

A. V. Dzyma, I. S. Shcherbyna, A. M. Shtimmerman, S. V. Prokopov

METHODS FOR ENCRYPTING TEXT INFORMATION USING BLOCKCHAIN TECHNOLOGIES

The article analyzes the methods of blockchain technologies for encrypting text information as a modern tool for protecting the text data of users on the network. During the rapid development of the Internet, the question of the secure transfer of text information between users is increasingly raised. Sending text information over the Internet is a common situation, and the protection of such data plays a very important role in the functioning of a large number of companies. Currently, there are a number of options for the transmission of text information, which require an appropriate level of protection during transmission. Transmission and encryption methods depend on the general needs of the sender and receiver.

Thanks to cryptography and blockchain, it is now possible to create technologies that will allow you to truly securely transmit textual information between users on the Internet. Methods of encrypting text information based on blockchain technologies make it possible to implement this. You need to consider what these methods consist of. Encryption is a way to hide the original meaning of a message or other document that distorts its original content. Converting plain, clear content into code is called encoding. This implies that there is a mutual unambiguous correspondence between the symbols of the text and the code — this is the fundamental difference between encoding and encryption. Encryption and decryption are often mistaken for the same thing, forgetting that to recover an encrypted message, it is enough to know the replacement rule, while to decrypt an already encrypted message in addition to knowing the rules of encryption, you need a cipher key. The key in this case means a specific secret state of the parameters of encryption and decryption algorithms.

Keywords: encryption; blockchain; smart contracts; messenger; cryptography.



УДК 621.395.348.4:004.4

DOI: 10.31673/2412-9070.2020.064448

V. M. DANYLCHENKO, Senior Lecturer;

V. R. MYKOLAICHUK, Senior Lecturer;

O. M. TKALENKO, PnD in technics, Associate Professor;

A. S. DIDKIVSKYI, student,

State University of Telecommunications, Kyiv

INITIAL SETUP OF PBX SERVER BASED ON ASTERISK

The development of information technology is very dynamic, in particular, actively developing computer networks, which are increasingly used for telephone conversations. Recently, there has been increased interest in IP-telephony technologies, in other words PBX, the use of which can significantly reduce the cost of telephone communication within the company. PBX (Private Branch exchange) is a system of devices that provides automatic connection and support of telephone communication between subscribers of this PBX, who use special end devices — telephones. A virtual PBX is a powerful telephone system that uses an Internet connection as opposed to standard telephone services. A standard PBX is used to transfer calls from the Internet to a public telephone switching network. Virtual PBX can be considered as a more economical version, because no equipment is involved, everything is virtual and hosted by the service provider. Currently, the open communication platform Asterisk occupies almost 85% of the open source PBX market. The Asterisk automatic telephone exchange supports both IP-telephony protocols and traditional communication lines. All basic and advanced PBX functions are supported: voice menu, call recording, call statistics, voicemail, queuing and operator distribution. Video communication is directly supported. The latest versions of Asterisk support call encryption. Asterisk has simple and well-documented interfaces for integration with other systems, making it easy to embed communications in business processes and business applications. There are a large number of various graphical tools for administering Asterisk, both paid and free, among which the most popular is the free WEB interface FreePBX.

Keywords: Server; IP-address; IP-telephony; Asterisk; FreePBX web-management; PBX; VoIP protocol.

Introduction

Today, the development of informative technologies is very active, in particular, computer networks are actively developing, they are increasingly used by users for telephone conversations. Recently, there has been an increased interest in IP-telephony technologies, in other words, automatic telephone exchange, the use of which can significantly reduce the cost of telephone communication within the company. For this reason, many companies began to switch to use PBX (private branch exchange) — the system of devices that provides automatic connection and maintenance of telephone communication between the subscribers of this PBX, using special terminal devices for this — telephone sets.

Research analysis

Asterisk, in conjunction with the required equipment, has absolutely all the capabilities of a traditional PBX, supports a large number of VoIP protocols and provides voice mail, conference, interactive voice menu, call queuing and other functions.

© V. M. Danylchenko, V. R. Mykolaichuk, O. M. Tkalenko, A. S. Didkivskiy, 2020

Purpose of the study

Initial server setup for making calls within the company and to other numbers using Asterisk server based on Linux operating system and using FreePBX web control.

Study results

The FreePBX control panel is used to configure the PBX. FreePBX is a web interface designed to manage the Asterisk VoIP telephony server and greatly facilitates system configuration due to the visual representation of data.

Much research is being done in the field of network administration. A. A. Pasyukov and R. I. Bazhenov [1] described the organization of a firewall using the Traffic Inspector software. M. Platov [2] revealed the essence of the Asterisk program on the Linux operating system. D. Nesterkin [3] described methods of transferring IP-telephony servers. A. V. Soloviev et al. [4] revealed the structure and problems of IP-telephony based on Asterisk. A. Bembiyeva, D. Namiot [5] talked about the disadvantages of using automatic telephone exchanges and methods of modernization. M. A. Sidorovich and A. I. Mikheev [6] described the construction of a mini-ATS based on the Raspberry PI microcomputer.

First, one need to download the distribution kit from the official software website www.freepbx.org. The starter version is fully functional and is quite enough for organizing communications in a medium or even a large company. For additional features, one can purchase various packages that will allow them to more accurately configure the PBX. When starting the distribution kit, the first step is to select the version of the program. In our case, we selected Asterisk 13 and the full installation. It should be noted that for installation the computer must be connected to the Internet (fig. 1).

Next, you need to configure the network. If the company does not have a dedicated IP address, you should leave everything by default and continue with the installation. If there is a dedicated IP address, then you need to go through the manual configuration and register it yourself (fig. 2).

Next, you need to set the time zone (fig. 3). An incorrectly set time zone will negatively affect the operation of the web interface and PHP. The transition between the elements is carried out with the Tab buttons and the selection of the element — with a space.

After setting the password, the software installation will start. The installer will check for compatibility, check your internet connection and format your hard drive, and then begin the process of installing and updating packages. Approximate installation time is 20-30 minutes, after which the server will reboot itself and a window will appear for creating a password for the main user, which allows you to connect to the server with full access (fig. 4).

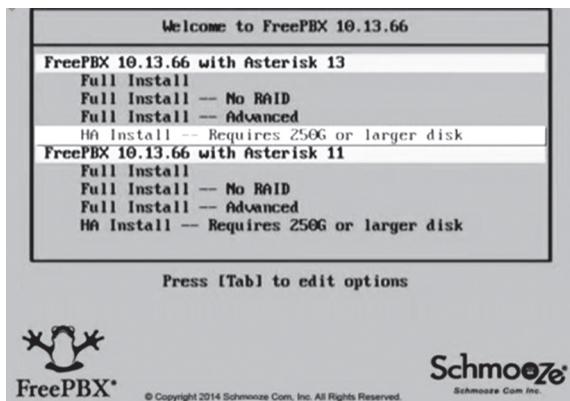


Fig. 1. Version selection



Fig. 2. Network configuration

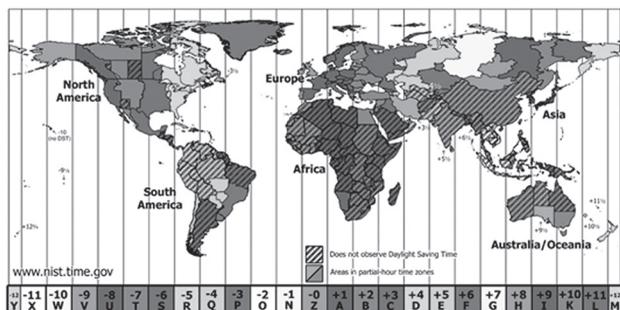


Fig. 3. Time zones



Fig. 4. Creating a password for the main user

Upon completion of the installation, the Linux console will be visible, where you will need to use the «root» login and the password entered earlier during installation for authorization in the PBX (fig. 5).

To go to the control panel, enter the IP address of the server in the address bar of the browser, which was specified after the complete installation of the system. After entering it will redirect to the FreePBX page (fig. 6).

```
SHMZ release 6.5 (Final)
Kernel 2.6.32-431.e16.i686 on an i686
localhost login: _
```

Fig. 5. Authorization in PBX

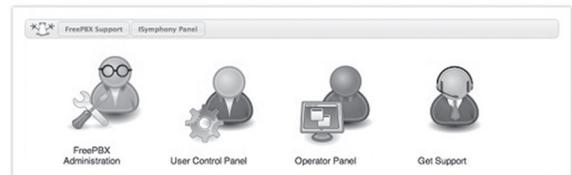


Fig. 6. FreePBX Control Panel

To start configuring the server, go to the «Free-PBX Administration» section and activate in the highlighted window. In this window, you will need to enter your mail, phone number and server location. After activation, go to the SIP settings, for this, first of all, in the «Allow Anonymous Inbound SIP Calls» line, change the switch position to «No», this blocked calls from external numbers and, thus, secured the threat network. In the line «Local Networks» you need to enter the trusted IP addresses of the network, which will not be blocked by the server when connecting and leave all other settings unchanged (fig. 7).

After initializing SIP, go to the FreePBX network card settings. To go to the settings, you need to go to the «System Admin» menu and after selecting the «Network Settings» tab in the «Network Interface» line, select the network card, in the «Static IP» line, manually enter the IP address of the server to connect, in the «Netmask» line, enter the network mask, in the «Gateway» line — the default gateway; and in the «Start Automatically» line, change the switch position to «Yes» so that when the server starts, the network card is automatically connected (fig. 8).

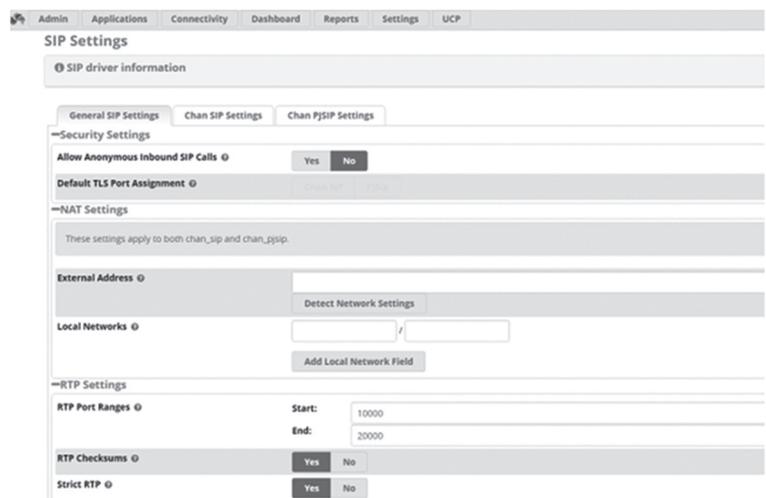


Fig. 7. SIP configuration

Next, you will need to set up notifications so that you are always aware of server failures, changes and current updates. To do this, in the «System Admin» menu on the «Notifications» tab. In the line «From Address» — the e-mail address that the PBX will indicate when forming the letter. The line «Storage Notifications» — indicates the mail to which notifications will be sent. The line «Intrusion Detection Notifications IP» indicates the mail to which notifications of hacking attempts will be sent (fig. 9).

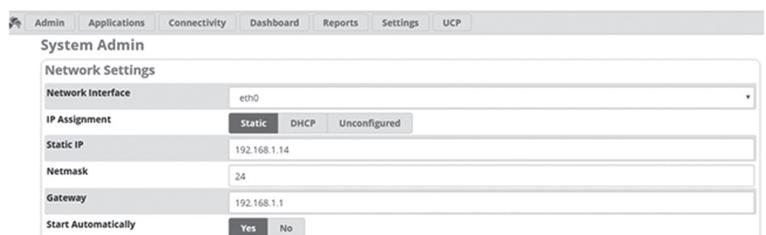


Fig. 8. Network configuration

Next, you will need to add extensions to make the call. To do this, go to the «Applications» menu, go to the «Extension» tab and add a new user, designating him with numbers that will be used when dialing the number. Then go to the setting and in the «Display Name» line specify the username and in the «Secret» line specify the password for editing the user (fig. 10).

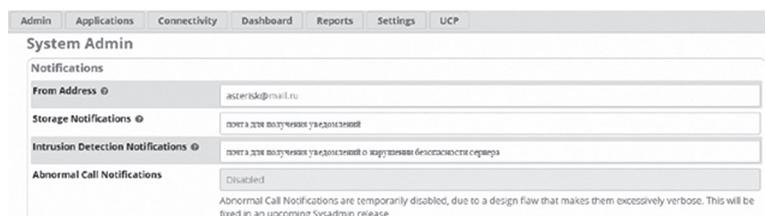


Fig. 9. Configuring notifications

One of the most important options when setting up Asterisk is connecting to an ISP that allows employees to make and receive

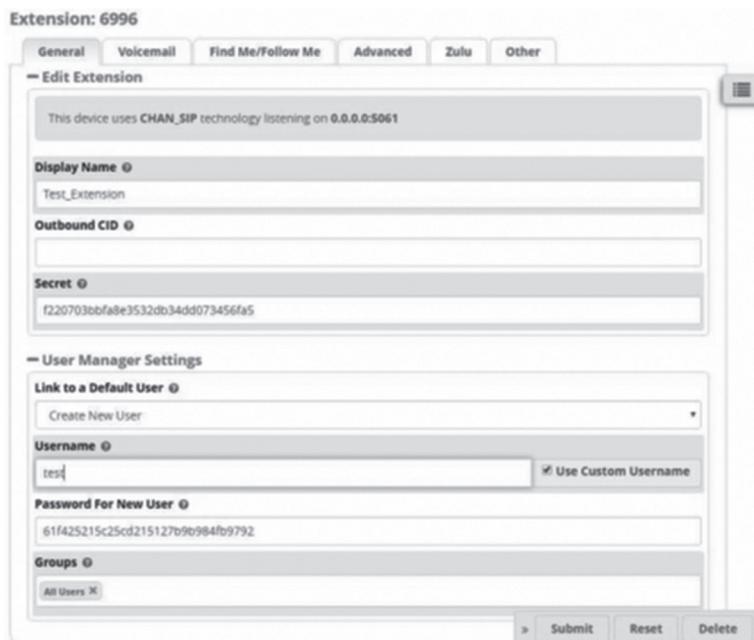


Fig. 10. Adding extensions

Add Trunk

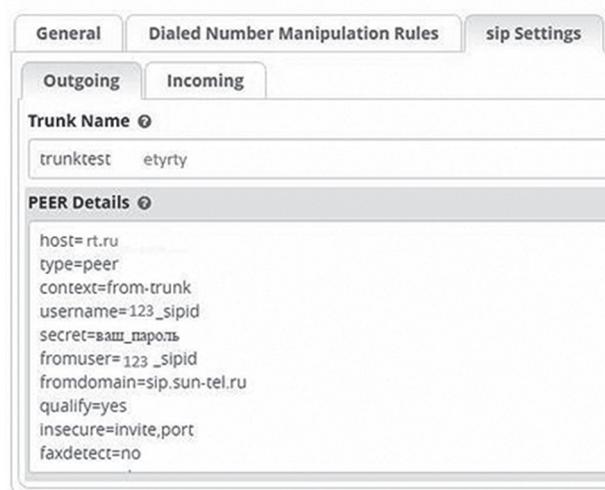


Fig. 11. Connecting to the provider

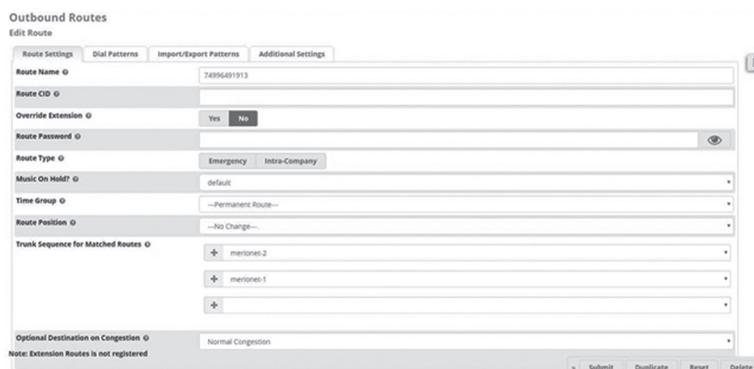


Fig. 12. Configuring outbound routing

calls. To do this, select the Add SIP (chan_sip) option in the «Connectivity» menu on the «Trunks» tab. After adding a new trunk, you need to come up with a name for it, specify the maximum number of simultaneous calls in the «Maximum Channels» line. Next, go to the «Sip Settings» tab and duplicate the trunk name (fig. 11).

Enter the following commands in the PEER details window:

```
host = rt.ru - provider's address
type = peer
context = from-trunk
username = 123_sipid - login issued by the provider
secret = your _ password - a password, issued by the provider
fromuser = 123_sipid
fromdomain = rt.ru
qualify = yes
insecure = invite, port
faxdetect = no
account = rt
```

The latter need to configure outbound routing, for this you need to go to the «Connectivity» menu and on the «Outbound Routes» tab in the «Route Name» line enter the name of the route, it is better to use a phone number for convenience. In the line «Route CID» we indicate the number that will be displayed by the provider. In «Music On Hold» we specify the melody of the incoming call and in «Optional Destination On Congestion» we select which trunks the forwarding will go to if the dialed number is not available (fig. 12).

After completing the server configuration, you will need to reboot the server, after which you can connect SIP phones using additional equipment. To make a call, you need to dial the short number that was entered when creating internal numbers. In the course of the work, the initial configuration of the Asterisk server was organized using the FreePBX web management, which is designed to save money on making phone calls within the company, as well as to other cellular and landline numbers.

References

1. Bryant R., Madsen L., Van Meggelen J. Asterisk // The Definitive Guide. 2013. No. 6. 222 p.
2. Nesterkin D. Transfer of telephone lines between offices on the basis of IP-PBX Asterisk and Linksys // System administrator. 2010. No. 4. P. 56–60.
3. Bembieva A., Namiot D. Voice dialogs for Asterisk // International journal of open information technologies. 2013. No. 7. P. 24–27.

4. Van Meggelen J., Madsen L., Smith J. Asterisk // *The Future of Telephony*. 2018. 317 p.

5. Sidorovich M. A., Mikheev A. I. *Building an IP-PBX for small business based on the Raspberry PI microcomputer // Scientific, technical and economic cooperation of the Asia-Pacific countries in the XXI century*. 2016. No. 1. P. 106–109.

В. М. Данильченко, В. Р. Миколайчук, О. М. Ткаленко, А. С. Дідківський

ПОЧАТКОВЕ НАЛАШТУВАННЯ СЕРВЕРА АТС НА ОСНОВІ ASTERISK

Розвиток інформаційних технологій відбувається дуже активно, зокрема активно розвиваються комп'ютерні мережі, які все частіше застосовуються користувачами для телефонних розмов. Останнім часом спостерігається підвищений інтерес до технологій IP-телефонії, іншими словами АТС, використання якої дає можливість значно знизити вартість телефонного зв'язку всередині компанії. АТС (автоматична телефонна станція) — це система пристроїв, що забезпечує автоматичне з'єднання і підтримання телефонного зв'язку між абонентами цієї АТС, які користуються для цього спеціальними кінцевими пристроями — телефонними апаратами. Віртуальна АТС — потужна телефонна система, яка використовує підімкнення до Інтернету на відміну від стандартних телефонних послуг. Стандартна IP-АТС застосовується для передавання дзвінків з інтернету на телефонну комутаційну мережу загального користування. Віртуальну АТС можна розглядати як більш економічну версію, оскільки не задіяно жодне обладнання, все віртуальне та розміщується у постачальника послуги. Сьогодні відкрита комунікаційна платформа Asterisk займає майже 85% ринку АТС з відкритим кодом. Автоматична телефонна станція Asterisk підтримує як протоколи IP-телефонії, так і традиційні лінії зв'язку. Підтримуються всі базові та розширені функції АТС: голосове меню, запис розмов, статистика викликів, голосова пошта, постановка дзвінків у чергу і розподіл по операторах. Безпосередньо підтримується відеозв'язок. В останніх версіях Asterisk підтримується шифрування розмов. Asterisk має прості і добре документовані інтерфейси для інтеграції з іншими системами, що дає можливість легко вбудовувати комунікації в бізнес-процеси і бізнес-додатки. Існує велика кількість всіляких графічних засобів адміністрування Asterisk як платних, так і безплатних, серед яких найбільш популярний безплатний WEB інтерфейс FreePBX.

Ключові слова: сервер; IP-адреса; IP-телефонія; Asterisk; веб-керування FreePBX; АТС; протокол VoIP.

В. Н. Данильченко, В. Р. Миколайчук, О. Н. Ткаленко, А. С. Дидковський

НАЧАЛЬНАЯ НАСТРОЙКА СЕРВЕРА АТС НА ОСНОВЕ ASTERISK

Развитие информационных технологий проходит очень активно, в частности активно развиваются компьютерные сети, которые все чаще применяются пользователями для телефонных разговоров. В последнее время наблюдается повышенный интерес к технологиям IP-телефонии, то есть АТС, использование которой позволяет значительно снизить стоимость телефонной связи внутри компании. АТС (автоматическая телефонная станция) — это система устройств, которая обеспечивает автоматическое соединение и поддержку телефонной связи между абонентами этой АТС, пользующимися для этого специальными конечными устройствами — телефонными аппаратами. Виртуальная АТС — мощная телефонная система, которая использует подключение к Интернету в отличие от стандартных телефонных услуг. Стандартная IP-АТС используется для передачи звонков из интернета на телефонную коммутационную сеть общего пользования. Виртуальную АТС можно рассматривать как более экономичную версию, поскольку не задействовано оборудование, все виртуальное и размещается у поставщика услуги. В настоящее время открытая коммуникационная платформа Asterisk занимает почти 85% рынка АТС с открытым кодом. Автоматическая телефонная станция Asterisk поддерживает как протоколы IP-телефонии, так и традиционные линии связи. Поддерживаются все базовые и расширенные функции АТС: голосовое меню, запись разговоров, статистика вызовов, голосовая почта, постановка звонков в очередь и распределение по операторам. Непосредственно поддерживается видеосвязь. В последних версиях Asterisk поддерживается шифрование разговоров. Asterisk обладает простыми и хорошо документированными интерфейсами для интеграции с другими системами, что позволяет легко встраивать коммуникации в бизнес-процессы и бизнес-приложения. Существует большое количество всевозможных графических средств администрирования Asterisk как платных, так и бесплатных, среди которых наиболее популярный бесплатный WEB интерфейс FreePBX.

Ключевые слова: сервер; IP-адрес; IP-телефония; Asterisk; веб-управление FreePBX; АТС; протокол VoIP.