

Analysis of packet switching in VoIP telephony at the command post of tactical level units

Marko R. Marković^a, Stefan M. Ivanović^b, Sava S. Stanišić^c

^a Khaoticen, Cybersecurity & System Integration Department, Belgrade, Republic of Serbia, e-mail: markomarkovicati@gmail.com, **corresponding author**, ORCID iD: <https://orcid.org/0009-0007-8040-6260>

^b Serbian Armed Forces, Center for Applied Mathematics and Electronics, Department for Cryptography in Telecommunications, Belgrade, Republic of Serbia, e-mail: stefanivanovic1012@gmail.com, ORCID iD: <https://orcid.org/0009-0000-1788-2095>

^c Serbian Armed Forces, Air Force and Air Defence, 98th Air Force Brigade, Lađevci, Republic of Serbia, e-mail: sava.stanistic@vs.rs, ORCID iD: <https://orcid.org/0009-0002-3118-0537>

DOI: <https://doi.org/10.5937/vojtehg72-48348>

FIELD: computer sciences, telecommunications, IT

ARTICLE TYPE: review paper

Abstract:

Introduction/purpose: This paper conducts a comprehensive analysis of a potential implementation of Voice over Internet Protocol (VoIP) systems, focusing on network architecture, VoIP phones, and servers. The study explores potential vulnerabilities and proposes solutions. The paper concludes by advocating for a holistic approach to securing VoIP systems, incorporating supplementary services to ensure the confidentiality, integrity, and availability of voice communications in the digital landscape.

Methods: Review of the underlying theory, analysis of the end-user needs and potential solutions, practical viability assesment.

Results: The theoretical points discussed were proven in practice, using commercially available resources. Communication was established in an expected manner.

Conclusions: Implementing solutions similar to the one presented in the paper would be a relatively inexpensive way to make diverse improvements to the operation of tactical level units, both in peacetime and during war.

Key words: VoIP, real-time communication, voice sessions, computer networks, SIP.

Introduction

Commutation, or redirection, of telephone signals had a long development. From manual switching, through the automation of telephone switchboards, to today's packet switching in digital Internet protocol systems, which will be the topic of this paper.

VoIP (Voice over Internet Protocol) telephony, the most modern form of voice transmission, is the result of the convergence of telephone and computer systems. In this form of communication, digitized voice is placed in packets, units of information of the third network layer of the OSI (Open Systems Interconnection) reference model. It enables the transmission of speech over the network infrastructure used in computer networks, which is especially convenient in the case of communication over long distances. VoIP telephony enables many more new functionalities (Ahmad et al, 2015) compared to the telephone systems that are currently in use, some of which will be mentioned in this paper.

The components necessary for the realization of a VoIP phone system are similar to those of other types of telephony. These are telephones, transmission medium, switching devices and telephone switchboard. This paper will describe the configuration of commercial devices to fulfill these functions.

This modern type of telephony would find its place in the Serbian Army. Lower cost of system implementation, greater possibility of integration with realized solutions applied in data transmission, simpler installation and the possibility of traffic management and monitoring are just some of the advantages of adopting such a system. Through this paper, one of the variants of the use of this system will be analyzed, using the example of the command post of a tactical level unit.

Network scenario

The starting point for designing a computer network is the user's needs (Fayyaz et al, 2016). This system is intended for use at the battalion level, the basic modular unit of the Serbian Army, and higher units. The battalion is the smallest unit that has headquarters in its formation, which represents the largest group of users of the implemented system. The users of this system are the heads of groups and sections within the command of the unit, the commander and the deputy commander of the unit. The system at the local level also supports the connection of other users from the unit, which would be tactically meaningful only in peacetime conditions. Each user has his own workplace, within which a computer and

a VoIP phone are of interest for this work. The role of this system is to enable communication between users at different workplaces.

In the implementation of this work, the task was defined as the establishment of communication at the command post of two battalions in the premises and their connection. The computer network realized for the execution of the task (Figure 1) can be divided into a local network and a network of large areas.

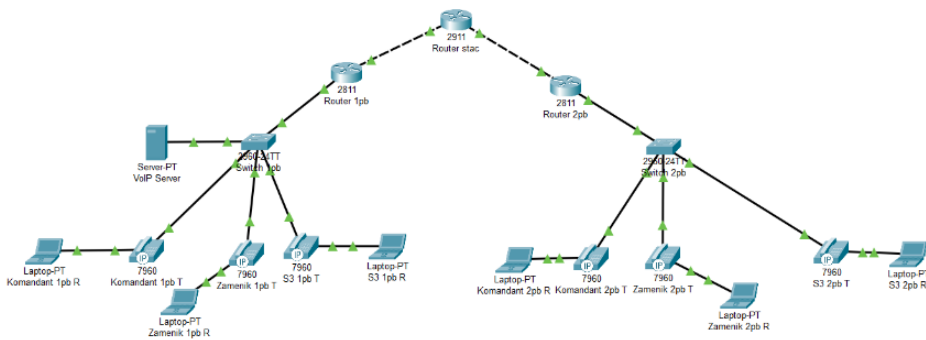


Figure 1 – Logical network topology

Switch configuration

The configuration of the switch, as well as the router, was performed using the PuTTY desktop application. It is an SSH (Secure SHell)/Telnet client through which the Command Line Interface (CLI) is accessed. In the command line, commands are entered for the general setting of the switch, as well as for individual interfaces, lines, VLANs (Virtual Local Area Network) and the like.

```

COM3 - PuTTY
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname SW_1.b
!
boot-start-marker
boot-end-marker
!
enable secret 5 $15oJIG2hNP/pU1jhAYk8Kebyixho.
!
username ssh
no aaa new-model
switch 1 provision ws-c2960x-24ps-1
!
ip domain-name SW_1.b
!
spanning-tree mode pvst
spanning-tree extend system-id
!
vlan internal allocation policy ascending
!
interface FastEthernet0
no ip address
!
interface GigabitEthernet1/0/1
switchport mode trunk
duplex full
!
interface GigabitEthernet1/0/2
switchport mode trunk
!
interface GigabitEthernet1/0/3
switchport mode trunk
switchport port-security maximum 5

```

Figures 2 and 3 – Part of the running configuration of the 1st battalion switch shown in the CLI

Access router configuration

The access router is the last device in the local network, and the boundary between the local network and the WAN. Each router interface is on a separate local area network, which is why routers are said to restrict local area networks. Due to technical limitations, access routers and one central router were used. In reality, there are a number of routers between the two command posts, but they are under the jurisdiction of the stationary component of the SAF's TcIS (Telecommunication Information System of the Serbian Armed Forces). (Marković, 2023)

In this paper, the OSPF routing protocol was used because it is used in the SAF. On the edge router, which is located between the stationary component of the SAF and the Internet provider, it may be necessary to configure BGP as well.

The general settings of access routers are similar to those of other network devices. They are assigned a name, an IP domain name to enable SSH and Telnet, a password for privileged access, and virtual lines. The difference between configuring a router and a switch is the interface. The C2620 router has only FastEthernet interfaces. Each of the router's interfaces is automatically disabled, and can be enabled by configuring the IP address. One of the capabilities of a router is to divide one physical interface into several logical subinterfaces. The use of subinterfaces is reflected in the definition of virtual local networks. In Cisco's 12.0(7) IOS (Internetwork Operating System), which is very outdated, the first virtual network must not belong to a subinterface, which is a difference from the configurations used in practice today. This restriction means that the native virtual local network (Native VLAN) must be the first VLAN used. This makes traffic isolation difficult and prevents the use of a "guest local area network".

Each of the interfaces has a defined IP address and netmask. The netmask determines the number of users in the local network. In this configuration, each of the VLANs on the access interfaces has 16 possible addresses, the first of which is the network address and the last is the broadcast address. This means that the maximum number of IP devices in each virtual network is 14. Subinterfaces must be assigned a VLAN tag. It is inserted into the Ethernet header to separate the associated VLAN (Ghini et al, 2009). The tags must match the VLAN number defined on the switch.

The last interface of interest is Serial0/0 (s0/0). Connecting the DCE/DTE cable connects the serial interfaces of the two routers. These types of interfaces have not been used for years, but due to technical

limitations of routers they are used in this system. The local area network of this interface is of size 4, which means that there can be two devices in it. It is the optimal network size for the case where two routers are connected.

DHCP (Dynamic Host Configuration Protocol) is configured on routers in the access plane. It assigns IP addresses at the request of the user, which is desirable in such systems. The method of determining the IP address is configured on the user's device, and in most cases it is desirable that it be dynamic. The exception in this system is the VoIP server itself, whose address is static. The address is dynamically assigned to other terminal devices. Considering that each user has two devices and the fact that the size of the subnet is 16, we reach a conclusion that the maximum number of workstations is 7. The size of the local network itself can be changed simply, but in this example the goal was to use the IP range in an efficient way. In addition to assigning IP addresses on the terminal device, DHCP can be used to configure over 100 parameters (DHCP options). We are also interested in the default gateway parameter. It is the IP address of the device used to exit the local network, in this case the router interfaces.

The last necessary option is to configure the routing protocol. The used routing process is assigned the number 1. In the configuration of the OSPF protocol, it is necessary to define the addresses and sizes of all directly connected local networks with the associated areas, and the address of the neighboring router. Area 0, the so-called "backbone" area, and 1 are assigned to local networks in this project. By assigning different areas, the router bordering the two areas would become an ABR (Area Border Router) and perform link aggregation. It would group local network addresses into one network, which it would advertise to the neighboring area. Link aggregation in an incorrect configuration leads to the creation of loops in routing, therefore care should be taken when planning the WAN.

One detail of good practice is to define passive interfaces in the routing process. The OSPF protocol only exchanges messages with devices of the same protocol, where some other conditions, such as the matching of the Hello timer, must be met to establish an OSPF adjacency (Strzeciwiłk, 2021). To prevent unnecessary traffic, router interfaces can be marked as passive, and they will then not send Hello packets. This is to be applied to access interfaces, interfaces that are connected to the local network.

The complete view of the router configuration can be found in Figures 4, 5 and 6.

```

COM3 - PuTTY
Current configuration:
!
version 12.0
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname R_1.b
enable secret 5 $1$Eb1E$5ttoazcQ9hArWaBhS9eZ..
!
!
!
ip subnet-zero
ip domain-name 1.b
!
ip dhcp pool vlan10
 network 10.10.9.0 255.255.255.240
 default-router 10.10.9.1
!
ip dhcp pool vlan20
 network 10.10.9.16 255.255.255.240
 default-router 10.10.9.17
!
interface FastEthernet0/0
 ip address 10.10.9.1 255.255.255.240
 no ip directed-broadcast
 duplex auto
 speed auto
!
interface FastEthernet0/0.2
 encapsulation dot1Q 20
 ip address 10.10.9.17 255.255.255.240
 no ip directed-broadcast
!
interface FastEthernet0/0.100
 encapsulation dot1Q 1
 ip address 10.10.9.99 255.255.255.248
 no ip directed-broadcast
--More--
interface Serial0/0
 ip address 10.10.9.33 255.255.255.252
 no ip directed-broadcast
 ip ospf network non-broadcast
 no ip mroute-cache
 no fair-queue
!
interface FastEthernet0/1
 no ip address
 no ip directed-broadcast
 shutdown
 duplex auto
 speed auto
!
interface Serial0/1
 ip address 10.10.15.1 255.255.255.0
 no ip directed-broadcast
!
router ospf 1
 passive-interface FastEthernet0/0
 passive-interface FastEthernet0/0.2
 network 10.10.9.0 0.0.0.15 area 0
 network 10.10.9.16 0.0.0.15 area 0
 network 10.10.9.32 0.0.0.3 area 0
 network 10.10.9.96 0.0.0.7 area 0
 network 10.10.9.128 0.0.0.127 area 0
 neighbor 10.10.9.34
!
ip classless

```

Figures 4, 5 and 6 – Access router configuration

Distributive and edge router configuration

Distribution routers are located outside the command post of the unit and are under the jurisdiction of the stationary component of TcIS. In the laboratory implementation, it was necessary to configure one such router.

The difference between access and distribution routers is the size of the local area network that they are directly connected to. Unlike access routers, distributive plane routers are connected only to neighboring routers. This reduces the complexity of the configuration, considering that only individual interfaces and the routing protocol need to be configured. The configuration of these parameters is similar to the parameters of access routers.

A specific case of distribution routers are edge routers. They are located on the border between our network and the network of other TcIS owners (telecom, post office, etc.). In addition to one of the internal routing protocols, these routers must also have an external routing process running. BGP (Border Gateway Protocol) configured on this router would

summarize the entire address range of the internal network and forward it as such to the neighboring BGP router. A higher level of protection is introduced on these routers, most often by using a Firewall. The system implemented in this work could be connected to the Internet, which will be discussed in the fourth thesis. Part of the configuration of the distribution router used in the implementation of this work can be found in Figure 7.

```
interface FastEthernet0/0
no ip address
no ip directed-broadcast
shutdown
duplex auto
speed auto
!
interface Serial0/0
ip address 10.10.9.34 255.255.255.252
no ip directed-broadcast
ip ospf network non-broadcast
!
interface Serial0/1
ip address 10.10.9.37 255.255.255.252
no ip directed-broadcast
ip ospf network non-broadcast
!
router ospf 1
network 10.10.9.32 0.0.0.3 area 0
network 10.10.9.36 0.0.0.3 area 1
neighbor 10.10.9.33
neighbor 10.10.9.38
!
ip classless
```

Figure 7 – Distribution router configuration

VoIP service

The network infrastructure implemented in the second point of this paper can be used for data exchange between users, but it is insufficient in itself for the operation of a VoIP system. The missing elements will be described at this point.

The function of a network is to provide communication between devices. In a VoIP system, these devices are servers and phones (Ali et al, 2013). The VoIP server plays the role of a telephone switchboard in a classic telephone system. It assigns telephone numbers, establishes and terminates telephone connection, performs remetering and switching, and enables monitoring and management of telephone traffic. Servers are often expensive devices that are placed in tightly controlled physical conditions. They are most often accessed via the Internet, and are often not owned by the organization that uses them to provide a specific service. This type of server is called a cloud server. VoIP services are often run on this type of server. However, the function of a server for certain services can also be performed by a personal computer located in a local network. Due to the nature of the information exchanged in the Serbian Armed

Forces, and other limitations, such a solution was chosen for the realization of this work.

In this work, the role of the server is performed by a virtual machine. It is a software emulation of a physical computer system. A virtual machine is allocated the hardware resources of the physical machine on which it is running. It is possible to run multiple virtual machines on a single physical machine. Processes within a virtual machine are isolated and independent, so a virtual machine can have its own operating system. The software layer that manages the virtual machine is called a hypervisor. Its role, among other things, is the allocation of hardware resources.

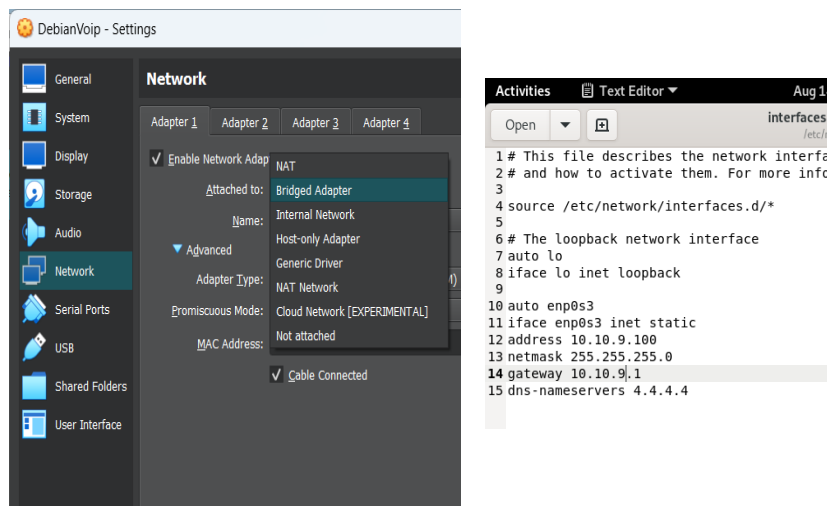
VoIP services use many protocols, but they can be said to be based on SIP and RTP (Abualhaj et al, 2021). SIP (Session Initiation Protocol) is a protocol whose role is to establish, modify and terminate a communication session. In its essence, it is a signaling protocol and its functions include the agreement of the codec used and the selection of the network path for data transmission. It is also active during call management, such as placing a listener on hold, redirecting and establishing a conference. The second protocol, RTP (Real-time Transport Protocol), is responsible for the transfer of packets after the connection is established. Some of its roles are packetizing the voice, assigning a sequence number to the packet, and reorganizing it in order of sending at the receiving end. It eliminates problems caused by jitter, delay and packet loss. It is also used in other real-time communications, such as video streaming and gaming.

Virtual machine

For the purposes of this work, a virtual machine built on the open-source application VirtualBox, from Oracle, was used. VirtualBox is installed on the Windows 11 operating system, which means that the virtual machine will be based on a type 2 hypervisor. VirtualBox offers various options for configuring and using virtual machines, such as machine cloning, machine state memory, folder sharing, and more. Of greatest interest for this paper are the virtual machine's network settings, shown in Figures 8 and 9. The virtual machine is configured to have its own network outlet that behaves as a separate device from the point of view of the rest of the network. The virtual machine is assigned 4 GB of RAM (Random Access Memory) and one logical processor core. Allocation of resources to virtual machines is done before startup. If necessary, more hardware resources can be allocated, where it is recommended to leave at least 30% of RAM and half of the logical processor cores to the physical machine. The virtual machine is running a

64-bit Debian operating system. It is a free, open-source operating system that offers various benefits for running servers over Windows. Less use of hardware resources, greater protection and ease of software installation are just some of them.

On the virtual machine, two lines of code are only needed to be entered into the terminal to install FusionPBX. To act as a server, a virtual machine must be connected to the rest of the network. A virtual Ethernet interface is configured for this purpose. The rest of the server settings are performed via the web interface, by connecting to the server's IP address.



Figures 8 and 9 – Network adapter configuration

FusionPBX VoIP server

FusionPBX is free, open-source software that serves as a switchboard for a wide range of communications. It is based on FreeSWITCH software, on which it builds a web GUI (Graphical User Interface). Another well-known derivative of FreeSWITCH is BigBlueButton, which is used on the distance learning platform in the SAF. FusionPBX enables VoIP, voicemail, fax, conference calling and many other services. It can also be used for traffic monitoring and management. It is used in commercial environments due to its large number of functionalities and ease of implementation. There are paid versions of the software that offer additional services such as notifying waiting users of their position in the waiting queue, sending emails to users upon

registration, and others. However, the biggest benefit of paying for this software is access to official "training recordings" and documentation that serves as a guide to the switchboard operator. The software is complex and contains too many functionalities that are not well documented in the software itself. Therefore, despite the price ranging between one hundred and one thousand dollars per month, a large number of companies that use this software have several subscribers. The \$1,000 per month offer offers a maximum of 6 hours of customer support per month.

An important term in this software is domain. Domain is the name for all software processes related to one system (company, neighborhood, etc.). A single server can serve multiple systems, but each system will have its own domain. The only privilege level valid for multiple domains within a server is the superadmin operator. Operator levels are divided into superadmin, admin and user. The superadmin has the ability to configure all domains on the server, the authority of the admin is limited only to a certain domain, and the other groups of operators have different restrictions within their domain.

Configuration is done through the web interface. In order to access the web interface, it is necessary to enter a URL (Uniform Resource Locator) link in case there is a DNS (Domain Name System) server, or a specific IP address as is the case in this paper.

After the operator logs in, the information about the operator and the system is displayed on the home screen of the website, such as received messages, the percentage of hardware resource utilization, the number of registered users, and the like. The following is an explanation of the individual settings.

User configuration

User management is done in the Extensions window. First it is necessary to add users. In the add user window, there are many options, such as recording the call, sending an e-mail after a missed call, even selecting music for other users in the call waiting queue. Of interest for this work are the configuration of password, domain, name on caller ID and phone number. It is possible to add multiple users at the same time, where they share the basic settings after adding, which can be changed separately by configuring the individual user. It is also possible to assign a specific MAC address to the user, whereby he will be automatically registered when connecting a device with a defined MAC address. After adding a user, it is possible to view the list of possible users, which can be seen in Figure 10.

| Extension | Effective CID Name | Outbound CID Name |
|-----------|--------------------|-------------------|
| 01 | SuperAdmin | SuperAdmin |
| 20 | Komandant | 1. bataljon |
| 21 | Zamenik | 1. bataljon |
| 22 | S1 | 1. bataljon |
| 23 | S2 | 1. bataljon |
| 24 | S3 | 1. bataljon |
| 25 | S6 | 1. bataljon |

Figure 10 – User configuration

SIP profile configuration

This software handles calls based on four SIP profiles. The internal profile for IPv4 is of greatest interest for this paper. There are 137 configurable options within this profile. They include settings for TLS or SSL (Secure Sockets Layer), certain timers, call forwarding and the like, but in this work it is necessary to change only a few parameters. The SIP socket configured in this section must be identical to the configurations of other VoIP devices. Figure 11 shows current SIP processes and possible profiles. The SIP protocol usually uses UDP (User Datagram Protocol) on the transport layer, but it can also be configured for TCP Websocket and WebSocketSecure, the last two of which are upgrades to HTTP and HTTPS (HyperText Transfer Protocol Secure) respectively. In this work, a standard configuration was used. Configured profiles must be run. The operator has the possibility to cancel the registration of all users registered on one profile at the same time.

| Name | Type | Data | State | Action |
|----------|---------|--|-------------------|--------|
| external | Profile | sp.mod_sofia@10.10.9.100:5080 | RUNNING (0) | |
| internal | Profile | sp.mod_sofia@10.10.9.100:5060 | RUNNING (0) | |
| internal | Profile | sp.mod_sofia@10.10.9.100:5066;transport=ws | RUNNING (0) (WS) | |
| internal | Profile | sps.mod_sofia@10.10.9.100:7443;transport=wss | RUNNING (0) (WSS) | |

| | |
|------------------------------------|---|
| sofia status profile external | <input type="button" value="FLUSH REGISTRATIONS"/> <input type="button" value="REGISTRATIONS (0)"/> <input type="button" value="STOP"/> <input type="button" value="RESTART"/> <input type="button" value="RESCAN"/> |
| sofia status profile external-ipv6 | <input type="button" value="FLUSH REGISTRATIONS"/> <input type="button" value="REGISTRATIONS (0)"/> <input type="button" value="START"/> <input type="button" value="RESTART"/> <input type="button" value="RESCAN"/> |
| sofia status profile internal | <input type="button" value="FLUSH REGISTRATIONS"/> <input type="button" value="REGISTRATIONS (0)"/> <input type="button" value="STOP"/> <input type="button" value="RESTART"/> <input type="button" value="RESCAN"/> |
| sofia status profile internal-ipv6 | <input type="button" value="FLUSH REGISTRATIONS"/> <input type="button" value="REGISTRATIONS (0)"/> <input type="button" value="START"/> <input type="button" value="RESTART"/> <input type="button" value="RESCAN"/> |

Figure 11 – SIP profiles and processes

Useful administrative views

FusionPBX, as previously mentioned, offers a great degree of control over all aspects of interest to a telephone exchange. Special attention in this paper will be devoted to the possibilities of monitoring and managing the operator. The operator, depending on the level of his account, in addition to the configuration of the user, has complete insight into the activities related to the users. Busy time, call list, e-mail list, redirects; all this is only part of the user data over which the operator has an overview. An operator with a superadmin level account in standard configurations has as many as 762 "permissions", while an ordinary user has less than 100, which include calling, adding to a conference, activating redirection, reading his voicemail, and the like. It is important to mention that the operator can even record calls between participants, listen to other people's voice mail and read other people's electronic mail. Figures 12 and 13 show some views that operators of a certain level have access to.

Devices (2)

Devices are endpoints that register to one or more extensions. They are added to the list m

| <input type="checkbox"/> | MAC Address | Label | Vendor |
|--------------------------|-------------------|-------|--------|
| <input type="checkbox"/> | bc-c3-42-52-8c-7a | 002 | |
| <input type="checkbox"/> | c8-00-84-ed-b9-c1 | 20 | cisco |

Figure 12 – Registered MAC addresses

| Ext. | Domain | Caller Name | Caller Number | Caller Destination |
|------|-------------|-------------|---------------|--------------------|
| ↔ 21 | 10.10.9.100 | S1 | 22 | 21 |
| ↔ 22 | 10.10.9.100 | S1 | 22 | 22 |
| ↔ 21 | 10.10.9.100 | S1 | 22 | 21 |
| ↔ 22 | 10.10.9.100 | Zamenik | 21 | 22 |
| ↔ 23 | 10.10.9.100 | Zamenik | 21 | 23 |
| ↔ 23 | 10.10.9.100 | Zamenik | 21 | 23 |
| ↔ 23 | 10.10.9.100 | Zamenik | 21 | 23 |
| ↔ 21 | 10.10.9.100 | S2 | 23 | 21 |
| ↔ 21 | 10.10.9.100 | Komandant | 20 | 21 |

Figure 13 – Global call list

Panasonic KX-HDV430X VoIP phone

A VoIP phone, one of the basic components of a VoIP phone system, differs from analog and ISDN (Integrated Services Digital Network) phones. In order for the user to access the telephone system, it is necessary to configure the telephone itself. In this paper, only network settings are of interest, attention is not paid to user settings such as ringtone volume and the like. It is important to note that these phones are powered by an adapter from the mains or via Ethernet when connected to a PoE (Power over Ethernet) switch. The phone used in this system is accessed physically, using a touch screen, and using a web interface. The settings necessary for logging into the telephone exchange are located on the web interface. The phone's physical settings are low-level settings and must be set before accessing the web interface. VLAN, IP address can be configured physically/statically (Figure 14) and via DHCP (Dynamic Host Configuration Protocol), CDP (Cisco Discovery Protocol), LLDP (Link Layer Discovery Protocol) and Embedded Web. In this paper, the IP address and Embedded Web are physically set, which enable access to the web interface. The phone also has the ability to send echo request packets of the ICM protocol (Internet Control Message Protocol) (Figure 15).



Figure 14 – Manual IP configuration



Figure 15 – Ping response

The rest of the necessary configuration was performed via the web interface (Figure 16). In order for the user to register to the VoIP server, he needs to configure his phone number, authentication identification number, password, IP address, port and domain of the server. All the mentioned settings are located within the line window of the SIP window.

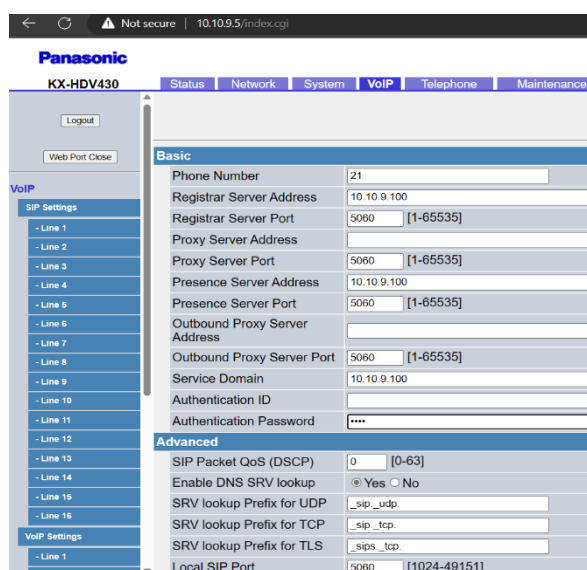


Figure 16 – Client-side SIP configuration

It is also possible to configure the IP address of the phone itself, caller ID, DNS and other options. This phone supports simultaneous use for a maximum of 16 user accounts, i.e. 16 phone numbers, which can also belong to different domains. One line is configured. After the configuration, the phone will automatically log on to the VoIP server. The settings remain saved in the phone's memory, and it is possible to delete them using the web interface or by typing a certain number on the phone itself. This function, similar to USSD (Unstructured Supplementary Service Data) codes in mobile telephony, should not be known to ordinary users.

After performing all the mentioned configurations, the system is ready for operation.

Additional services

The configurations realized in parts 2 and 3 of this paper are sufficient for the operation of one VoIP phone system. As part of this work, additional

functionalities have been implemented, and the addition of services and functionalities that were not implemented either due to time or technical limitations will be theoretically considered. Advantages in the application of the described solutions are reflected in the spheres of efficiency, protection, provision of redundancy and scalability. They are also important for the operator because they enable faster and easier installation and management of the system.

SSH

SSH is a cryptographic network protocol used to access, manage, and exchange data with remote computer systems. It was developed as a replacement for insecure protocols like rlogin and Telnet. The purpose of using SSH in this paper is to enable remote configuration of network devices. This protocol is based on key exchange. After accessing the network device through the terminal, in this case Command Prompt on the Windows operating system, it is necessary to agree on the key exchange method and the encryption algorithm. After exchanging the keys and confirming the matching of the hashed authentication parameters, an SSH connection is established to transmit commands to the network device. The user can then access the device in the same way as they do via console port and flat cable with RS (Recommended Standard) 232 connector. The routers used in this paper do not support SSH because they were manufactured in 1998, so SSH is configured only on the switch. To log in using the SSH algorithm, one needs to know the IP address of the device, the username for SSH access, and the access password, which is configured in the second chapter of this paper. In this example, the Diffie-Hellman cryptographic algorithm for key exchange and the AES (Advanced Encryption Standard) encryption algorithm with a key length of 256 bits were used.

DNS

The role of the DNS service is to translate domain names into IP addresses. DNS servers work like a phone book. Most services that rely on computer networks communicate based on IP addresses. Users, on the other hand, do not have an easy time remembering IP addresses. When a user makes a request to a browser or other application for a resource on the Internet, that request is forwarded to a DNS server that will translate the requested domain name into an IP address. The translated IP address is returned to the user's device, and it becomes a parameter for establishing communication between the user and the requested resource. DNS servers can be of different hierarchical levels, and store different

types of data. Most often, the Internet provider has its own DNS resolver that stores data about frequently used domains and IP addresses. When a request is made to the DNS resolver for an unknown domain, it forwards the request to higher-level DNS servers.

The purpose of using a DNS server in this system would be reflected in the case of expansion of this type of telecommunication system. Introducing a local DNS server would make logging in and administration of this system easier. For example, in the event that the same VoIP server is shared by all units of a reinforced brigade-level tactical group, each subordinate unit would have to remember the exact IP address of its domain on the VoIP server. Using a DNS server, instead of remembering an IP address, users and operators would log in using a domain name like "komandant.1pb@1br.tg1". This type of name is similar to an email address. All email services address users by name and associated domain. Without the DNS service, the e-mail address of a gmail user would look like "username@177.217.9.219".

Soft VoIP phones

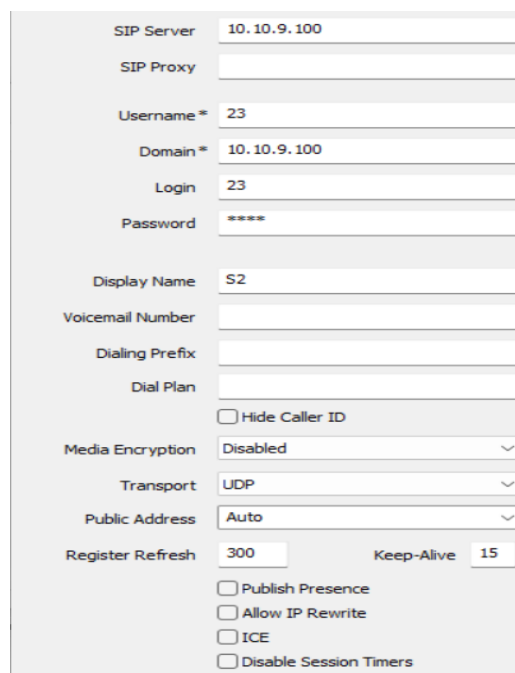
Soft phones are applications that allow users to use VoIP telephony services without a physical phone. Depending on the software itself, they offer a number of benefits and improvements over physical VoIP phones (Singh et al, 2014). They reduce system cost, facilitate configuration and remote management, and can be integrated with other applications. They can be installed on computers, mobile phones, tablets and similar devices.

Use on mobile phones, with appropriate expansions of the network infrastructure (WLC (Wireless LAN Controller) and multiple wireless access points) would enable user mobility at the command post, while retaining all the good features of the basic system. A mobile phone without a SIM (Subscriber Identity Module) card does not connect to the civil mobile communications network. Even with the card, it is possible to turn off the transmission power of the mobile phone by entering the appropriate configuration window, using a certain USSD code defined by the operator (Bhattacharjee et al, 2010). By turning off the transmission power for the mobile network, the phone becomes invisible to the adversary. The advantage of VoIP telephony is that it relies on the Internet, so mobile phones can rely on a local Wi-Fi (Wireless Fidelity) network that would originate from wireless access points at the command post. A Wi-Fi signal has a much shorter range than a cell phone signal, so it would be very difficult for a potential enemy to detect. Such an upgrade of the implemented system would retain the features of anti-electronic protection, along with the great benefits offered by mobility.

The software phone was very useful in the realization of this work, due to the technical limitations of the laboratory and the existing VoIP phones. The MicroSIP application is installed on the server computer. It is free, open-source software that supports all the functionality of physical phones, except for video calls. In addition, it offers the possibility to configure protection at the transport layer of the OSI reference model using TLS and SRTP protocols.

The configuration of MicroSIP is simpler than the configuration of a physical phone, and is done in just one window, which is shown in Figure 17. It should be noted that to use this application it is not necessary to be connected to the Internet, and it only takes a few MB of memory space. From that aspect, and bearing in mind that the application is open-source, it can be concluded that the use of this application does not represent a security risk.

Figure 18 shows the appearance of the application after the call is made.



The screenshot displays the MicroSIP configuration window with the following settings:

- SIP Server: 10.10.9.100
- SIP Proxy: (empty)
- Username *: 23
- Domain *: 10.10.9.100
- Login: 23
- Password: ****
- Display Name: S2
- Voicemail Number: (empty)
- Dialing Prefix: (empty)
- Dial Plan: (empty)
- Hide Caller ID
- Media Encryption: Disabled
- Transport: UDP
- Public Address: Auto
- Register Refresh: 300
- Keep-Alive: 15
- Publish Presence
- Allow IP Rewrite
- ICE
- Disable Session Timers

Figure 17 – MicroSIP configuration

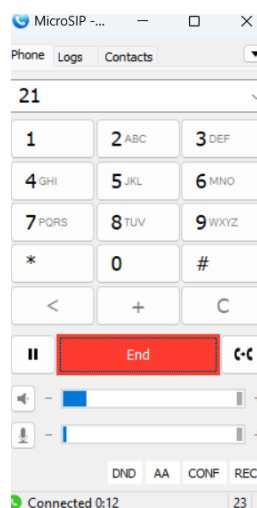


Figure 18 – Call established using MicroSIP

Redundancy and load balancing

The implemented system, in the topological sense, has a centralized structure. In the case of application during combat operations, this type of implementation may adversely affect the continuity of communications (Thirunavukkarasu & Karthikeyan, 2015). Therefore, it is necessary to implement certain solutions that ensure redundancy. These solutions increase the complexity and cost of the system, but are necessary in the case of more mass use of the system.

In an organizational sense, some kind of redundancy would be provided by defining the rank of the unit running its own VoIP server. Battalion-level units already possess technical resources for the implementation of such a system, in the form of PKČb (Serb. Battalion Mobile Switching Hub). The lower the rank of the unit that implements such a system, the more resistant the entire telecommunications system is to interruptions. In the event of the loss of its VoIP server, provided the switch is still functional, the unit could rely on the other unit's server with negligible configuration changes, providing a high degree of redundancy. Connecting several such systems is simple from a technical point of view, and does not require any hardware additions compared to separate systems, but due to technical limitations it was not realized in this work.

Technical measures to ensure redundancy can be implemented at several levels. Today's commercial servers have multiple network cards,

which can be connected to different switches. Such an implementation would ensure that the immediate consequences of the loss of one switch are reflected only on the users connected to that switch, and not on the entire system. The process of deciding which path the server will choose is configurable, and can be static (one switch is primary and the other is backup) or involve load management based on certain metrics. Some other advantages of a server with multiple NICs are link aggregation and QoS filtering, which are not of interest in this paper.

The last level of redundancy relates to the router. Configuring HSRP, VRRP, or GLBP allows a group of routers to share a single virtual IP address. The first two protocols work in a similar way. They assign a virtual IP and MAC address to one physical router according to a certain metric, which all other network devices use in communication. The biggest difference between HSRP and VRRP is that the first protocol is proprietary to Cisco, while the second is an open standard for all manufacturers. GLBP is an improvement over these two protocols, as it also offers the possibility of load management. The main router (AVG (Active Virtual Gateway)), selected according to a certain configurable metric, assigns virtual MAC addresses to other routers (AVF (Active Virtual Forwarder)), which forward the traffic on. AVG is responsible for the resolution of ARP requests that are directed to a shared virtual IP address. Based on certain metrics and network conditions, it assigns different virtual MAC addresses to different routers. An AVG router can be an AVF router at the same time. In addition to these two types of routers, there is also an SVF (Standby Virtual Forwarder) router, whose task is to monitor the state of the AVF router and, if necessary, take over part of the traffic.

Security

Information security features are an important indicator of the quality of a TCI system. In an ideal TCI system, organizational, technical and other protection measures are implemented at all levels of the OSI reference model. In the previous chapters, some protection measures were mentioned, such as TLS, SSH, WSS (Web Socket Secure) and others. In this part of the paper, the technical protection measures implemented on the second and third layers of the OSI model are of interest.

Data link layer protection techniques often include device MAC addresses. Protection at this level is mainly implemented on the switch. Apart from the division into virtual local networks, which in itself carries some features of protection by isolating groups of users, port security measures (Port Security) were implemented in the realization of this system. Traffic filtering by known MAC addresses is enabled on the

switch's access interfaces. Considering that each device has its own unique MAC address, the interfaces are configured to protect the network from access by unknown devices. It is possible to define the exact MAC address of the allowed device before access itself, or with the sticky command allow the addresses of devices connected to the interface to be automatically remembered. In this system, the security implemented is configured to allow access to the first five devices that connect to this interface. In case of unauthorized access, it is possible to completely disable the interface of the unauthorized device or automatically reject traffic without disabling it. An operator accessing the switch in privileged mode can see statistics related to protection of this type. The switch protection configuration used in this work is shown in Figure 19.

Greater diversity in protection is possible at the network layer of the OSI model. The basic form of protection at this layer is the use of an access control list (ACL). The traffic parameters that will be forwarded or rejected are defined within the ACL. AC lists are divided into standard and extended. The first type makes a decision based only on the source IP address. They are simpler to configure but offer an unsophisticated form of protection. Extended AC lists allow or deny traffic based on source and destination IP address, port, and protocol type. They allow for more precise traffic control. It is important to note that the criteria (rules) defined in the list are applied hierarchically. If the lower-numbered criteria in the list allow traffic, the higher-numbered criteria are not considered. The practice is to enter the command deny 0.0.0.0 at the end of the list, which prohibits all traffic. In this way, it is ensured that the network device does not forward traffic that was not previously defined by the operator.

Protection of a certain level can be configured on any device, but there are also devices for which protection is the main task. A firewall is a device or software that monitors, filters, and controls traffic between two devices. It is placed between a protected and an unprotected network, and makes decisions based on predefined criteria. Their functioning is not limited to one layer of the OSI model, and the possibility of traffic inspection even allows the interruption of the traffic flow upon detection of a prohibited string of characters within the text file. The firewall analyzes the traffic according to various parameters, which makes the effective use of these devices very complex. Protection as well as the attacks are becoming more and more complicated, especially with the introduction of artificial intelligence in this fight. The analysis of techniques that can be applied in protective walls will not be covered in this paper.

Traffic often goes beyond the reach of the locally owned network. In the event that sensitive information must be transmitted through a part of

the network over which we have no control, that traffic needs to be protected. The set of protocols of the third layer of the OSI model used for these purposes is called IPsec (IP Security). It has a dual function: it confirms the identity of the other communication participant and ensures that the traffic between the two participants remains unknown to all other devices that forward that traffic. The first function is provided by the Authentication Header protocol. AH prevents data from packet headers from being altered and verifies the identity of the other participant using a hash calculated based on the original header and a key known only to the end participants. The key exchange algorithm (IKE (Internet Key Exchange)) will not be given attention in this paper. The role of traffic encryption is performed by the ESP (Encapsulating Security Payload) protocol. It can be realized in two ways. It is possible to encrypt only the useful information without the header or the entire packet. These two modes of operation of the IPsec group of protocols are called transport type and tunnel type. In addition to encryption, ESP also offers authentication. The difference between AH and ESP is that the first protocol performs authentication taking into account the content of the entire packet, while the second protocol uses only information from the header for authentication. IPsec is the basis for various implementations of VPNs, which will be discussed in the next chapter.

```
!
interface GigabitEthernet1/0/3
 switchport mode trunk
 switchport port-security maximum 5
 switchport port-security
 switchport port-security violation restrict
 switchport port-security mac-address sticky
 switchport port-security mac-address sticky bcc3.4252.8c68
!
interface GigabitEthernet1/0/4
 switchport access vlan 10
 switchport mode access
 switchport port-security maximum 5
 switchport port-security
 switchport port-security violation restrict
 switchport port-security mac-address sticky
 switchport port-security mac-address sticky bcc3.4252.8c7a
!
```

Figure 19 – Switch security configuration

VPN tunneling and the Internet

A virtual private network (VPN) is a technology that allows users to protect and hide traffic passing through an unprotected part of the network. It is based on the principles of authentication and encryption, functions for

which implementation uses different protocols. The most famous VPN solutions basically work on IPSec, SSL/TLS, OpenVPN and WireGuard protocols (Singh et al, 2014). In this paper, their specificities will not be considered.

VPNs are used for various purposes, such as providing anonymity on the Internet, bypassing location restrictions, remote access, and the like. In this paper, attention is paid to VPN tunneling, i.e. establishing a protected connection between two devices connected by an unprotected network. VPN tunnels can be established with or without a VPN server. By using a VPN server, the system is centralized, but also easier to configure. This is the most common implementation of virtual private networks. The server establishes tunnels, encrypts and decrypts traffic between users. VPN servers can be run on the Internet or independently. OpenVPN is one such software, offering the option of using their own servers or running your own. It is an open-source application, which means that it can also be used for military purposes without security risks¹, with prior testing and modification of the algorithm for additional protection. Depending on the amount of traffic that passes through the VPN server, the function of the server can also be performed by a personal computer. In the case of tunnel implementation using a server, the traffic of all computers in the local network that communicate with devices at another location through the Internet would be processed in the server. This implementation is called a "site-to-site" VPN tunnel. Another way of using it is called "point-to-point". In this embodiment, each user establishes its own tunnel with another user. The advantage of this method is that it is not necessary to use a server computer, but configuring individual tunnels is more complex. The use of the Internet to transmit military traffic using upgraded commercial technologies to achieve secure tunnels is already widespread in foreign militaries, depending on the cryptographic value of the traffic.

Conclusion

In this paper, the implementation of a VoIP phone system is analyzed and demonstrated. The system was implemented using commercial solutions of newer and older production. During the realization of the

¹ The TETRA radio system, used by many government institutions around the world, including the Ministry of Defense, has an encryption algorithm that was publicly revealed at the end of 2020. In January 2021, a team of researchers discovered a number of risks, perhaps the most dangerous of which is a backdoor. Exploitation of this "deliberate" security flaw weakens the 80-bit key to just 32 bits, allowing even commercially available systems to "break" the encryption with a brute-force attack in less than a minute

system, due to technical and time constraints, it was not possible to implement certain functionalities, which were therefore considered from the theoretical side. The implemented system represents the basis for the development of new and complex solutions that would increase the properties of scalability, protection, redundancy, ease of installation and administration, and introduce many other benefits. By analyzing existing commercial solutions, one can create an insight into the advantages, disadvantages, challenges and limitations that the introduction of such a system into use in the Serbian Armed Forces would achieve.

The existing telephone system in the Serbian Army is a mixture of analog and ISDN systems. VoIP telephony represents a step towards a future that brings better quality, more efficient communication. This path to the future is not without its challenges, both of a technical, organizational and logistical nature. The current infrastructure of the stationary component of the telecommunications and information system of the Serbian Army does not support the introduction of such a system in its entirety, but with certain adaptations, this system would be easily adapted to the existing solutions implemented in the mobile component, i.e. PKČ. Bearing in mind that there is already an L3 (Layer 3) switch and a computer located in the vehicle cabin, for the implementation of this system, depending on the number of users, there would be no need for any hardware changes. This system is very flexible, to use the basic telephone service, only one switch is needed, a computer that would function as a server, and a VoIP phone or a combination of a handset and a microphone in case of running a software phone on the user's computer. To implement more advanced functionalities, it would be enough to add one router, switch and firewall to the vehicle.

Within the existing computer network, the only requirements before introducing such a system would be operator and user training. The system is highly modular and can be run on a variety of hardware, which is another logistical benefit. The protection of such a system can be achieved on different layers, by combining different technologies. The ability to safely use existing civilian infrastructure for military communications purposes is an enticing aspect of this project that also deserves attention.

Introducing VoIP telephony in the SAF will be a big and challenging feat. However, following the trends in the development of commercial solutions and systems of foreign armed forces, such a feat seems inevitable. The purpose of this work is to serve as an introduction and basis for that technological transformation.

References

- Abualhaj, M.M., Al-Tahrawi, M.M. & Al-Zyoud, M. 2021. Contracting VoIP Packet Payload Down to Zero. *Cybernetics and Information Technologies*, 21(1), pp.137-150. Available at: <https://doi.org/10.2478/cait-2021-0010>.
- Ahmad, B., Gilani, S.A., Iqbal, R., Sherazi, H. & Iranmanesh, V. 2015. Deployment of VoIP Communications in B&A Spy Agency: Design and Implementation. *International Journal of Computer Networks and Communications Security*, 3(11), pp.424-431 [online]. Available at: https://ijcnscs.org/published/volume3/issue11/p3_3-11.pdf [Accessed: 20 October 2023].
- Ali, M.A., Rashid, I. & Khan, A.A. 2013. Selection of VoIP CODECs for Different Networks based on QoS Analysis. *International Journal of Computer Applications*, 84(5), pp.38-44. Available at: <https://doi.org/10.5120/14575-2702>.
- Bhattacharjee, P.K., Koner, C., Bhunia, C.T. & Maulik, U. 2010. Biometric Entity Based Mutual Authentication Technique for 3-G Mobile Communications. *International Journal of Computer Theory and Engineering*, 2(1), pp.26-30. Available at: <https://doi.org/10.7763/IJCTE.2010.V2.111>.
- Fayyaz, Y., Khan, D.M., Fayyaz, F., Qadri, S., Naweed, S. & Fahad, M. 2016. The Evaluation of Voice-over Internet Protocol (VoIP) by means of Trixbox. *International Journal of Natural and Engineering Sciences*, 10(3), pp.33-41 [online]. Available at: <https://www.ijnes.org/index.php/ijnes/article/view/276/249> [Accessed: 20 October 2023].
- Ghini, V., Lodi, G. & Panzneri, F. 2009. Always Best Packet Switching: the Mobile VoIP Case Study. *Journal of Communications*, 4(9), pp.700-713. Available at: <https://doi.org/10.4304/jcm.4.9.700-713>.
- Marković M. 2023. *Analiza paketske komunikacije kod VoIP telefonije na komandnom mestu jedinica taktičkog nivoa*. BS thesis. Belgrade, Serbia: University of Defence (in Serbian).
- Singh, H.P., Singh, S., Singh, J. & Khan, S.A. 2014. VoIP: State of art for global connectivity - A critical review. *Journal of Network and Computer Applications*, 37, pp.365-379. Available at: <https://doi.org/10.1016/j.jnca.2013.02.026>.
- Strzeciwiłk, D. 2021. Performance Analysis of VoIP Data over IP Networks. *International Journal of Electronics and Telecommunications*, 67(4), pp.743-750. Available at: <https://doi.org/10.24425/ijet.2021.139801>.
- Thirunavukkarasu, E.S. & Karthikeyan, E. 2015. A survey on VoIP packet loss techniques. *International Journal of Communication Networks and Distributed Systems*, 14(1). Available at: <https://doi.org/10.1504/IJCND.2015.066029>.

Análisis de la conmutación de paquetes en telefonía VoIP en el puesto de mando de unidades de nivel táctico

Marko R. Marković^a, Stefan M. Ivanović^b, Sava S. Stanišić^c

^a Khaoticen, Departamento de Ciberseguridad e Integración de Sistemas, Belgrado, República de Serbia, **autor de correspondencia**

^b Fuerzas Armadas de Serbia, Centro de Matemáticas Aplicadas y Electrónica, Departamento de Criptografía en Telecomunicaciones, Belgrado, República de Serbia

^c Fuerzas Armadas de Serbia, Fuerza Aérea y Defensa Aérea, 98.a Brigada de la Fuerza Aérea, Lađevci, República de Serbia

CAMPO: ciencias de computación, IT

TIPO DE ARTÍCULO: artículo de revisión

Resumen:

Introducción/objetivo: Este artículo realiza un análisis integral de una posible implementación de sistemas de Voz sobre Protocolo de Internet (VoIP), centrándose en la arquitectura de red, los teléfonos VoIP y los servidores. El estudio explora posibles vulnerabilidades y propone soluciones. El documento concluye abogando por un enfoque holístico para proteger los sistemas VoIP, incorporando servicios complementarios para garantizar la confidencialidad, integridad y disponibilidad de las comunicaciones de voz en el panorama digital.

Métodos: Revisión de la teoría subyacente, análisis de las necesidades del usuario final y posibles soluciones, evaluación de la viabilidad práctica.

Resultados: Los puntos teóricos discutidos fueron probados en la práctica, utilizando recursos comercialmente disponibles. La comunicación se estableció de la manera esperada.

Conclusión: Implementar soluciones similares a la presentada en el documento sería una forma relativamente económica de realizar diversas mejoras en la operación de unidades de nivel táctico, tanto en tiempos de paz como durante la guerra.

Palabras claves: VoIP, comunicación en tiempo real, sesiones de voz, redes informáticas, SIP.

Анализ коммутации пакетов VoIP-телефонии в командном пункте тактического подразделения

Марко Р. Маркович^а, Стефан М. Иванович^б, Сава С. Станишич^в

^а «Khaoticen», отдел кибербезопасности и системной интеграции, г. Белград, Республика Сербия, **корресподент**

^б Вооруженные силы Республики Сербия, центр прикладной математики и электроники, департамент криптографии в телекоммуникациях, г. Белград, Республика Сербия

^в Вооруженные силы Республики Сербия, Военная авиация и противовоздушная оборона, 98-ая авиационная бригада, Ладжевци, Республика Сербия

РУБРИКА ГРНТИ: 20.15.05 Информационные службы, сети, системы в целом

49.33.29 Сети связи

ВИД СТАТЬИ: обзорная статья

Резюме:

Введение/цель: В данной статье проводится всесторонний анализ потенциального внедрения системы передачи голоса по интернет-протоколу (VoIP). В статье особое внимание уделяется сетевой архитектуре, телефонам VoIP и серверам. В статье исследуются потенциальные недостатки и предлагаются определенные решения. В заключении отстаивается целостный подход к обеспечению безопасности системы VoIP, включающий дополнительные услуги для обеспечения конфиденциальности, целостности и доступности голосовой связи в цифровой среде.

Методы: В данной статье применены следующие методы: обзор основной теории, анализ потребностей пользователей, анализ потенциальных решений, оценка практической устойчивости.

Результаты: Обсуждаемые теоретические положения были подтверждены на практике при использовании имеющихся в продаже ресурсов. Связь была налажена в соответствии с ожиданиями.

Выводы: Внедрение решений, аналогичных представленному в статье, было бы относительно недорогим способом повышения эффективности деятельности тактических подразделений как в мирное время, так и во время войны.

Ключевые слова: VoIP, коммуникации в режиме реального времени, голосовые сеансы, компьютерная сеть, SIP.

Анализа пакетске комутације у VoIP телефонији на командном месту јединица тактичког нивоа

Марко Р. Марковић^а, Стефан М. Ивановић^б, Сава С. Станишић^в

^а Khaotisen, Одељење за сајбер безбедност и системску интеграцију, Београд, Република Србија, **аутор за преписку**

^б Војска Србије, Центар за примењену математику и електронику, Одељење за криптографију у телекомуникацијама, Београд, Република Србија

^в Војска Србије, Ратно ваздухопловство и противваздухопловна одбрана, 98. ваздухопловна бригада, Лађевци, Република Србија

ОБЛАСТ: рачунарске науке, телекомуникације, ИТ
КАТЕГОРИЈА (ТИП) ЧЛАНКА: прегледни рад

Сажетак:

Увод: У раду је спроведена темељна анализа могуће имплементације система Voice over Internet Protocol (VoIP), уз фокус на мрежну архитектуру, VoIP телефоне и сервере. Истражене су потенцијалне рањивости и предложена решења. Такође, препоручује се целисходан приступ обезбеђивању VoIP система, укључујући додатне услуге како би се осигурала поверљивост, интегритет и доступност гласовних комуникација у дигиталном окружењу.

Методе: У раду су презентовани: преглед основне теорије, анализа потреба крајњих корисника и потенцијалних решења, као и практична процена одрживости.

Резултати: Теоријске тачке о којима се расправљало доказане су у пракси, коришћењем комерцијално доступних ресурса. Комуникација је успостављена на очекиван начин.

Закључак: Имплементација решења сличних оном представљеном у раду био би релативно јефтин начин да се створе различита побољшања у деловању јединица тактичког нивоа, како у миру, тако и у рату.

Кључне речи: VoIP, комуникације у реалном времену, гласовне сесије, рачунарске мреже, SIP.

Paper received on: 21.10.2023.

Manuscript corrections submitted on: 03.03.2024.

Paper accepted for publishing on: 04.03.2024.

© 2024 The Authors. Published by Vojnotehnički glasnik / Military Technical Courier (www.vtg.mod.gov.rs, втг.мо.унр.срб). This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution license (<http://creativecommons.org/licenses/by/3.0/rs/>).

