Enterprise network with software Asterisk PBX based on the PLC technology

Michal Maár, Júlia Sitárová and Miloš Orgoň

***Abstract*—This article presents the software Asterisk PBX solution design in enterprise PLC network. The description of the installation and configuration of software Asterisk PBX is involved in the design. The secure interconnection of two enterprise PLC network is implemented via the telecommunication tunnel with security grant using the Cisco routers. The connection between two Asterisk PBXs is designed in context of the establishment of the tunnel. The subject of the article is also cross/connection of exchanges Asterisk PBX and hardware PBX - IP Panasonic PBX K-NS500.**

***Keywords*—Asterisk PBX solution, PLC technology, IP Panasonic KX-NS500**

I. Introduction

VoIP (Voice over IP) technology has a number of advantages unlike public telecommunication network PSTN (Public Switched Telecommunication Network). The biggest advantage is cost savings when calling. Instead of paying telephone lines and circuits, customers pay only for the data connection. In addition, IP packets can be routed to any location with an Internet connection. As a part of the cost savings, employees can call in the enterprise network for free. Another advantage is the use of an existing network infrastructure, so it is no longer necessary to use the traditional telephone cables for interconnection of PBX. It is also possible configuration of the PBX from any location via the command line CLI or web interface. When communicating via VoIP because of additional cost savings for the company. VoIP technology is characterized by interoperability with older public telecommunication system PSTN. [1] In addition, voice in VoIP technology does not require high bandwidth (several kbit/s) and therefore is in the actual calls in corporate network, constructed based on PLC (Power Line Communication) technology which is described in [2], does not expect a significant reduction in quality of service. Therefore, PLC technology with low-cost software PBX Asterisk is suitable for the creation of a telecommunication platform for small and medium enterprise networks.

Manuscript received August 19, 2016. This article is a part of research activities conducted at Slovak University of Technology Bratislava, Faculty of Electrical Engineering and Information Technology, Institute of Telecommunications, within the scope of the project KEGA No. 039STU-4/2013 “Utilization of Web-based Training and Learning Systems at the Development of New Educational Programs in the Area of Optical Transmission Media”.

M. Maár completed his studies at the Department of Telecommunications FEI STU Bratislava in July 2016, Slovakia. (e-mail: michal.maar@gmail.com).

J. Sitárová completed her studies at the Department of Telecommunications FEI STU Bratislava in July 2016, Slovakia. (e-mail: sitarovajulia@gmail.com).

M. Orgoň is Associate Professor in the Institute of Telecommunications FEI STU in Bratislava, Ilkovičova 3, 81219 Bratislava, Slovakia,. (e-mail: orgon@ktl.elf.stuba.sk).

II. Softvare PBX Asterisk

PBX Asterisk is freely available software solution based on Linux. In addition to IP telephony, this PBX allows to use digital ISDN (Integrated Services Digital Network) and analog phones that are still in use in many companies. Asterisk also supports connectivity to the PSTN and other VoIP networks. Nowadays, the software PBX Asterisk has become a big competitor for traditional hardware PBX. One of the Asterisk advantages is the low cost for constructing PBX, whereas the PBX can be run on a personal computer or server. Another advantage is quick and easy installation and management over web interface control panel. Asterisk supports multiple protocols such as IAX, SIP, H.323 and MGCP. Asterisk solution is designed mainly for schools, hotels, small and medium-sized companies, where it's possible to call the flaps completely free. Asterisk provides a large number of services and functionalities. The most common include conference calls, forwarding, own numbering plan, voicemail, detailed information about each call, IVR, ACD, etc. [3]

The introduction of software PBX Asterisk in corporate environments has several advantages. Software PBX which is working on a more powerful PC or smaller server can convey up to several hundred calls. PBX advantage is that employees in the enterprise network can call each other for free.

A. Design and Implementation of Software PBX AsteriskNOW

In Fig. 1, there is an enterprise PLC network based on PLC technology, where was implemented design of software PBX. Enterprise PLC network consists of a ground floor and two floors. Floors are connected to each other by PLC technology, which uses the powerline communication in the building. Software and hardware IP phones, two switches, personal computers, router R-BA, printer and Wi-Fi router that provides connectivity for mobile phones with the application Zoiper are connected to the enterprise PLC network. Router R-BA is used to connect enterprise PLC network to external networks or Internet. Asterisk PBX which is running on a laptop is also implemented in enterprise network, too. Numbering and IP addressing plan are created to be able to connect up to 100 IP phones in each floor. Numbering and IP addressing plan are in Table I.

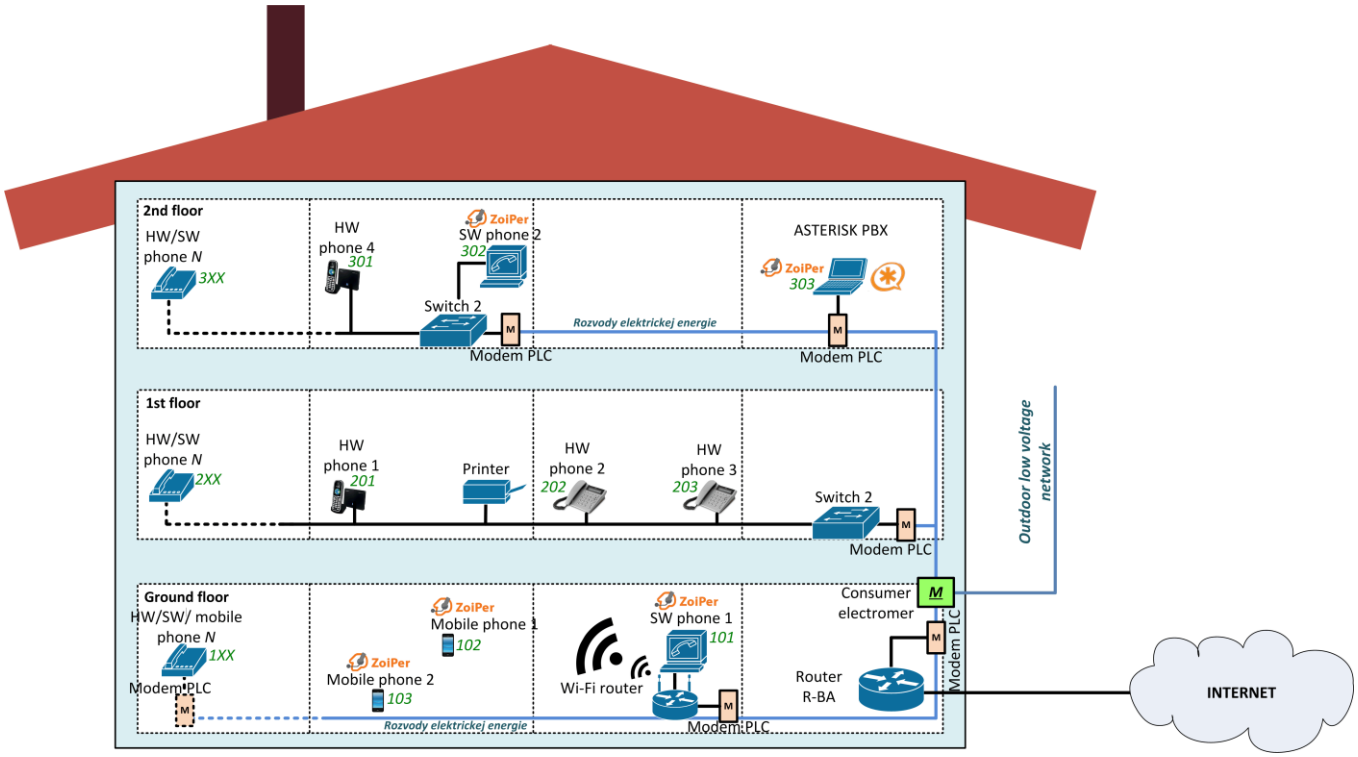

Fig. 1 - Design of enterprise PLC network

TABLE I –
Numbering and IP addressing plan

Floor	Extension number	Position	Device	Device IP address	PBX IP address
ground floor	101	Call center operator	SW phone	10.0.0.30/23	10.0.0.4/23
ground floor	102	Seller num.1	Mobile phone	10.0.0.31/23	10.0.0.4/23
ground floor	103	Seller num.2	Mobile phone	10.0.0.32/23	10.0.0.4/23
ground floor	1XX	New employee	SW/HW phone	10.0.0.33 - 10.0.0.130/23	10.0.0.4/23
1. floor	201	CEO	HW phone	10.0.0.131/23	10.0.0.4/23
1. floor	202	Accountant	HW phone	10.0.0.132/23	10.0.0.4/23
1. floor	203	Economist	HW phone	10.0.0.133/23	10.0.0.4/23
1. floor	2XX	New employee	SW/HW phone	10.0.0.134 - 10.0.0.230/23	10.0.0.4/23
2. floor	301	Programmer num.1	HW phone	10.0.1.1/23	10.0.0.4/23
2. floor	302	Programmer num.2	SW phone	10.0.1.2/23	10.0.0.4/23
2. floor	303	IT technician	SW phone	10.0.1.3/23	10.0.0.4/23
2. floor	3XX	New employee	SW/HW phone	10.0.1.4 - 10.0.1.100/23	10.0.0.4/23

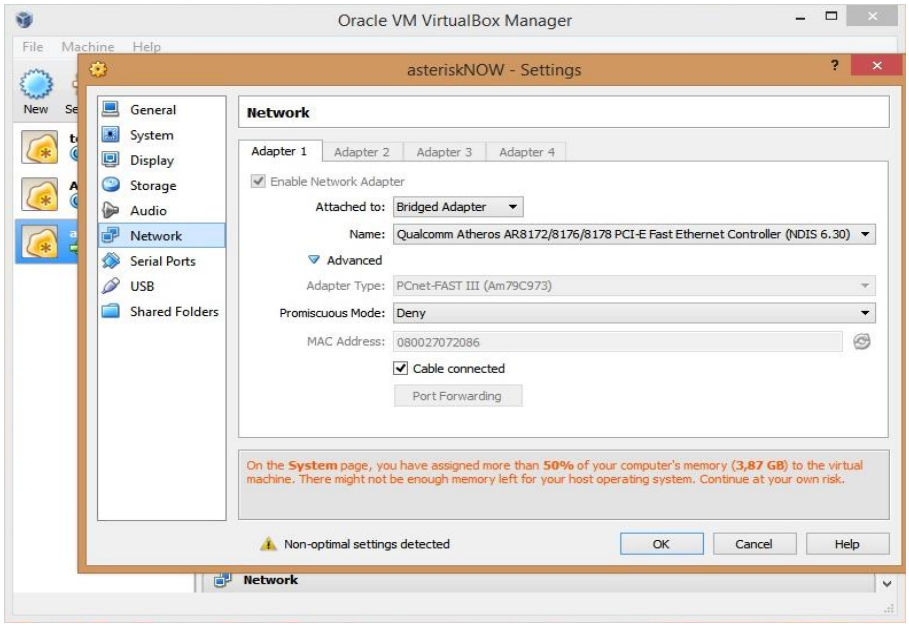

Fig. 2 - Network settings

It was necessary to install virtualization tool Oracle VM VirtualBox to create a PBX Asterisk. VirtualBox can be used on your personal computer to run more virtual operating systems. In this case, the virtual PC serves like as a Asterisk PBX. Installation of Asterisk requires a relatively powerful computer to be able to deliver traffic for its original operating system, but also for virtual computer system. For that reason, CPU Intel Core i5-3210M, operating system Linux (type: Other Linux 64 bit) and three GB RAM were used to create a virtual server.

New virtual machine operating on the platform Linux in 64 bit version was created by the installed software VirtualBox. Than it was necessary to open AsteriskNOW.iso file which is freely available in the 32 or 64 bit version. During the installation, it was necessary to choose the network interface, with which it should Asterisk cooperate. In our case eth0 interface was used. In the next step it was necessary to specify TCP/IP settings and time zone, namely Slovakia/Bratislava. Finally, it was necessary to set the username and password in the Asterisk PBX. Access data are used for remote connections over SSL protocol.

After successful installation of Asterisk it was necessary to make a few configuration settings. In VirtualBox settings in created virtual machine AsteriskNOW, there was allowed network adapter and a type of connection was selected to bridge adapter. The network adapter and the type of connection to the bridged adapter was enabled in the network settings of the newly created virtual machine AsteriskNOW in VirtualBox. These settings are shown in Fig. 2. At next step, it was necessary to set the size of operational memory and number of processor cores that are used by Asterisk server. In the network settings it was necessary to set up sharing for VirtualBox access type. This setting allows to other network users to connect through a local computer connection. In the next step it was necessary to set up IP address from private ranges, in our case „10.0.0.3", subnet mask „255.255.254.0" and preferred DNS server „10.0.0.1" on this type of access. As to communicate with other computers in created LAN, ethernet interface of the server has been set from the same IP address range, therefore „10.0.0.5" and subnet mask „255.255.254.0". In order to allow communication with other networks, was also necessary to set up the default gateway „10.0.0.1" on the router located on the edge of the network.

B. AsteriskNOW Configuration

In addition to the already mentioned settings it was necessary to create and customize other settings. Asterisk allows to manage through a web interface or the command line CLI. To access the command line you need to enter authentication credentials that were set during the installation. Because of its difficulty, Asterisk configuration over the command line interface CLI is mainly used by experienced administrators. Asterisk runs on the operating system Linux so network administrators use for management Linux commands. All files have the same syntax, but in each file are set various functions. The file structure looks like:

```
[section_title]
option=value.
```

After authentication, it was necessary to set general network settings like PBX IP address, subnet mask, network and default gateway. There settings are located in */etc/sysconfig/network-scripts/ifcfg-eth0* and their modification is possible with the *nano* Linux command. After installation, PBX IP address was obtained by DHCP protocol in the default configuration. But if we need static IP address of PBX then it would be necessary to change the *BOOTPROTO* value to *"none"*. It was necessary to set up:

```
  IPADDR="10.0.0.4"       ;      PBX      IP
address
  NETMASK="255.255.254.0"; subnet mask
  NETWORK="10.0.0.0"      ; network ID
  GATEWAY="10.0.0.1"      ;         default
gateway
```

After saving the Asterisk PBX it was necessary to restart computer using the command „service network restart". Asterisk IP address and config.d network settings can be verified by the command „ifconfig eth0". After these settings were Asterisk installed with the basic configuration, which was necessary for further work with PBX.

```
[root@localhost ~]#
[root@localhost ~]#
[root@localhost ~]#
[root@localhost ~]# ifconfig
eth0      Link encap:Ethernet  HWaddr 08:00:27:68:BC:ED
          inet addr:10.0.0.4  Bcast:10.0.1.255  Mask:255.255.254.0
          inet6 addr: fe80::a00:27ff:fe68:bced/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:0 errors:0 dropped:0 overruns:0 frame:0
          TX packets:367 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:0 (0.0 b)  TX bytes:18238 (17.8 KiB)
          Interrupt:19 Base address:0xd020

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:16436  Metric:1
          RX packets:3647 errors:0 dropped:0 overruns:0 frame:0
          TX packets:3647 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:337199 (329.2 KiB)  TX bytes:337199 (329.2 KiB)

[root@localhost ~]#
[root@localhost ~]# _
```

Fig. 3 – Sample of Asterisk PBX command line

C. *Configuration by Web Interface*

Through a web browser and IP address of Asterisk PBX, which can be odtained from the command line of virtual PBX (Fig. 3).

D. *Creating Etensions*

Asterisk supports multiple protocols to create extensions, such as SIP, IAX2, DAHDi, etc. In this solution are used SIP extensions. First, you need to select an *Applications* and than *Extensions* item. In this way it is possible in the web interface to create, modify and delete extensions. When creating extensions, there are important parameters like *User Extension*, *Display Name* and *Secret*. Each modification in the management of Asterisk PBX must be confirmed by the *Apply Config* item.

E. *Hardware Phones Configuration*

In this solution of Asterisk PBX in PLC network, there have been implemented hardware (Gigaset C470IP and Telco PH800N) and software (Zoiper) IP phones.

Wireless IP phone Gigaset C470IP can communicate with its base station up to 300 meters. It allows mixed telephony (PSTN and VoIP). Handset with ECO DECT technology reduces transmission power automatically. The transmission power is increased by distance - reduction of the transmitting power drops almost to zero if the handset is placed in dock station. This technology allows reducing energy consumption up to 60%. Gigaset supports multiple voice codecs including the most widely used G.711, G.729 and G.723.

The advantages of IP phone Telco PH800N include simplicity, small size, phone and extension configuration directly on IP phone without using web interface (configuration is also possible over the web interface).

Telco PH-800N may also be used in combination with other VoIP services. The phone should be powered from AC power. Firmware is upgradeable over Internet. The device also supports the PIN code protection, call forwarding or wait for the next call function.

On the left side of Fig. 4, there is a wireless IP phone Gigaset with the base station and the right side displays the IP phone Telco.

Fig. 4 – IP phones Gigaset C470IP and Telco PH800N

The advantage of softphones is a quick configuration and possiblity to access the phone on a PC or a portable device such as a mobile phone or tablet. There are many applications that supports softphones. For our solution was selected frequently used software called Zoiper – free software with possibility of multiple voice and video codecs, which supports creation of multiple extension types like SIP, IAX, etc. Zoiper is also available for Android and iOS. Softphone is suitable for employees who work outdoors, such as sellers or managers.

When you create an extension using SIP software Zoiper, you must enter three important parameters: extension number, password and Asterisk PBX IP address. Fig. 5 shows the config.d and registered SIP extension.

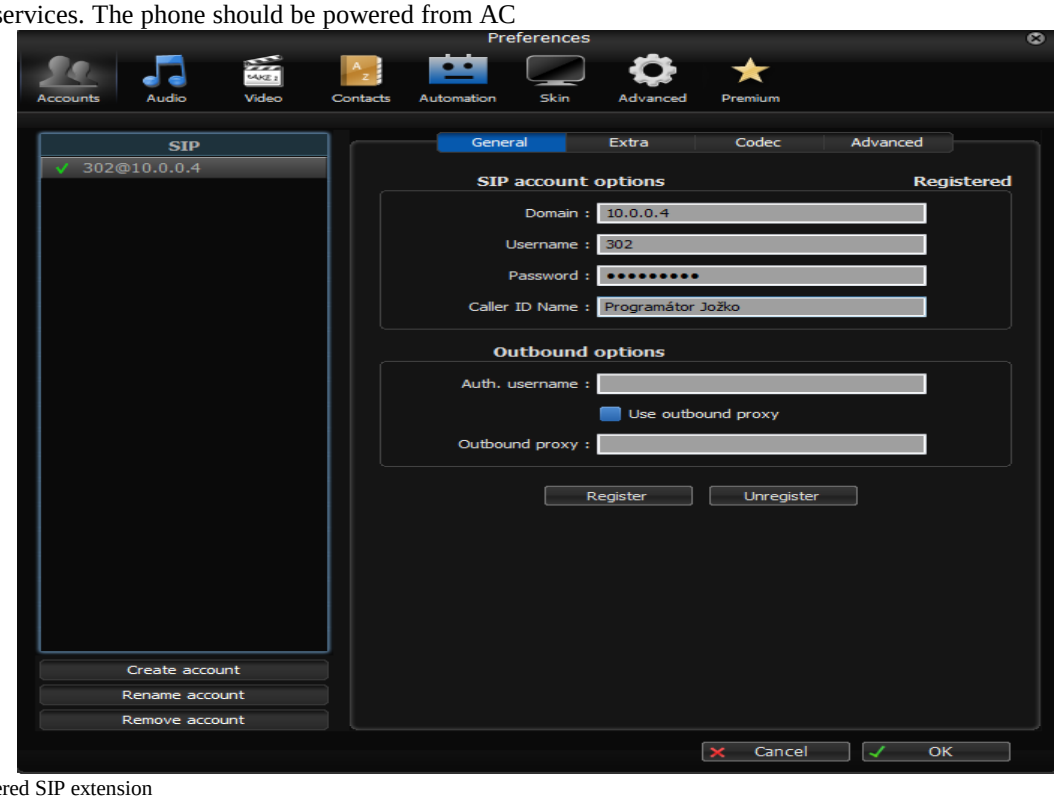

Fig. 5 – Registered SIP extension

III. Interconection of Two Corporate Networks Design for the Telecommunication Purposes

Telecommunication networks provide a wide range of opportunities to get new information, communicate and work over long distances. Demands on the quality of services are still increasing. Enterprises require not only fast, but also secure communication, both within one building or two buildings, but also between multiple remote offices often located abroad. Tunneling is used to satisfy the quality of these services, but also to increase safety. Tunneling is a process of transferring data from the local network A to the local network B over public network (e.g. Internet). After implementing site-to-site tunnel, sites can communicate just as if they were placed in the same segment. To prevent interception of communications, the connection between sites can be secured by encryption. Telecommunication tunnels are mainly used in corporate networks to secure connection between two or more remote sites. In general, there are several tunneling protocols that differ from each other in implementation, possibility to use and security. The most common tunneling protocols are: GRE, IPsec, PPTP, L2TP, 6to4, SSH, etc. Some of these protocols has began to use in combination with another tunneling protocols due to their diverse functionality, for example pair GRE and IPsec or L2TP and IPsec. [4]

GRE (Generic Routing Encapsulation) was developed by Cisco and documented in RFC 2784. GRE creates a virtual point-to-point link between remote locations by Cisco routers over IP network. Through this protocol, that operates at Layer 3 of RM OSI model, you can encapsulate a wide variety types of packets to IP tunnel. Fig. 6 shows the structure of encapsulated packet. The advantage of GRE is to support unicast, broadcast and multicast transmission between multiple sites and also GRE allows to transmit static and dynamic routing protocols such as RIP, OSPF, etc. In fact, other tunneling protocols are not able to provide this functionality so the GRE is irreplaceable. [5].

Fig. 6 The structure of encapsulated packet

IPsec (Internet Protocol Security) is an IETF standard that defines how to safely access to a virtual private networks and also provides secure IP packets transmission. IPsec works at Layer 3 of RM OSI model in two modes: transport and tunneling mode. It is implementable with IPv4 and IPv6 protocol. However, IPsec can not encapsulate packets and routing protocols. For this reason, functionality of protocol GRE is very elegantly combines with safety of protocol IPsec. Universal tunnel GRE is placed inside a secure tunnel IPsec, as you can see in Fig. 7.

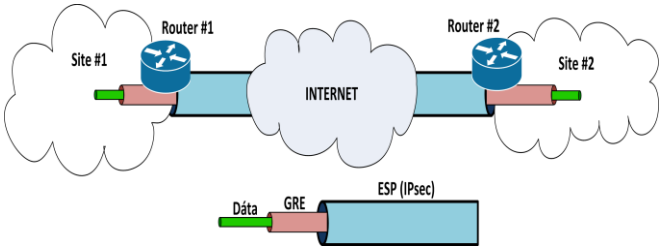

Fig. 7 GRE over IPsec

A. *Interconnection of Two Sites by GRE over IPsec Protocol*

The network design was designed for the company with office in Bratislava, assuming expansion to the Thorn city (opening branch in Poland). The new office in Poland was necessary to connect with the office in Bratislava. Those two connected sites should have to act like being in single segment of enterprise network. A very important requirement was the security of data transfer between these sites. Creating a GRE tunnel and subsequent security through IPsec ensuring, respectively, use the GRE over IPsec protocol, seemed to as to be the most ideal way to connect these sites.

The tunnel through GRE protocol can be formed between routers placed in the edges of two local area networks. The Cisco 1841 routers with operating system IOS version 12.4 were used for these purposes. The GRE tunnels with IPsec protocols are supported by the routers mentioned above. License package *securityk9* need to be installed and activated for support of security protocols in newer versions of operating system IOS (version 15 and upper).

Fig. 8 - Cisco ISR 1841

Cisco ISR 1841 (Fig. 8) are modullar routers with LAN and WAN interfaces. Routers provide basic features, such as linking multiple computer networks, security, fast and high quality service transmission for small to medium sized enterprises. Cisco routers contain flash memory the most common of 64 MB, AUX port, USB port, console port, two serial ports and two fastethernet ports. You can buy additional modules, which allow expansion of port capacity.

Cisco ISR 1841 routers have been config.d by free software PuTTY. PuTTY is used as a client SSH, Telnet, Rlogin and is also used for a serial COM port connections. At first configuration router sused COM port - it is possible to manage the Cisco router through console and command line after connecting the router's console port with PC's COM port. The computer network was formed to create a connection between two remote areas as is shown in fig. 9. Router ISP serves as a simulation of the Internet, because the left and right side of the router ISP are networks with public IP address range. R-BA and R-TO routers are on the edge of the networks and provide routing between sites.

Between R-BA and R-TO was created GRE over IPsec tunnel.

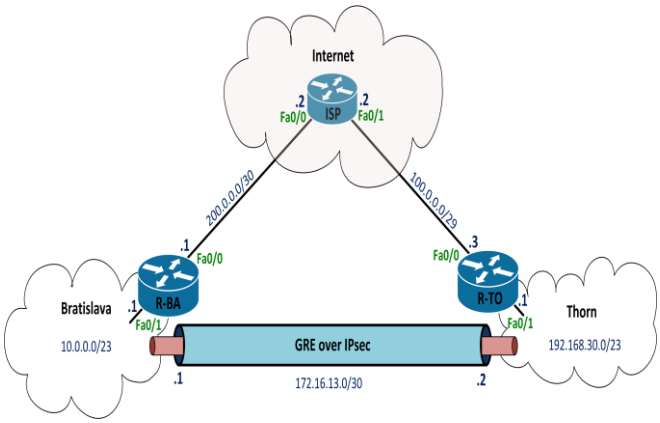

Fig. 9 – Connection of two remote locations design via Cisco routers

Routers R-BA and R-TO were config.d as follows:

1) The router was renamed from the original name „Router“ to „R-BA“ and at the interfaces FastEthernet 0/0 and 0/1 have been set up IP addresses, like in Fig. 9. Each interface has been enabled by command „noshutdown“.

   The router was renamed from the original name „Router“ to „R-BA“ and at the interfaces FastEthernet 0/0 and 0/1 have been set up IP addresses, like in Fig. 9. Each interface has been enabled by command „noshutdown“:

```
Router#configure terminal
Router(config)#hostname R-BA
R-BA(config)#interface fa0/0
R-BA(config-if)#ip address 200.0.0.1
255.255.255.252
R-BA(config-if)#no shutdown
R-BA(config-if)#exit
R-BA(config)#interface fa0/1
R-BA(config-if)#ip address 10.0.0.1
255.255.254.0
R-BA(config-if)#no shutdown
R-BA(config-if)#exit
```

2) Static routing through an ISP router due to interconnection of routers R-BA and R-TO was set by the following command:

```
R-BA(config-if)#ip route 100.0.0.3
255.255.255.255 200.0.0.2
```

3) Between routers R-BA and R-TO, GRE tunnel has been created by virtual interface called „tunnel 1“. Tunneling mode was used and set to GRE. Source IP address which is located at the interface FastEthernet 0/0 was specified by the command „source“. Subsequently, the destination IP address was specified by the command „destination“. Then, on R-BA router was set start IP address „172.16.13.1“ and on the router R-TO end IP address „172.16.13.2“ of the tunnel. These two IP addresses must be on the same subnet, in this case „255.255.255.252“. Finally, the dynamic routing protocol OSPF was applied, which will be transmitted by GRE tunnel. OSPF requires the IP address of the neighbor network, wildcard mask and set the area. In this case was set area 0. Depending on the configuration of the router R-BA, router R-TO is config.d analogically:

```
R-BA#configure terminal
R-BA(config)#interface tunnel 1
R-BA(config-if)#tunnel mode gre ip
R-BA(config-if)#tunnel source
fastEthernet 0/0
R-BA(config-if)#tunnel destination
100.0.0.3
R-BA(config-if)#ip address 172.16.13.1
255.255.255.252
R-BA(config-if)#router ospf 1
R-BA(config-router)#network 172.16.13.0
0.0.0.3 area 0
R-BA(config-router)#network 10.0.0.0
0.0.1.255 area 0
```

4) To verify the configuration, it is possible to use several commands, for example ,,show ip interface brief | include Tunnel", ,,show interface Tunnel 1" or ,,show ip route ospf".

5) In this part of the configuration was created GRE tunnel between two routers, if you like between LAN networks in Bratislava and Thorn. Communication over GRE tunnel is not encrypted. To secure communication between sites, GRE was placed into IPsec tunnel. Then it was necessary to create ISAKMP policy on R-BA. In ISAKMP policy AES encryption algorithm, authentication with shared password, Diffie-Hellman group 2 and lifetime 3600 seconds were set. The configuration was repeated analogically on the router R-TO and finally was set on both routers shared key „PASS“ with the IP address of the remote neighbor:

```
R-BA(config)#crypto isakmp policy 10
R-BA(config-isakmp)#encryption aes 256
R-BA(config-isakmp)#authentication pre-
share
R-BA(config-isakmp)#group 2
R-BA(config-isakmp)#lifetime 3600
R-BA(config)#crypto isakmp key PASS
address 100.0.0.3
```

6) In the next step there was created transform set, in which was set IPsec to transport mode. Using AH or ESP protocols, encryption standard AES with key length of 256 bits and hash algorithm HMAC-SHMA were defined in the created set of transformation named TRANS. This transform set was analogacally set on the router R-TO:

```
R-BA(config)#crypto ipsec transform-set
TRANS esp-aes 256 esp-sha-hmac
R-BA(config-if)#mode transport
```

7) The next step was to create encrypted map named MYMAP. The map contains the definition of neighbor (100.0.0.3), link to transform set TRANS and *access*

list 100. Access lists define packets which will be encrypted by crypto map. By using the list of *access list 100* is permitted all GRE traffic which is not blocked. Crypto map and access list was created analogically on R-TO router:

```
R-BA(config)#crypto map MYMAP 10 ipsec-isakmp
R-BA(config-crypto-map)#set peer 100.0.0.3
R-BA(config-crypto-map)#set transform-set TRANS
R-BA(config-crypto-map)#match address 100
R-BA(config)#access-list 100 permit gre any any
```

8) The last step was the activation of crypto map. The map refers to the interface that serves as the end point of the tunnel.

```
R-BA(config)#interface fastEthernet 0/0
R-BA(config-if)#crypto map MYMAP
```

There are several ways to verify the functionality of the GRE tunnel encryption. Probably the quickest way is a listing of command „`show crypto session`“, which is shown in Fig. 10:

```
R-BA#show crypto session
Crypto session current status

Interface: FastEthernet0/0
Session status: UP-ACTIVE
Peer: 100.0.0.3 port 500
  IKE SA: local 200.0.0.1/500 remote 100.0.0.3/500 Active
  IPSEC FLOW: permit 47 0.0.0.0/0.0.0.0 0.0.0.0/0.0.0.0
        Active SAs: 2, origin: crypto map
```

Fig. 10 – Verify the encryption functionality

All data that are transmitted between the routers R-BA and R-TO with the public IP addresses at the network edge are encrypted. The traffic between routers R-BA and R-TO was captured using the PC with software Wireshark which was placed to the connection between the routers. Fig. 11 shows encapsulated packets using the protocol ESP.

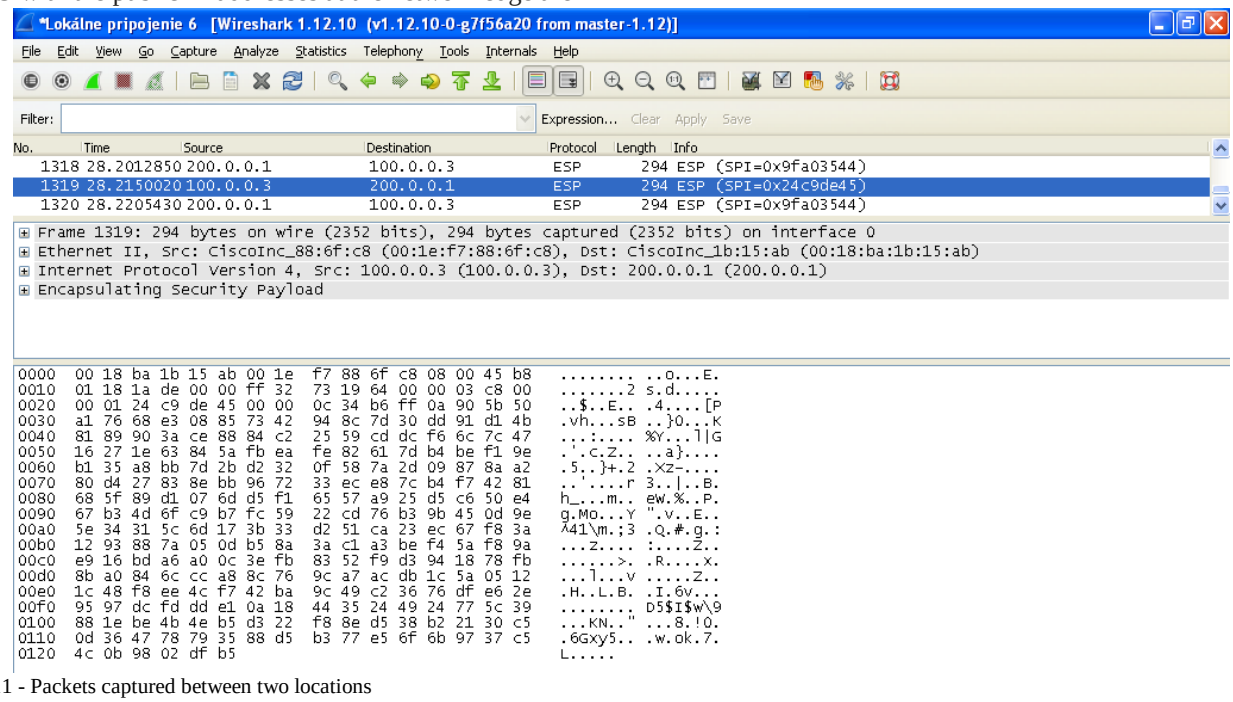

Fig. 11 - Packets captured between two locations

Communication between two sites has been provided by GRE over IPsec. This allowed that employees can securely send internal data to each other.

B. Interconnection of Two Asterisk PBXs by IAX Protocol

The introduction of two Asterisk PBXs and their interconnection through trunk allows a reduction in load of the link, redundancy and prevention against outages. For two sites (A and B) it is prefered to have one branch PBX for each site. Calls in each site (A and B) runs through internal PBX and in the event of connection loss between sites A and B, employees in site B can communicate between each other. If the PBX is only in the site A and all users from the site B would be connected to PBX from site A, as in the case of connection loss between site A and B, you wouldn't make calls between employees in the site B. Some enterprises, such as factories, can not afford these failures. The advantage of introducing PBX in each of the sites is redundancy. In the case of outage PBX in the site A, the employee IP phones can connect to the PBX in site B and thus continue in the communication.

Interconnection of PBXs is often established via protocol SIP or IAX2 in practice. The advantage of SIP trunk is easier error detection, which are in the form of text messages. In IAX2 trunk are error messages in binary form. On the other hand, the advantage of IAX2 trunk is configuration simplicity when connecting two PBXs, which are located in other networks. SIP trunk is more difficult to config. if PBXs are located in other networks.

After secure interconnection of sites in Bratislava and Thorn using routers R-BA and R-TO, employees can share internal data and communicate with each other. The interconnection of two software PBXs using IAX2 protocol was designed and implemented for reasons of redundancy and to save the bandwidth. Interconnection configuration of two software PBXs is shown in Fig. 12.

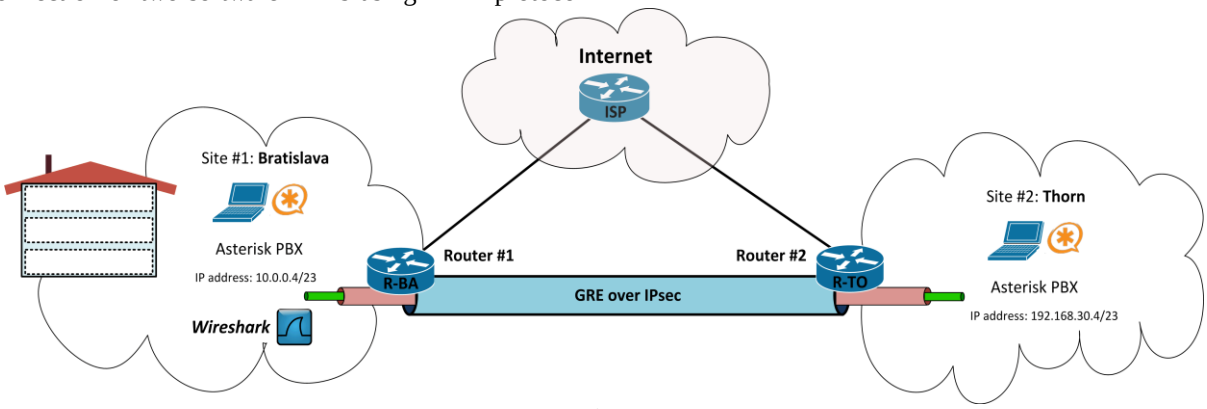

Fig. 12 - Connection of two sites by IAX2 trunk

TABLE 2
IAX2 trunk parameters

Parameter:	**Value:**	**Note:**
Trunk Name:	To Thorn_iax	Trunk name
Outbound CallerID:	Call from Bratislava	Name, which is displayed on the phone to user in Thorn
Dialed Number Manipulation Rules:	8XX 9XX	Extension ranges in Thorn (800-899 and 900-999)
Peer details:	host=192.168.30.4 username=thorn secret=passtrunk type=peer qualify=yes context=from-internal trunk=yes	IP address of PABX, on which heads trunk (in Thorn) named: *thorn* and password: *passtrunk*
User Context ID:	Bratislava	Account name associated with the parameter User Details
User Details:	secret=passtrunk type=user host=192.168.30.4 context=from-trunk	Connection parameters (trunk)

IAX2 trunk configuration between two Asterisks consists of three basic steps: trunk configuration, inbound and outbound routes. It is necessary to configure both Asterisks analogically. The following procedure describes how to config. Asterisk PBX in Bratislava part.

It is necessary in the management of PBX Asterisk select *Trunks* button. To interconnect of Asterisk PBXs in this design was selected IAX2 protocol, and it was necessary to set the following parameters (Table 2).

The second step was configuring of outbound route, then was created new outbound route named *ThornExt_iax* and the following parameters was set (Table 3).

TABLE 3
Outbound route parameters *ThornExt_iax*

Parameter:	**Value:**	**Note:**
Route Name:	ThornExt_iax	Outbound route name
Dial Petterns that will use this Route:	8XX 9XX	Extension range in Thorn (800-899 and 900-999)
Trunk Sequence for Matched Routes:	To Thorn_iax	Trunk with which will outbound route cooperate

Finally, it was created Inbound route named *From_Thorn_iax*. In the Inbound route it was necessary to create *Ring Groupe*. When creating a ring group, it has been set it's number, a list of all extensions and destination extension required in case of problems. After configuration of all required parameters for Asterisk PBX in Bratislava it was necessary to config. Asterisk PBX analogically in Thorn.

To verify IAX2 trunk between PBX's the Wireshark software was used. It was possible to watch the communication between PBX's by Wireshark. A computer with installed software Wireshark was placed between the R-BA router and Asterisk PBX in Bratislava. Fig. 13 shows captured communication of VoIP call between PBX's in Bratislava (IP 10.0.0.4/23) and Thorn (IP 192.168.30.4/23).

The call was processed from the extension 101 in Bratislava to extension 805 in Thorn. Asterisk PBX web interface enables a several functions. One of them is monitoring of every activity of PBX, known as LogFiles. Fig. 14 illustrates the process of dial an extension 805 in Thorn from extension 101 located in Bratislava.

This log in the Fig. 14 shows successfull establish of connection between two software PBXs in Bratislava and Thorn.

C. Interconnection Design of Two PBXs via MPLS Network

The telecommunication infrastructure design was designed for the company that founded another office in Slovakia (in the Poprad city). The office disposed of IP Panasonic PBX KX-NS500, the PLC backbone communication network composed of ZyXEL PLA5206 modems with transfer speed up to 1000 Mbps. The IP Panasonic PBX had also an extension module KX-NS520 that allows you to connect a larger number of telephones. Therefore, it was necessary to resolve interconnection of hardware PBX Panasonic KX-NS500 with software Asterisk PBX in Bratislava additionally.

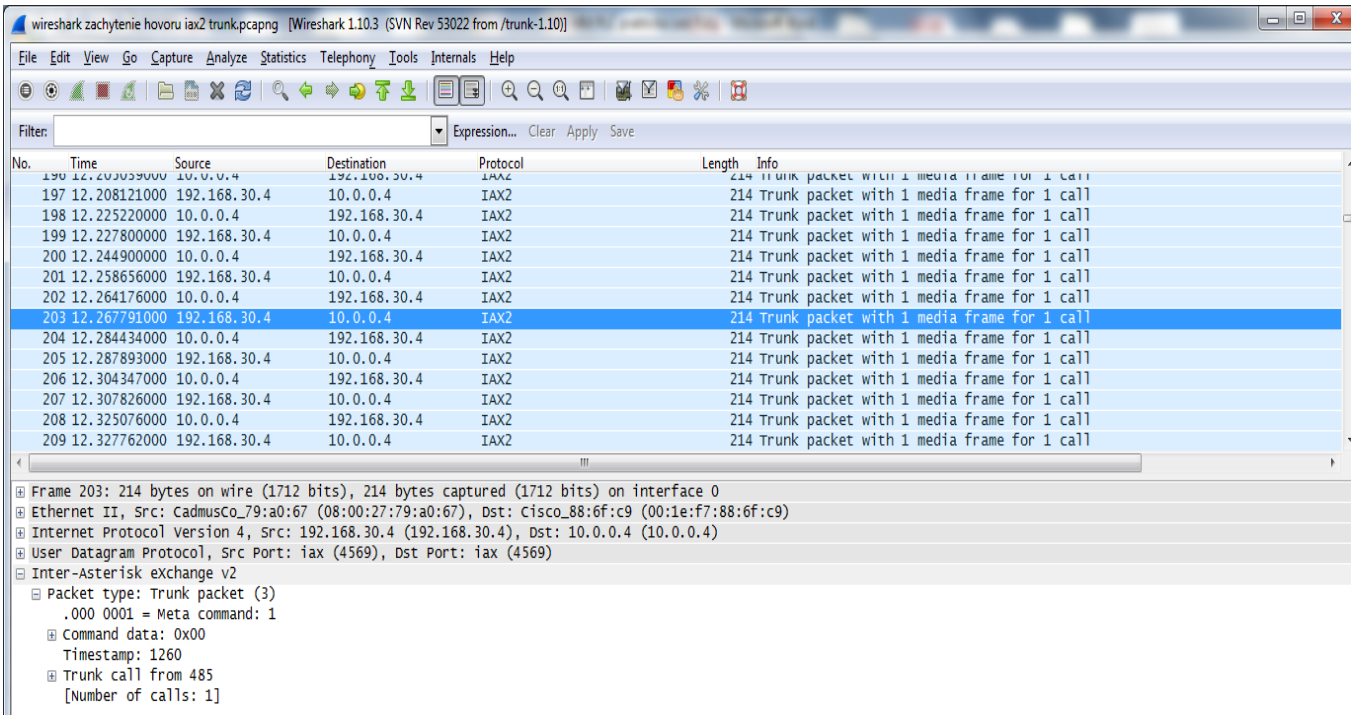

Fig. 13 - Captured communication between two Asterisk PBXs

Fig. 14 - Capturing event of dial extension 805 in Thorn

PLC modem ZyXEL PLA5206 is one of the newest products of PLC technology, which is based on the HomePlug AV2 standard and is also compatible with previous standards. ZyXEL PLA5206 is show in Fig. 15. This modem provides a theoretical bit rate up to 1000 Mbit/s. Modem operates in the frequency range from 2 to 86 MHz and has the function of QoS support, which is important in VoIP voice services. These new modems are much easier to use than the older one. It is necessary to connect PLC modems to the power lines and also to the devices. Then the communication between these devices can be established. Management via web interface is not needed, because the modems are automatically paired. Secure communication using AES encryption with a key length of 128 bits is automatically established too.

The Panasonic PBX KX-NS500 shown in Fig. 16 creates an intelligent hybrid IP communications system designed for small and medium-sized businesses which is easily configurable and expandable according to the needs of the business. The PBX supports to connect many different types of terminals – analogue, digital phones, SIP software and IP telephones. The advantage in economic terms is the ability of using analogue and digital telephone. As a result, reuse of an older communication system of the company is possible. The PBX provides many helpful features that can simplify the communication of the company – for example call centers which CTI server function is not needed, or Unified Communications function. The PBX provides recording and backup of conversations in relation to improving the communications services of company using statistics and analysis of customer calls. The PBX is managed through a web interface, where all the PBX`s settings can be config.d and managed.

Fig. 15 Modem ZyXEL PLA5206

Fig. 16. Panasonic PBX KX-NS500

The designed scheme of interconnection between two segments of enterprise network is shown in Fig. 17. The first segment was served by Asterisk PBX and the second

segment was served by hardware Panasonic PBX KX-NS500.

In previous section the design and forming of LANs in Bratislava and Poprad were described in detail. At this stage the networks were ready for interconnection. It would be necessary to use a provider`s network to connect the sites via MPLS network. The network design involves this way of interconnection due to its reliability, speed and security. MPLS network is set of switches or routers that switch all the packets according to their tag. The tag is added to each packet at the entrance of the network. As a result of simplicity, the transfer speed of the packets is higher because the packets are not routed with complex logic – packets are simply switched.

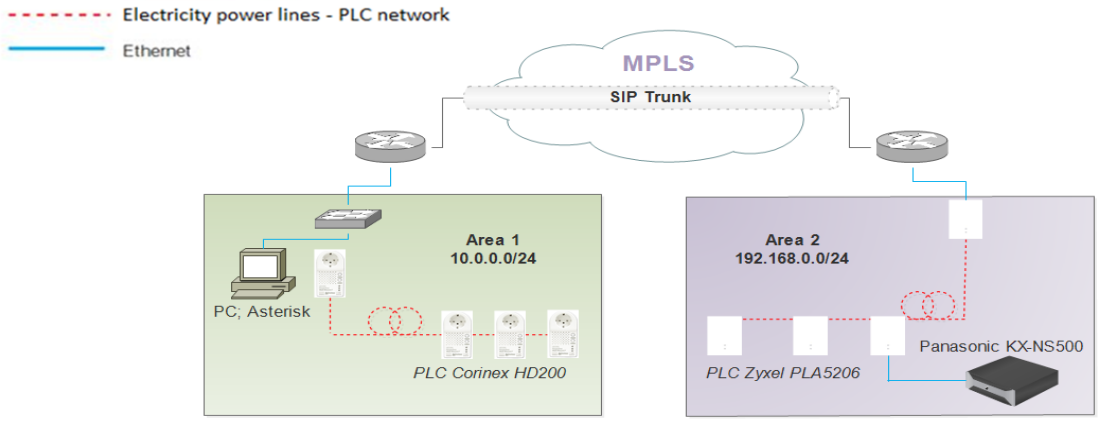

Fig. 17 Interconnection of PBXs via MPLS network

Considering the VoIP traffic in our design, we had to select the reliable, fast and QoS providing connection. The MPLS network has all of mentioned requirements – apart of its speed it is a very stable network because of the simple switching logic. The QoS guarantee is related to ability of assigning different levels of priority to each packet in MPLS network. Considering these reasons, use of the MPLS network in the design was selected.

Finally, only the logical connection between software Asterisk PBX and hardware Panasonic PBX KXNS500 via SIP Trunk was implemented due to economical reasons. However, this solution is a subject of another article because of the scope of this article.

IV. Conclusion

The purpose of the article was the software Asterisk PBX solution design in enterprise PLC network. The description of the installation and configuration of software Asterisk PBX was involved in the design. The secure interconnection of two enterprise PLC network was implemented via the telecommunication tunnel with security grant using the Cisco routers. In final part, the connection between two Asterisk PBXs was designed in context of the establishment of the tunnel. A part of the design was the design of connection with hardware IP Panasonic PBX K-NS500.

Acknowledgment

This article was created with the support of the project KEGA No. 039STU-4/2013 “Utilization of Web-based Training and Learning Systems at the Development of New Educational Programs in the Area of Optical Transmission Media”.

References

[1] B. Hartpence, Packet Guide to Voice over IP, O'Reilly Media Inc., ISBN 978-1-449-33967-8

[2] M. Orgoň, R. Róka, J. Mišurec,: **Smart Grid a komunikace PLC,** Nakladateľstvo STU Bratislava, 396 pages, 2015, ISBN 978-80-227-4356-3, č. kateg. 85-214-2015

[3] M. Vozňák, Telefonní ústředny Asterisk, Teorie a praxe IP telefonie 3, dvoudenní odborný seminář, 2008

[4] D. Adam, M. Gemeranová, L. Maršík, P. Sucha, Tunneling, Univerzita Komenského – Fakulta matematiky, fyziky a informatiky, Bratislava

[5] Cisco Networking Academy, CCNA4 Routing and Switching, Connecting to Networks, Securing Site-to-Site (Module 7), <www.netacad.com>

Michal Maár was born in Bratislava, Slovakia, in 1992. He received the B.E. and M.E. degrees in Faculty of Electrical Engineering and Information Technology of Slovak University of Technology (FEI STU) Bratislava in 2014 and 2016, respectively. He currently works in the field of traffic safety telecommunications networks.

Júlia Sitárová was born in Bratislava, Slovakia, in 1992. She received the B.E. and M.E. degrees in Faculty of Electrical Engineering and Information Technology of Slovak University of Technology (FEI STU) Bratislava in 2014 and 2016, respectively. She is currently working on the design of optical networks.

Miloš Orgoň was born in Piešťany, Slovakia, in 1956. He received the Master degree and PhD degree in the Faculty of Electrical Engineering and Information Technology, Slovak University of Technology in Bratislava in 1980 and 1988, respectively. Nowadays he works as an assistant professor at the Department of Telecommunications of FEI STU Bratislava. He has been engaged in research and development of telecommunication networks and services in liberalized environment for area of convergent technologies. At present he is currently engaged in research on the optimal design of networks and technological components, implementation of functions, services and applications and data security in projects KEGA No. 039STU-4/2013 “Utilization of Web-based Training and Learning Systems at the Development of New Educational Programs in the Area of Optical Transmission Media”.