BULETINUL Universităţii Petrol – Gaze din Ploieşti	Vol. LXVIII No. 2/2016	47 – 53	Seria Tehnică

Implementing a Data Network Infrastructure with Unified Services of Videoconference and VoIP

Otilia Cangea

Petroleum-Gas University of Ploiesti, Bd. Bucuresti 39, Ploiesti
e-mail: ocangea@upg-ploiesti.ro

Abstract

From the point of view of a secured data transmission, virtual private networks offer an extremely attractive solution to the business environment. At the same time, virtual private networks represent the most efficient way of satisfying the clients demands related to a large capacity and high speed transmission.

The paper presents the technologies specific to virtual private networks and Internet telephony, emphasizing the particular advantages and disadvantages. A case study presenting a videoconference system is configured using dedicated equipment.

Key words: *data network, infrastructure, videoconference, VoIP*.

Introduction

Globalization and industrialization have led to a continuous search of efficient communication solutions for all professional organizations. The need to reduce expenses with travel, the environmental care issues, or the work/leisure time ratio of the employees impose innovative solutions for communication and collaboration. In this context, Internet has produced radical changes in the definition and leadership of a business, offering solutions for informing and communicating, and thus increasing the management. Nowadays, and so much the more in the future, the business success relies upon the state-of-the-art communication technologies and, particularly, upon developing the Virtual Private Network (VPN) and VoIP (Voice over Internet Protocol) systems [1].

VPN systems support high data speed and offer the advantage of mobility and configuring communication using a very large band width. They can also be used in order to transport VoIP and video packages on a TCP support, actually improving voice quality, a very important demand for data transmission. VPN connects all the components and resources of a private network by means of a public network [2]; in other words, a VPN is a company network implemented on a mutual infrastructure, using the same security, management and performance politics that usually apply in a private network (figure 1).

VPN can be implemented on various transport networks, such as public Internet or the network specific to the IP services provider. VPN technology uses a combination of tunneling, encryption, authentication and control access mechanisms and services to transport traffic on Internet by means of an IP administrated network or a services provider network.

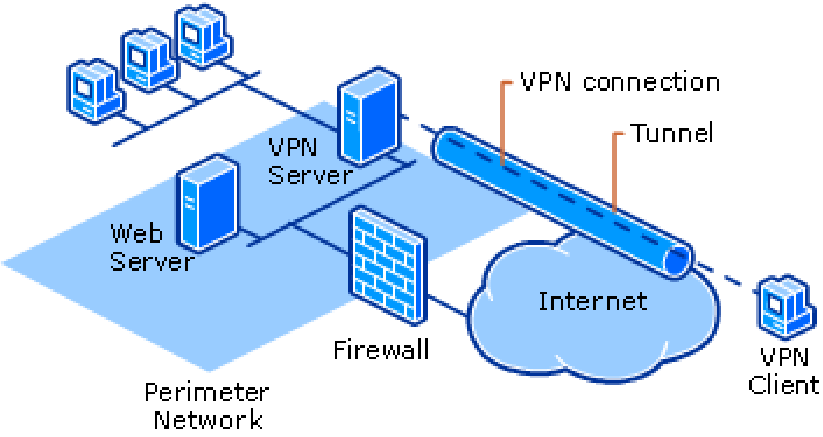


Fig. 1. How VPN works [2]

In order to ensure data privacy when using unsecured communication channels, such as Internet, various cryptographic techniques can be employed; some solutions encrypt the whole message (IP header and message data), while others encrypt only the data. There are four transmission techniques in VPN area, as follows [3]:

- *In Place Transmission Mode*, a custom-made solution that encrypts only the data, without affecting the dimension of the packages, and, therefore, the transport mechanisms are not at all affected;
- *Transport Mode*, that encrypts only the IP payload, so that the size of the package will increase; this mode offers a suitable privacy for data considering site-to-site VPN systems;
- *Encrypted Tunnel Mode*, that encrypts the IP header information, as well as the data, attaching a new IP address, mapped on VPN terminals, and thus ensuring a global privacy of data;
- *Non - encrypted Tunnel Mode*, that has no encrypted component, all data being transmitted as plain text and, consequently, with no data privacy at all.

Depending on the used VPN type – remote-access or site-to-site - in order to built it, the requisite components are:

- a software client program for each remote user;
- a dedicated hardware, such as a VPN concentrator or a security PIX firewall;
- a VPN server dedicated to dial-up services;
- a network access server (NAS) used by the service provider for remote users access to VPN;
- an administration center of VPN politics.

All VPN systems provide reliability, performances and security associated to traditional WAN systems, but they have the advantage of lower costs and Internet Service Provider connections much more flexible. At the same time, VPN technology can be used in an Intranet in order to ensure security and access control related to information, resources or vital information systems.

VoIP technology represents the future and the very present of voice telephony services. Considering the globalization and service convergence tendencies, implementing this technology has already become an important requirement, being a viable and preferred alternative to classical telephony. The start of the IP telephony was given in 1995, when VocalTec company launched the product Internet Phone, that allowed a multimedia PC to dial-up another one for a phone call over Internet. The structure of a VoIP network [4] is presented in Figure 2.

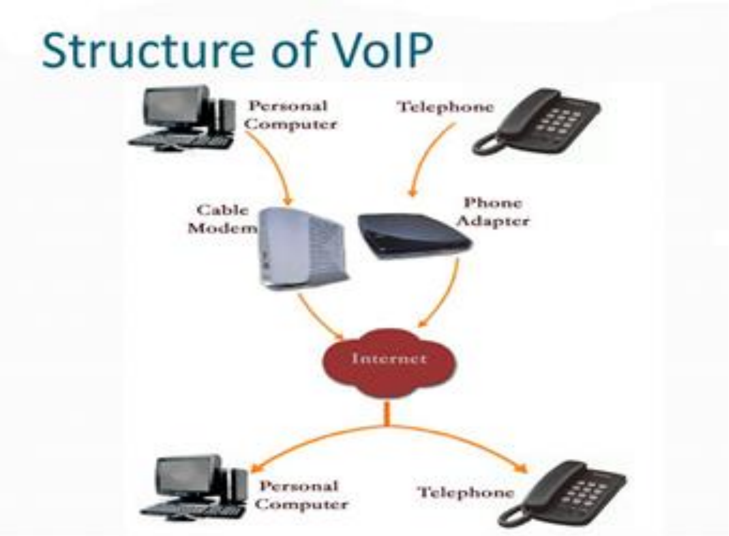


Fig.2. Structure of VoIP [4]

Using VoIP telephony is nowadays performed in three ways, as follows [4]:

- *by means of a classical telephony*, using an ATA (Analogue Telephone Adapter), with two sockets (a RJ-45 for Ethernet and a RJ-11for classical telephony). ATA connects the user phone to the Internet connected VoIP provider network;
- *using IP phones,* fitted out with a RJ-45 (Ethernet socket) and required hardware and software equipment;
- *a two-computers communication*, Internet (or another LAN) connected, that have to be equipped with special software programs, microphone, tweeters, headphones, and a soundcard. The band width has to be broad enough for these specific calls.

Among the most important advantages offered by VoIP technology, one can emphasize:

- *the cost*: represents the major advantage, due to the fact that the same transport mode is used for voice, as well as for data; in addition, VoIP users have free calls;
- *an improved performance compared to classical telephony,* considering the fact that an IP phone can be used wherever there is an Internet connection;
- *supplementary services*, such as video or text files transmission at the same time with the call, due to shared data connection.

In the same time, there are important disadvantages, as follows:

- *implementing issues*, on account of IP technology, that does not ensure a Quality of Service mechanism, and, consequently, there are delays and quality variations;
- *Weak stability*, due to possible problems regarding Internet connection, that affect VoIP services;
- *Difficulties in directing emergency calls*, with relation to geographical locating of an user.

Videoconference System

The structure of a VPN videoconference system (figure 3) is composed of videoconference terminals and a terminal management server (TMS). Videoconference terminal integrates a combination of equipment, as follows:

- *a videoconference codec***,** that is the main equipment that connects the terminal to the videoconference server, and ensures the control of the terminal-server communication;
- *a high resolution video camera* (namely a TANDBERG precision HD camera),
- *a monitor*.

The videoconference codec is a Tandberg Edge 75/85/95 MXP system [2], used for conference rooms and offices, that integrates characteristics and functions of performance systems, ensuring signal optimal quality and simultaneously displaying the speaker and the presentation on the screen using the “Dual Streaming” function. It assures telephony network connection according to H.320/H.323 standard at a 384/768 Kbps band width.

The encryption method is A.E.S., that has the advantage of speed, it is easy to implement and has a solid mathematical foundation, being not very vulnerable to cryptographic attacks.

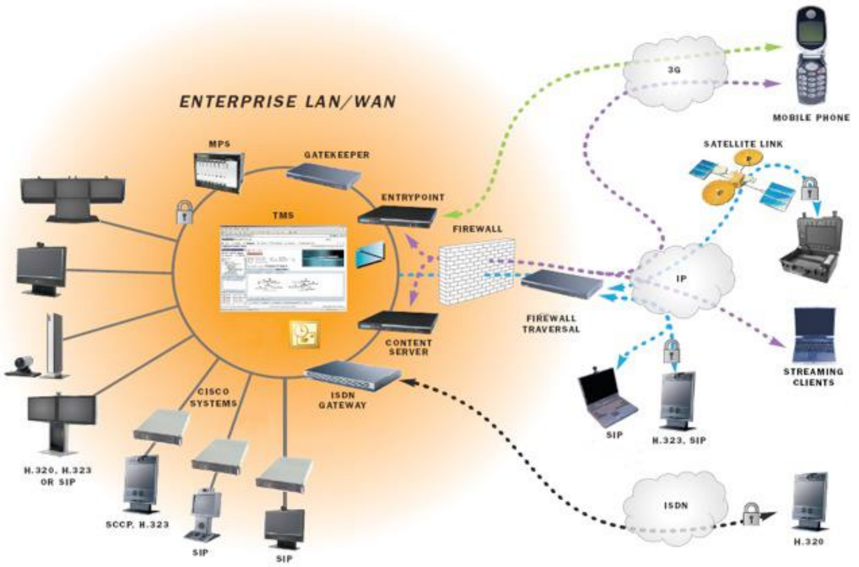


Fig. 3. Videoconference system

The interconnection mode of the terminal equipment is presented in figure 4 [4].

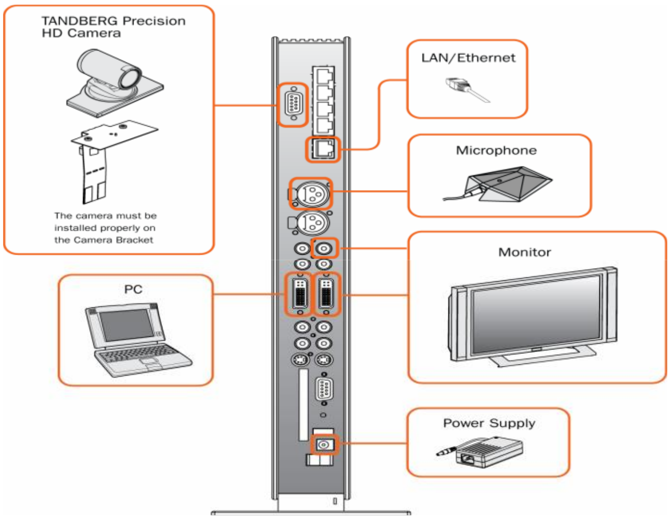

TANDBERG Precision HD Camera
The camera must be installed properly on the Camera Bracket
LAN/Ethernet
Microphone
Monitor
PC
Power Supply

Fig. 4. Interconnection mode of the terminal equipment

In order to configure the structure of VPN, it is necessary to fit up every location with:

- at least an Internet provider, so that the data transfer speed should be as fast as possible;
- a set of routers, one active, the other one passive, both on WAN and working together, so that interruptions in data, voice or video paths functioning should be avoided.

CISCO routers configuration [5,6] for data, VoIP and videoconference is carried out by performing a number of stages, some of the most important being the following:

- router authentication (user name, password, current configuration);
- presenting routers software version and encrypting the passwords; a sequence of the corresponding particular configuration is:

```
crypto pki trustpoint TP-self-signed-400687573
enrollment selfsigned
subject-name cn=IOS-Self-Signed-Certificate-400687573
revocation-check none
rsakeypair TP-self-signed-400687573
crypto pki certificate chain TP-self-signed-400687573;
```

- defining the authentication certificates and central routers addresses to whom they are subordinating;
- defining a group of addresses that will have access to all the servers from the respective area;
- defining a group of addresses that will have access to all the IP's in LAN;
- defining tunneling addresses for GigaBit Ethernet 0/1 interface;
- defining tunnels for data link with the central router and with all the other local points;
- data authentication and encryption on LAN defined addresses and their prioritization, such as presented in the following sequence:

```
standby 102 name VLAN102
standby 103 ip 10.116.4.31
standby 103 priority 200
standby 103 preempt.
```

Software Management Platform for a Videoconference

TMS (Tandberg Management Suite), the management server of the videoconference terminals, is a software platform (figure 5), built on the basis of a SQL server, that ensures management, implementation, and programming for the video network in the entire VPN, so that it can offer visibility and centralized control for the local systems, as well as remote video services. TMS ensures support for remote systems using VPN. Remote systems are accepted for reservation, software updating, and receiving phone cards, and represent a part of the statistics created in TMS.

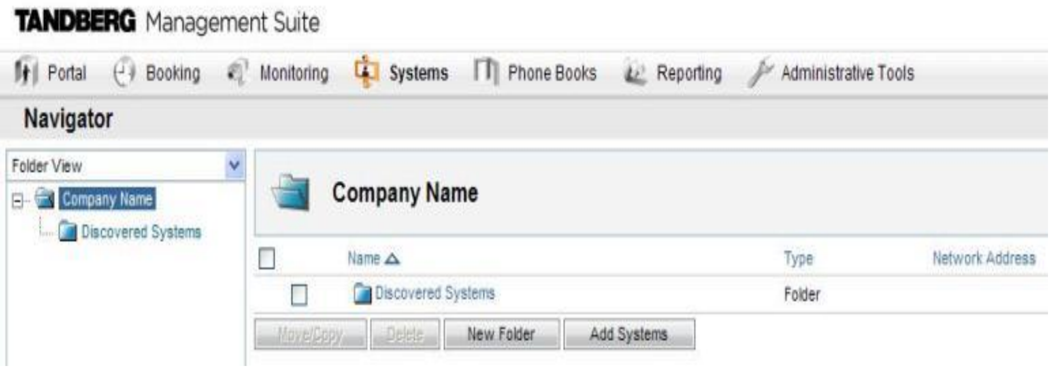
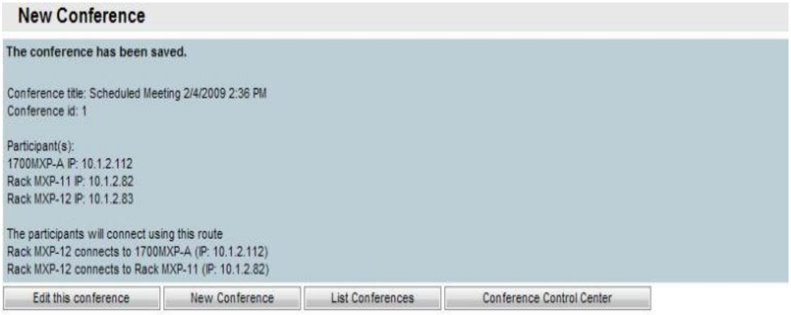


Fig. 5. TMS graphical interface

Programming a videoconference is performed by TMS using the *New Conference* page:

- *New Conference* page is opened accessing *Reservation;*
- A conference title is introduced; this becomes visible in all TMS interfaces, as well as in all sent e-mail messages;
- The conference beginning hour and duration are set;
- *Participant* page allows adding new participants, thus generating a *Display available participants list* window;
- Consequently, TMS will determine the best way of connecting the selected participants, by selecting the protocol, checking the compatibility of the available systems, handling ISDN numbers and required infrastructure resources.

In the case when TMS is not able to finalize a reservation request, due to unavailability or network resources deficiency, a banner message will be displayed on the conference page, specifying the reasons. In the case when the request is finalized, a *New Conference* confirmation page will be displayed (figure 6), pointing out the scheduled meeting details, including the participants list and the manner in which these participants are programmed to be connected to the conference.



New Conference

The conference has been saved.

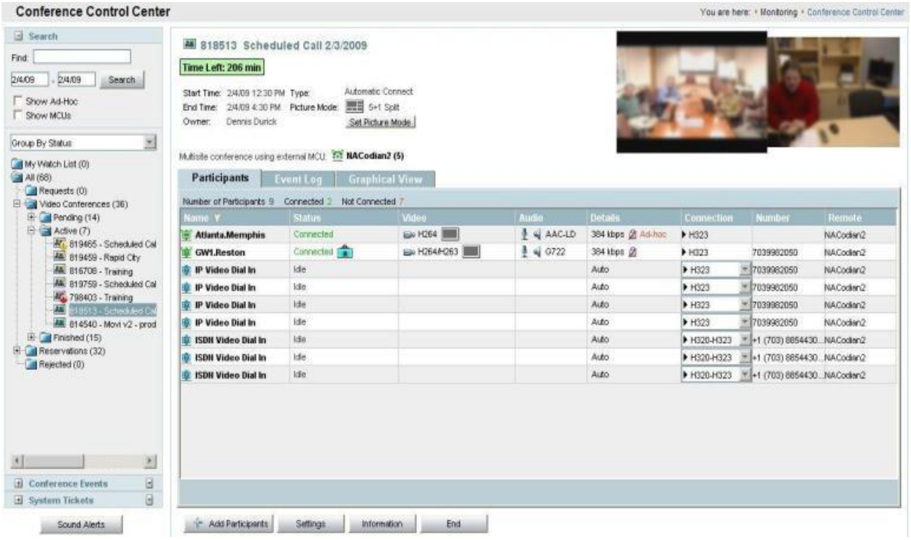
Conference title: Scheduled Meeting 2/4/2009 2:36 PM
Conference id: 1

Participant(s):
1700MXP-A IP: 10.1.2.112
Rack MXP-11 IP: 10.1.2.82
Rack MXP-12 IP: 10.1.2.83

The participants will connect using this route
Rack MXP-12 connects to 1700MXP-A (IP: 10.1.2.112)
Rack MXP-12 connects to Rack MXP-11 (IP: 10.1.2.82)

Fig.6. Example of a *New Conference* page with reservation confirmation

In order to real-time monitor and manage in-process conferences, TMS has a *Conference Control Center* interface (figure 7), that also allows creating new conference events by the operator; these are the so-called ad-hoc conferences, that enable conference operators to work with individual participants apart from the usual programmed sessions. The commands for these conferences are available in the monitoring menu of TMS.



Conference Control Center

You are here: › Monitoring › Conference Control Center

Find:
2/4/09 - 2/4/09
□ Show Ad-Hoc
□ Show MCUs
Group By Status

818513 Scheduled Call 2/3/2009

Time Left: 206 min

Start Time: 2/4/09 12:30 PM Type: Automatic Connect
End Time: 2/4/09 4:30 PM Picture Mode: 5+1 Split
Owner: Dennis Durick

Multisite conference using external MCU: NACodian2 (5)

Number of Participants 9 Connected 2 Not Connected 7

Name	Status	Video	Audio	Details	Connection	Number	Remote
Atlanta.Memphis	Connected	H264	AAC-LD	384 kbps Ad-hoc	H323		NACodian2
GW1.Reston	Connected	H264/H263	G722	384 kbps	H323	7039982050	NACodian2
IP Video Dial In	Idle			Auto	H323	7039982050	NACodian2
IP Video Dial In	Idle			Auto	H323	7039982050	NACodian2
IP Video Dial In	Idle			Auto	H323	7039982050	NACodian2
IP Video Dial In	Idle			Auto	H323	7039982050	NACodian2
ISDN Video Dial In	Idle			Auto	H320-H323	+1 (703) 8854430...	NACodian2
ISDN Video Dial In	Idle			Auto	H320-H323	+1 (703) 8854430...	NACodian2
ISDN Video Dial In	Idle			Auto	H320-H323	+1 (703) 8854430...	NACodian2

Fig. 7. Example of a *Conference Control Center* interface

Conclusion

VPN support high data speed and offer the advantage of mobility and configuring communication using a very large band width. They can also be used in order to transport VoIP and video packages on a TCP support, thus improving voice quality, a very important demand for data transmission. Nowadays, specialists try to create unified technologies for communication, practically establishing an integrated interface system for all communication services.

The paper presents the virtual private networks and Internet telephony own technologies, emphasizing the specific advantages and disadvantages and a comparative analysis with classical telephony. A case study presenting a videoconference system is configured using dedicated equipment, with a highlight upon the body parts of the system and the specific operations.

As a future research, it is important to develop the integration of both components: real-time and non real-time communication services. Although VoIP is very attractive, the technology has not been so far adequately developed so that it could replace the services and the quality provided by PSTN.

References

1. Cangea, O. – *Algoritmi de criptare pentru securitatea sistemelor informatice*, Editura Universitatii Petrol-Gaze din Ploiesti, 2012.
2. *How VPN works*, TechNet Microsoft Library, March 2003.
3. Seurre, E., Savelli, P., Pietri, P.J. – *GPRS for Mobile Internet*, Artech House, 2003.
4. S.Mahesh, A.R. – *Smart Call. Intro Present communication Techniques. Telephone call, Fax, E-mail, Postal System, Telegram*, Dwain Palmer Editor, 2011.
5. Thomas,T., Stoddard, D. – *Network Security First-Step*, 2nd Edition, Ciscopress, 2012.
6. Duggan, M. – *Cisco CCIE Routing and Switching v5.0 Configuration Practice Labs*, Ciscopress, 2014.

Analiza implementării unei infrastructuri de reţea de date care oferă servicii unificate de videoconferinţă şi VoIP

Rezumat

Reţelele virtuale private (VPN) oferă mediului de afaceri o soluţie extrem de atractivă pentru transmiterea securizată a datelor. Totodată, VPN reprezintă şi cea mai eficientă cale de a satisface cerinţele clienţilor care necesita, pe langă transmisii securizate de date, şi capacitate mare de transmitere şi viteză ridicată.

Lucrarea prezintă o analiza a tehnologiilor proprii reţelelor virtuale private şi ale telefoniei prin Internet, cu evidenţierea avantajelor şi dezavantajelor asociate, precum şi a avantajelor şi dezavantajelor telefoniei prin Internet în comparaţie cu telefonia clasică. Studiul de caz pentru sistemul de videoconferință este efectuat pe echipamente dedicate, fiind evidențiate și detaliate toate elementele componente ale sistemului, precum si maniera de configurare.