Secured Voice over VPN Tunnel and QoS

Feature Paper

Powering communications with Security

Table of Contents

Secured Voice over VPN tunnel and QoS

To integrate the data, voice and video into a single device, to provide security mechanism of certain levels, and to realize bandwidth management, are what every system provider endeavors to accomplish.

Preface

Today, the mid- and high-level household or business routers are featured with built-in VPN (Virtual Private Network), which can protect important data from being illegally captured and decoded while transferring via VPN. Also, due to the varied Internet resources and the availability of data, household and office users have been introduced “Quality of Service (QoS),” a bandwidth management solution, to their work environment to ensure that their data are transferred in real time and the bandwidth are not illegally used or viciously abused. Since 2004, QoS has been deemed as one of the basic features, even for the ADSL routers, which are gateways responsible for outside connections. Abundant resources on the Internet often fascinate general Internet users. As they always download or share data with others on the Internet, how to play on-line games and send emails with ease has become an essential, and QoS is undoubtedly the best solution. Making calls over the Internet has been the dream of many people in early days. And since the Internet became popular, many people tried to take advantage of the Internet to transfer Voice over Internet Protocol, VoIP, for free calls without any distance limitation. Thanks to the maturity of Internet technology, such as SIP (Session Initiation Protocol) of VoIP and the expansion of bandwidth, the ADSL2/2+ now allows users to upgrade the download rate of 8 Mbps and the upload rate of 1 Mbps to 24 Mbps and 1 Mbps, respectively. All of the functions seem to be independent, however, through integrating them continuously, one single router can now perform all of the functions that originally were performed by many devices.

Chapter 1 The Introduction of Virtual Private Network (VPN)

1.1 The Functions and Types of VPN

VPN is a virtual tunnel built between two communication points on the Internet. All of the data transferred via the tunnel are secured. The greatest advantage

of VPN is that if there is important data transferred via the Internet and has been illegally captured, the hacker will not be able to read the data if they don't have the original encryption protocol. This feature is essential for the business users especially when they exchange information/data among their branches. Most of the mid- and high-level routers support VPN feature. Besides, because of the fierce competition in the communication market, some routers that are designed for household use also support the VPN feature and no longer just support VPN pass through feature.

There are three common types of VPN, as follows:

- PPTP
- IPSec
- L2TP within IPSec

PPTP is the earliest type of VPN solutions, which protects data by building a virtual tunnel between two points. Data transferred through the tunnel are plain-coded.

IPSec transfers data through general routers, however, the data are complex encrypted and it generates a new packet to be transferred. Because the encryption and decode processes are extremely complicated, it needs processors with higher performance in order to increase the bandwidth to process the data.

L2TP within IPSec: L2TP integrates the functions provided by the PPTP from Microsoft and L2F provided by the Cisco System. It also builds a virtual tunnel for data transfer. However, in order to ensure the privacy of the transferred data, it encrypts the data in the tunnel again with advanced data protection.

1.2 The Integration of VPN and VoIP

VoIP is one of the hottest issues today. It also represents the great improvement of voice transfer in recent years. In early days, most of the VoIP systems were H.323, and were too huge and complicated. Thus, recently two new standards, MGCP and SIP, have been introduced to replace the existing H. 323. SIP protocol is more popular and prevalent now and is the main investment target for many companies.

However, as VoIP has been flourishing, the security problem haunted the

Internet for a long time has also become the nightmare for VoIP. VoIP transforms the voice into data and transfers it in IP packet format. It means that during data transfer, data might be sabotaged, attacked or stolen. However, on the existing architecture, as long as the routers support VPN, the users can easily set up the system to allow both parties have a call connection that is protected and safe. Next we'll discuss how to set up the system to protect voice data on the existing VPN routers.

SIP not only supports proxy but also P2P (peer to peer). The P2P is a call connection method that users can call the IP address directly without any authentication. It will build a direct point-to-point connection to transfer voice data.

Figure 1: Point-to-Point via VoIP

We can build a VPN connection between the caller and the receiver to encrypt the voice data, secure the call and protect the content. The caller and the receiver's external IP address is the remote subnet or single IP address that are designated by the caller and the receiver when they set up the VPN.

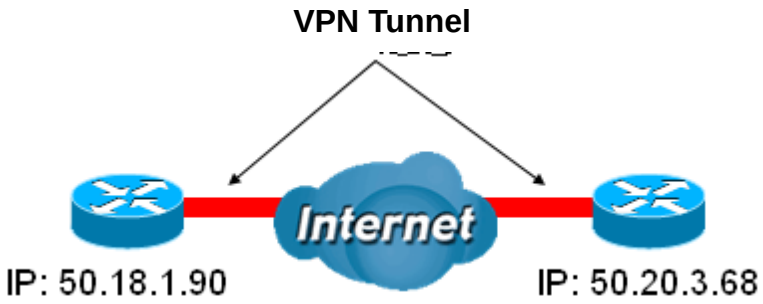


Figure 2: Building a VPN tunnel and Designation IP address

Therefore, when the users want to build the connection, they have to transfer the data to the remote devices, and then the routers will check it and confirm that the data are transferred to the destination IP address via a VPN tunnel. The voice data now can be transferred via the VPN to accomplish the goal of voice encryption for VoIP.

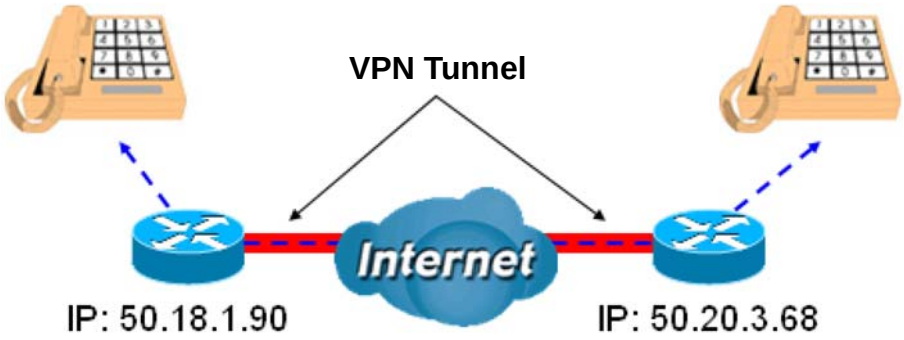


Figure 3: Voice Encryption for VoIP via VPN Tunnel.
Source: Billion Electric Co., Ltd

BiPAC 7402VGO
BILLION VoIP ADSL2+ VPN Firewall Router

It is especially suitable for the business users. Most of the business users' intranet infrastructures use VPN for data communication between headquarters and its branches. How To take advantage of VoIP to save expensive phone charges is also the goal that many business users endeavor to accomplish. After all, phone bills are accounted for a fairly large proportion of operating costs. How to take full advantage of the VoIP to reduce phone expenses and to secure the calls is a very important subject in the future.

Taking Billion Electric's BiPAC 7402VGO Router as an example, it supports 16 IPSec VPN tunnels that allow office users to build a secured data transfer tunnel through the public Internet that embedded with 3DES accelerator to enhance the performance of IPSec VPN significantly. Meanwhile, it supports SIP, which is prevalent among the industry, to allow users to connect to ordinary phones to make a VoIP call through the two built-in FXS ports. When the power failure happens or the Internet is disconnected, the users still can make traditional calls via Public Switched Telephone Network (PSTN).

Chapter 2 The Introduction of Quality of Service (QoS)

2.1 VLAN and Quality of Service (QoS)

In early days, the Internet applications were simpler. Most of the business users had encountered a lot of problems and most of the problems were about how to improve intranet environment, where there were too many broadcast packets and multicast packets, and about how to separate different departments for security reason to avoid unauthorized access to data. Virtual LAN (VLAN) is the early mechanism to separate multi-Ethernet-port into different groups. Although the switch/hub provides an intelligent, auto-learning mechanism, it will send the packets to all of the Ethernet ports as it gathers broadcast packets and multicast packets, and thus resulting in unnecessary bandwidth usage. VLAN is designed to solve these problems. All of the broadcast packets and multicast packets are only sent to their own groups. However, this mechanism can only help to prevent too many broadcast packets being sent.

In Quality of Service (QoS), VLAN can only help to get rid of unnecessary data broadcasting, but it cannot really help the applications required real time transfer, such as VPN, voice data, etc. The data that are transferred via VPN tunnels must be of some importance, and the bandwidth for the data transfer cannot be allocated to other resources and allow no delay, especially voice data. It was not until recent years that VoIP broke its bottleneck and gained users' attention for some of the most important reasons, such as better computing compression, the expansion of bandwidth and so on, in order to enhance the quality of call service and provide more comprehensive phone services in comparison to that of traditional phones.

The major reason that people love digital technology now more than ever is that due to the expansion of bandwidth, the service providers now can provide more diversified services to their customers. Also, QoS is the most important factor when people come to choose their Internet services and is one of the key requirements for the office and general household users. So, the important subject now is how to let everybody access and use the Internet resources conveniently and enjoy the good quality service with limited budget and bandwidth.

2.2 QoS Application- ATM QoS and IP QoS

QoS: In early days, most of the network backbones were built on Asymmetric Transfer Mode (ATM) network. Every ATM network node builds multi-VC (Virtual Circuit) to transfer data. It is like the third layer routing table of the network layers and different VCs are designated to transfer the data to different service hosts. Because the bandwidth between two nodes is fixed, the default bandwidth for all VCs is equally allocated. However, since there is priority for the data transfer, the QoS mentioned in early days was related to how to control the bandwidth to achieve the optimal performance under the fixed bandwidth. The QoS was then referred to the ATM QoS. Recently the IP-based network backbones have been growing fast, and ATM QoS is obviously not suitable for IP network backbone. That is why people nowadays favor IP QoS over ATM QoS. Meanwhile, the SIP that applied to the VoIP is also based on IP level and its voice data transfer allows no delay.

Today, the main IP QoS technologies are IntServ, DiffServ, QoS routing and MPLS. DiffServ is the most common QoS with easy-to-use and high scalability features. The basic application of DiffServ is to divide the user's data processing procedure into different levels based on the service application requirements and all data can pass through the network gateway freely. However, when the data flow reaches a certain level and the network traffic is jammed, the high-level data flow is prior to the low-level data flow with regard to data transfer and resource allocation. DiffServ only provides comparative service quality and guarantees the proportion of bandwidth available for the users based on different levels, but it doesn't guarantees any specific index of service quality for users. In physical applications, in comparison to general household users whose VoIP, game playing and Internet browsing needs should be handled with highest priority, VPN, VoIP and Email sending and receiving needs should be handled with highest priority for office users. The reason to set priority is that there are many P2P files sharing programs that will ask the users to approve the upload in order to share the resources on the Internet. Consequently, the programs like Bit Torrent or eMule will occupy the bandwidth and some companies may not aware that their employees have been used up the bandwidth available. So when the network speed slows down, it doesn't mean that the users need more bandwidth, but need to analyze the utility rate and control it effectively in order to achieve optimal Internet services.

Building network backbone has been implemented for years, while ISPs (Internet Service Provider) keep expanding their network backbone bandwidth. Most of the terminal equipment supports QoS to allocate the management resource, but the real Internet bottleneck for the business users or general household users are existed in the external gateway. Taking the popular ADSL as example, although every ISP claims that they have enough bandwidth support to provide services to their customers, but the maximum bandwidth for each user is only 8 Mbps for download and 1 Mbps for upload. Even ADSL 2/2 + has only the bandwidth of 24Mbps(download) / 1Mbps(upload). That is why QoS is essential for every user. The bandwidth allocation for home users, small and medium-sized office users is illustrated in the following two tables.

Table 1: QoS Example of Data Ratio and Priority setting for Home Users

QoS application	Data Ratio (%)	Priority
On-line game	30%	High
Skype	5%	High
Email	10%	High
FTP Upload/Download	20%	Upload (High), Download (Normal)
Others	35%	

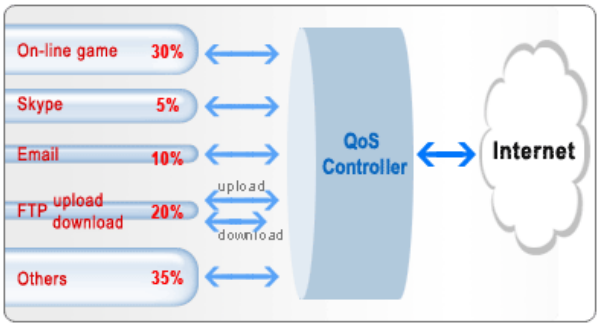
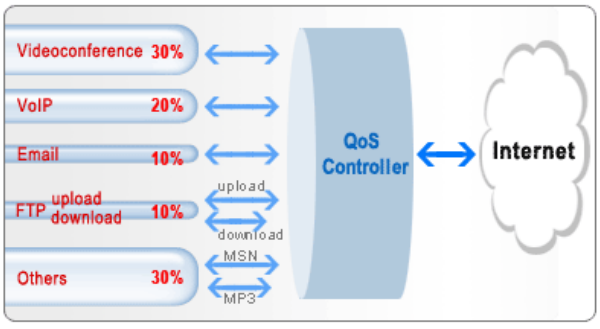


Table 2: QoS Example of Data Ratio and Priority settings for Office Users

QoS application	Data Ratio (%)	Priority
Videoconference	30%	High
VoIP	20%	High
Email	10%	High
FTP upload /download	10%	Upload (High), Download (Normal)
Others	30%	MP3 (Low), MSN (Normal)



Source: Billion Electric Co., Ltd

Taking Billion Electric's BiPAC 7402VGO Router as an example for quality of service (QoS) control, the router's DiffServ structure encompasses easy-to-use and high scalability features to ensure its bandwidth availability and QoS feature. It also allows users to set up priority level for data transfer, such as voice packet, FTP data or videoconference, etc. Moreover, it controls

speed of the network to allow business users to build VPN structure between headquarters and its branches, and thus allows users to make cheap VoIP calls, while enjoying fast and smooth connection. With easy and fast installation, this router integrates all functions into one device, and is perfectly designed for every system integration provider to meet every user's needs.