The Virtual Enterprise Network based on IPSec VPN Solutions and Management

Sebastian Marius Rosu, Marius Marian Popescu
Radio Communications & IT Department
Special Telecommunications Service
Bucharest, Romania

George Dragoi, Ioana Raluca Guica
Department of Engineering in Foreign Languages
University "Politehnica" of Bucharest
Bucharest, Romania

***Abstract*—Informational society construction can't be realized without research and investment projects in Information and Communication Technologies (ICT). In the 21st century, all enterprises have a local area network, a virtual private network, an Intranet and Internet, servers and workstations for operations, administration and management working together for the same objective: profits. Internet Protocol Security is a framework of open standards for ensuring private communications over public networks. It has become the most common network layer security control, typically used to create a virtual private network. Network management represents the activities, methods, procedures, and tools (software and hardware) that pertain to the operation, administration, maintenance, and provisioning of networked systems. Therefore, this work analyses the network architecture for an enterprise (industrial holding) geographically dispersed. In addition, the paper presents a network management solution for a large enterprise using open source software implemented in the PREMINV Research Center, at the University "Politehnica" of Bucharest.**

Keywords-Enterprise network; IPSec; network architecture; VPN; network management.

I. INTRODUCTION

Under the concept of a global economy, enterprises are assigning design and production environments around the world in different areas. The requirement for highly reliable and available services has been continuously increasing in many domains for the last decade [1]. The optimization of product benefit must be the focus of all network activities [2]. The work comprises components for integration of information systems, visualization of the planning and production situation, communication to enable cooperative decision making under uncertainty, optimization of plans and simulation of the decisions, network diagnostics and performance monitoring among others [3]. This involves a number of challenges such as providing members access to network-wide real time information, enable visualization of the available information, secure the interaction between advanced information and communication technologies (ICT) based decision support tools and human decision making, creating a coordinated and collaborative environment [2] for planning and decision making. The implementation phase in ICT system is done by doing several socialization activities such as training, hands-on workshop, coaching or even giving a grant for the users who use the system correctly [4].

Monitoring of such process execution may allow the manager to detect faults and guarantee correct execution [5] - e. g. voicedata packets have to arrive at the destination in time, with a defined cadence and with low and constant delay in order to allow the real time voice reconstruction [6]. Because the new communication system enables many more interactions between many more participants, it has security requirements beyond the conventional confidentiality, integrity and availability properties provided by conventional security systems [7]. The idea of NGN (Next Generation Network) is developed with the purpose of integrating different multiple services (data, voice, video, etc.) and of facilitating the convergence of fixed and mobile networks [8]. However, the effects of ICT devices on the productivity of companies cannot be measured unequivocally at the microeconomic level because of certain statistical and methodological imperfections, the difficulties in measuring network effect at a business level and the lack of data enabling to make international comparisons [9]. Development of information technology and communication has led to widespread deployment of technical solutions for [10]:

- Accessing and processing data and information;
- The transmission of data and information in a network environment with distributed destinations;
- Connect different users regardless of their geographical distance and position.

The complexity of the human enterprise continues to grow at an accelerating pace as larger numbers of people take on increasingly ambitious tasks in a world that grows in size, complexity, and constraining factors [11]. On-line applications (e.g. e-banking, electronic voting, information sharing and searching) require anonymous measures to prevent third parties from gathering online private information. As a general requirement for an infrastructure support is than the enterprises must be able to inter-operate and exchange information and knowledge in real time so that they can work as a single integrated unit [12], although keeping their independence/autonomy.

Various network services can be used by everyone, either supplying or demanding them. A large range of distribution, the platform independence, a big number of user friendly services that are easily accessible through the World Wide Web as well as the open standards used and free or budget-priced products (such as browsers, html editors, software

updates) have lead to a high and continuously growing proliferation of the Internet [13]. More and more people are using Internet to access information and communicate with each other. Development of ICT leaves much more freedom to the designers and consultants to accommodate organizations to other influences, both internal and external [14]. Enterprises are now facing growing global competition and the continual success in the marketplace depends very much on how efficient and effective the companies are able to respond to customer demands [15]. Starting from these considerations, this work analyzed the virtual enterprise network (VEN) architecture for an enterprise geographic dispersed as support for virtual private networks (VPNs) possible structures (based on Internet Protocol Security – IPSec) and presents a network monitoring solution using open source software to enterprise business improvement.

II. The Enterprise Network General Architecture

An enterprise network consists of a group (departmental, interdepartmental, etc.) of *local area networks* (LANs), located in the same place or geographically dispersed, interconnected using *wide area networks* (WANs) and contains a number of inter-networking devices (e.g. switches, routers, gateways, etc.) which is under the control of the organization or a telecommunication company. A communication network forms the backbone of any successful organization [16]. Metropolitan networks play a critical role in the overall expansion of network services because they not only provide for services within individual metropolitan areas, but they also serve as the gateways for wide-area national - and international - scale networks [17]. In an enterprise network, a large number of nodes are interconnected together through a computer network as follow [18]:

- End-user nodes represented by access points such as workstations, personal computers, printers, mainframe computers, etc.
- Network active elements consist of devices such as multiplexers, hubs, switches, routers, and gateways; the active elements and links provide the needed physical communication paths between every pair of end-user nodes.

Today, traditional infrastructures type Internet/Intranet/Extranet have now a fast dynamic, marking the transition to new generation networks to provide higher speeds to the user (end to end), for different types of activities and transactions and a significant reduction in the number of servers by passing information between two nodes [19].

In the last decade, specially, the idea of virtual enterprise (VE) called on a *virtual enterprise network* (VEN) or a *virtual enterprise business network* (VEBN) is meant to establish a dynamic structure of the organization by a synergetic combination of dissimilar enterprises (i.e. small and medium sized enterprises) with different core competencies, thereby forming a best of everything temporary alliance inan industrial group or holding to perform a given business project to achieve maximum degree of customers requirements and customer satisfaction [15].

In the last years, the trend toward IP-based transport infrastructures for all real-time and non-real-time applications opens the door for a new paradigm in integrated voice and data communications. A hierarchical network design model breaks the complex problem of network design into smaller, more manageable problems [15]. An important step in designing an enterprise network is to define a network perimeter. The enterprise network perimeter (see figure 1) defines a security layer complemented with other security mechanism [20], [21]. Communications within and outside the enterprise perimeter must be through a traffic control point - provided by firewalls and other security devices [19]. Large area networks (WANs, specific for large enterprise or for businesses geographically dispersed) were designed to solve connection problems between different workstations and different local networks, or only a local network where the distances are too large to be able to use a simple cable connection. The network designs are examples of secure network architecture that are scalable for home offices, small and medium sized businesses, or business enterprises. A variety of hardware, operating systems, and applications can be used in their implementation. Both commercial and free open source products can be used for the workstations, web servers, security servers, and database servers.

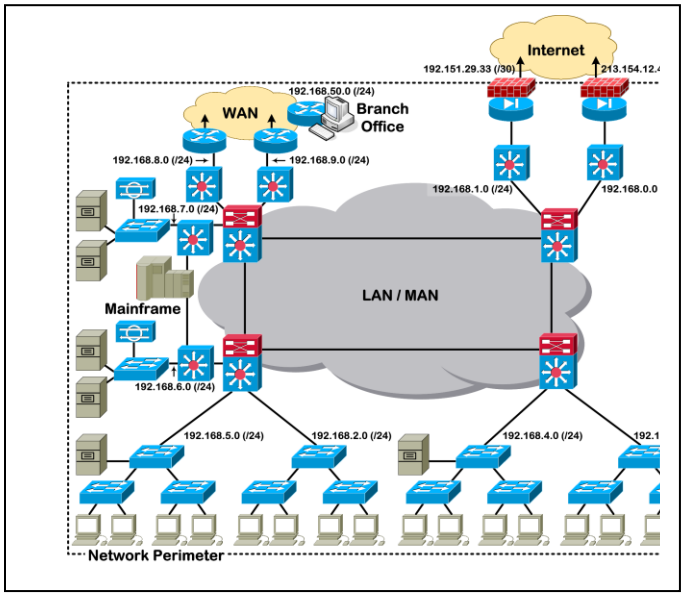


Figure 1. The enterprise network perimeter

A high performance backbone has an intrinsic value for an ultra-fast Internet connection only if the points of connection and network users, POP (*Point of Presence*), providing an equivalent level of performance. ATM (*Asynchronous Transfer Mode*) is a packet-switched technology that uses virtual circuits over a single physical connection from each location to the ATM cloud. Data is transferred in cells or packets of a fixed size. The small, constant cell size allows ATM equipment to transmit video, audio and computer data over the same network. ATM creates a fixed channel between two points whenever data transfer begins. This makes it easier to track and bill data usage across an ATM network (see figure 2), but it makes it less adaptable to sudden surges in network traffic.

Four types of service are available: *constant bit rate* (CBR), *variable bit rate* (VBR), *available bit rate* (ABR) and *unspecified bit rate* (UBR). In this idea, we propose in figure 3 a general virtual enterprise network architecture for a large enterprise or an industrial holding (with headquarters and branches) formed by a temporary alliance of different small and medium sized enterprises, geographically dispersed, with ATM Points of Presence (PoPs).

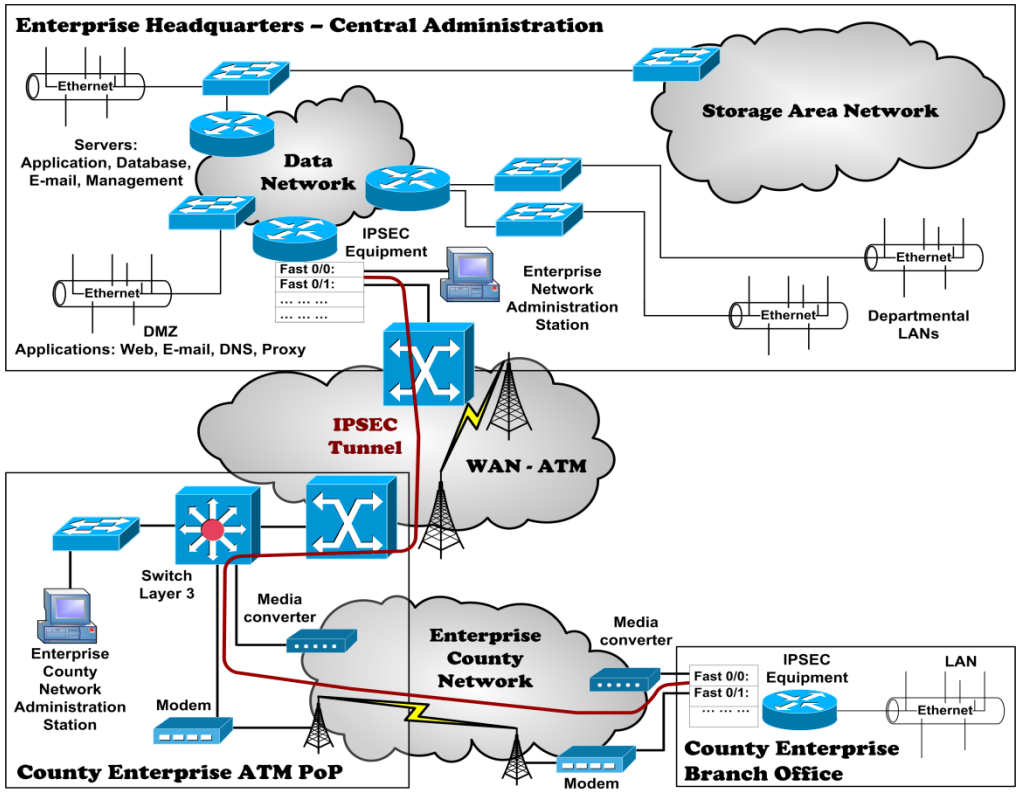


Figure 2. An ATM network for an enterprise geographically dispersed with PoPs to support transfer of large volumes of data over long distances

This solution is implemented in the PREMINV e-platform at the University "Politehnica" of Bucharest, where the virtual enterprise network (VEN) is based on a virtual private network (VPN). This is an emulated network built on public infrastructure (shared), and particularly dedicated to a client (the private) to connect the different users in locations and capable to ensure similar conditions of integrity, confidentiality and quality similar with those of a private network.

Virtual Enterprise Networks allows the provisioning (i.e. private network services) for a dynamic organization over a public or shared infrastructure such as the Internet or service provider backbone network.Appearance of a virtual enterprise network is related to the evolution switches. The first and the most important role of a virtual enterprise network is to realize a synergetic combination of a group of users regardless of their geographical position but in such a manner that it flows together and provide the best performances. Secondly, a VEN provide administrative solutions which accompany the products, allowing users moving from one group to another through a simple reconfiguration of the equipment [22].However, the application-to-application communication problem still exists. Businesses have needed a standardized way for applications to communicate with one another over networks; no matter how those applications were originally implemented [23].

III. THE ENTERPRISE VPNS IPSEC SOLUTIONS

In fact,emulated VPN is a network build on public infrastructure (shared), dedicated to a client (privacy), to connect the users and to ensure the conditions of integrity, confidentiality and quality similar with a private network. It purposes the following classification of VPN's:

a) After the length of structures:

- Permanent VPN
- Enabled VPN (tunneling): Client Tunnel Compulsory Tunnel.

b) As responsible for implementing:

- VPN's provider's responsibility
- VPN's client responsibility
- VPN's provider's and customer responsibility

If VPN is the responsibility of the supplier and is reduced to connectivity, the content and inter-location communication are the responsibility of the recipient (customer) and the provider should not restrict the type of inter-location intercommunication that only it would to the extend that it would have repercussions on the physical network).

c) Type of access in VPN:

- VPN remote access (Dial to client);

- Intranet VPN (site to site model);
- Extranet VPN (Business to Business model).

d) After expanding territories of:

- Local VPN;
- National VPN;
- International VPN.

e) After topology:

- Hub and Spoke VPN;
- Any to any VPN;
- Hybrid VPN.

f) After the type of date:

- VPN "pure" (connectivity);
- VPN and contents services (content) (Internet, voice, voice VPN, video) ;
- Content provider is the provider of VPN;
- Content provider other than VPN provider.

Figure 3. VPN IP/MPLS Network

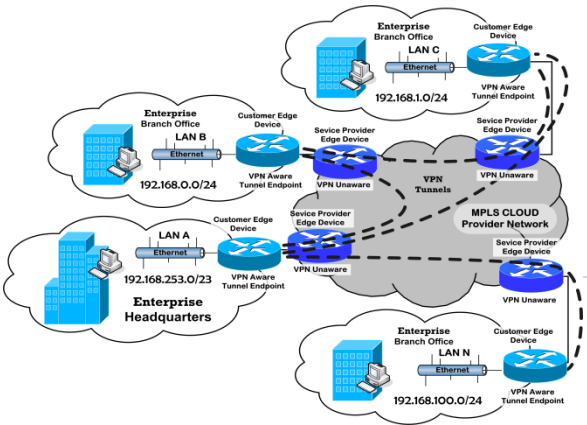
VPN provisioned using technologies such as Frame Relay and Asynchronous Transfer Mode (ATM) virtual circuits (VC) have been available for a long time, but over the past few years IP and IP/Multi-Protocol Label Switching (MPLS) – based VPNs have become more and more popular (see figure 3). The central idea of MPLS is to attach a short fixed-length label to packets at the ingress router of the MPLS domain.

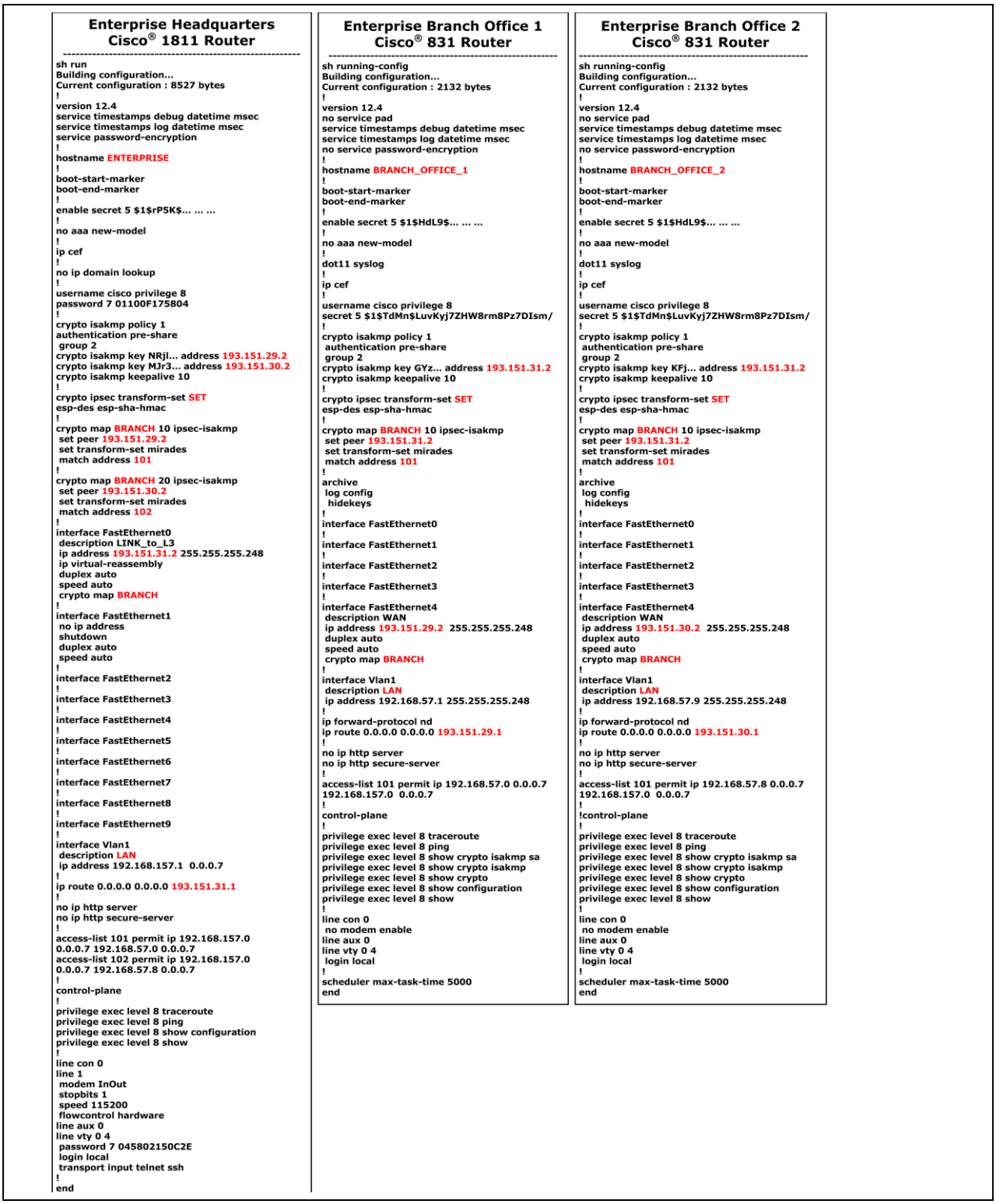
Packet forwarding then depends on the tagged label, not on longest address match, as in traditional IP forwarding [24]. VPN may be service provider or customer provisioned and falls into one of two broad categories: site-to-site VPN which connect the geographically dispersed sites of organizations and remote access VPN which connect mobile or home-based users to an industrial holding [25]. There are three primary models for VPN architectures that can be implemented at the enterprise level [15]:

- *Host-to-host* – used to protect communication between two computers. The model is most used when a small number of users must be online or is given a remote that requires protocols that are normally uncertain.
- *Host-to-gateway* – protects communications between one or more individual hosts belonging to a specific network of an organization. Host-to-gateway is used to allow hosts of unsecured networks, access to internal organization services such as email and web servers.
- *Gateway-to-gateway* – this model protects communications between two specific networks, such as organization's headquarters networks and organization's branch offices or two business partners' networks.

IPSec is a framework of open standards for ensuring private communications over public networks. It has become the most common network layer security control, typically used to create a virtual private network (VPN). IPSec Tunnel mode is used to secure gateway-to-gateway traffic. IPSec Tunnel mode is used when the final destination of the data packet is different from the security termination point. IPsec Tunnel mode protects the entire contents of the tunneled packets. The IPSec Tunnel mode data packets sent from the source device are accepted by the security gateway (a router or a server) and forwarded to the other end of the tunnel, where the original packets are extracted and then forwarded to their final destination device [26]. IPSec tunnel is usually built to connect two or more remote LANs via Internet so that hosts in different remote LANs are able to communicate with each other as if they are all in the same LAN. Common commands to create an IPSec tunnel (for Cisco®equipments) are presented in figure 4 (connects Enterprise headquarter LAN through an IPSec tunnel to 2 Enterprise Branch Office LANs). A VPN solution based on IPsec (see figure 5)typically requires integration of several services (design, network management services, dial-up or dedicated access).

A VPN solution typically requires integration of several services (design, network management services, dial-up or dedicated access). The trend is now evolving to intranets and extranets defined logic, which will lead to the reintegration of the various networks in a single logical subdivision. Structures that allow the approximation of this goal are virtual private networks.Possible solutions in the PREMINV platform to implement a VPN structure for a VE system realization in a geographically dispersed enterprise (see figure 5) can be [15] [26]: local VPN based on VLAN (Virtual Local Area Network), local VPN based on IPSec (Internet Protocol Security), VPN wide area based on IPSec, VPN wide area based on MPLS (Multi-Protocol Label Switching), VPN based on PPPoL2TP (Point-to-Point Protocol over Layer 2 Tunneling Protocol), etc.





Enterprise Headquarters
Cisco® 1811 Router

```
sh run
Building configuration...
Current configuration : 8527 bytes
!
version 12.4
service timestamps debug datetime msec
service timestamps log datetime msec
service password-encryption
!
hostname ENTERPRISE
!
boot-start-marker
boot-end-marker
!
enable secret 5 $1$rP5K$... ... ...
!
no aaa new-model
!
ip cef
!
no ip domain lookup
!
username cisco privilege 8
password 7 01100F175804
!
crypto isakmp policy 1
authentication pre-share
 group 2
crypto isakmp key NRjl... address 193.151.29.2
crypto isakmp key MJr3... address 193.151.30.2
crypto isakmp keepalive 10
!
crypto ipsec transform-set SET
esp-des esp-sha-hmac
!
crypto map BRANCH 10 ipsec-isakmp
 set peer 193.151.29.2
 set transform-set mirades
 match address 101
!
crypto map BRANCH 20 ipsec-isakmp
 set peer 193.151.30.2
 set transform-set mirades
 match address 102
!
interface FastEthernet0
 description LINK_to_L3
 ip address 193.151.31.2 255.255.255.248
 ip virtual-reassembly
 duplex auto
 speed auto
 crypto map BRANCH
!
interface FastEthernet1
 no ip address
 shutdown
 duplex auto
 speed auto
!
interface FastEthernet2
!
interface FastEthernet3
!
interface FastEthernet4
!
interface FastEthernet5
!
interface FastEthernet6
!
interface FastEthernet7
!
interface FastEthernet8
!
interface FastEthernet9
!
interface Vlan1
 description LAN
 ip address 192.168.157.1  0.0.0.7
!
ip route 0.0.0.0 0.0.0.0 193.151.31.1
!
no ip http server
no ip http secure-server
!
access-list 101 permit ip 192.168.157.0
0.0.0.7 192.168.57.0 0.0.0.7
access-list 102 permit ip 192.168.157.0
0.0.0.7 192.168.57.8 0.0.0.7
!
control-plane
!
privilege exec level 8 traceroute
privilege exec level 8 ping
privilege exec level 8 show configuration
privilege exec level 8 show
!
line con 0
line 1
 modem InOut
 stopbits 1
 speed 115200
 flowcontrol hardware
line aux 0
line vty 0 4
 password 7 045802150C2E
 login local
 transport input telnet ssh
!
end
```

Enterprise Branch Office 1
Cisco® 831 Router

```
sh running-config
Building configuration...
Current configuration : 2132 bytes
!
version 12.4
no service pad
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname BRANCH_OFFICE_1
!
boot-start-marker
boot-end-marker
!
enable secret 5 $1$HdL9$... ... ...
!
no aaa new-model
!
dot11 syslog
!
ip cef
!
username cisco privilege 8
secret 5 $1$TdMn$LuvKyj7ZHW8rm8Pz7DIsm/
!
crypto isakmp policy 1
 authentication pre-share
 group 2
crypto isakmp key GYz... address 193.151.31.2
crypto isakmp keepalive 10
!
crypto ipsec transform-set SET
esp-des esp-sha-hmac
!
crypto map BRANCH 10 ipsec-isakmp
 set peer 193.151.31.2
 set transform-set mirades
 match address 101
!
archive
 log config
  hidekeys
!
interface FastEthernet0
!
interface FastEthernet1
!
interface FastEthernet2
!
interface FastEthernet3
!
interface FastEthernet4
 description WAN
 ip address 193.151.29.2  255.255.255.248
 duplex auto
 speed auto
 crypto map BRANCH
!
interface Vlan1
 description LAN
 ip address 192.168.57.1 255.255.255.248
!
ip forward-protocol nd
ip route 0.0.0.0 0.0.0.0 193.151.29.1
!
no ip http server
no ip http secure-server
!
access-list 101 permit ip 192.168.57.0 0.0.0.7
192.168.157.0  0.0.0.7
!
control-plane
!
privilege exec level 8 traceroute
privilege exec level 8 ping
privilege exec level 8 show crypto isakmp sa
privilege exec level 8 show crypto isakmp
privilege exec level 8 show crypto
privilege exec level 8 show configuration
privilege exec level 8 show
!
line con 0
 no modem enable
line aux 0
line vty 0 4
 login local
!
scheduler max-task-time 5000
end
```

Enterprise Branch Office 2
Cisco® 831 Router

```
sh running-config
Building configuration...
Current configuration : 2132 bytes
!
version 12.4
no service pad
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname BRANCH_OFFICE_2
!
boot-start-marker
boot-end-marker
!
enable secret 5 $1$HdL9$... ... ...
!
no aaa new-model
!
dot11 syslog
!
ip cef
!
username cisco privilege 8
secret 5 $1$TdMn$LuvKyj7ZHW8rm8Pz7DIsm/
!
crypto isakmp policy 1
 authentication pre-share
 group 2
crypto isakmp key KFj... address 193.151.31.2
crypto isakmp keepalive 10
!
crypto ipsec transform-set SET
esp-des esp-sha-hmac
!
crypto map BRANCH 10 ipsec-isakmp
 set peer 193.151.31.2
 set transform-set mirades
 match address 101
!
archive
 log config
  hidekeys
!
interface FastEthernet0
!
interface FastEthernet1
!
interface FastEthernet2
!
interface FastEthernet3
!
interface FastEthernet4
 description WAN
 ip address 193.151.30.2  255.255.255.248
 duplex auto
 speed auto
 crypto map BRANCH
!
interface Vlan1
 description LAN
 ip address 192.168.57.9 255.255.255.248
!
ip forward-protocol nd
ip route 0.0.0.0 0.0.0.0 193.151.30.1
!
no ip http server
no ip http secure-server
!
access-list 101 permit ip 192.168.57.8 0.0.0.7
192.168.157.0  0.0.0.7
!
!control-plane
!
privilege exec level 8 traceroute
privilege exec level 8 ping
privilege exec level 8 show crypto isakmp sa
privilege exec level 8 show crypto isakmp
privilege exec level 8 show crypto
privilege exec level 8 show configuration
privilege exec level 8 show
!
line con 0
 no modem enable
line aux 0
line vty 0 4
 login local
!
scheduler max-task-time 5000
end
```

Figure 4. VPN IPSec tunnel configuration between the enterprise headquarters and branch offices using Cisco® equipments

Newer, VPN can be used in different ways to support business processes. This is the ideal solution if it is not efficient in terms of construction costs a particular network for a firm with a workforce highly mobile, or for small firms that can not justify the cost of their telecommunications network.

Also, VPN can be purchased from a telecommunications company and as an alternative they can use existing network infrastructure as the Internet or public switched telephone network and software through the tunnel crossing.

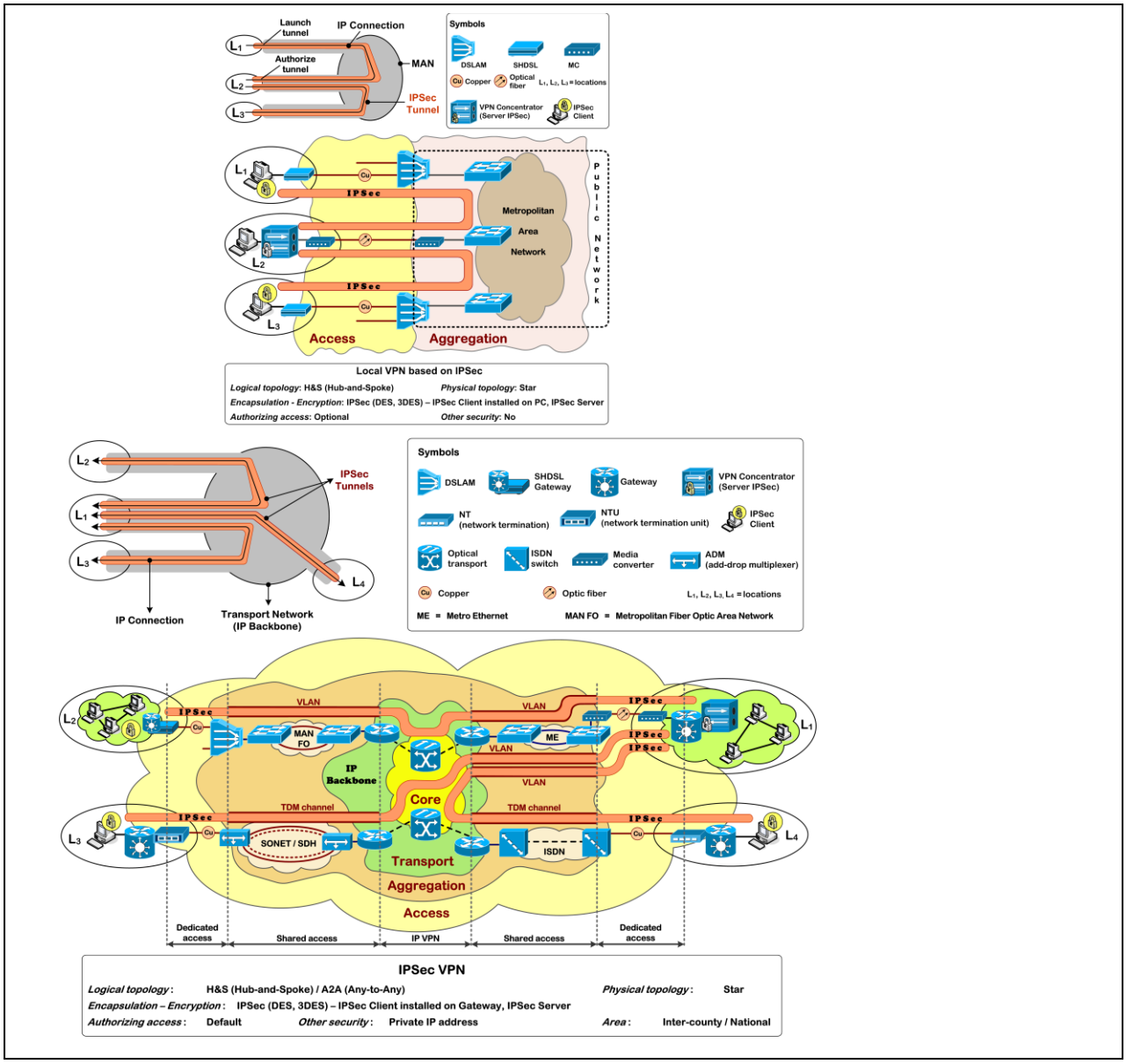


Figure 5. The local VPN & wide area VPN (e.g. national VPN) based on IPSec [15] [26]

IV. THE ENTERPRISE NETWORK MANAGEMENT

Enterprise networks are often large, run a wide variety of applications and protocols, and typically operate under strict reliability and security constraints; thus, they represent a challenging environment for network management [27]. Exactly network topology information is required to perform management activities (e.g. fault detection, root cause analysis, performance monitoring, load balancing, etc.) in enterprise networks. The importance of effective network management, not just in terms of controlling cost but in achieving the strategic aims of business, is also highlighted by some of the benefits respondents attributed to it, including improved inventory planning across the entire network, avoidance of *fire-fighting* situations by improved production and dispatch planning, reduced lead times and improved responsiveness and transparency at the enterprise level [28].

Network management represents the activities, methods, procedures, and tools (software and hardware) that pertain to the *operation*, *administration*, *maintenance*, and *provisioning* of networked systems. Method of solving this problem is to use a host and service monitor designed to inform as of network problems before your clients, end-users or managers do [15].

We implementedNagios® to an enterprise part of an industrial groupconstituted as a dynamic alliance of many different small and medium sized enterprises (see figure 6 and 7) which has its headquarters in Bucharest and branch offices (agencies) in the country – in big cities but also in medium and small cities. All industrial holding locations have a local area network and communicate among themselves through a virtual private network. In each location were made two or three loops – one copper, one optical fiber and/or radio. The solution proposed and implemented by us was to use.

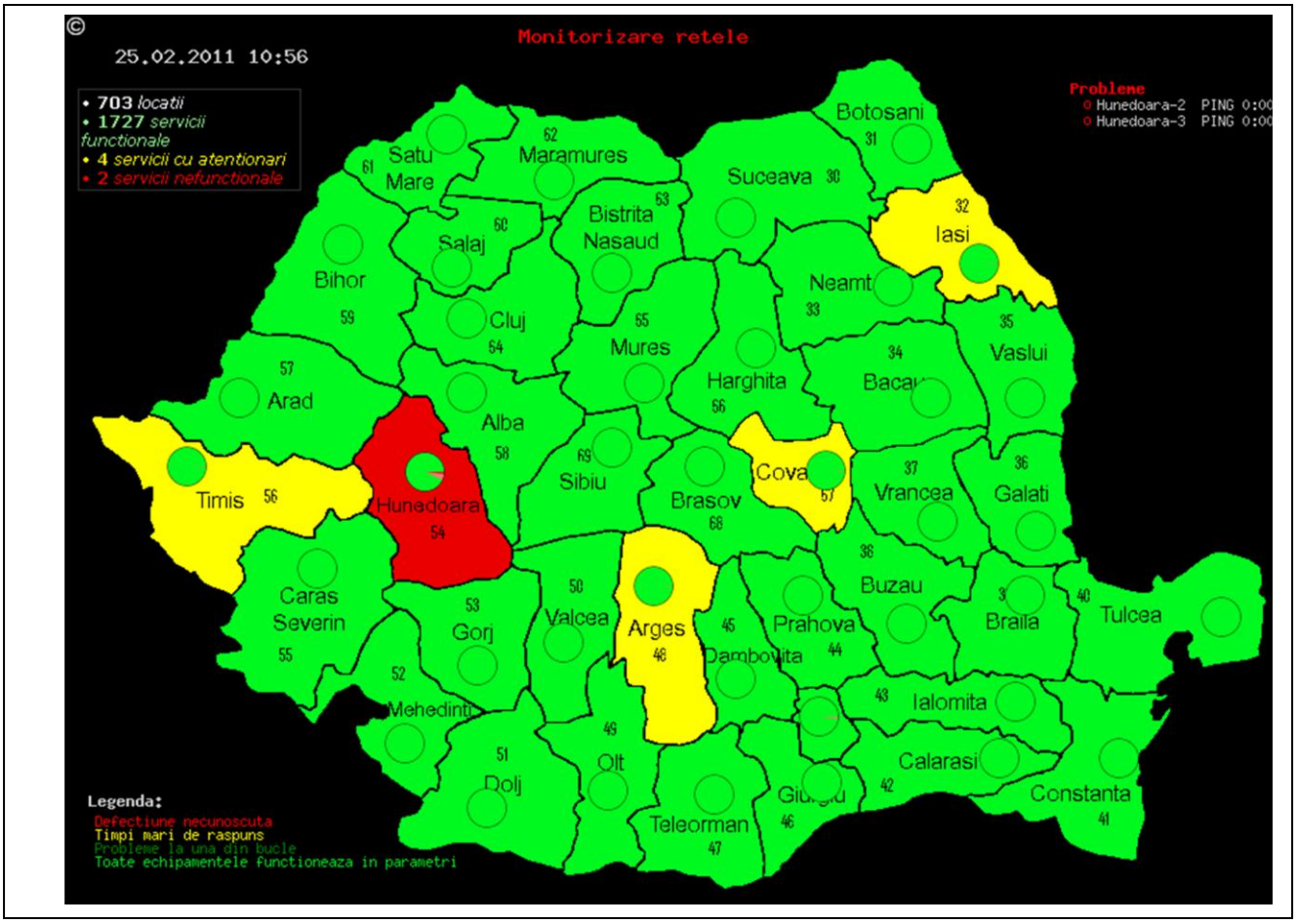


Figure 6. Status for an enterprise network – the local enterprise agency of Hunedoara County is down and the local agencies of Arges, Covasna, Iasi and Timis Counties have long response times

Nagiosas a host and service monitor designed to inform as of network problems before your clients, end-users or managers do.It is based on queries that can be done at scheduled intervals with small programs called plug-ins. Those programs make queries on public services and returns results as follows: *0 – OK*, *1 – Warning* and *2 – Critical*. Nagios® architecture consist of a nucleus that collects data generated by plug-ins and notices on them, a number of plug-ins and an optional web interface where are viewed the state services and hosts monitored, history, notices sent, etc.In terms of performance, Nagios® scales very well and depending on the hardware configuration can verify tens of thousands of services. It can also be installed in cluster configuration.This software is licensed under the terms of the *GNU General Public License* Version 2 as published by the *Free Software Foundation* (GNU General Public License is a free, copy left license for software and other kinds of works). This gives legal permission to copy, distribute and/or modify Nagios® under certain conditions. Some of the many Nagios® features include [29]:

- Monitoring of network services (SMTP, POP3, HTTP, NNTP, ICMP) and monitoring of host resources (processor load, disk and memory usage, running processes, log files, etc.) and monitoring of environmental factors such as temperature;
- Simple plug-in design that allows users to easily develop their own host and service checks and ability to define network host hierarchy, allowing detection of and distinction between hosts that are down and those that is unreachable;
- Contact notifications when service or host problems occur and get resolved (via email or other user-defined method);
- A Web interface – viewing current network status, notification and problem history, etc.

To implement this application we have used over five hundred locations. In figure 6 and 7 are presented the locations monitored for this large enterprise – we eliminate the beneficiary name for advertising reason. We've installed Nagios® in the PREMINV e-platform on a server with the following technical characteristics: 2 Dual Core Intel Xeon (TM) 3.6 GHz processors (64-bit), 2 GB RAM, 2 x 80 GB Hard Drives and Debian Linux 4.0 Operating System.We realized in the PREMINV e-platform more scripts as support for different operations.

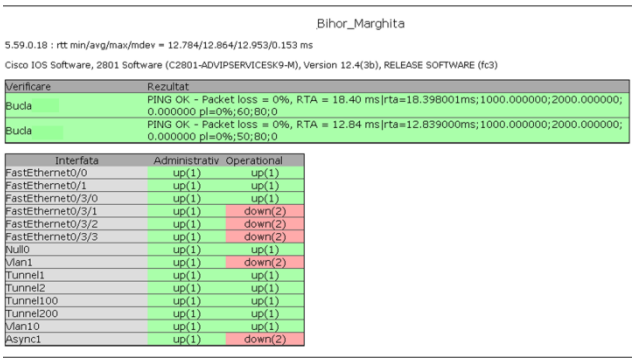


Figure 7. Status for an enterprise agency – the local enterprise agency of Bihor County providers loop status

In figure 8 we present a script that save configurations for some Cisco®equipments. With this script one can connect the device (having entered at the command line user login and password) and copy line by line equipment configuration.

```
get_conf.php :
<?php
function get_conf($iip,$uname,$upass,$epass,$gr)
{
  $ip=$iip;

$date=date('Ymd_His');
$fnume=$ip.'_'.$date;
$fstart=fopen($gr.'/start_'.$fname.'.cfg','w');
$frun=fopen($gr.'/run_'.$fname.'.cfg','w');
  $link=fsockopen($ip,23,$errn,$errm);
  if(!$link){
//      echo "Connection error"; exit;
     return 0;
  }
  else{
//      echo "IP : ".$ip;
     fputs($link,"$uname\n");
     fputs($link,"$upass\n");
  if(strlen($epass)){
        fputs($link,"en\n");
        fputs($link,"$epass\n");
     }
     fputs($link,"\n\n\n");
     $gata=0;
  while($gata<1)   {
     $ras=fgets($link,128);
//  echo $ras."\n";
  if(strpos('  '.$ras,'invalid')>1){echo '\nUser/password wrong !\n';return 1;}
  if(strpos('  '.$ras,'Bad')>1){echo '\npassword enable wrong !\n';return 1;}
  if(strpos('  '.$ras,'#')>1){$gata=2;}
     }
     fputs($link,"sh run\n");
     fputs($link," ");
     $gata=0;$isrun=0;
  while($gata<10000)   {
     $ras=trim(fgets($link,128));
  if(strncmp($ras,'A',1)<0){$ras=trim(substr($ras,8));
  while((strlen($ras)>0) && (strncmp($ras,'A',1)<0)){$ras=substr($ras,1);}
      }
//  echo $ras."\n";
  if($isrun){fputs($frun,trim($ras)."\n");}
     fputs($link," ");
  if(!strncmp($ras,'end',3) )  {$gata=100000;}
  if(strpos($ras,'bytes')>0){$isrun=1;}
     $gata++;
     }
     fputs($link,"\n\nsh start\n");
     fputs($link," ");
     $gata=0;$isstart=0;
  while($gata<10000)   {
        $ras=trim(fgets($link,128));
  if(strncmp($ras,'A',1)<0){$ras=trim(substr($ras,8));
  while((strlen($ras)>0) && (strncmp($ras,'A',1)<0)){$ras=substr($ras,1);}
     }
//  echo trim($ras)."\n";
  if($isstart){fputs($fstart,trim($ras)."\n");}
     fputs($link," ");
  if(!strncmp($ras,'end',3) )  {$gata=100000;}
  if(strpos($ras,'bytes')>0){$isstart=1;}
     $gata++;
     }
     fputs($link,"\n\nexit\n");
     fputs($link,"\n\nexit\n");
     fputs($link,"\n\nexit\n");
     echo "$date OK!\n";
  fclose($fstart);fclose($frun);
  return $date;
     }
}
```

Figure 8. The Nagios® script example

V. CONCLUSIONS

In the actual context of the virtual enterprise network expanding, companies are much more preoccupied to build such structures and/or to be part of different structures that already exist. These will give them more business opportunities and by the knowledge transfer processes, they will gain competitiveness. Therefore, enterprises continue to implement information and communication technology systems solutions and strategies to improve their business processes in virtual networks.

Considering future product development as collaboration and communication oriented we implemented in the PREMINV e-platform a solution based on a virtual enterprise network (VPN IPSec solution) concept using integrated data sets and tools. As a general requirement for this virtual network based application the companies must be able to inter-operate and exchange data, information and knowledge in real time so that they can work as a single integrated unit, although keeping their autonomy. Also, virtual networked business teams need a strategic framework in which to operate. Today's virtual business teams don't appear to be able to fully leverage the much-touted opportunities offered by always-on interconnectedness, easy access to unlimited information sources and real-time communication tools. They also need good planning and in-depth project analysis, effective and accessible technologies, constant coaching, systematic fine-tuning, feedback processes and the full understanding that their success cannot be determined by a pre-designated set of communication technologies [26].

A solution for a large enterprise geographically dispersed network monitoring using open source software (Nagios®) has been presented in this paper. For an enterprise, network monitoring is a critical and very important function, which can save significant resources, increase network performance, employee productivity and maintenance cost of infrastructure. Nagios® compares the features and performance with expensive commercial monitoring applications as HP Operations Manager or Microsoft System Operations Manager. This software (Nagios®) can be developed and implemented at a corporate level but also in a company that provides telecommunication services.

This work was realized at the UPB-PREMINV Research Centre. The validation of this solution by a case study in the ORGVIRT &PROGPROC& ID 1022 research projects is to determine the new organization type for integrating the virtual enterprise medium and to outsource shared resources from UPB-PREMINV research centre to industrial partners.

REFERENCES

[1] R. Ekwall and A. Schiper, "Replication: Understanding the Advantage of Atomic Broadcast over Quorum Systems", Journal of Universal Computer Science, vol. 11(2), pp. 703–711, 2005.

[2] J. Niemann, S. Tickiewitch and E. WestKamper, Design and Sustainable Product Life Cycles, Spinger-Verlag Berlin Heidelberg, Germany, 2009.

[3] J. B. Ayers, Handbook of supply chain management (2nd Ed.), Taylor & Francis Group, New York, USA, 2006.

[4] R. Ferdiana and O. Hoseanto, "Instruction Design Model for Self-Placed ICT System E-Learning in an Organization", International Journal of Advanced Computer Science and Applications, vol. 3(8), pp. 1-7, 2012.

[5] T. Huang, G. Q. Wu and J. Wei, "Runtime monitoring composite Web services through state full aspect extension", Journal of Computer Science and Technology, vol. 24(2), pp. 294-308, 2009.

[6] A. D. Potorac, "Considerations on VoIP Throughput in 802.11 Networks", Advances in Electrical and Computer Engineering, vol. 9(3), pp. 45-50, 2009.

[7] C. H. Hauser, D. E. Bakken, I. Dionysiou, H. K. Gjermundrod,V. S. Irava, J. Helkey and A. Bose, "Security, trust and QoS in next-generation control and communication for large power system", Int. J. Critical Infrastructures, vol. 4(½), pp. 3-16, 2008.

[8] Z. Hulicki, "Drivers and Barriers for Development of Broadband Access – CE Perspective", Journal of Universal Computer Science, vol. 14(5), pp. 717-730, 2008.

[9] P. Sasvari, "The macroeconomic effect of the information and communication technology in Hungary", International Journal of Advanced Computer Science and Applications, vol. 2(12), pp. 75-81, 2011.

[10] G. Dragoi, A. Draghici, S. M. Rosu, A. Radovici and C. E. Cotet, "Professional Risk Assessment Using Virtual Enterprise Network Support for Knowledge Bases Development", Communications in Computer and Information Science", vol. 110, part II, J.E. Quintela Varajao et al. (Eds.), Springer-Verlag Berlin Heidelberg, Germany, pp. 168-177, 2010.

[11] L. J. Osterweil, "Formalism to support the definition of processes", Journal of Computer Science and Technology, vol. 24(2), pp. 198-211, 2009.

[12] G. Dragoi, A. Draghici, S.M. Rosu and C. E. Cotet, "Virtual Product Development in University-Enterprise Partnership", Information Resources Management Journal, vol. 23(3), pp. 43-59, 2010.

[13] A. Shakya, H. Takeda and V. Wuwongse, "StYLiD: Social information sharing with free creation of structured linked data", in SWKM'2008: Workshop on Social Web and Knowledge Management @ WWW 2008, April, Beijing, China, 2008.

[14] M. Cudanov, O. Jasko and M. Jevtic, "Influence of Information and Communication Technologies on Decentralization of Organizational Structure", Computer Science and Information System, vol. 6(1), pp. 93-109, 2009.

[15] S. M. Rosu and G. Dragoi, "VPN Solutions and Network Monitoring to Support Virtual Teams Work in Virtual Enterprises", Computer Science and Information System, vol. 8(1), pp. 1-26, 2011.

[16] Cisco System, Enterprise QoS Solution Reference Network Design Guide, Version 3.3, Cisco Systems Inc., San Jose, CA, USA, 2008.

[17] R. Skoog, A. Von Lehmen, G. Clapp, J. W. Gannett, H. Kobrinski and V. Poudyal, "Metro network design methodologies that build a next-generation network infrastructure based on this generation's services and demands", Journal of Lightwave Technology, vol. 22(11), pp. 2680-2692, 2004.

[18] H. Youssef, S. M. Sait and S. A. Khan, "Topology design of switched enterprise networks using a fuzzy simulated evolution algorithm, Engineering Applications of Artificial Intelligence", vol. 15, pp. 327-340, 2002.

[19] S. M. Rosu and G. Dragoi, "Virtual Enterprise Network General Architecture", in Proceedings of the 8th International Conference on Communications, pp. 313-316, Bucharest, Romania, ©IEEE, 2010.

[20] A. G. Mason, Cisco Secure Virtual Private Networks, Published by Pearson Education, Cisco Press, 2001.

[21] A. Moreno and K. Reddy,Network virtualization, Published by Pearson Education, Cisco Press, 2006.

[22] S. M. Rosu, G. Dragoi, L. Rosu and M. Guran, "Virtual Enterprise Network Solutions to Support E-learning Sites Development", in DAAAM International Scientific Book 2010, chapter 63, B. Katalinic (Ed.), DAAAM International Press, Vienna, Austria, pp. 725-742, 2010.

[23] J. Ward and J. Peppard, Strategic planning for information systems, John Wiley & Sons Press, West Sussex, UK, 2002.

[24] A Jamali, N. Naja and D. El Ouadghiri, "An Enhanced MPLS-TE for Transferring Multimedia packets", International Journal of Advanced Computer Science and Applications, vol. 3(8), pp. 8-13, 2012.

[25] R. Deal, The Complete Cisco VPN Configuration Guide, Published by Pearson Education, Cisco Press, 2005.

[26] S. M. Rosu and G. Dragoi, "Virtual Enterprise Network Solutions and Monitoring as Support for Geographically Dispersed Business", in Handbook of Research on Business Social Networking: Organizational, Managerial and Technological Dimensions, IGI Global, Hershey, PA, USA, pp. 34-62, 2012.

[27] M. Casado, M. J. Freeman, J. Pettit, J. Luo, N. Gude, N. McKeown and S. Shenker, "Rethinking enterprise network control", Transactions on Networking, vol.17, no. 4, pp. 1270-1283, 2009.

[28] N. Jones and Q. Wang, "A mixed integer programming approach for logistic network design and optimization information and value adding networks", in DET2009 Proceedings, AISC66, Huang G et al. (Eds.), Springer-Verlag Berlin Heidelberg, pp. 1227-1241, 2010.

[29] E. Galstad, Nagios® Version 2.x Documentation, Published by www.nagios.org, 1999-2006.

AUTHORS PROFILE

Dr. Sebastian Marius Rosureceived the B.E. in Aerospace Construction and in Informatics from University "Polytechnica" of Bucharest, in 2000 and University „Dunărea de Jos" of Galaţi in 2002, respectively. In 2009 obtained doctoral degree in Automatics from University "Polytechnica" of Bucharest. He is telecommunications engineer at the Romanian Special Telecommunications Service. He has been active in the fields of the quality control, risk management, industrial informatics, knowledge management, computers, computer integrated enterprise, computer networks, networks design and collaborative design systems. Since 2004, he has been associated with the PREMINV Research Laboratory at the Polytechnic University of Bucharest first as PhD Student and from 2009 as PhD.

Marius Marian Popescureceived the B.E. in Electronics from Military Technical Academy of Bucharest. Currently he is PhD candidate at University of Piteşti, Faculty of Electronics, Communications and Computers. Since as 2001 he is IT engineer at the Romanian Special Telecommunication Service. His interest areas are pattern recognition, network security, network operations center development, network project management and network equipment (VPN, IPSec).

Dr. George Dragoi received the B.S. in Electronics & Telecommunications and doctoral degrees in Industrial Informatics from University "Polytechnica" of Bucharest, in 1982 and 1994, respectively. From 1982-1986, he was an Associate Researcher of the Romanian National Research Center in Telecommunication of Bucharest. From 1986 to 1990 he was a Research Assistant, from 1990 to 1993 lecturer, from 1993 to 1998 associate professor and from 2006 to present professor at the "Politehnica" University of Bucharest,Faculty of Engineering in Foreign Languages. He has been active in the fields of the industrial robots control, industrial informatics, computer integrated enterprise, computer networks and telecommunications, virtual enterprise and collaborative design systems. Since 1998, he has been associated with the Institute National Polytechnic at Grenoble, France, as Associate and Visiting Professor. He received the Romanian Academy Award "AurelVlaicu" in 1993 and it has served as a member of the National Council for Technological Education and Innovation after 1999.

IoanaRalucaGuica is is PhD candidate at University "Polytechnica" of Bucharest. Currently she is assistant professor at the "Politehnica" University of Bucharest, Faculty of Engineering in Foreign Languages.