaling device supporting SIP and H.323 protocols. Journal of Computer Networks and Communications, 2014, art. No. 605274 (2014)

6. Samoui, S., El Bouabidi, I., Obaidat, M.S., Zarai, F., Hsiao, K.F., Kamoun, L.: Improved IPSec tunnel establishment for 3GPP-WLAN interworking. International Journal of Communication Systems, 28 (6), pp. 1180–1199 (2015)
7. Vratonjic, N., Huguenin, K., Bindschaedler, V., Hubaux, J.-P.: A location-privacy threat stemmingfrom the use of shared public IP addresses. IEEE Transactions on Mobile Computing, 13 (11), art. No. 6757043, pp. 2445–2457 (2014)
8. Wang, S., Lv, H.: A distributed object-based IPSec multi-tunnels concurrent architecture. International Conference on Computational Problem-Solving, ICCP 2011, art. No. 6089933, pp. 471–476 (2011)
9. Wang, M., Lian, X., Zhang, X., Wu, Y., Yang, J.: Design of VoIP encryption algorithm based on H.323 protocol International Conference on Multimedia Technology, ICMT 2011, art. No. 6002243, pp. 4913–4916 (2011)
10. Xu, M.C., Radcliffe, P.J.: Building secure tunnel from PPP wireless network (2011) Wireless Personal Communications, 58 (2), pp. 337–353 (2011)