LANCOM™ Techpaper: Security in Voice over IP environments

1 Voice communication in computer networks

Throughout the course of history, technical innovations have often lead to significant changes in interpersonal communication. New inventions offered entirely new communication forms which often had a great influence on all of society.

In recent years a new type of communication technology has been gaining ground: Interactive networks that allow users to send or receive large amounts of information. The largest and fastest growing interactive network is the Internet. Just a few years ago, use of the Internet was reserved for scientists and technology fanatics. But the number of users has grown drastically in a very short period due to simpler access requirements, more affordable and powerful computers and most of all, due to the growing informational and entertainment character of the Internet.

Meanwhile, the availability of broadband internet connections has increased dramatically and we are on the verge of a breakthrough innovation that will combine old and new communication methods and once again have a decisive influence on society as a whole: Internet telephony.

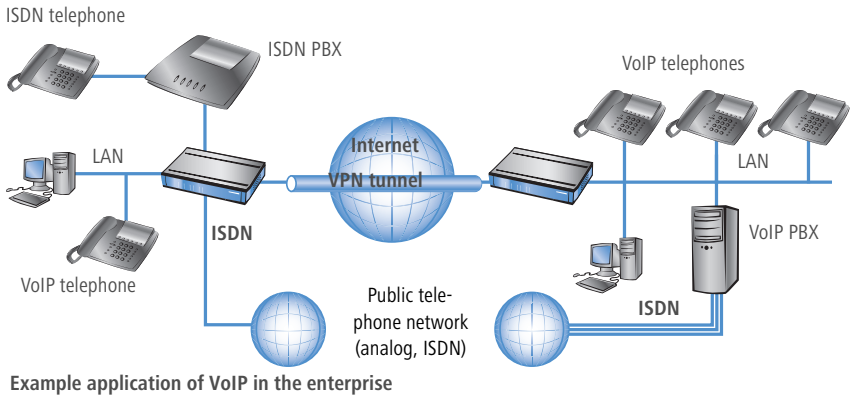
No market has grown as rapidly or caused so much hype as the field of Voice over IP (VoIP). While private users are largely interested in reducing their telephone charges, the cost advantages for enterprises lie primarily in the synergistic effects the technology creates along with the consolidation of existing telecommunications and IT infrastructures into Ethernet.

Despite the excitement over technology that is sure to breathe new life into the struggling IT and telecommunications world, we should be aware that Internet telephony is vulnerable to the same risks that IP users are all too familar with. For this reason, security is of central importance. Unfortunately, the security of VoIP is not at the forefront of most users' minds; rather, they are more occupied with ensuring that calls can be made in the first place.

The importance of security in the area of Voice over IP—particularly in business communications—is demonstrated by the number of studies that have been published regarding this subject, the latest of which was conducted by the German Federal Office for Information Security (BSI).

2 Fields of application

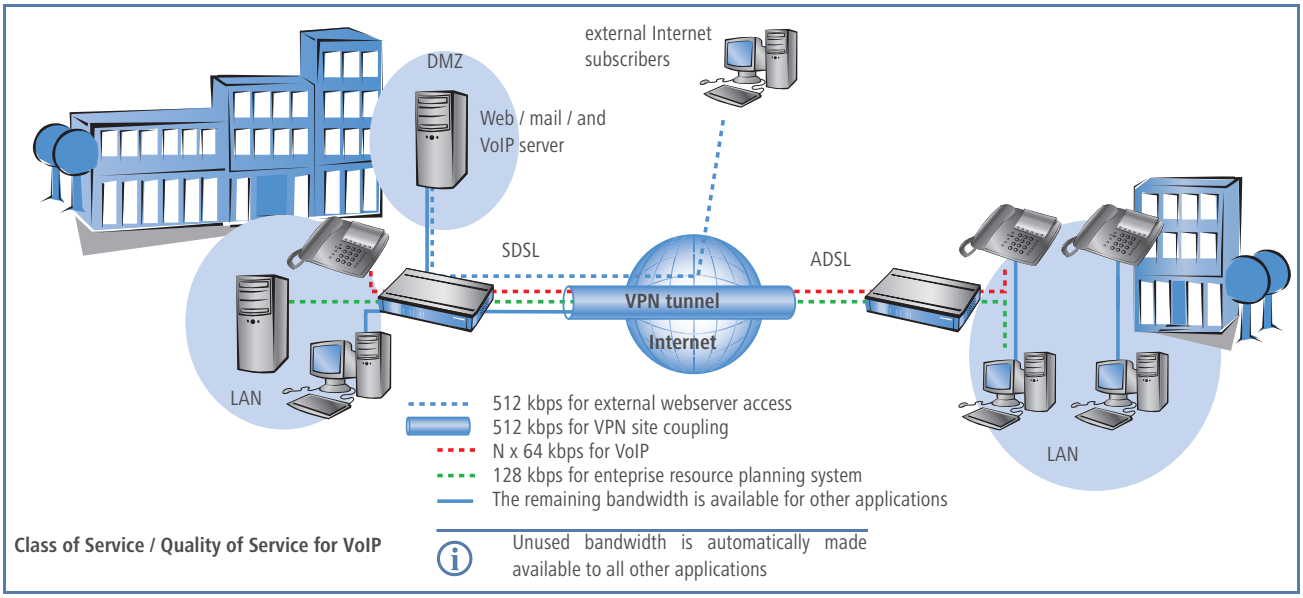
In the following document - as in the BSI study - the primary focus is placed on VoIP telephony which is transported via media that reside within the operator's area of resonsiblity. According to information gathered so far, the main field of application for enterprise VoIP is the simplification of internal paths of communication and connecting remote sites or home offices to the enterprise PBX infrastructure. It is imperative that communication take place via an encrypted VPN connection here. Thus, IP calls can be made between individual locations over the VPN connection while remaining secure against eavesdropping. The data stream should be directed through the firewall at both locations before it is forwarded to the respective VoIP terminal equipment.



Example application of VoIP in the enterprise

LANCOM Systems

LANCOM™ Techpaper: Security in Voice over IP environments



Class of Service / Quality of Service for VoIP

3 Class of Service / Quality of Service

In addition to traditional security measures such as strict firewall rulebases that keep public and private networks separate, protection against layer 2 and layer 3 attacks (e.g. ARP, VLAN, DHCP, MAC attacks, IP spoofing), and defense against denial of service attacks, it is also necessary to have a mechanism which ensures the quality of service of voice transmissions. This can be accomplished using seamless Quality of Service Management and the corresponding rules. The VoIP terminal equipment used (telephones, routers, PBX systems) is generally capable of tagging the Ethernet frame of a voice packet with DiffServ information. This allows the voice packets to be forwarded according to priority providing the routers in use are capable of analyzing the Class of Service field in the Ethernet frame.

The voice and data networks can be separated logically in order to assure Quality of Service as well as management and scalability. In view of the current speeds of wired networks with 100 Mbps or 1 Gbps, these safeguards are not absolutely necessary from the Quality of Service point of view. However, it does increase security in general while minimizing the influence that data transfer has on voice. To meet the highest security standards as prescribed in the area of classified document communication, it is recommended that all terminal equipment (data and voice) should be authenticated with 802.1x and static MAC addresses should be assigned per switch port. However, there are currently no IP telephones that are explicitly approved for classified document communication.

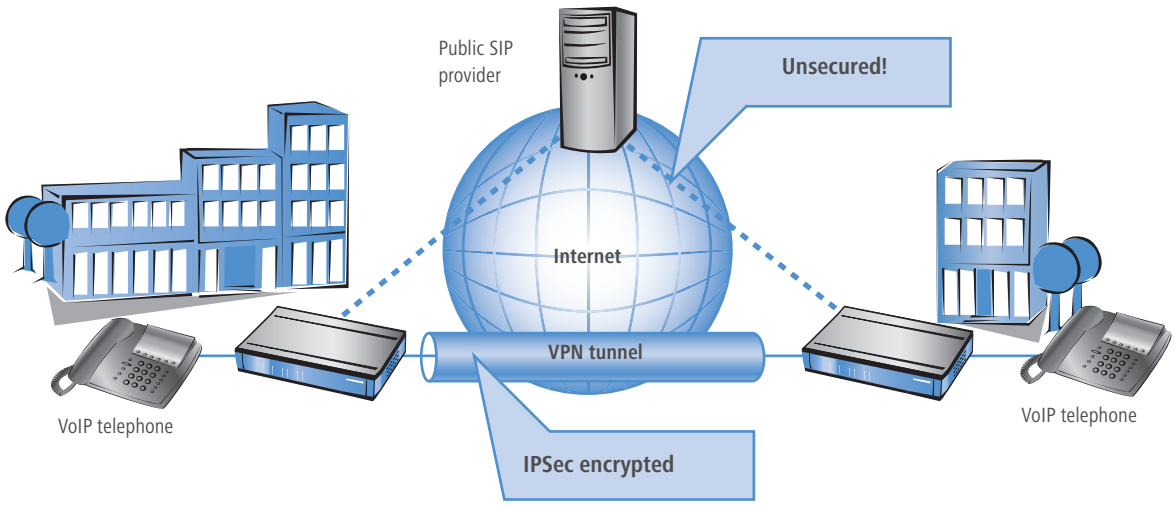
4 Availability

The availability of the VoIP gateway must be ensured at all times. If the existing internet connection fails, the appropriate redundancy protocols (e.g. VRRP) should be used in order to switch to a suitable replacement medium. Since the current availabilty of DSL connections is listed at 97% (this translates into downtime of approximately 11 days), an alternative backup interface (e.g. ISDN or UMTS) must be available in order to ensure data communications. All current LANCOM devices with the "VoIP ready" logo are also cabable of using the ISDN interface for voice transmission as well as data communication. Subdivision takes place at the B channel level, i.e. one channel can continue to be used for data traffic and the second channel is used for voice traffic. In addition to allowing employees to be reached by telephone using their existing telephone number, emergency calls and local calls can be transmitted directly to the public telephone network.

Furthermore, the gateway should include a "lifeline" function which through-connects the internal and external ISDN connection via hardware relay in case of a power outage. The functionality of the ISDN telephones

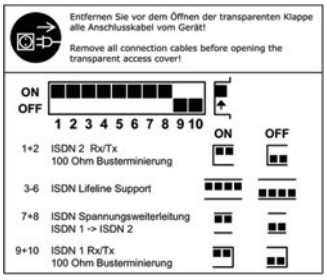
LANCOM Systems

LANCOM™ Techpaper: Security in Voice over IP environments



Integrating a SIP provider.

directly connected to the gateway is secured by the phantom injection over the provider's ISDN bus.



Lifeline support on the LANCOM 1722 VoIP

5 Integration of SIP providers

Most VoIP gateways currently available give users the option to register their terminal equipment with one of the main SIP providers. This feature is valued highly among private users, but it creates two major disadvantages for business customers:

1. Currently, very few SIP providers offer the capability to use extension numbers comparable to that of an ISDN point-to-point connection. This severely restricts the application in business scenarios.
2. The SIP protocol transfers voice data in unencrypted form. This allows even technically inexperienced per-

VoIPong session recording

```
efe:[voipong]# voipong -d4 -f
EnderUNIX VOIPONG Voice Over IP Sniffer starting...
Release 2.0-DEVEL, running on efe.dev.enderunix.org [FreeBSD 4.10-STABLE FreeBSD 4.10-STABLE #0: Thu Dec i386]

(c) Murat Balaban http://www.enderunix.org/
19/11/04 13:32:10: EnderUNIX VOIPONG Voice Over IP Sniffer starting...
19/11/04 13:32:10: Release 2.0-DEVEL running on efe.dev.enderunix.org [FreeBSD 4.10-STABLE FreeBSD 4.10-STABLE
#0: Thu Dec i386]. (c) Murat Balaban http://www.enderunix.org/ [pid: 71647]
19/11/04 13:32:10: fxp0 has been opened in  promisc mode, data link: 14 (192.168.0.0/255.255.255.248)
19/11/04 13:32:10:  [8434] VoIP call detected.
19/11/04 13:32:10:  [8434] 10.0.0.49:49606 <--> 10.0.0.90:49604
19/11/04 13:32:10:  [8434] Encoding: 0-PCMU-8KHz
19/11/04 13:38:37: [8434] maximum waiting time [10 sn] elapsed for this call, call might have been ended.
```


LANCOM Systems

LANCOM™ Techpaper: Security in Voice over IP environments

sons to listen in on business-critical telephone conversations. "VoIPong" is a powerful tool that is able to extract the voice portion of a data connection and make it audible to the attacker. Therefore, as long as encrypted protocols such as SRTP and SIPS are not offered by providers, integration should be avoided.

6 Requirements of a VoIP gateway

In conclusion, the following requirements must be placed on a VoIP gateway in order to fulfill current security requirements for Internet telephony:

- Availability
  - Integrated ISDN interfaces with Lifeline support
  - Class of Service / Quality of Service fuctionality in send and receive directions
  - Assurance of high availability through the use of suitable protocols and communication paths such as VRRP and ISDN
- Security
  - Protection mechanisms such as firewalls and Denial-of-Service protection
  - VPN functions for secure voice transmission between locations
  - Support for logical networks (VLAN)
  - Authentication options for terminal equipment